Performance Evaluation of Trust Management in Mobile Ad-hoc Networks

Hassan Jari

Supervisor: Dr. Nigel Thomas
Dr. Matthew Forshaw

School of Computing
Newcastle University

This dissertation is submitted for the degree of
Doctor of Philosophy

August 2023

I dedicate this thesis to my loved ones who have been my constant source of love, resilience, and support. This work symbolises the journey I have embarked upon, a journey that was guided and shaped by their unwavering belief in me.

To my beloved father and mother, whose unwavering support and unconditional love have been the foundation upon which I have built my life. Your sacrifices and commitment to my success have never gone unnoticed, and I will forever be grateful for the guidance and strength you have given me throughout my journey. Thank you for teaching me the value of hard work, perseverance, and compassion. Your wisdom echoes in every page of this manuscript.

To my incredible wife, *Reem*, my partner in life and my best friend, who has been my rock and my inspiration during this academic pursuit. Your patience, encouragement, and understanding have made it possible for me to reach this milestone. I am grateful for your companionship and love, and I am proud to share my life with you. This thesis is not merely a reflection of my hard work but also a testament to your resilience, your belief in me, and your unwavering support.

To my precious daughter, *Larein*, who has brought immeasurable joy and purpose to my life. You are my motivation to be the best version of myself, and I hope my accomplishments serve as an example of what you can achieve with determination and dedication. May you continue to grow into the remarkable individual I know you will become.

To my supportive brothers and sisters, my first friends and lifelong companions, who have always stood by me and believed in my abilities. Your camaraderie and love have been essential to my growth as a person, and I am grateful for each of you. Thank you for your endless encouragement and for being a constant source of joy. This achievement is as much yours as it is mine.

Lastly, to my cherished friends, who have been there through thick and thin, sharing in my successes and providing solace during my setbacks. Your friendship has enriched my life in countless ways, and I am grateful for the laughter, wisdom, and memories we have

shared. Thank you for being a part of this journey and for making it all the more meaningful.

This thesis is dedicated to each of you as a testament to the invaluable impact you have had on my life. It is through your love, support, and encouragement that I have been able to achieve this significant accomplishment. May we continue to learn from one another, grow together, and celebrate the interconnectedness that makes our lives richer and more fulfilling.

Declaration

I hereby declare that this thesis, entitled "Performance Evaluation of Trust Management in Mobile Ad-hoc Networks" is a result of my original research and analysis. The contents of this thesis have not been submitted for a degree or any other examination at Newcastle University or any other institution. All sources of information used in this thesis have been duly acknowledged, and all contributions from other researchers or authors have been appropriately cited.

Hassan Jari
August 2023

Acknowledgements

First and foremost, I extend my gratitude and praise to Allah, who has showered me with countless blessings and has bestowed upon me the patience and determination required during this research endeavour and, indeed, throughout my entire life.

I am immensely grateful to my esteemed supervisors, Dr. Nigel Thomas and Dr. Matthew Forshaw, for their unyielding guidance, invaluable insights, and unwavering support throughout the journey of my PhD study. Your advice and support were invaluable and played a crucial role in my studies. Your patience and constructive feedback have helped me refine my research capabilities and have indeed set the bar high for the scholar I aspire to be.

I would also like to extend my sincere gratitude to Jazan University, Saudi Arabia, for providing me with the magnificent opportunity to undertake my PhD study at Newcastle University. I am truly grateful for the trust you have placed in me, and the support you have provided has been instrumental in my academic journey.

Thank you all for being part of this incredible journey. Your impact has been significant, and your influence will continue to shape my academic and professional journey in the years to come.

Abstract

Mobile Ad-hoc Networks (MANETs) are characterised by their self-organising nature, dynamic topology, and lack of centralised control, which make them vulnerable to various security threats. Trust management mechanisms have emerged as a promising solution to address these challenges by establishing trust among nodes in the network and ensuring reliable and secure communication. The thesis presents a comprehensive approach to trust management in MANETs, focusing on the development, evaluation, and comparison of direct, indirect, and global trust management mechanisms for the Ad-hoc On-demand Distance Vector (AODV) routing protocol.

The proposed direct trust management mechanism enhances the AODV protocol by incorporating trust values based on nodes' historical behaviour during the route discovery and maintenance process. This mechanism allows nodes to make informed decisions when selecting routes, thereby improving the reliability and security of the network. The indirect trust management mechanism extends the direct trust approach by considering recommendations from neighbouring nodes to establish trust among nodes that have not previously interacted. This mechanism fosters cooperation among nodes and mitigates the impact of malicious or compromised nodes in the network. Finally, the global trust management mechanism takes a more holistic approach, combining direct and indirect trust information to calculate a global trust value for each node. This mechanism enables nodes to make routing decisions based on a broader understanding of the network's overall trust landscape.

To assess the performance and security of these trust management mechanisms, we conduct extensive simulations using the network simulators NS-2 and NS-3. Our results demonstrate significant improvements in key performance metrics, such as packet delivery ratio, throughput, end-to-end delay, and routing overheads, when trust management mechanisms are integrated with the AODV routing protocol. Furthermore, we evaluate the robustness of these mechanisms in the presence of malicious nodes, such as black hole attacks, and show their effectiveness in mitigating the impact of such security threats.

In summary, this paper presents a comprehensive approach to trust management in Mobile Ad-hoc Networks, encompassing the development, evaluation, and comparison of direct, indirect, and global trust mechanisms for the AODV routing protocol. Through

rigorous analysis and extensive simulations, we demonstrate the effectiveness of these mechanisms in improving the security and performance of MANETs across various scenarios and environments. By highlighting potential future research and emphasising the importance of interdisciplinary collaboration, the thesis contributes to the ongoing efforts to create more secure, robust, and efficient ad-hoc networking solutions.

Publication

Throughout my PhD studies, I have published the following papers:

1. A. Alzahrani, H. Jari, and N. Thomas, "Analysing the effect of mobility on the performance of MANET routing protocols," *Proceedings of the 35th Annual UK Performance Engineering Workshop (UKPEW 2019)*, vol. 35, pp. 1 – 11, 12 2019.

2. H. Jari, A. Alzahrani, and N. Thomas, "Performance evaluation of manet trust-based AODV protocol in the presence of black hole attacks," *Proceedings of the 36th Annual UK Performance Engineering Workshop (UKPEW 2020)*, vol. 36, pp. 30 – 40, 12 2020.

3. H. Jari and N. Thomas, "Performance evaluation of indirect trust management in MANET routing protocols," *Proceedings of the 38th Annual UK Performance Engineering Workshop (UKPEW 2022)*, vol. 38, pp. 79 – 89, 12 2022.

4. H. Jari, A. Alzahrani, and N. Thomas, "A novel indirect trust mechanism for addressing black hole attacks in MANET," *DIVANet 2021 - Proceedings of the 11th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, pp. 27–34, 2021.

Table of contents

List of figures

List of tables

Chapter 1

Introduction

1.1 Introduction

Wireless networks are typically classified into two main types: infrastructure-based and infrastructure-less. Infrastructure-based wireless networks rely on strategically positioned devices, including access points and base stations, to facilitate communication between nodes. As mobile nodes move within the network, they can effortlessly maintain connectivity by transitioning from the coverage area of one base station to another. In contrast, infrastructure-less networks operate without fixed base stations, depending on mobile nodes to dynamically generate and uphold routing among themselves, with each node functioning as a self-contained router.

Mobile Ad-hoc Networks (MANETs) exemplify a distinct class of wireless networks that can be rapidly deployed without requiring any pre-existing infrastructure [5]. These networks consist of a group of mobile devices that establish communication with one another, either directly or indirectly, via wireless links, forming a network that emerges spontaneously. Within a MANET, nodes have the autonomy to move independently, causing the network topology to evolve continuously.

MANETs are known for their versatility and applicability to a wide range of use cases, such as military operations, disaster recovery efforts, search and rescue missions, and various civilian settings, including transportation and healthcare systems [6]. They offer significant advantages in situations where implementing a wired infrastructure is either impractical or not cost-effective. The dynamic nature of MANETs enables rapid reconfiguration and adaptability to meet the demands of ever-changing environments, making them an ideal choice for scenarios that necessitate a high degree of flexibility and responsiveness.

Furthermore, the decentralised nature of MANETs offers additional benefits, such as robustness against single points of failure and the ability to scale effectively with the

number of nodes. As a result, MANETs are well-suited for situations where centralised control is not possible or desirable. However, the dynamic and decentralised nature of MANETs also poses unique challenges, particularly in terms of security, routing, and resource management [7]. Addressing these challenges remains an active area of research, with the goal of optimising the performance, reliability, and security of MANETs in a variety of contexts.

1.2 Motivation for Research

MANETs are characterised by their highly dynamic and decentralised nature, enabling rapid deployment and adaptability across a wide range of applications, such as disaster recovery, military operations, and civilian settings like transportation and healthcare [6]. The absence of centralised control and the constantly changing topology of MANETs, however, give rise to unique challenges, particularly with respect to security, routing, and resource management. The research motivation can emerge from the increasing demand for reliable, efficient, and secure wireless communication in various applications and scenarios in MANETs. MANETs are characterised by their dynamic nature, with nodes constantly joining and leaving the network, leading to frequent changes in network topology. This necessitates continual investigation and improvement in the areas of routing, resource management, and security since it provides unique problems in these areas [8].

Trust management mechanisms have become crucial for effectively addressing various challenges in MANET routing, as they can aid in identifying and isolating malicious nodes, thus enhancing the overall security, trust and efficiency of the network. Despite recent advancements in trust management mechanisms for MANETs, several gaps and limitations persist. Existing trust management mechanisms may not fully account for the dynamic behaviour of nodes or the diverse and evolving threats they face. Moreover, some current trust management approaches might lack the ability to differentiate between malicious nodes and nodes experiencing temporary performance degradation due to external factors, such as low battery power. Consequently, there is a need for a comprehensive, adaptive, and robust trust evaluation system that effectively assesses the trustworthiness of nodes, adapts to changing network conditions, and mitigates the impact of malicious nodes on network performance [9].

Additionally, trust management mechanisms for MANETs should be capable of accommodating the varying requirements and constraints of different application domains. For instance, military operations may prioritise security and resilience against attacks, while vehicular networks might require more emphasis on real-time communication and low latency. Designing trust management mechanisms that can adapt to these unique

application scenarios is essential to maximise the effectiveness of the trust evaluation process [10].

Another critical aspect of trust management mechanisms in MANETs is the ability to encourage nodes to actively participate in the trust evaluation process, share accurate information, and contribute to the overall network security. Cooperative and collaborative trust management mechanisms can play a vital role in enhancing the security and performance of MANETs by leveraging the collective knowledge and experiences of nodes. However, designing appropriate incentives and reputation systems to encourage node cooperation is crucial to prevent malicious behaviour [9].

1.3 Research Questions, Problem Statement and Objectives

This section discusses possible research questions related to the use of trust in MANET routing. Further, this section presents the problem statement and objectives for the proposed research work.

1.3.1 Research Questions

Following is the list of possible research questions in the context of using trust management techniques in MANET routing protocols to overcome various security issues and enhance the reliability of the communication.

- What are the key parameters and metrics that influence the trustworthiness of nodes in a mobile ad-hoc network, and how can these be effectively incorporated into a trust management mechanism?

  This is discussed in Chapter 3, specifically in Section 3.3.

- What is the impact of incorporating different types of trust management mechanisms into the Ad-hoc On-Demand Distance Vector (AODV) protocol on the overall performance, security, and efficiency of routing processes within mobile ad-hoc networks?

  This research centres around the principal inquiry, which is explored comprehensively across Chapters 3, 4, and 5. Furthermore, Chapter 6 undertakes a comparative analysis of the distinct trust management mechanisms to assess their respective performance.

- What role can cooperative and collaborative trust management mechanisms play in enhancing the security and performance of mobile ad-hoc networks, and how

can incentives be designed to encourage nodes to participate in these mechanisms actively?

This topic is explored in Chapter 3, specifically in Section 3.6, Chapter 4 in Section 4.3 and Chapter 5 in Section 5.3.

- How can trust management mechanisms be designed to consider and balance the trade-offs between security and performance in mobile ad-hoc networks?

  This matter is covered in Chapter 3 within Sub-Section 3.2.2, Chapter 4 in Section 4.1 and Chapter 5 in Section 5.1.

- How does the performance of various trust management mechanisms in comparison to the standard AODV protocol affect metrics such as packet delivery ratio, throughput, end-to-end delay, and routing overhead within the AODV routing protocol?

  This subject is addressed in Chapter 3, specifically in Sections 3.4 and 3.5. Also, it is discussed in Chapter 4 within Section 4.2 and Chapter 5 in Section 5.2.

1.3.2 Problem Statement

The primary research aims of this study involve conducting a thorough investigation to evaluate the impact of incorporating trust management mechanisms into the AODV protocol on the overall performance, security, and efficiency of routing processes within mobile ad-hoc networks. Through an analysis of key factors and parameters that significantly influence the performance, efficiency, and reliability of the AODV protocol, this study seeks to understand the interactions between these parameters and their effects on the overall network performance.

Trust management mechanisms contribute to the enhancement of routing in MANETs by improving the reliability of communication. However, the integration of trust mechanisms into MANETs can potentially have negative implications for the performance of the routing protocols. Consequently, it is crucial to evaluate the impact of implementing various trust mechanisms within the AODV protocol. Additionally, an examination of the effects of incorporating three distinct types of trust mechanisms on the AODV protocol will be conducted, considering diverse network scenarios and parameters.

By implementing a range of trust management mechanisms into the AODV protocol and thoroughly assessing their performance under various scenarios, network configurations, and performance metrics, this research aims to generate a comprehensive understanding of the accuracy, efficiency, and adaptability of these trust management mechanisms. The findings from this research will be instrumental in the development of more effective, robust, and resilient trust management mechanisms for mobile ad-hoc networks, ultimately

enhancing security, performance, and adaptability across diverse application scenarios and contexts. Furthermore, the research aims to advance the state of the art in trust management for mobile ad-hoc networks, offering valuable insights and recommendations for future research and development in this field.

1.3.3 Research Objectives

The research work aims to achieve following objectives through a systematic and rigorous approach.

- A systematic assessment is to be conducted to determine the impact of incorporating trust management mechanisms into the AODV protocol on the overall performance, security, and efficiency of routing processes within mobile ad-hoc networks.
- Key factors and parameters that significantly influence the performance, efficiency and reliability of the AODV protocol are to be identified and evaluated, with the aim of understanding the interactions between these parameters and their consequences on the network's overall functionality.
- Various trust management mechanisms are to be implemented and evaluated within the AODV protocol, and their performance is to be compared under diverse scenarios, network configurations, and performance metrics to develop a comprehensive understanding of the accuracy, efficiency, and adaptability of these mechanisms.
- Valuable insights and recommendations are to be provided for future research and development in trust management for mobile ad-hoc networks, with the aim of advancing the state of the art in this field and offering guidance for researchers working in this field.

1.4 Thesis Contributions

In order to address the research objectives mentioned in above Section, various trust management mechanisms were integrated into the AODV protocol, and their performance was subsequently assessed in comparison to the original AODV protocol. This was done with the aim of evaluating the accuracy and efficiency of the implemented trust management mechanisms. A thorough investigation was conducted by employing diverse scenarios and performance metrics, which enabled the examination of the performance of the trust-enhanced AODV protocol under a wide range of conditions and network configurations. This approach provided a comprehensive understanding of the impact of trust management on the overall performance of the AODV protocol.

The research contributions outlined in this study are broken down into the following categories:

- Enhancement of routing protocols: This research contributes to the advancement of routing protocols within MANETs by proposing refined algorithms that consider the network's dynamic nature and address efficiency, reliability, and scalability concerns. Chapters 3, 4, and 5 present DTAODV, ITAODV and GTAODV routing protocols which are trust-based extensions of the AODV routing protocol.
- Strengthening security mechanisms: The study introduces comprehensive security mechanisms to safeguard MANETs from various attacks and threats. This includes the design and implementation of trust management systems that foster secure communication between nodes. Chapter 3, 4, and 5 discusses how proposed DTAODV, ITAODV and GTAODV routing protocols overcome security issues in the routing process.
- Analysing and evaluating various trust management mechanisms: This research delves into the exploration of diverse trust management mechanisms and examines their efficacy and performance under an array of scenarios and metrics. The research contributes to the development of sophisticated simulation tools and models, facilitating the assessment and validation of novel techniques, protocols, and algorithms in realistic MANET settings. Chapter 3, 4, and 5 discusses experimental evaluations of DTAODV, ITAODV and GTAODV routing protocols and compares the performance of these protocols against the AODV routing protocol in the presence and absence of a Black-hole attack.
- Investigating diverse trust management mechanisms under security threats: This research evaluates a variety of trust management techniques in the context of mobile ad hoc networks when faced with security challenges. Chapter 6 presents a detailed comparative analysis of proposed DTAODV, ITAODV and GTAODV routing protocols under various test conditions.

1.5 Thesis Structure

The thesis will investigate trust management mechanisms in mobile ad-hoc networks (MANETs) to enhance the performance and security of the Ad-hoc On-Demand Distance Vector (AODV) routing protocol. The thesis is structured as follows:

Chapter 1 The introduction provides an overview of the research problem, the research aims and objectives, the research methodology (including network simulators NS-2 and

NS-3, confidence interval, and performance metrics), and the motivation and contributions of the thesis.

Chapter 2 A comprehensive literature survey and background analysis cover MANET routing protocols, security issues in MANETs, the trust concept in MANET routing protocols, trust management techniques, and applications of trust. The Chapter concludes with the limitations of existing trust-based routing protocols and known countermeasures.

Chapter 3 Direct trust management in AODV routing is examined, including the need for trust in AODV, proposed direct trust management mechanisms, integration of direct trust mechanisms into the AODV protocol, and performance evaluation and analysis using NS-2 and NS-3.

Chapter 4 Indirect trust management in AODV is explored, detailing the proposed indirect trust management mechanism for AODV, integration of direct and indirect trust in the ITAODV routing protocol, and performance evaluation and analysis of the proposed protocol.

Chapter 5 Global trust management in AODV routing is discussed, with a focus on the proposed global trust management mechanisms, integration of global trust in the AODV protocol, and performance evaluation and analysis.

Chapter 6 The comparative analysis of direct, indirect, and global trust mechanisms in MANETs was discussed. Also, the strength and limitations of each mechanism were discussed, providing a deeper understanding of their potential applications and pitfalls.

Chapter 7 The conclusions, limitations, and future work chapter summarises the findings and suggests potential directions for future work.

1.6 Summary

In this chapter, the thesis is introduced, offering a brief explanation of MANETs. Also, it explains the problem statement and research questions, as well as presents the research aims and objectives. Additionally, the chapter outlines the research methodology, thesis motivation, and contributions. A summary of each chapter's content is provided within the thesis structure. The following chapter will cover the literature survey and background.

Chapter 2

Literature Survey and Background

This chapter presents a literature survey on various issues related to MANETs and trust-based MANET routing. The chapter starts by introducing MANET and MANET routing protocols in Section 2.1. Furthermore, Section 2.1 discusses various classifications of MANET routing protocols in details. The security issues in MANETs and some of the techniques to overcome the attacks are presented in Section 2.2. Section 2.3 introduces the trust concept and its characteristics in MANETs. Further, this section explains the type of trust, parameters used for deriving trust, and application of trust. Popular research work related to the trust-based protocol is presented in Section 2.4. While in Section 2.5 discusses the limitation of the existing trust-based routing protocol. Finally, Section 2.6 summarises the chapter.

2.1 MANET Routing Protocols

2.1.1 Introduction to MANET Routing

Mobile Ad-hoc Networks (MANETs), sometimes referred to as wireless ad-hoc networks, are a cutting-edge technology that do not rely on fixed infrastructure or centralised administration for communication purposes. A MANET is generally characterised as a mobile network consisting of numerous independent nodes. Often, it is made up of mobile devices or other mobile nodes that can organise themselves in various configurations and operate without rigid network administration rules. These nodes can join or exit the network at any time, resulting in a dynamic network topology. Additionally, MANET nodes typically have lower CPU capabilities, small memory sizes, and limited battery power [11]. In a MANET, each node can function as both a router and a host. Therefore, these nodes must cooperate to transmit data packets from a source node to a destination node [11].

MANET is a collection of autonomous mobile nodes that communicate with each other through radio signals. Mobile nodes within the radio range can directly communicate, while those outside of the radio range require assistance from intermediate nodes to route their packets. Figure 2.1 shows a simple MANET network with three participating nodes. We assume that nodes *A* and *B* are within each other's radio range, as are nodes *B* and *C*. Furthermore, we assume node *A* needs to communicate with node *C*. However, since node *C* is not within node *A* radio range, node *B* can be used to forward data packets between nodes *A* and *C*. In this scenario, node *B* serves as a router, forwarding information packets from node *A* to node *C*, creating a mobile ad-hoc network among the three nodes. MANETs incorporate various protocols, each with its advantages and disadvantages, such as Ad-Hoc On-Demand Vector Routing protocol (AODV), Greedy Perimeter Stateless Routing (GPSR), and Optimised Link State Routing Protocol (OLSR).

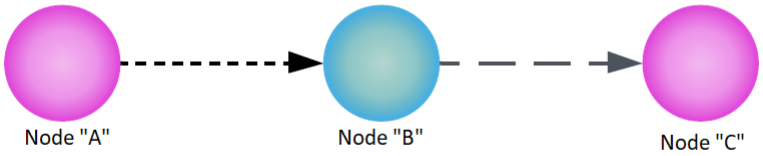

Figure 2.1 Simple MANET with 3 Nodes

The origins of ad-hoc networking applications can be traced back to the Defence Advanced Research Projects Agency (DARPA) as part of the Packet Radio Networking (PRNET) project in 1972, which later evolved into the Survivable Adaptive Radio Networks (SURAN) program [12]. Ad-hoc networks have played a significant role in military applications and related research efforts, such as the Global Mobile information systems (GloMo) and Near-Term Digital Radio (NTDR) projects [5]. There has also been a growth in the usage of such networks in disturbed areas by the police, the commercial sector, and emergency organisations. Ad-hoc network research has long been associated with the military. In the middle of the 1990s, with the support of commercial radio and wireless innovations, awareness spread of the significant advantages of MANETs outside the military battlefield domain. Active research work subsequently began on ad-hoc networks in 1995 at an Internet Engineering Task Force (IETF) conference session [6]. Afterwards, in 1996, this work evolved to develop a mobile ad-hoc network, which at the time concentrated on military satellites, wearable computers, and tactical networks.

MANETs are helpful in circumstances when the establishment of a regular wireless network is difficult or impossible, such as in disaster responses, military operations, or isolated locations. They are also beneficial for Internet of Things (IoT) applications, in which devices may be distributed and must interact with one another without the usage of a central server. Research into MANETs has recently become very active due to their many potential applications in daily life. Table 2.1 describes a few of the major applications of ad hoc networks.

Table 2.1 Applications of Ad-hoc Networks

Field of Applications	**Services of Ad-hoc Networks**
Tactical Networks	Military operations and communication.
Emergency Services	Search and rescue missions such as in wilderness and mountainous areas; police and fire-fighting operations; providing supporting services to hospital doctors.
Sensor Networks	Smart sensors in consumer electronics devices; tracking of data such as environmental conditions and animal movements
Education	Universities campus locations and classrooms, and faculty and staff meetings.
Conferences and Events	Temporary networking facilities for conferences and other large events.

2.1.2 Classification of MANET Routing Protocols

Routing in MANETs is a process of identifying and selecting the most efficient paths for data to travel along from one device to another. The unique characteristics of MANETs, such as the lack of a central infrastructure, the presence of mobile devices that can change their connectivity, and the dynamic nature of the network topology, make routing in these networks a challenging task [13]. Unlike traditional wired networks where routing paths are predetermined and fixed, the paths in MANETs need to be constantly re-evaluated and re-established due to the mobility of the devices. Currently, there are many MANETs routing protocols which are inspired by either distance-vector or link-state routing algorithms.

In MANETs, routing protocols can be categorised according to two criteria: routing philosophy and routing architecture [5].

2.1.2.1 Routing Classification based on Routing Philosophy

The routing philosophy classifies protocols based on the characteristics of the mechanisms used to update routing information and the implementation of routing schemes. According to these criteria, there are three primary routing protocol types: reactive (on-demand), proactive (table-driven), and hybrid protocols [14]. The following provides a detailed explanation of these three types of routing protocols.

- **Proactive (Table-Driven) Routing Protocols**

  In MANETs, routing protocols play a crucial role in establishing and maintaining communication between nodes. Proactive routing protocols in MANETs are also known as table-driven routing protocols. These maintain up-to-date routing information for all nodes in the network by periodically broadcasting routing information throughout the network. This information is then stored in routing tables at each node, allowing for quick and efficient routing decisions.

  Table-driven protocols, also known as proactive routing protocols, necessitate that each node maintains one or more tables with routing information for all other nodes in the network. When network topology changes occur, updates must be disseminated throughout the network [4]. This feature is advantageous for datagram traffic, but it generates substantial signalling traffic, resulting in increased power consumption. Furthermore, proactive routing protocols are suited for large networks since they must maintain entries for every node within each node's routing table. In proactive, table-driven protocols, the number of control messages in the network escalates quickly due to the increase in messages. Prominent proactive routing protocols include the Wireless Routing Protocol (WRP), Optimised Link State Routing (OLSR) protocol, and Destination-Sequenced Distance Vector (DSDV) routing protocol.

- **Reactive (On-Demand) Routing Protocols**

  Reactive routing protocols, also referred to as on-demand routing protocols, belong to a category of routing protocols that establish routes only when required. In this type of protocol, routes are generated when a source needs to transmit data to a destination node, meaning that these protocols are initiated by a source as needed [14]. This approach is different from proactive (table-driven) routing protocols, which consistently maintain updated routing information about the entire network.

The primary goal of reactive routing protocols is to reduce the routing overhead and resource consumption associated with maintaining and updating routing tables for the whole network. However, these protocols often involve longer routes when transferring data packets from a source to a destination, resulting in network latency [13]. Prominent reactive routing protocols include Ad-hoc On-demand Vector Routing (AODV), Dynamic MANET On-demand (DYMO), and Dynamic Source Routing (DSR) protocols.

- **Hybrid Routing Protocols**

  Hybrid routing protocols in MANETs combine the strengths of both the proactive (table-driven) and the reactive (on-demand) routing protocols to achieve efficient and scalable routing in dynamic network environments [15]. These protocols aim to strike a balance between the low-latency route discovery of proactive routing protocols and the reduced routing overhead of reactive routing protocols. Hybrid routing protocols are designed to adapt to varying network conditions and topology changes by integrating the proactive and reactive approaches in different zones or layers of the network.

  The primary idea behind hybrid routing protocols is to maintain up-to-date routing information for nearby nodes using proactive techniques while discovering routes for distant nodes on-demand using reactive techniques. This approach reduces the routing overhead associated with maintaining global routing information while still providing quick route discovery for local communication. Hybrid routing protocols are particularly suitable for large-scale MANETs with diverse mobility patterns and communication requirements. However, their control mechanisms are more sophisticated, and the selection of the optimal routing protocol for a given case may not be simple [15]. One of the most well-known hybrid routing protocols is the Zone Routing Protocol (ZRP).

2.1.2.2 Routing Classification based on Architecture

Routing protocols can also be categorised based on network topology as either flat or hierarchical routing [5].

- **Flat Routing**

  Flat routing, also known as non-hierarchical routing, is a type of routing scheme used in MANETs where all nodes in the network participate in the routing process without any hierarchical structure or predefined roles [16].In flat routing, all nodes have equal responsibilities, and there are no distinctions between them. The process of

determining routes is distributed among the network nodes in flat routing algorithms. In this type of routing, all nodes are treated as peers and they participate in the routing process without any hierarchy or organisation. This distributed architecture is characterised by consistent features and behaviours across all nodes. Nodes can make decisions using local information without relying on a centralised node. This approach lowers overheads and delays, resulting in enhanced network performance. Flat routing protocols are simple and easy to implement, and they do not require any additional information or knowledge about the network [17].

In flat routing, when a node needs to send a packet to another node, it first checks its routing table to see if it has a route to the destination. If it does not have a route, the node will initiate a route discovery process by broadcasting a route request packet to its neighbours. The neighbours will then forward the route request packet to their own neighbours until the destination or an intermediate node that has a route to the destination is identified.

One significant benefit of flat routing protocols is their simplicity and ease of implementation, which allows them to function effectively in networks with a moderate degree of mobility. However, they also have disadvantages. For example, they do not take into account the different characteristics of nodes in the network, such as their energy levels or mobility patterns [16]. Additionally, they may generate high overheads due to the frequent exchange of routing information. Examples of flat routing protocols include Ad-hoc On-demand Distance Vector (AODV) and Dynamic Source Routing (DSR) protocols.

- **Hierarchical Routing**

  Hierarchical routing, also known as hierarchical or cluster-based routing, is an approach used in MANETs to improve the scalability and efficiency of routing by organising the network into a hierarchical structure [17]. Hierarchical routing is a method of organising the network into different levels or layers, each with a specific function. This type of routing divides the network into clusters and assigns a cluster head to manage the routing within each cluster. Compared to flat routing protocols, hierarchical routing protocols are more complex but can provide greater efficiency and scalability.

  Hierarchical routing protocols aim to reduce the routing overhead and complexity associated with flat routing by limiting the scope of routing updates and organising the network into manageable clusters [18]. This approach can enhance the performance and scalability of routing protocols in large-scale MANETs and adapt to varying network conditions and mobility patterns. When a node needs to send a packet to

another node in a hierarchical routing network, it first checks if the destination is in the same cluster. If it is, the node uses the proactive routing protocol within the cluster to reach the destination. If the destination is not in the same cluster, the node uses the reactive routing protocol between clusters to establish a route.

Hierarchical routing protocols take into account the different characteristics of network nodes and can reduce the control overheads and improve routing efficiency. Additionally, they can handle large networks and those with high levels of mobility. However, they may require more complex control mechanisms and the selection of an appropriate routing protocol for a specific scenario may not be straightforward [18]. Several hierarchical routing protocols have been proposed for MANETs, such as the Cluster-Based Routing Protocol (CBRP), Cluster Head Gateway Switch Routing (CGSR), and Zone Routing Protocol (ZRP).

2.1.3 Exploring Diverse Applications and Uses of Mobile Ad-hoc Networks (MANETs)

MANETs are highly dynamic, self-organising wireless networks without the need for a fixed infrastructure, such as base stations or routers [19]. MANETs are frequently used in disaster recovery and relief scenarios. For instance, communication infrastructure may be severely damaged during a natural disaster, making it difficult for rescue teams to communicate and coordinate their rescue efforts. In such a case, a MANET can be immediately established to speed up communication between rescue personnel, emergency medical personnel, and relief organisations [11]. Each individual's device (e.g., smartphones, tablets, or laptops) functions as a network node, enabling them to communicate directly with nearby devices or transmit messages via intermediate nodes. This adaptable, decentralised architecture contributes to the reliability of a communication system in challenging environments with limited or damaged infrastructure.

Moreover, MANETs can be used in smart cities. In urban environments, MANETs can facilitate communication among IoT devices, creating interconnected systems that optimise city services. For example, smart parking solutions can use MANETs to inform drivers of available parking spaces, reducing time spent searching and improving traffic flow [20]. Intelligent traffic control systems can optimise traffic signal timings based on real-time data, improving overall traffic efficiency. Also, environmental monitoring can benefit from MANETs, with interconnected sensors providing real-time data on air quality, noise levels, and other parameters [21].

In the field of research and education, MANETs can be used to during field research or outdoor educational activities. Researchers and students can create ad hoc networks to exchange data, collaborate on projects, or access remote resources [8]. In environmental

or wildlife studies, for example, MANETs can enable real-time data sharing among researchers, enhancing their understanding of the subject and improving decision-making.

Another use of MANETs subclass is the vehicular ad-hoc networks (VANETs). VANETs use the same principle of MANETs [22]. It enables vehicles to exchange information with one another and with roadside infrastructure. This can lead to better traffic management through real-time updates on road conditions, accidents, and congestion. Moreover, safety warnings can be transmitted between vehicles, reducing the risk of accidents. VANETs can also support location-based services, providing drivers with relevant information such as nearby parking spots or points of interest [23].

In the military scenarios, MANETs provide a self-configuring, self-healing communication network that can adapt to the rapidly changing battlefield conditions. Soldiers equipped with wearable communication devices can share real-time intelligence and coordinate operations, increasing their effectiveness and safety [11]. Furthermore, MANETs can support communication between autonomous vehicles and ground-based sensors, enabling efficient and secure reconnaissance and surveillance missions. The dynamic nature of MANETs ensures reliable communication in the presence of jamming or other electronic warfare tactics [24].

Finally, MANETs can be used in event organising such as at concerts, sports events, or conferences. MANETs can establish temporary communication networks that support information sharing and coordination among participants. This can include sharing event schedules, real-time updates, or multimedia content. MANETs can also provide Internet connectivity in crowded venues where conventional cellular networks may become overloaded.

Overall, MANETs provide adaptable communication solutions for a variety of sectors, addressing the unique difficulties and needs of each application. They are well-suited to environments where fixed infrastructure is unfeasible or undesirable due to their self-organising and adaptable natures.

2.1.4 Ad-hoc On-Demand Distance Vector (AODV) Protocol

In this research work, trust-based extensions to the Ad-hoc On-Demand Distance Vector (AODV) routing protocol are proposed. In this section, the operation of the AODV protocol is discussed in detail.

The AODV routing protocol operates as a reactive mechanism, facilitating self-initiating, dynamic, and multi-hop routing among the nodes involved. AODV routing protocol assists nodes in rapidly identifying routes to novel destinations, as it eliminates the need for nodes to maintain information about inactive routes. Using an on-demand methodology for route discovery, AODV employs a destination sequence number to ascertain the most up-to-date

path, thereby ensuring the route's freshness [25]. Additionally, it ensures loop-free routes and tackles any disruptions in the routing connections [5].

AODV employs a conventional routing table with a single entry for each destination. Each entry documents the subsequent hop toward the specified destination, and a sequence number, generated by the destination, is used to determine if the routing information is current and to prevent routing loops. The AODV protocol encompasses various message types – route requests (RREQs), route replies (RREPs), route errors (RERRs) – and a HELLO packet for navigation within the ad hoc network [5]. AODV can elucidate network topology by broadcasting a HELLO message to neighbouring mobile nodes. Furthermore, a HELLO message can identify an invalid link by broadcasting to mobile nodes in the network.

When a source node intends to establish communication with a destination node, it disseminates an RREQ packet, generating temporary route table entries for the reverse path through which the RREQ message was sent [26]. The source node disseminates the RREQ to neighbouring nodes, as illustrated in Figure 2.2, with each node relaying the RREQ packet to adjacent nodes until it reaches the destination node. RREQ packets include a requested destination sequence number, which is incremented by one from the destination sequence number currently recognised by the source [27]. This approach prevents outdated routing information from being used as a reply message to RREQ packets, addressing the primary cause of routing loop issues in traditional distance vector algorithms [26]. While the RREQ does count the number of nodes it passes, it does not record them. Nonetheless, every node that the RREQ packet passes through sets up a temporary reverse link, identifying the preceding node from which the RREQ packet originated, allowing the response to be sent back to the source node. When the RREQ arrives at the target destination or an intermediate node that has an up-to-date route to the destination, it sends a unicast reply by forwarding the RREP packet through the reverse path created during the route discovery process, as illustrated in Figure 2.3. The RREP packet includes the total hop count and the destination sequence number of the route. Figure 2.4 demonstrates the source node initiating the transmission of data packets to the destination node by sending them to each neighbouring node that responds to the RREQ with an RREP, eventually reaching the destination node, as shown in Figure 2.4. Finally, if the transmission to the destination node encounters an interruption, neighbouring nodes identify the broken route resulting from movement and proceed to broadcast a route error (RERR) packet to every active upstream neighbour, as depicted in Figure 2.5.

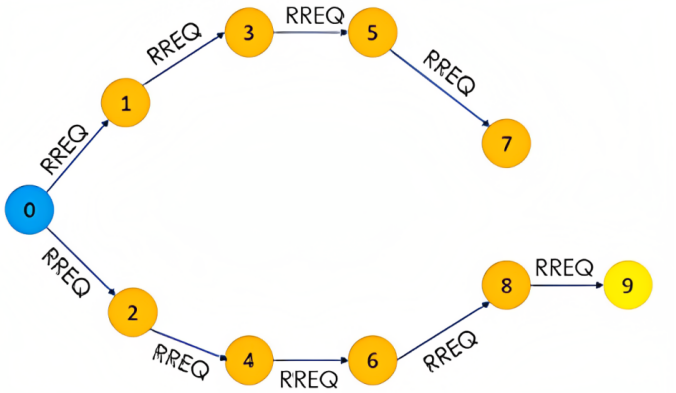

Figure 2.2 Source Node Sends a RREQ Packet

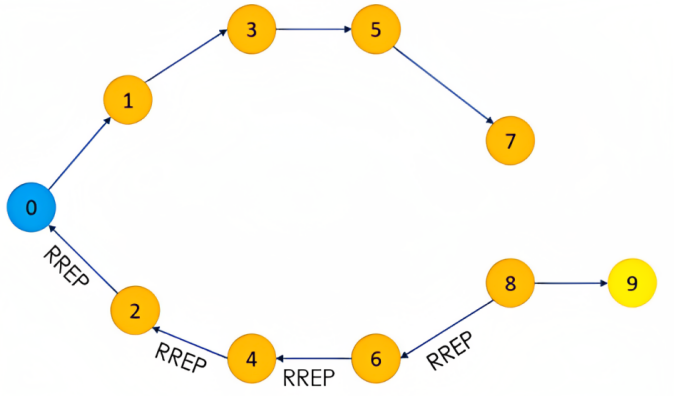

Figure 2.3 Destination Node Sends RREP Packet

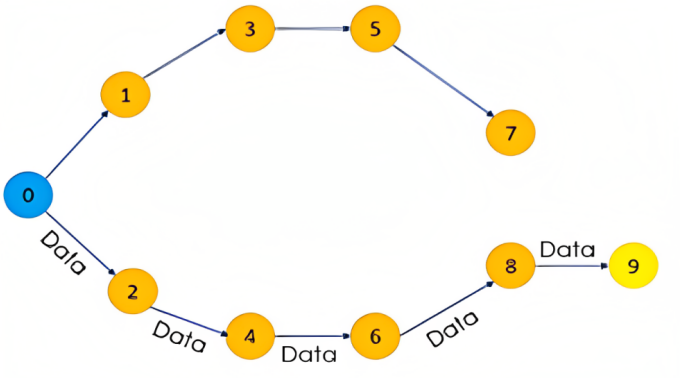

Figure 2.4 Source Node Sends a Data Packet

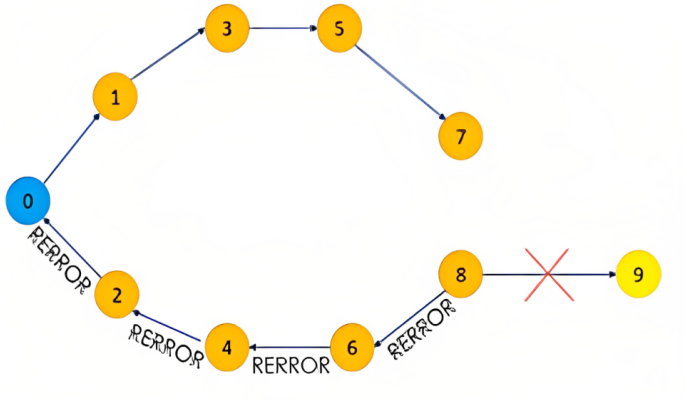

Figure 2.5 Intermediate Node Sends RERR Packet

The RFC3561 [28] was published by the Internet Engineering Task Force (IETF) in 2003 and describes the AODV routing protocol for MANETs. The document provides a detailed specification of the AODV protocol, including the format and contents of the various control messages used such as RREQ, RREP, and RERR messages. Based on RFC3561 [28], there are several factors which need attention in the AODV routing protocol which are as follows:

1. AODV protocol lacks specific security measures and is susceptible to a variety of security threats.
2. If there is a link failure during communication in the route maintenance mechanism, then there is a need to have some mechanism to decrease the resulting delay.
3. The route maintenance procedure should be optimised to fix link failure during communication.
4. The Quality of Service (QoS) of the protocol needs to be improved.
5. General enhancement to the protocol is required to make it more reliable for end users.

2.2 Security Issues in MANETs

2.2.1 Importance of MANETs Security Issues

One of the biggest challenges in securing MANETs is the lack of a centralised authority. In traditional wired networks, a central authority can be used to enforce security policies and to monitor the network for suspicious activity. However, in a MANET, there is no central

authority, and each node must rely on its own security measures to protect itself. Due to their unique characteristics, MANETs are more susceptible to security breaches compared to traditional fixed networks. The mobility aspect of MANETs presents a significant obstacle in ensuring that security protocols remain effective despite constant changes in network topology [4]. Furthermore, the dynamic nature of MANETs makes it difficult to differentiate between legitimate and illegitimate routes and also increases the likelihood of attacks. Conventional security measures implemented in wired networks are not directly applicable to MANETs given their decentralised structure, and lack of a fixed infrastructure eliminates the possibility of a centralised governing body or trusted third party [29].

A routing protocol is a set of rules and procedures that determine how data is transmitted between nodes in a network. In order to ensure the reliability and security of data transmission, it is essential for a routing protocol to incorporate a comprehensive set of security mechanisms. These must be able to prevent, detect, and respond to potential security threats such as unauthorised access, data tampering, and denial-of-service attacks. Routing protocols must prioritise key security requirements such as confidentiality, availability, authentication, integrity, and non-repudiation in their design to ensure their effectiveness in securing the network [29]. These requirements help to minimise the risks associated with data transmission and ensure that data is transmitted in a reliable and secure manner. However, due to the dynamic nature of MANETs, it can be challenging to implement these security requirements in MANET routing protocols. Nonetheless, research continues to be conducted in this area in order to develop new methods to secure MANETs.

It is important to secure MANETs for the following different reasons:

1. Protecting Confidentiality
   One of the main challenges in securing MANETs is to maintain confidentiality, which refers to the protection of sensitive information from unauthorised access. Since MANETs are often used in applications that require secure communication, such as military operations or emergency response scenarios, maintaining confidentiality is critical. Without proper security mechanisms in place, network nodes can be vulnerable to eavesdropping or unauthorised access, which can compromise the confidentiality of the data being transmitted.

2. Ensuring Integrity
   In addition to maintaining confidentiality, it is important to ensure the integrity of data in MANETs. Data integrity refers to the protection of data from unauthorised alteration or corruption. In MANETs, data can be altered, deleted, or added in transit, which can compromise its accuracy or usefulness. Ensuring data integrity helps to guarantee the accuracy and reliability of the data being transmitted, which is critical in many applications.

3. Preserving Availability
   Availability refers to the ability of network nodes to maintain connectivity and support communication [7]. Since MANETs rely on the availability of network nodes in order to function properly, the securing of MANETs is critical in preserving their availability. Security threats can disrupt the availability of network nodes or the network as a whole, causing communication failures or degradation. Protecting MANETs from security threats helps to preserve the availability of network nodes and ensure continued communication.

4. Preventing Malicious Attacks
   MANETs are vulnerable to various types of malicious attacks, including denial-of-service (DoS) attacks, black hole attacks, and wormhole attacks, among others [30]. These can compromise the network, disrupt communication, and potentially cause harm to users. The securing of MANETs helps to prevent these types of malicious attacks and protects the network and its users. By detecting and blocking malicious activity, security mechanisms help ensure the safety and reliability of the network.

5. Supporting Trust
   In MANETs, nodes may need to rely on each other to relay messages, route traffic, or perform other tasks [4]. Without security mechanisms in place, nodes cannot trust each other, which can lead to communication failures or the compromising of the network. Securing MANETs helps to establish trust between nodes and ensures the reliability and integrity of the network. By authenticating and verifying the identity of nodes, security mechanisms can help ensure that nodes can trust each other and the network as a whole.

6. Enabling Privacy
   Privacy is a critical consideration in many applications that use MANETs. Without proper security mechanisms in place, network nodes can be vulnerable to surveillance or tracking, compromising the privacy of users. Securing MANETs helps enable privacy by providing mechanisms for encrypting data and protecting the identities of network nodes. This helps ensure that users can communicate without fear of being monitored or tracked.

7. Facilitating Scalability
   MANETs can be used in a variety of applications, from small-scale sensor networks to large-scale disaster response operations. To ensure that MANETs can scale effectively, it is important to have robust security mechanisms in place. By providing efficient and effective security solutions, MANETs can be scaled up to support a

wide range of applications, making them more versatile and valuable for a variety of use cases.

2.2.2 Security Attacks on MANETs

MANETs are wireless networks characterised by their self-organising nature, mobility, and lack of centralised control or infrastructure. They are employed in a range of applications, including commercial, disaster response, and military contexts. Nonetheless, these networks possess certain vulnerabilities due to their unique features, such as limited resources and dynamic topology, making them prone to security attacks [23, 31, 32].

There are various surveys published by researchers in the domain discussing different types of security attacks on MANET routing protocols [33–36]. This section explains in more detail the various security threats that are commonly encountered in MANETs, outlining their different forms and how they impact network security.

Denial of Service (DoS) Attacks: DoS attacks aim to disrupt network services by overwhelming network nodes with a flood of packets or by exhausting network resources such as bandwidth or memory [30]. In MANETs, DoS attacks can be particularly harmful, because they can quickly bring down the entire network, preventing legitimate nodes from communicating with each other. DoS attacks can be launched using various techniques, such as flooding, spoofing, or amplification.

Black hole Attack: In a black hole attack, a malicious node falsely advertises that it has a shorter path to the destination node, thereby attracting all the traffic to itself [37]. The malicious node then drops all the packets, which leads to the disruption of network communication. Black hole attacks can be launched by compromising a node's routing table or by using false route-reply messages.

Grey hole Attack: A grey hole attack is similar to a black hole attack, except that instead of dropping all the packets, the malicious node drops only a certain percentage of packets [38]. This type of attack can be more difficult to detect, as it may not be immediately clear that there is a problem with the network.

Wormhole Attack: In a wormhole attack, a malicious node tunnels packets through a low-latency, high-bandwidth channel to a remote location in the network [39]. This can allow the attacker to eavesdrop on or modify network traffic, or launch other types of attacks. Wormhole attacks can be launched using various techniques, such as packet replay, packet modification, or packet injection [39].

Sybil Attack: In a Sybil attack, a malicious node creates multiple identities or fake personas within the network, in order to gain an unfair advantage or to disrupt network communication [33]. This type of attack can be particularly difficult to detect, as the mali-

cious nodes may appear to be legitimate. Sybil attacks can be launched by compromising a node's identity or by using false identities.

Byzantine Attack: In a Byzantine attack, a malicious node behaves arbitrarily, ignoring or disobeying the rules of the network [34]. This can include the sending of false or misleading information, dropping packets, or forging messages. Byzantine attacks can be launched by compromising a node's processing or by using false messages.

Jamming Attack: In a jamming attack, a malicious node transmits radio signals on the same frequency as the legitimate nodes, thereby causing interference and disrupting communication [40]. Jamming attacks can be launched using various techniques, such as constant jamming, reactive jamming, or deceptive jamming.

To protect against these attacks, various security mechanisms can be implemented, and these are discussed in the next section.

2.2.3 Techniques to Overcome MANET Security Attacks

One of the key security challenges with MANETs is to maintain the confidentiality, integrity, and availability of communication [41]. Confidentiality ensures that only authorised parties can access the data, integrity ensures that the data has not been tampered with, and availability ensures that the data can be accessed when needed. To achieve these goals, several techniques have been developed to overcome MANET security attacks, including secure routing protocols, cryptography, intrusion detection and prevention systems (IDPS), and trust-based systems.

However, the nodes in a MANET typically have limited computational capabilities and battery power, which poses a challenge in implementing cryptography and key management algorithms such as public key algorithms that require high computational resources. These limitations in the mobile nodes contribute to the security challenges faced by MANETs, and thus researchers are continually working to develop solutions to defend against various types of attacks, ranging from passive eavesdropping to active interference.

2.2.3.1 Cryptographic Approaches

Cryptography is an essential technique used in MANETs to provide the confidentiality, integrity, and authenticity of the data transmitted over the network. Cryptography is the process of converting plain text into cypher text using an encryption algorithm and a secret key, making it unreadable by unauthorised users. Cryptography is used in MANETs to secure communication between nodes and to prevent unauthorised access to sensitive information. Encryption can be employed to ensure the confidentiality of data, while digital signatures can be used to guarantee the authenticity and integrity of data.

One of the benefits of the use of cryptography in MANETs is that it provides a high level of security for sensitive information that is being transmitted. The use of encryption can prevent unauthorised access to data, thus ensuring confidentiality. Digital signatures, on the other hand, can help to ensure that data is not tampered with and that it originates from a trusted source, providing authenticity and integrity to the data. Additionally, the use of cryptographic techniques can make it more difficult for attackers to intercept or manipulate data, which can increase the overall security of the network.

However, there are also some drawbacks to the use of cryptography in MANETs. One of the main disadvantages is that cryptographic methods can add significant computational overheads to the network, which can lead to more frequent and longer delays and reduced throughput. This can be especially problematic in networks where resources are limited, such as in MANETs. Furthermore, the use of encryption and digital signatures can increase the complexity of network operations and specialised knowledge is required to implement and manage these techniques, which can be a challenge for some users.

Many researchers have studied cryptography techniques in order to improve MANET security. For example, Alapati et al.[42] provided an efficient cryptography algorithm for safe data transfer in a MANET. The proposed method involves a robust cryptographic approach which generates and manages keys while ensuring secure distribution to trustworthy nodes while mitigating potentially malicious nodes. The method detects and excludes malicious nodes from participating in communication, thereby improving packet delivery rate and minimising network delay. In this approach, a node functions as a MANET Key Calculator (MKC), which is responsible for key generation and chooses another node as the MANET Key Distributor (MKD) to enable secure data transfer in the MANET through cryptographic methods. Comparisons with traditional methods indicated that the proposed method performs better.

In conclusion, cryptography is a critical technique used in MANETs to provide confidentiality, integrity, and authenticity in the transmission of data over the network. Encryption and digital signatures are two of the most common cryptographic techniques used in MANETs to provide confidentiality and authenticity. By using cryptographic techniques in combination with secure routing protocols, network administrators can help ensure the integrity, confidentiality, and availability of their MANETs.

2.2.3.2 Intrusion Detection and Prevention Systems (IDPS)

Intrusion Detection and Prevention Systems (IDPS) are critical security mechanisms used in MANETs to detect and prevent malicious activities that may endanger network security. The IDPS performs its function by monitoring network traffic and analysing it so as to identify any anomalous activity that may indicate a security breach. Once suspicious

activity is detected, the IDPS can either take action to prevent the attack or notify the network administrator of a possible security threat.

One significant advantage of IDPS in MANETs is their ability to detect and prevent security breaches in real time. This is particularly important since MANETs have a constantly changing network topology, and nodes are frequently joining or leaving the network. Rapid identification of security breaches allows the IDPS to respond promptly, minimising damage to the network. Another advantage of IDPS in MANETs is that they can help determine the origin of an attack. This is critical in identifying the attacker and preventing future attacks. By identifying the attack's source, an IDPS can help protect the network from further attacks by preventing the attacker from launching more attacks on the network. However, there are also some drawbacks to the use of IDPS in MANETs. The main disadvantage is that the IDPS can itself be vulnerable to attacks. Since the IDPS is responsible for monitoring network traffic, it can be a target for attackers who want to bypass the IDPS and launch attacks on the network.

Additionally, IDPS can be resource-intensive, which can impact network performance. The constant monitoring of network traffic by the IDPS consumes a significant amount of network resources. The processing power required to analyse network traffic can also be significant, affecting network performance.

Researchers have studied the implementation of IDPS in MANETs. For instance, Islabudeen et al.[43] proposed an approach for the detection and prevention of attacks in MANETs through machine learning techniques in the form of the Smart approach for intrusion detection and prevention system (SA-IDPS). Mobile users first register with a trusted authority utilising a one-way hash chain function for authentication. The user submits their user identification, finger vein biometrics, and geographical coordinates in order to verify their identity. The intrusion detection process consists of four components: a packet analyser, pre-processing unit, feature extraction unit, and classification unit. The packet analyser utilises a type 2 fuzzy controller to identify any attack patterns by analysing packet header information. The pre-processing unit implements logarithmic normalisation and encoding schemes suitable for any application. The feature extraction unit uses mutual information to determine the optimal set of packet features for classification. The classification unit then classifies packets into five categories: DoS, Probe, U2R, R2L, and Anomaly using the Bootstrapped Optimistic Algorithm for Tree Construction in combination with an artificial neural network. Following classification, the Association Rule Tree is used to determine whether the attack is frequent or rare, and historical tables are used for packet classification. The SA-IDPS was evaluated through experiments that assessed the system's effectiveness in terms of detection rate (%), false positive rate (%), detection delay (s), and energy consumption (J).

In conclusion, the IDPS is a crucial security mechanism in MANETs used to detect and prevent security breaches. Its ability to detect real-time security breaches and identify the source of the attack is essential in maintaining the network's security. However, the vulnerability of the IDPS itself to attacks and its resource-intensive nature are significant drawbacks to consider when implementing IDPSs in MANETs. It is important for network administrators to assess the benefits and drawbacks of using IDPSs in MANETs and to ensure their proper implementation in order to maintain network security.

2.2.3.3 Trust-Based Mechanisms

Trust-based systems are considered to be one of the most effective security mechanisms for MANETs[9]. In a trust-based system, nodes establish trust relationships with one another through the exchange of information and the evaluation of each other's behaviour. By monitoring the behaviour of other nodes in the network, a node can determine whether the behaviour is consistent with trustworthy behaviour. If a node is deemed to be untrustworthy, the system can take steps to isolate or ignore that node.

Trust-based systems in MANETs have several advantages over other security mechanisms. One major advantage is that they are capable of adaptation to changes in network topology. Since MANETs are highly dynamic, the topology can change frequently, and new nodes can join or leave the network at any time. Trust-based systems are designed to adapt to these changes, and trust levels can be re-evaluated based on the current network state. In the next sections, detailed explanations are provided of the mechanisms of trust and reputation methods and their use by researchers. The trust-based mechanism is the technique used in this thesis because it is more advantageous compared to other techniques.

2.3 Trust Concept in MANET Routing Protocols

Trust management mechanisms in MANETs are techniques and algorithms that are used to evaluate the trustworthiness of nodes in the network and to make decisions based on this trustworthiness [44]. These mechanisms are designed to ensure that only trusted nodes are allowed to participate in the communication process and that the data transmitted by these nodes are trustworthy.

In a MANET, nodes are mobile and communicate with each other in a decentralised manner, without the need for a fixed infrastructure or centralised control [5]. This means that nodes have limited information about each other and may not be able to verify the identity and trustworthiness of other nodes in the network. Moreover, the lack of a fixed infrastructure and centralised control means that the network is vulnerable to attacks by

malicious nodes that may attempt to disrupt the communication process or compromise the security of the network.

Trust management mechanisms in MANETs use a variety of methods to evaluate the trustworthiness of nodes. These methods may include evaluating the past behaviour of nodes, considering the recommendations of other nodes in the network, and analysing the quality and consistency of data transmitted by nodes. A combination of these methods may be used to generate a trust score for each node in the network. Once such trust scores have been generated, trust management mechanisms can be used to make decisions about whether or not to allow a particular node to participate in the communication process. For example, nodes with high trust scores may be allowed to participate in the network, while nodes with low trust scores may be blocked or restricted in their access to the network.

The concept of trust management in MANETs is particularly important in securing these networks against various security threats, such as *black hole* attacks, *Sybil* attacks, and *data tampering*. By using these mechanisms to evaluate the trustworthiness of nodes, MANETs can be made more resilient against attacks and a higher level of security and reliability can be provided for their users. Moreover, to mitigate the challenges faced, trust management mechanisms are used to evaluate the trustworthiness of nodes based on many factors such as their behaviour, reputation, and history in the network. These mechanisms use mathematical or computational models to assign values representing levels of trust to nodes which allow decisions to be made about whether or not to trust a node based on its trust value.

One of the challenges in the implementation of trust management mechanisms in MANETs is the dynamic and decentralised nature of these networks. Nodes may join or leave the network at any time, and the quality of wireless links between nodes may vary over time. This means that trust scores may need to be updated frequently so as to reflect the changing nature of the network.

Another challenge of trust management mechanisms in MANETs is the potential for collusion between malicious nodes. Malicious nodes may attempt to manipulate the trust scores of other nodes in the network by providing false recommendations or by engaging in other deceptive behaviour. To address this, trust management mechanisms may use a variety of techniques such as reputation systems and distributed consensus algorithms to mitigate the impact of collusion.

2.3.1 Features of Trust Management Systems in MANETs

Trust management systems that are implemented in MANETs possess many characteristics similar to those in trust management mechanisms. Nevertheless, there are certain specific

characteristics that are unique to their design and implementation. The key features of trust management systems in MANETs are as follows:

- Integration with network protocols: In order to make decisions about which nodes should be permitted to participate in the network, trust management systems in MANETs must be integrated with the network protocols that underlie them. To ensure that the system is resilient to attacks and has minimal impact on network performance, this integration must be meticulously designed.
- Heterogeneity: MANETs often consist of nodes that possess different resources and capabilities [9]. Thus, trust management systems in MANETs must be designed to take account of this heterogeneity and offer different trust levels according to the capabilities of each node.
- Flexibility: Trust management systems in MANETs must be adaptable and flexible to accommodate the dynamic requirements of the network. They must be capable of modifying trust scores based on changing network conditions and incorporating new types of data and feedback from nodes [45].
- Multi-dimensionality: Trust management systems in MANETs frequently employ multi-dimensional trust models to evaluate the reliability of nodes. Such models take into account several factors, such as past behaviour, reputation, and network performance, in order to produce a comprehensive trust score for each node.
- Self-organisation: Trust management systems in MANETs are often self-organising, which means that they function in a decentralised manner without requiring central coordination or control [6]. This is crucial in ensuring that the system can operate effectively and withstand attacks in a dynamic and unpredictable network environment.

2.3.2 Parameters Used in the Derivation of Trust Scores

In trust management systems for MANETs, there are a variety of parameters that can be used to derive trust scores for individual nodes in the network. The choice of parameters can depend on the specific requirements of the network and the design of the trust management system. Most research into MANETs has been influenced by several factors impacted by the trustworthiness of a node in a MANET, including the use of the reputation, location and resource availability of a node, and some common parameters that are often used to derive trust scores in MANETs include the following:

- Node Reputation: Nodes that have a good reputation are more likely to be trustworthy than those with a poor reputation. Reputation can be based on various factors, such as the history of the node's interactions with other nodes and the quality of the data that it has shared.
- Node Characteristics: These refer to the inherent characteristics of a node such as its location, battery life, processing power, and available bandwidth. These features can be used to make inferences about the node's ability to provide reliable network services and to contribute to the overall performance of the network.

2.3.3 Trust Mechanisms Using Node Reputation in MANETs

Node reputation is one of the key parameters used in trust management systems for MANETs [46]. It is a measure of a node's past behaviour in the network, and nodes with a good reputation are more likely to be trusted. A node's reputation can be based on a variety of factors, such as its successful delivery of data, responses to network requests, and compliance with network protocols. The reputation of a node can be determined by considering its interactions with other nodes in the network. For example, a node that consistently delivers data packets to its destinations without delays or errors may be considered to have a good reputation. Similarly, a node that promptly responds to requests for network services, such as by providing routing information or forwarding data packets, may be considered reliable and trustworthy.

In contrast, a node that fails to deliver data packets, responds slowly to network requests or violates network protocols may be considered to have a poor reputation. Nodes with a poor reputation are typically avoided or deprioritised in routing decisions, since they are seen as more likely to contribute to network congestion, errors, or security threats. In addition to the monitoring of a node's direct interactions with other nodes, the assessment of reputation can also be influenced by feedback from other nodes in the network. For example, a node may receive feedback from other nodes indicating that it is not responding to requests in a timely manner or is providing inaccurate routing information. This feedback can be used to adjust the node's reputation score which will then inform routing decisions.

Node reputation is an important parameter for trust management in MANETs since it provides a measure of a node's past behaviour and helps to inform routing decisions [47]. By prioritising nodes with a good reputation and avoiding or deprioritising nodes with a poor reputation, trust management systems can improve the security, reliability, and performance of network communication in MANETs.

According to Yu et al.[10], a trust management mechanism is a measure of the confidence in the future behaviour of nodes based on the services they have provided previously. The authors also categorise trust and reputation management systems into two groups:

individual-level trust and system-level trust. Individual-level trust mechanisms allow a node, acting as an agent, to gather information about interactions with a target node, obtain feedback from other nodes regarding potential communication with the target node, assess the target node's trustworthiness based on previous encounters, and determine whether to communicate with the target node based on this assessment. On the other hand, system-level trust mechanisms concentrate on imposing penalties according to node trustworthiness and reputation in order to enhance the overall utility of reliable nodes [10].

Sirisala et al.[48] proposed a Weight-Based Trusted QoS (WBTQ) protocol that addresses both security and quality concerns. Rather than employing encryption algorithms, it ensures a secure network by calculating the trustworthiness of each node, thus maintaining its performance. The proposed WBTQ is an enhancement to the OLSR protocol, where node trust values and QoS metrics are disseminated through the network via HELLO packets. This protocol offers users a flexible and viable approach to select a superior route by attributing weight to quality and trust values [48].

2.3.4 Trust Mechanisms Using Node Characteristics in MANETs

Node characteristics are among the parameters that trust management systems use in MANETs to calculate trust scores. Individual nodes in the network are evaluated taking into account their hardware capabilities, battery power levels, and mobility patterns, in order to determine their trustworthiness [5]. For instance, nodes with better hardware capabilities, such as faster processing speed and more memory may be considered more reliable and trustworthy in managing network communication. Similarly, nodes with higher power levels, such as those with more efficient power management systems or larger batteries, may be regarded as more trustworthy because they may be more resilient against power failure and able to stay connected for longer periods. Mobility patterns are another consideration when calculating trust scores. Predictable or consistent mobility patterns may make nodes more trustworthy since they are easier to locate and communicate with. However, nodes with highly variable mobility patterns may be considered less trustworthy as it may be difficult to predict and maintain their location and connectivity.

Trust mechanisms in MANETs can be implemented using any node characteristics such as node location information. Trust can be determined based on a combination of factors including physical location, duration of communication events, number of successful communications, and the node's movement patterns. The location information can also be used to determine the proximity of a node to other nodes in the network, which can be part of the evaluation of the trustworthiness of the node.

For example, a node's physical location can be determined using GPS or other location-based technologies, and nodes that are geographically close to each other are more likely

to be trustworthy. However, a node's location alone may not be enough to establish trust, and so other factors such as the duration of communication and the number of successful communications can also be used to establish trust. In a node location-based trust system, each node maintains information about its location and shares this information with other nodes in the network. The location information can be used to verify the identity of a node and to ensure that it is not an impostor or a Sybil node, which is a single node posing as multiple nodes.

Moreover, movement patterns can be used to establish trust in MANETs, given that nodes that move in a consistent and predictable manner are more likely to be trustworthy. For example, a node that frequently changes its location or moves in a random manner may be considered less trustworthy than a node that moves in a consistent and predictable manner.

The use of a combination of these factors can improve the security and reliability of MANETs by providing a more sophisticated approach to the establishment of trust among nodes. This can prevent malicious nodes from participating in the network, and also allows for the more accurate identification of legitimate nodes, which can improve the overall performance of the network.

However, there are several challenges in the use of node location information for determining trust in MANETs, including the following:

- Inaccurate or outdated location information: The location information of a node may not always be accurate or up-to-date, which can affect the reliability of the trust system.
- Location spoofing: A malicious node may attempt to falsify its location in order to gain an unfair advantage or to evade detection.
- Limited accuracy: The accuracy of location information can be limited by the accuracy of the positioning system being used, such as GPS.

Despite these challenges, node location-based trust systems can be an effective way to establish trust in MANETs and can help to ensure the reliability and security of the network. It is important to design the trust system in such a way that it is resistant to attacks and takes into account the potential limitations of location information.

Mostafavi et al.[49] proposed a new routing protocol called QMAR-AODV that is based on the AODV protocol. It provides quality of service assurances and takes mobility into account. QMAR-AODV determines the best route by considering both stability and quality factors among the available options. The evaluation of QMAR-AODV's performance demonstrated improvements in stability, data gathering, and throughput, as well as reductions in end-to-end delay, packet loss, and link-breakage rates.

Resource availability is another node characteristic used as a parameter in trust mechanisms for MANETs. Salient resources in MANETs can include power, bandwidth, storage, and computational power, and nodes that have ample resources available, such as high battery power or a large amount of storage, are more likely to be deemed trustworthy. This assessment can be accomplished using sensors or other methods to determine the availability of resources at each node. Additionally, the way in which nodes use their resources can also be used to establish trust. For example, nodes that use their resources efficiently, such as by turning off their transmissions when not in use or using energy-efficient protocols, may be considered more trustworthy than nodes that waste resources.

Nodes that are willing to share their resources with other nodes can also be considered to be more trustworthy. For example, a node that is willing to share its power or bandwidth with other nodes may be considered more trustworthy than a node that is unwilling to share its resources. The willingness to share resources can be determined by analysing the node's behaviour and communication patterns.

Another factor that can be used to establish trust is the node's capability to provide resources, so that nodes with higher capabilities, such as is the case with more powerful devices or those with larger storage capacity, are more likely to be identified as trustworthy.

A sophisticated approach to establishing trust using resource availability involves the use of a combination of these factors, including resource availability, resource usage, willingness to share resources, and resource provision capability. This approach can provide a more comprehensive evaluation of a node's trustworthiness and can be used to establish trust in a dynamic and adaptive manner.

Kasa et al.[50] introduced a trust-based quality of service model that considers quality of service parameters like energy consumption, bandwidth availability, and delay when calculating a node's trustworthiness value. The researchers used fuzzy logic to strike a balance among the quality of service parameters. The proposed model demonstrated improved performance when integrated with the AODV routing protocol.

Overall, the analysis of node characteristics is an important aspect of trust management in MANETs, since it provides important information about the capabilities, reliability, and behaviour of individual nodes in the network. By considering node characteristics, trust management systems can make more comprehensive routing decisions, identify nodes that may be potential security risks, and ensure that nodes are appropriately prioritised based on their trustworthiness.

In conclusion, there are many parameters used to derive measurements of trust. The reputation and characteristics of nodes have been discussed above as they are a particular focus in the present research. Other parameters which could be used for the derivation of trust include a node's interaction and willingness to cooperate, among many others.

2.4 Trust Management Techniques

This section summarises some commonly used trust management techniques that are employed to evaluate trust and reputation in different applications. In the previous section, various trust and reputation management models were discussed which are used in different types of networks such as e-business, peer-to-peer (P2P), and MANETs. However, many of these proposed models employ closed techniques which are based on the observation of the behaviours of entities within a community in order to establish trust relationships. These trust relationships represent the degree of trustworthiness that one entity can ascribe to another, and they are useful in making decisions about whether or not to interact with specific entities. These closed techniques focus on observing the behaviour of entities within the community to establish trust.

In most trust and reputation management models, trust metrics are calculated using three main techniques: game theory, fuzzy theory, and probability theory. This thesis, however, specifically focuses on the development and implementation of a technique based on probability theory for the computation of trust metrics in MANETs, due to this approach being less resource-intensive. The use of game theory and fuzzy theory are also acknowledged in this review for their importance and applicability in trust and reputation management, but these techniques are not subject to further examination in this study.

2.4.1 Fuzzy Theory Techniques

The theory of fuzzy logic was first developed by Zadeh [51] and has been applied in a considerable range of research fields to model the uncertainty, vagueness and imprecision associated with concepts of trust, as well as in risk analysis during interaction with strangers and decision-making processes to identify trustworthy entities. Fuzzy logic or fuzzy inference is a powerful mathematical framework that allows for the handling of uncertain and imprecise information and can be used to make decisions and draw conclusions in a wide range of applications, including trust management in mobile ad-hoc networks and other distributed systems. Fuzzy inference is the process of using fuzzy logic to make decisions or draw conclusions based on uncertain and imprecise information [52]. This is done by using a set of fuzzy rules, which are logical statements that relate input variables to output variables [51]. These rules are usually formulated in a natural language and then translated into mathematical expressions.

Wei et al.[53] proposed a trust management model for e-businesses which uses the theory of Fuzzy Cognitive Time Maps (FCTMs) to model and evaluate trust relationships. The model is based on the idea that trust is a multi-dimensional concept that is influenced by various factors, including the sources and credibility of trust. The FCTM model addresses

the essential factors related to trust in virtual environments by examining the three-way relationship between the trustor, trustee, and their surroundings. Moreover, the model takes into account the dynamic nature of trust and allows for the evolution of trust over time by considering changes in the trustor's opinion of the trustee. This is achieved by examining inter-organisational trust based on the sources of trust and their credibility. The model provides a comprehensive approach to trust management that takes into consideration the various factors that influence trust and the dynamic nature of trust relationships in virtual enterprises.

Trust is also an important concept in peer-to-peer (P2P) networks because it is necessary to determine which nodes can be trusted to share resources or forward data. Chen et al.[54] proposed a fuzzy trust model for P2P networks that consists of two phases: recommendation of trust and direct trust. The primary objective of the recommendation trust phase is to extract trust links and calculate the recommendation trust degree through the application of a fuzzy decision-making technique. The fuzzy trust model employs various sets that rely on the fuzzy decision-making method to derive a fuzzy trust evaluation metric. In the recommendation trust phase, the model extracts the trust link by considering various factors such as the number of common neighbours, the length of the shortest path, and the similarity of the peers. Meanwhile, the focus of the direct trust phase is mainly to update the direct trust degree using the experience and recommendations of peers. The proposed model is designed to handle the uncertainty and imprecision of trust information in P2P networks by implementing the fuzzy decision-making method and updating the trust degree.

In MANETs, fuzzy logic allows for the handling of uncertain and imprecise information about the trustworthiness of nodes and can be used to make trust-based decisions in the network. This technique is particularly useful in mobile ad-hoc networks where nodes are often mobile, and the topology is constantly changing. Helen et al.[55] proposed an energy-aware routing mechanism called Energy-Aware Fuzzy Controlled Routing (EAFCR) that incorporates fuzzy decision-making tools to improve the stability and energy efficiency of the route discovery phase. The mechanism uses fuzzy logic to take into account various parameters such as per-hop delay, available energy, and link quality when determining the most stable route. The EAFCR algorithm was evaluated through simulations, and the results showed that it improved the packet delivery ratio, end-to-end delay, residual energy, and throughput.

2.4.2 Game Theory Techniques

Game theory is a formal method for the analysis of the decisions and interactions of rational players using mathematical tools [56]. It has had a significant impact in many

fields, including engineering, economics, and computing. In recent years, there has been increased use of game theory in the study of communication networks, since it is useful in improving the understanding behaviour in autonomous, distributed, and mobile networks [56]. Additionally, game theory can be used to design efficient algorithms which represent competition or cooperation between entities in a network.

In game-theoretical trust management, the concept of trust is represented as a game played among different agents. The agents make choices based on their perceptions of the actions of others, and the goal is to create strategies that are resilient against the actions of others and achieve a desired outcome. This method can be applied in various fields such as security, systems with multiple agents, and distributed systems.

Li[57] proposed a mechanism which uses game theory to improve the trust relationships between buyers and sellers in e-business transactions. The mechanism aims to help buyers identify trustworthy sellers by providing them with a means to report on the quality of the sellers and, in turn, encourages sellers to act cooperatively by providing accurate and timely information about their products. The mechanism also includes a rebate system which gives sellers the opportunity to provide feedback about buyers, such as their responsiveness in making payments. This feedback can be used to build a reputation system for buyers and sellers which can further enhance the trust relationships between them. The overall goal of this mechanism is to improve the overall performance of e-commerce transactions by promoting cooperation and trust between buyers and sellers.

The application of game theory in the design and analysis of trust mechanisms in peer-to-peer (P2P) networks has become a popular research area. Game theory provides a formal framework to model and analyse the strategic interactions among rational agents in P2P networks. Harish et al.[58] presented a trust framework for the evaluation of the trustworthiness of peers in a network using game theory. The proposed framework takes into account both a peer's self-experience and reputation in calculating trust. The framework uses the self-experience of the peer to determine its past behaviour and reputation so as to determine the view of peers about the agent. By combining these factors, the framework can provide a more accurate and comprehensive assessment of a peer's trustworthiness. To select peers for the completion of tasks and to evaluate the results, the authors propose six strategies. The *Game Tree* strategy uses game-theoretical methods to determine the best peers to use for a given task, while the *Tit for Tat* strategy uses a cooperative approach where a peer will only work with other peers that have cooperated with it in the past. The *Self Trust* strategy relies on a peer's self-experience and reputation to determine the trustworthiness of other peers, whereas the *Dynamic* strategy adapts to changes in the network by continuously updating the trustworthiness of peers and the *Auditing* strategy uses a third party to evaluate the trustworthiness of peers. Finally, the *Redundant Job Submission* strategy uses multiple peers to perform the same task and then compares the

results to determine the most reliable peer. The proposed trust framework and strategies for selection of peers are shown to improve the performance of the network by promoting cooperation and trust among peers [58].

Lu et al.[59] questioned the traditional belief that peers in a peer-to-peer (P2P) network act selflessly and provide services without any expectation of reward. Instead, they developed a reputation model that incorporates punishment for peers that do not offer their own content, for example, and then classifies them as defective peers. Additionally, the authors use game and evolutionary theories to model the adaptive behaviour of peers, allowing them to adjust their strategies to become more effective. These insights are then applied to the existing *EigenTrust* reputation management system to enhance its performance.

In game theory, players make decisions the outcomes of which are impacted by the choices of other players. This is similar to the nodes in an ad-hoc network, in which nodes make independent decisions that are also affected by the actions of other nodes. This similarity enables a direct association between the elements of traditional game theory and the components of an ad-hoc network. Table 2.2 illustrates the common components of an ad-hoc networking game [60].

Table 2.2 Game Theory and MANET components

Game Theory Components	**MANET Components**
Players	Nodes inside the network
Strategies	Actions being analysed (such as forwarding packets)
Service function	Performance metrics (such as packet delivery ratio)

Game theory can be used to model ad-hoc networks at different layers of the network stack, including the physical layer (such as distributed power control and waveform adaptation), the link layer (such as medium access control), and the network layer (such as packet forwarding) [60].

Khan et al.[61] presented a novel packet forwarding approach that uses game theory and takes into account the reputations of nodes. The approach also employs an incentive model to encourage cooperation among the mobile nodes in a MANET routing scenario. The system is designed using evolutionary game perspectives to meet the quality-of-service (QoS) requirements. The experimental results support the proposed design and demonstrate that the reputation and trust-based game approach increases the efficiency of packet forwarding by achieving high throughput and minimal network overheads.

Yu and Liu[62] proposed a game-theoretical framework to examine the stimulation of cooperation and enhancement of security in MANETs. The framework is based on a game with two players in which nodes are considered to be players. The authors' analysis demonstrates that, in this two-player game, the optimal strategy for each node in terms of being cheat-proof, is to only assist the opponent to the same extent that the opponent has assisted them. This is referred to as the Nash equilibrium in game theory. The results of the study underline the importance of considering the incentives for the nodes and the impact of their actions on overall cooperation in and the security of the network.

2.4.3 Reputation and Probability Techniques

Probabilistic trust and reputation techniques are methods that create trust models using a probability calculus and advanced statistical methods [46]. These models represent trust and reputation as probability distributions as opposed to fixed values, allowing for the consideration of uncertainty and randomness within the system. Using probability theory, these models can be simplified to make them easier to comprehend and analyse, while retaining the ability to use a variety of derivation methods such as Bayesian networks, and the Markov Chain and Hidden Markov models to extract useful information and make predictions. Peer-to-peer network, multi-agent and security systems can all use these techniques to model the interactions and decision-making of agents and to design robust and efficient systems.

Beta distributions and Bayesian inference are techniques widely used by researchers in the modelling of trust and reputation [46]. These methods are based on binary ratings which take only two inputs as either positive or negative. They are used to compute trust scores by updating beta probability density functions (PDFs) using statistical methods. These techniques are known for their simplicity and flexibility, making them widely used in various fields of computing. The beta distribution provides a useful way to model trust and reputation as it can handle the uncertainty in the system, and the Bayesian inference technique allows for trust scores to be updated based on new evidence. These methods may be used to simulate the interactions and decision-making of agents and to create resilient and effective systems.

The Trust and Reputation model for Agent-based Virtual Organisations (TRAVOs system) was developed to ensure high-quality interactions between participants in a large open system [63]. It relies on two sources of information and uses a probabilistic method to evaluate the credibility of witnesses. It includes metrics of confidence in and the reliability of direct interaction information sources while using a single-rating system.

FBit [64] is an approach proposed for the improvement of fairness and robustness against maliciousness in peer to peer (P2P) systems like BitTorrent and addressing Sybil

attacks. It prioritises each peer based on their level of cooperation in order to improve motivation, resource management, network safety, fairness and efficiency. The results show that the proposed method is very robust and can efficiently mitigate popular attacks on P2P overlay networks [64].

MANETs frequently employ trust-based reputation and probability methodologies for the modelling and evaluation of the interactions between and decision-making of network nodes. Sen et al.[47] described a trust-based approach to identify malicious nodes that drop packets in a network. This mechanism makes use of the reputation of surrounding nodes and takes into consideration the weakening of trust over the course of the network's lifetime. In order to protect user identities from attacks, the suggested mechanism makes use of public and private key pairs; however, owing to potential scalability concerns, this solution may not be applicable to larger networks. Mundinger and Boudec [65] were among the first authors to analyse the robustness of reputation systems through deviation testing. They applied a mean-field approach in a stochastic model and demonstrated that liars have minimal effect until their number exceeds a certain threshold, which is a phase transition. They also provided formulae for critical values and recommendations for optimal parameter selection. Their study is notable for its evaluation of a system's resistance to untrusted nodes, but reputation evaluation is based solely on the identification of 'fake' information.

2.5 Application of Trust

Trust and reputation management refers to the process of establishing, building, and maintaining trust and a positive reputation [9]. In the field of computing, trust and reputation management refers to the use of technology to establish, build, and maintain trust and a positive reputation among various entities in a digital environment, which can include individuals, organisations, and software systems.

The development of trust and reputation models for applications of this kind is an important area of study that may assist in the mitigation of risk and ensure successful outcomes of network operations. Trust management models which have a design that is both flexible and effective are able to maintain emerging and efficient trustworthiness data for the various entities that make up a distributed system [9]. Additionally, these models can be used to mitigate a variety of attacks that are associated with such systems.

Trust and reputation management mechanisms have been an effective tool for the analysis and evaluation of the trustworthiness of any entities, such as those in distributed systems. In distributed systems such as e-business or peer-to-peer systems and MANETs,

trust and reputation management play a powerful role in maintaining security in the face of many types of malicious activity.

2.5.1 Trust Applications in E-Business

This section explains the use of trust mechanisms in the area of e-businesses, which allows an understanding of the use of trust and reputation in the field of computing. E-business is involves a computing platform that provides an Internet-based infrastructure for market participants to share information, conduct transactions, and engage in other relevant activities [66]. E-business is expanding and growing each year, which reinforces the need for security and trustworthiness measurements [67]. A great deal of research has been devoted to the development of trust and reputation mechanisms in the e-business sector, according to which customers can be evaluated for each activity they take part in [67].

Many online commercial organisations, such as Amazon and E-bay, use forms of reputation and trust mechanisms. For instance, Amazon uses a trust and reputation system to help customers make informed purchasing decisions. This system includes a variety of features such as customer reviews, ratings, and feedback on products and sellers. Customers can post reviews and ratings of products they have purchased, and these reviews and ratings are visible to other customers. Sellers also provide ratings and feedback, which are based on factors such as their selling history and customer service. This information helps customers to determine which products and sellers are trustworthy, and which ones they should avoid. Additionally, Amazon also uses its own algorithm to detect and remove fake reviews, in order to ensure that the reviews published are authentic and unbiased.

Zhang et al.[68] developed a distributed reputation architecture called *Direct* that was developed with the goal of preventing dishonesty in e-businesses websites and e-commerce and online applications in general. Using statistical distribution methods, *Direct* identifies and monitors and harmful attacks carried out by dishonest users. To address the issue of dishonest feedback, all feedback is separated into two categories of green or red, and only true reputation data collected from the green group is retained. This approach may minimise the negative impact of dishonest feedback.

In another study [69], the authors emphasised the importance of trust and reputation systems in e-commerce. For example, data such as seller ratings, product reviews, and verified customer reviews can help to build trust with potential customers. The authors also discussed the challenges of trust and reputation management in e-commerce, such as the difficulties of managing and responding to large amounts of customer feedback and the potential for untrusted and fake reviews. The trust and reputation methods used in e-business organisations such as E-bay and Amazon have motivated the research in this

thesis which aims to understand and improve the aggregation, propagation, and calculation of the recommendation mechanism in a MANET.

2.5.2 Trust Applications in Peer-to-Peer (P2P) Networks

This section explains trust mechanisms employed in peer-to-peer environments in order to enhance the understanding of the use of trust and reputation in the field of computer networks. A peer-to-peer (P2P) network is a highly sophisticated type of distributed network architecture in which nodes (peers) can communicate and share resources directly with each other without the need for a central server [70]. In P2P networks, peers often engage with unknown entities whose trustworthiness is also uncertain. To ensure cooperation and to address the potential negative impact of misbehaving peers, such as those who take advantage of the network without contributing, trust management is necessary.

This decentralised approach to networking allows for the efficient distribution of data and services among the participating nodes, resulting in increased scalability, reliability and security [70]. P2P networks are often used for file sharing, where users can share and download files directly from each other's computers. They can also be used for distributed computing, where each node contributes its processing power to a larger task. P2P applications can be implemented on both wired and wireless networks. P2P networks are widely used for various applications, such as file sharing, instant messaging, streaming, and online gaming. They have been adapted for a wide range of use cases, from small-scale local networks to large-scale global networks.

In order to ensure the security and reliability of communication within a P2P network, it is essential that peers have the ability to identify and communicate with reliable and trustworthy nodes. This is particularly challenging in P2P networks that are characterised by highly dynamic and constantly changing environments, where the trustworthiness of peers may be uncertain and subject to change.

In address this issue, trust management and reputation systems have become crucial approaches for securing large-scale P2P networks. These systems enable peers to assess the trustworthiness of other nodes based on several factors, such as previous actions, recommendations from other peers, or the outcomes of security and performance evaluations [71]. Employing trust management and reputation systems allows peers to make better-informed choices about which nodes to interact with and helps minimise the potential adverse effects of misbehaving or malicious nodes.

Trust management and reputation systems can also help to encourage cooperation and the fair distribution of resources within a P2P network. For example, by using reputation systems to identify and discourage free-riding behaviour, in which nodes take advantage

of network resources without contributing, trust management can foster a more equitable and sustainable P2P network [70].

A variety of trust and reputation systems have been developed by researchers to encourage cooperation among peers. These systems aim to identify and remove misbehaving peers by assigning values of trustworthiness to them. P2Prep [72] is a protocol that uses reputation data to identify malicious peers in P2P networks. It works by allowing a peer searching for a resource to check the reputations of all peers that can provide that resource before downloading. The reputation of a peer as either good or bad is determined by soliciting opinions from other peers who have previously interacted with that peer. There are two variations of P2PRep: basic polling and enhanced polling. The main difference between them is that a basic polling protocol gives equal weight to all opinions about a peer's reputation, while enhanced polling protocols also take into account the credibility of the peers providing the opinions [72].

2.5.3 Trust in Mobile Ad-hoc Networks (MANETs)

As previously stated, a mobile ad-hoc network is a type of wireless network that consists of a group of devices that communicate with each other without the need for a central network infrastructure or fixed network topology. In a MANET, the devices can act as both routers and clients, dynamically forming a network on the fly as needed [4]. The devices in a MANET can be mobile, and the network can change rapidly as devices move in and out of range. The primary goal of MANETs is to ensure the security of network routing, including maintaining confidentiality, integrity, availability, and anonymity in the network. However, despite this goal, MANETs face significant vulnerabilities due to their open peer-to-peer architecture.

MANET routing protocols are designed under the assumption that all nodes will collaborate without maliciously disrupting the operation of the protocol [35]. However, this assumption is not always met, and MANETs are vulnerable to malicious attacks. As a result, from a security design perspective, MANETs lack defence mechanisms and this makes them more vulnerable to security threats.

The wireless nature of MANETs also exposes them to the security threats that both wireless and wired networks face [31]. Furthermore, MANETs are also exposed to unique attacks that are specific to their characteristics. For instance, the mobility of nodes in MANETs results in increased numbers of collisions, unidirectional links, and repeated path breaks, all of which can lead to higher rates of packet loss and affect the security of the network.

MANETs also pose a challenge to trust and reputation systems, since nodes in the network can frequently interact with anonymous entities whose trustworthiness is also

unknown [44]. Therefore, trust management is necessary so as to guarantee cooperation and mitigate the influence of misbehaving peers.

Sharing information and collaborating in a distributed manner are crucial functions in MANETs for achieving implementation goals. Such collaboration is only beneficial when all participating nodes act in a reliable and trustworthy way. Trust and reputation management in MANETs is used for two primary reasons [73]. First, the trust management mechanism aids in the detection and isolation of malicious nodes, reducing the impact of misbehaving or malfunctioning nodes. Furthermore, the trust management mechanisms provide predictions of a node's future behaviour and analyse the probabilities to enhance the quality of service offered by the network. MANETs lack a central management unit to supervise the activities of nodes; therefore, any node should be cautious when communicating with other nodes because node behaviour might change depending on the time and environmental circumstances [4]. As a result, the establishment and measurement of node behaviour from a trustworthy and reliable perspective is critical in assuring a MANET's reliable operation.

Most reputation-based trust management schemes in MANETs are designed to improve the security of collaborative routing by identifying and addressing nodes that exhibit misbehaviour [9]. These nodes can be either selfish or malicious, and their actions can negatively affect the network's overall performance. Reputation-based trust management schemes aim to detect these misbehaving nodes and limit their impact on the network employing various methods such as trust metrics, reputation systems, and trust-based routing protocols. These methods are meant to ensure the reliable and efficient functioning and overall reputation of of the network by maintaining the trustworthiness of the nodes.

He et al.[74] proposed a reputation-based trust management scheme called Secure and Objective Reputation-based Incentive (SORI) in a study which utilises an incentive mechanism to encourage packet forwarding and discourage selfish behaviour among nodes in MANETs. The scheme is based on quantifiable objective measurements and reputation propagation that is enabled through the use of one-way hash chain-based authentication. This reputation-based incentive mechanism aims to balance the trade-off between the cost of forwarding packets and the benefit of having packets forwarded by providing an incentive for nodes to act in the interest of the network. However, the proposed scheme has not been extensively evaluated in the presence of the malicious nodes which may be prevalent in hostile environments, and its robustness in such scenarios remains uncertain.

In a study published by Marti et al.[75], a reputation-based trust management methodology was proposed to enhance the security of routing in MANETs. This scheme comprises of two components: a watchdog that observes the behaviour of nodes, compiles reputation information, and then takes appropriate actions such as isolating nodes that exhibit misbehaviour. This approach aims to combine direct observations to generate trust values for

secure routing by extending the Dynamic Source Routing (DSR) protocol. However, this approach has limitations, as it is based only on direct observation and is used with the DSR protocol. This means that this scheme is not able to take into account indirect observations or other information that may be relevant in determining the trustworthiness of nodes.

Sun et al.[76] proposed a trust modelling and evaluation method for secure ad-hoc routing and malicious node detection in MANETs. The novel aspect of their method is the use of entropy to model trust as a measure of uncertainty. This approach allows for a greater understanding of the dynamics of trust in MANETs, since trust is considered to be a continuous variable, and does not rely on an assumption of the transitivity of trust. This method also provides a mathematical framework for trust evaluation which can be useful in determining the trustworthiness of nodes in the network. However, a limitation is that the method takes into account packet dropping as the only component of direct observation used to evaluate trust. This means that it does not consider other factors that may be relevant in determining the trustworthiness of nodes in a network, such as the node's past behaviour, recommendations from other nodes, or other contextual information.

Confidant[77] is a trust management mechanism that supports cooperation in MANETs by detecting and isolating malicious nodes using both direct observation and recommendations. The model uses a personal experience method to address the issue of dishonest recommendations by applying a deviation test on recommendations received and eliminating those that exceed a threshold value. The reputation value of a recommending node is then updated based on the results of the deviation test. However, this approach also has limitations. It cannot prevent the dissemination of false recommendations, and the only information exchanged between nodes relates to negative recommendations. Additionally, the model is limited to the use of a single trust metric based on the cooperation of nodes in packet forwarding, and does not take into account other important evaluation metrics such as energy consumption, delay, and node collisions in assessing the trustworthiness of nodes.

2.6 Limitations of Existing Trust-Based Routing Protocols and Known Countermeasures

Existing trust management systems in MANETs have various limitations that affect their effectiveness and reliability. Some of the more significant limitations are as follows:

1. Lack of scalability
   A lack of scalability is a common limitation of many existing trust management systems in MANETs. As the number of nodes in the network increases, the overheads associated with the maintenance of trust scores for all nodes can become a significant

performance bottleneck. This is because trust management systems typically require nodes to maintain and update trust scores for all of their neighbours, which can result in a large amount of network traffic and computational load. In addition, as the network grows, it becomes more difficult to ensure that trust scores are accurately maintained and updated. Nodes may enter or leave the network frequently, which can lead to inconsistencies and inaccuracies in trust scores. This can compromise the security and reliability of the network, where nodes may make decisions based on incorrect or outdated trust scores [10].

To address this limitation, researchers have proposed a number of techniques to improve the scalability of trust management systems in MANETs. These include the use of distributed and decentralised approaches to trust management, sampling techniques to reduce the amount of trust data that needs to be stored and processed, and different techniques to automate the process of trust evaluation. Despite these efforts, lack of scalability remains a significant challenge in the design and implementation of trust management systems in MANETs. As the size and complexity of these networks continue to grow, it is important for researchers to continue to explore new techniques and approaches to address this problem and ensure the security and reliability of MANETs [78].

2. Vulnerability to attacks

Trust management systems in MANETs are vulnerable to various types of attacks which can compromise the accuracy and effectiveness of trust scores. [79] discusses various security attack against trust management systems and also provides possible countermeasures against each of these possible attacks. One common type of attack is the Sybil attack, in which a malicious node creates multiple false identities and uses them to manipulate the trust scores of other nodes. This can allow attackers to gain high levels of trust and participate in network activities even though they are not trustworthy.

Another type of attack is the collusion attack in which multiple nodes work together to manipulate the trust scores of other nodes. This can be particularly effective if the colluding nodes have high levels of trust, since they can use their trusted status to deceive other nodes. Other types of attacks that compromise the effectiveness of trust management systems include the selfish node attack, in which nodes manipulate their own behaviour to increase their trust scores at the expense of other nodes.

To mitigate these types of attacks, trust management systems in MANETs need to be carefully designed so as to incorporate strong security measures. In addition,

the systems need to be able to adapt to changing network conditions and to learn from past experience in order to improve the accuracy of trust scores over time. This can help to minimise the impact of attacks and to ensure that the network is able to operate effectively in the face of evolving security threats.

3. Fairness of trust systems
   Trust management systems in MANETs may face limitations in terms of fairness. One issue is that trust scores can be affected by various factors such as node behaviour and network performance, which can result in trust cliques or the exclusion of certain nodes from the network. This can create a situation where certain nodes are systematically excluded or have limited access to network resources, leading to a sense of inequality. In addition, there is a risk of bias in the trust evaluation process, because trust scores can be influenced by past behaviour, reputation, and network performance, as well as the subjective opinions of nodes providing feedback. If some nodes are systematically favoured or discriminated against, it can result in an unfair and biased system [9].

   To overcome these limitations, trust management systems should be designed to be fair and unbiased, taking into account the capabilities and trustworthiness of all nodes in the network. This can be accomplished by using transparent and objective evaluation criteria and incorporating feedback from a diverse range of nodes so as to ensure a balanced representation of trustworthiness in the network.

4. Complexity of trust systems
   One of the challenges associated with trust management systems in MANETs is their complexity. The process of deriving trust scores for nodes in the network can involve the collection and analysis of large amount of data which can be difficult to manage and process effectively. For example, multi-dimensional trust models that take into account multiple factors to generate a comprehensive trust score for each node can be very complex, requiring a significant amount of processing power and storage space. This complexity can lead to increased overheads in the network as well as longer processing times for the updating of evaluations of trust. In addition, the complexity of the systems can also make them more vulnerable to attack. Attackers may try to exploit the complexity of the system to introduce false data or manipulate the trust scores of nodes in the network. This can be particularly challenging in a decentralised, self-organising network like a MANET, where there is no central authority to oversee the system and ensure its security [78].

5. Lack of standardisation
   One of the limitations in the design of existing trust management systems is the lack

of standardisation. The absence of standardisation has resulted in a proliferation of different trust management systems, each with its own unique set of features, algorithms, and metrics. This lack of standardisation makes it difficult to compare the performance of different trust management systems and to develop proper solutions that can be used across multiple MANET deployments. The lack of standardisation has also made it difficult to develop a common language to describe trust and security requirements in MANETs. This has resulted in inconsistencies and confusion when trying to define and measure trust and security in MANETs [80].

To address this limitation, there have been efforts to develop standardised metrics, frameworks, and protocols for trust management in MANETs. For example, the IEEE 802.11s standard defines a set of metrics for the evaluation of the performance and security of wireless mesh networks, which can be used to inform trust management decisions. Similarly, the IETF has developed a number of standards and protocols for secure routing and authentication in MANETs, such as the Secure Neighbour Discovery (SEND) protocol and the Cryptographically Generated Address (CGA) specification [81]. These standards and protocols provide a common framework for the development and evaluation of trust management systems in MANETs, which can help to address the lack of standardisation in this area.

6. Computational overheads
   The computational overheads associated with trust management systems in MANETs can represent a significant constraint. Trust management systems typically require a substantial amount of computational resources for the evaluation and maintenance of trust scores for all nodes in the network, including for the processing of data from multiple sources, such as feedback from neighbouring nodes, sensor data, and network performance metrics [36].

   The computational demands of trust management systems can increase with the size of the network and as the number of trust metrics and evaluation criteria rises. This can lead to delays and bottlenecks in the network, as well as increased energy consumption and reduced battery life for mobile devices [9]. To overcome these limitations, researchers have proposed various methods to alleviate the computational overheads of trust management systems in MANETs.

   One approach is to use distributed algorithms that allow nodes to share the computational load of trust evaluation and decision-making. Additionally, researchers have explored the use of lightweight cryptographic algorithms and protocols to secure trust management systems and reduce the computational overhead of cryptographic operations. These techniques can enhance the efficiency and scalability of trust management systems in MANETs, enabling more effective and secure communica-

tion in these dynamic and resource-limited environments. The minimisation of the computational requirements of trust management systems can help to mitigate the limitations associated with computational overheads in these networks.

In conclusion, while trust management systems are an important component of securing MANETs, existing systems have limitations that need to be addressed in order to make them more effective and robust. Future research effort should focus on the development of more efficient and effective trust systems that are adaptive and resilient, and which can work in a wide range of MANET environments. Research work proposed in this Thesis addresses scalability, vulnerability of attacks, and fairness of trust systems challenges. The details of proposed approaches are mentioned during the discussion of DTAODV, ITADOV and GTAODV routing protocols in Chapter 3,4,and 5 respectively.

2.7 Summary and Discussion

A Mobile Ad-hoc Network (MANET) is a decentralised, self-configuring wireless network composed of mobile devices or nodes connected by wireless links. Due to their flexibility and ease of deployment, MANETs are well-suited for various applications, including disaster recovery, military operations, and temporary communication networks. MANETs are a versatile and dynamic networks that offer several advantages, such as self-configuration, rapid deployment, and robust communication. However, they also face challenges related to dynamic topology, limited resources, routing overhead, security, and quality of service. Routing protocols play a crucial role in MANETs by establishing and maintaining communication paths between nodes. These protocols can be broadly classified into proactive, reactive, and hybrid categories. The need for continuous route discovery and maintenance in a dynamic network environment can lead to significant routing overhead, consuming valuable resources and bandwidth. The open and decentralised nature of MANETs exposes the network to various security and privacy risks, including eavesdropping, data tampering, and denial of service attacks [25].

The study of existing literature shows that trust management mechanisms contribute to the enhancement of routing in MANETs by improving the reliability of communication. However, the integration of trust mechanisms into MANETs can potentially have negative implications for the performance of the routing protocols. Consequently, it is crucial to evaluate the impact of implementing various trust mechanisms within the AODV protocol. Additionally, an examination of the effects of incorporating three distinct types of trust mechanisms on the AODV protocol considering diverse network scenarios and parameters, is necessary. After going through the literature survey and gap identification in, the same primary goal of this research work is to evaluate the impact of incorporating trust

management mechanisms into the AODV protocol on the overall performance, security, and efficiency of routing processes within mobile ad-hoc networks. Chapters 3, 4 and 5 discuss in detail the research work done to achieve this goal.

Chapter 3

Direct Trust Management in AODV Routing Protocol

Direct trust, Indirect trust and Global trust are major distinctions of trust mechanisms. This thesis focuses on the performance evaluation of these 3 types of trust mechanisms under different experimental conditions. Chapter 3 focuses on the design and performance evaluation of the direct trust mechanisms in the AODV routing protocol. This chapter proposes the Direct Trust AODV (DTAODV) protocol, which is an extension of the AODV routing protocol that incorporates a trust mechanism to improve the security and performance of the protocol. The design of the DTAODV protocol is inspired by direct trust protocols from existing literature. This chapter presents the proposed protocol in detail. Moreover, this chapter examines the impact of a security attack on the AODV and DTAODV protocols under different test conditions. The effect of a black hole attack in both protocols is investigated, and some of the results have been published. [2].

This chapter is structured as follows. Section 3.1 describes the AODV routing protocol and how it works, and the need for trust in the AODV protocol is then discussed. Section 3.2 describes the direct trust management mechanism and the proposed Direct Trust AODV (DTAODV) protocol. In Section 3.3, the research methodology was discussed in depth. In Section 3.4, the impact of varying node movement speed and varying node density on AODV and DTAODV is analysed and evaluated using the NS-2 network simulator. Section 3.5 examines the performance evaluation of the impact of varying node movement speed and density while assigning different weights to node reliability and hop counts. The performance evaluation of AODV and DTAODV in the presence of a Black hole attack is subsequently examined in Section 3.6. Finally, Section 3.7 summarises the chapter.

3.1 AODV Routing and the Need for Trust Mechanisms

The Ad-hoc On-Demand Distance Vector (AODV) is a routing protocol for MANETs. It is a reactive protocol that establishes routes only when needed and is, therefore, an on-demand protocol [5]. AODV uses a distributed route discovery mechanism to identify the destination node and then creates a route from the source node to the destination node [6]. The AODV protocol uses route discovery, route reply, route maintenance and route deletion operations to establish a route inside the network so as to send a packet from a source to a destination node.

3.1.1 Route Discovery Process in AODV

Route discovery is the process by which AODV finds a route from a source node to a destination node in a MANET. The process begins when the source node wants to send a packet to the destination node but does not have a valid route [26]. Figure 3.1 presents a flowchart of the procedures of creating the route discovery and route reply from a source node to a destination node [82].

The route discovery and route reply processes in AODV are explained in detail next [83].

Step 1: Source node broadcasts Route Request (RREQ) packet.
When the source node wants to send a packet to the destination node but does not have a valid route to it, it initiates the Route Discovery process by broadcasting a RREQ packet [83]. The RREQ packet contains the following fields:

1. Source IP address: This represents the IP address of the source node.
2. Source Sequence Number: This represents a unique sequence number assigned to each RREQ packet generated by the source node.
3. Destination IP address: This represents the IP address of the destination node.
4. Destination Sequence Number: This represents the last known sequence number of the destination node.
5. Hop Count: This represents the number of hops from the source node to the current node.
6. Broadcast ID: This represents a unique identifier assigned to each RREQ packet in order to prevent the processing of old packets.

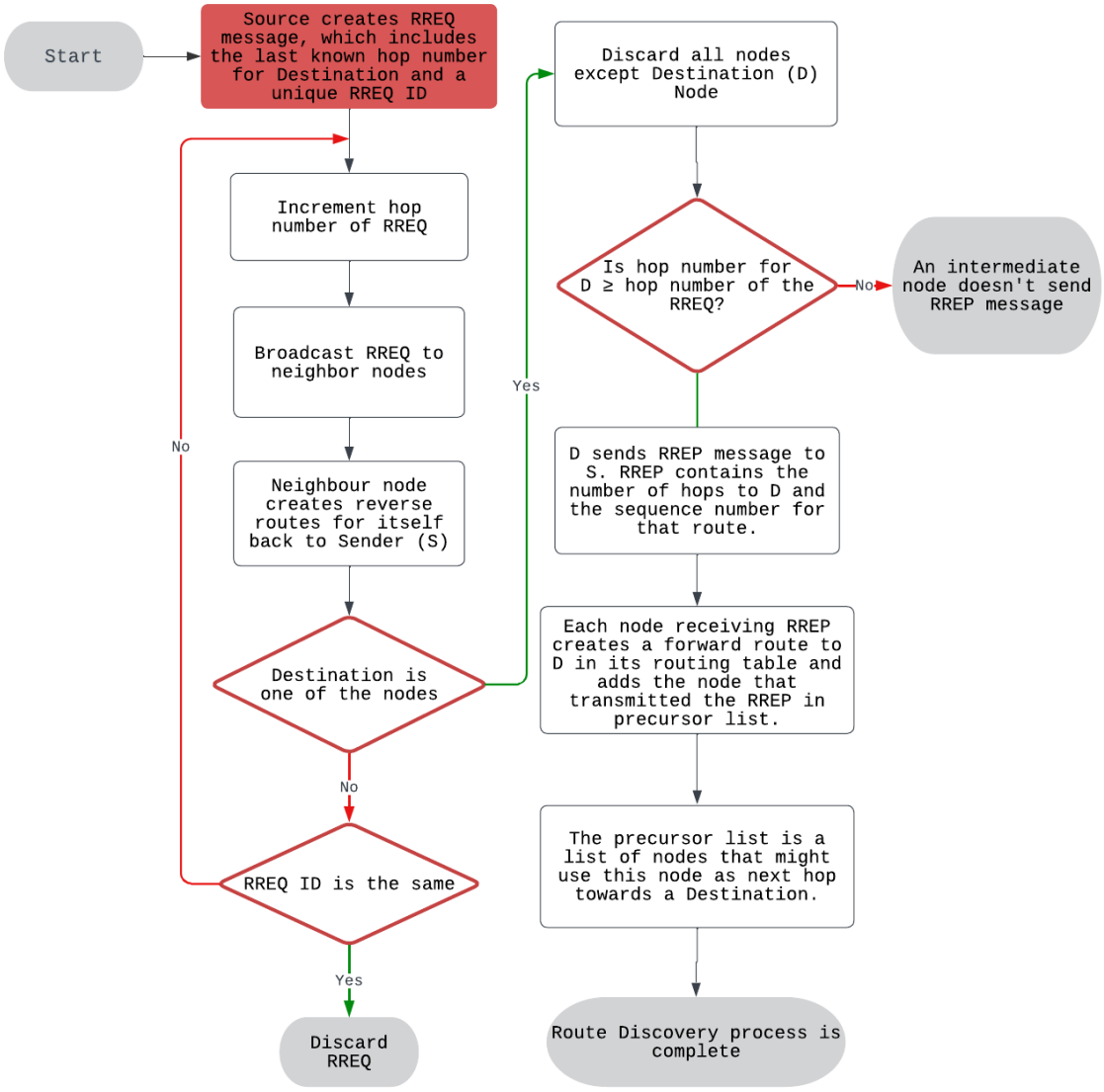

Figure 3.1 AODV Route Discovery and Reply Procedure

Step 2: Intermediate nodes receive and process the RREQ packet.
When an intermediate node receives the RREQ packet, it checks its routing table to determine if it has a route to the destination node. If it does not have a valid route, it forwards the RREQ packet to its neighbouring nodes. If it does have a valid route, it generates a Route Reply (RREP) packet and unicasts it to the source node.

Step 3: Destination node generates Route Reply (RREP) packet.
When the RREQ packet reaches the destination node, it generates a Route Reply (RREP) packet and unicasts it to the source node. The RREP packet contains the following fields:

1. Destination IP address: It represents the IP address of the destination node

2. Destination Sequence Number: It represents the current sequence number of the destination node
3. Source IP address: It represents the IP address of the source node
4. Hop Count: It represents the number of hops from the destination node to the source node
5. Lifetime: It represents the time duration for which the route is valid

3.1.2 Route Maintenance in AODV

Route Maintenance is the process by which AODV ensures that the routes established between nodes are still valid and functional. Figure 3.2 presents a flowchart of the procedures of creating the route discovery and route reply from a source node to a destination node [26].

The following steps give a detailed explanation of the route maintenance process in the AODV [84].

Step 1: Nodes periodically broadcast Hello messages.
Each node in the network periodically broadcasts a Hello message to its neighbours. The Hello message contains the following fields: Source IP address, destination IP address, and current sequence a number of the sending node. When a node receives a Hello message, it updates its routing table to reflect the presence of the neighbour node.

Step 2: Nodes monitor the freshness of their routes.
Each node in the network periodically checks the freshness of the routes in its routing table. A route is considered fresh if it has been recently used to send data packets or if a Hello message has been received from the next-hop node within a certain time interval. If a route is stale (that is, not fresh), the node marks the route as invalid in its routing table.

Step 3: Nodes generate Route Error (RERR) messages when a route is broken.
If a node discovers that a route is broken so that the next-hop node is no longer reachable, it generates a Route Error (RERR) message and broadcasts it to its neighbours. The RERR message contains the following fields: the Destination IP address, the sequence number of the destination node at the time the RERR message was generated, the IP address of the node that is no longer reachable, and the sequence number of the node that is no longer reachable at the time the RERR message was generated. When a node receives a RERR message, it updates its routing table to reflect the broken route.

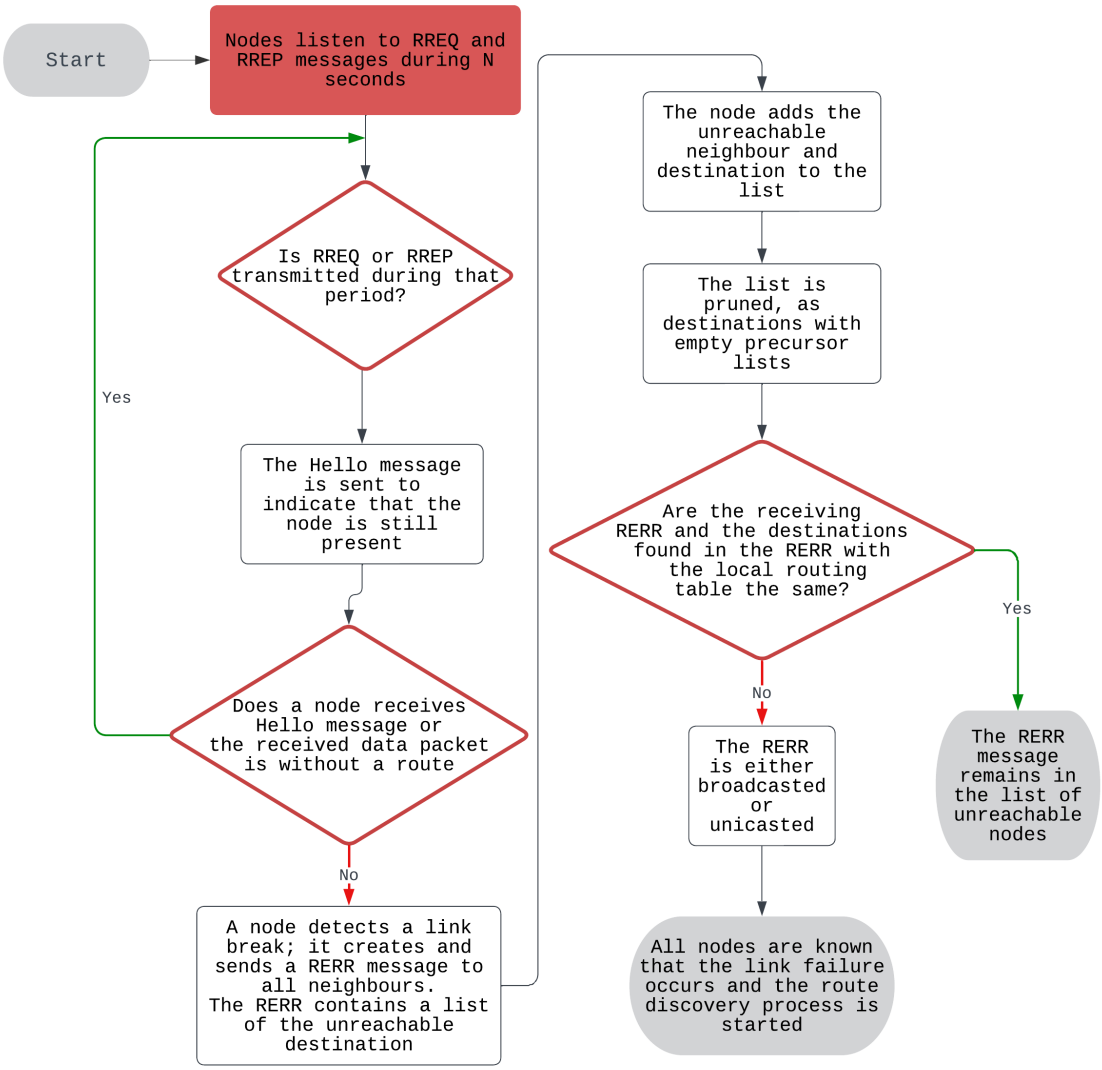

Figure 3.2 Route Maintenance and Deletion Procedure

3.1.3 Route Deletion in AODV

The route deletion process is triggered when a node no longer requires a route or when a node goes out of range or is shut down [26]. The process involves the deletion of the corresponding route from the node's routing table and the broadcasting of a Route Error (RERR) message to inform other nodes in the network about the deletion [83]. The following steps give a detailed explanation of the route deletion process in AODV [84].

Step 1: Node decides to delete a route.

When a node no longer needs a route, it decides to delete it from its routing table. This can happen, for example, when a data transfer is complete or when a node is shut down.

Step 2: Node deletes the route from its routing table.
The node deletes the corresponding route from its routing table. This involves the route being marked as invalid and the route's lifetime is set to zero.

Step 3: Node generates a Route Error (RERR) message.
After the deletion of the route, the node generates a Route Error (RERR) message to inform other nodes in the network about the deletion. The RERR message contains the following fields: the IP address of the destination node for which the route is deleted, the sequence number of the destination node at the time the RERR message was generated, the IP address of the node that deleted the route, and the sequence number of the node that deleted the route at the time the RERR message was generated.

Step 4: Node broadcasts the Route Error (RERR) message.
The node broadcasts the RERR message to its neighbours in the network.

Step 5: Nodes update their routing tables.
When a node receives a RERR message, it updates its routing table to include the information about the deleted route. The node marks the route as invalid and sets its lifetime to zero.

Step 6: Route deletion confirmation.
When a node receives a RERR message and deletes the invalid route, it may send a confirmation to the original sender of the RERR message. This confirmation can be in the form of an acknowledgement or through a passive mechanism such as observing that the original sender has removed the route from its routing table.

Step 7: Route rediscovery.
If a node still needs a route to a destination after the deletion of the invalid route, it may initiate a new route discovery process by sending a Route Request (RREQ) message. This process will help the node to find an alternative route to the destination.

Step 8: Maintaining fresh routes.
As part of the route maintenance process, nodes periodically check their routing tables for active routes. If a route is found to be invalid or stale, the node removes it from the routing table to ensure that only fresh routes are used for communication.

Overall, the route deletion process in AODV plays a vital role in maintaining an efficient and accurate routing system in dynamic networks. By ensuring that nodes only use valid routes, AODV can provide reliable and efficient communication between nodes in mobile ad-hoc networks.

3.1.4 Need for Trust in the AODV Protocol

The implementation of trust mechanisms can prove to be a crucial element in enhancing the efficacy and security of the AODV routing protocol. Trust mechanism is needed in the

AODV protocol for several reasons, including to improve the performance and security of the protocol and to ensure the reliability of routing information in the network [85]. One of the key characteristics of MANETs is their decentralised nature, which means that there is no centralised infrastructure to oversee node behaviour or manage routing decisions [7]. In such a setting, nodes need to rely on each other for the routing and forwarding of data packets. Therefore, trust management mechanisms can provide a way for nodes to assess the trustworthiness and reliability of their neighbours, allowing them to make better-informed routing decisions.

Moreover, a primary reason for using trust mechanisms in AODV is to address the security threats that can arise due to the distributed and dynamic nature of the ad-hoc network. In AODV, each node is responsible for forwarding packets to their destination, and the protocol relies on the cooperation of all nodes to discover and maintain routes [86]. However, due to the lack of centralised control, nodes with malicious intent or faulty behaviour can cause significant problems and damage to the overall performance of the protocol. These nodes can disrupt the routing process by injecting false routing information, dropping packets, or even launching denial-of-service attacks [35].

Furthermore, MANETs are characterised by their dynamic topology due to the mobility of nodes and frequent changes in network connectivity [8]. This makes them susceptible to various security threats and routing disruptions. Trust management mechanisms can help nodes to adapt to these changes by continuously updating trust values and ensuring that reliable nodes are selected for routing. By using trust management mechanisms, the AODV protocol can dynamically adapt to changes in network topology and maintain reliable routes for data transmission.

Trust can be established through various mechanisms, such as reputation-based systems, digital signatures, and secure key exchange protocols [9]. Reputation-based systems involve the evaluation of a node's behaviour and actions over time to determine their trustworthiness. Digital signatures can provide authenticity and integrity to messages exchanged between nodes, while secure key exchange protocols can ensure that only trusted nodes can access sensitive information [87]. In AODV, trust mechanisms can improve the performance and security of the protocol by detecting and isolating malicious nodes, preventing the propagation of false routing information, and maintaining the integrity of routing paths [88]. Trust mechanisms can also enhance the resilience of the network by enabling nodes to detect and recover from attacks quickly.

In summary, trust mechanisms can address security threats and vulnerabilities by establishing and maintaining trust among nodes in the network. Trust can be defined as the degree of confidence a node has in the behaviour and intentions of another node [44]. By using trust mechanisms, nodes can assess the trustworthiness of their neighbours based on their past behaviour and interactions. This can help to detect and isolate malicious nodes,

prevent the propagation of false routing information, and maintain the integrity of routing paths.

3.2 Proposed Direct Trust Management Mechanisms for AODV Protocol

3.2.1 Protocol Overview

As discussed above, trust concepts are useful in addressing the security threats posed by malicious nodes and the lack of centralised control in ad-hoc networks. This research work proposes the Direct Trust AODV (DTAODV) protocol, which is an extension of the AODV routing protocol that incorporates a direct trust mechanism to improve the security and performance of the protocol. The DTAODV protocol uses direct trust to make routing decisions, whereby nodes observe their neighbours in a passive manner and assess their trustworthiness. As a result, a node relies entirely on its own experience to determine values of direct trust, which are subsequently employed when making routing decisions.

The design of the proposed DTAODV protocol is inspired by [41, 89, 63, 88]. The proposed protocol uses an appropriate combination of parameters for a node's behaviour observations. The proposed protocol considers the following parameters for measuring the trust value of a node participating in the network: packet forwarding rate, availability of battery power, rate of battery drain, and level of congestion around the node. Based on these factors, a trust value is assigned to each neighbouring node according to the direct trust mechanism. This selection process aims to ensure reliable and efficient communication in the MANET environment. The algorithm was implemented as an extension of the AODV protocol. Network Simulator NS-2.35 was used to evaluate the performance of the AODV and proposed DTAODV protocols. Afterwards, a newer version of the network simulator 3 (NS-3) was used to validate the results found using NS-2. The algorithm improves the reliability of a node by measuring, and each parameter's value will be in the range of 0 (worst) to 1 (best).

In DTAODV, each node maintains a trust table containing information about its neighbours' behaviours and actions. Based on this information, for each neighbour, a node calculates direct trust values representing the levels of trust the node has in its neighbours' behaviour and intentions. DTAODV uses direct trust values to make routing decisions. When a node needs to forward a packet to its destination, it first selects the neighbour with the highest value of direct trust value as the next hop for the packet. This ensures that packets are forwarded to trusted and reliable nodes, reducing the risk of malicious nodes causing problems for the overall performance of the protocol. DTAODV provides a

robust and secure routing protocol that can effectively address the security threats posed by malicious nodes in ad-hoc networks. By incorporating trust mechanisms, DTAODV can improve the performance and reliability of the AODV protocol.

DTAODV is designed to evaluate the trustworthiness of nodes within the network based on their past interactions and behaviour. Trust management mechanisms help maintain network reliability, security, and resilience against malicious or compromised nodes. Here's an overview of how direct trust management mechanisms work in MANETs:

1. Monitoring and Observation: Each node in the network monitors and observes the behaviour of its neighbouring nodes during communication. This can include factors such as the number of successfully forwarded packets, the response time, or the willingness to participate in routing processes.

2. Trust Computation: Based on the collected data, each node computes a trust value for its neighbours. Various mathematical models and algorithms can be used to calculate trust values, this research used Bayesian Inference. The trust value is usually represented as a number between 0 and 1, with 0 indicating complete distrust and 1 indicating complete trust.

3. Trust Threshold (δ): The network sets a trust threshold value which is denoted by δ, which determines the minimum trust value required for a node to be considered trustworthy. Nodes with trust values below this threshold may be excluded from certain routing or communication processes to prevent potential attacks or network disruptions.

4. Decision Making: When a node needs to select a route or a neighbor to forward a packet, it will consider the trust values of the candidate nodes. Only the nodes with trust values above the trust threshold are considered for routing or other network operations. This process helps ensure that only trustworthy nodes participate in network activities, thereby enhancing network security and reliability.

5. Trust Update: As nodes continue to interact and communicate, they may update their trust values based on the latest observations and experiences. This dynamic trust evaluation allows the network to adapt to changing conditions and maintain an up-to-date view of each node's trustworthiness.

By incorporating direct trust management mechanisms in MANETs, the network can effectively mitigate risks associated with malicious nodes, reduce the impact of attacks, and improve overall network performance and reliability.

3.2.2 Proposed Direct Trust Routing Protocol

In the proposed mechanisms, the central aspect is the trust management system that operates within each node in the network to maintain a trust value for all of the other nodes it has interacted with in the past. The establishment of a relationship of trust between nodes is based on the accumulation of positive and negative findings from the outcomes of the monitoring of successful and failed transactions. Following each measurement, the trust value held by the evaluating node is updated concerning the node being evaluated. Trust is represented as a continuous variable in the range of 0 to 1, where 0 indicates complete untrustworthiness, 1 represents complete trustworthiness, and 0.5 signifies uncertainty in understanding the behaviour of the node. In this context, a continuous variable is better equipped to represent the property of uncertainty concerning trustworthiness than a binary variable.

In the proposed protocol, a node's direct trust is represented by the level of dependability and trustworthiness it provides during the packet routing process. Each node monitors its neighbours for specific events related to the reliability of the nodes' packet forwarding capabilities. Every node documents positive (α) and negative (β) observations about its neighbouring nodes, and then calculates a value for the reliability and trustworthiness of each neighbouring node using Bayesian inference. This statistical approach for making inferences uses Bayes theorem to update the probability of a hypothesis being supported as more evidence or information becomes accessible [90].

Due to the nature of wireless communication as consisting of broadcasts, each node can monitor the behaviour of its neighbouring nodes. The parameters used for node observations are shown in Table 3.1. The table presents details about different observation parameters, the frequency of recording of each parameter, and events to update the values of α and β.

Table 3.1 presents a comprehensive breakdown of the parameters involved in assessing trust in the context of implementing trust into the AODV protocol. The table consists of five columns, including the serial number, observation parameter, frequency of recording the observation, positive observation (α), and negative observation (β).

1. Packet forwarding ability: This parameter evaluates a node's ability to forward data packets. Positive observations (α) are incremented for each data packet successfully forwarded, while negative observations (β) are incremented for each data packet dropped.

2. Node battery: This parameter assesses the battery power of a node at the beginning of a new data transmission session. A positive observation (α) is incremented if the node's battery power is greater than *MBT*(Minimum Battery Threshold), while a

negative observation (β) is incremented if the node's battery power is less than or equal to *MBT*. After many experimental evaluations 30% accepted as optimal value for *MBT*.

3. Node's participation in network routing activities: This parameter evaluates a node's involvement in routing activities, based on observed Route Reply (RREP) packets. A positive observation (α) is incremented for the node that initiates a control packet, while negative observations (β) are incremented for nodes that drop control packets or cause route errors.

4. Node's packet forwarding queue capacity: This parameter assesses the available capacity in a node's packet forwarding queue at the beginning of a new data transmission session. A positive observation (α) is incremented if more than *MEQ*(Minimum Empty Queue), while a negative observation (β) is incremented if the available queue capacity is less than or equal to *MEQ*. After many experimental evaluations 30% accepted as optimal value for *MEQ*.

Table 3.1 Trust Observation Parameters

Sr.	**Observation Parameter**	**Frequency of Recording the Observation**	**Positive Observation (α)**	**Negative Observation (β)**
1	Packet forwarding ability	For each observed data packet	α++ for each data packet forward	β++ for each data packet drop
2	Node Battery	At beginning of a new data transmission session	α++ if node's Battery Power > MBT	β++ if node's Battery Power <= MBT
3	Node's participation in network routing activities	For each observed RREP packet	α++ for the node which initiated control packet	β++ for the node which dropped a control packet. Also, β++ for a node caused a route error.
4	Node's packet forwarding queue capacity	At beginning of a new data transmission session	α++ if more than MEQ of queue capacity is empty	β++ if available queue capacity is less than equal to MEQ

The reliability of a node's packet routing service is an important factor in determining its ability to provide dependable service. A node's reliability (r) is the probability that a node offers reliable service in packet routing. Node unreliability (n) is the probability that the packet routing service it offers is unreliable. Meanwhile, node uncertainty (u) is the

probability of it not being possible to predict whether or not the node is reliable in packet routing. The above three values together are represented as *rnu* (reliability, unreliability, and uncertainty). Values of *rnu* can be calculated using direct observations as represented by *dt_rnu*). Each node performs the following actions to calculate these values:

- The values of α_i and β_i for each neighbour node *i* are consistently observed.
- The *rnu* metric (represented by dt_rnu_i) is computed using values of α_i and β_i. The *rnu* metric stands for node reliability, unreliability, and uncertainty and is computed using Bayesian Inference.

3.2.2.1 Calculation of a Node's RNU (dt_rnu_i) Using Direct Observations

In wireless networks, cooperation between nodes is crucial if packet transmission is to be reliable. The reliability of a node can be evaluated using a Beta distribution function with the two parameters α and β which represent the posterior distribution. Due to the use of only two observation parameters, the Beta distribution function is chosen in this study in the modelling of the behaviour of nodes. Here, *x*, and *y* are two neighbouring nodes in the network, and node *x* has made a total of *n* observations about node *y*. At this point, *T* represents the likelihood that node *y* will exhibit positive behaviour at time *n+1*. The posterior distribution of successful cooperation between two nodes *x* and *y* is then represented by a Beta distribution function with the density function given in Equation 3.1:

$$Beta(\theta|\alpha,\beta) = \frac{\tau(\alpha+\beta+2)}{\tau(\alpha+1)\tau(\beta+1)}\theta^{\alpha}(1-\theta)^{\beta} \tag{3.1}$$

In the above Equation, θ is the old value of the level of trust node *x* has in node *y*. The updated value of trust *T_new* is then calculated as follows:

$$T_{new} = E(Beta(\theta|\alpha,\beta)) = \frac{\alpha}{\alpha+\beta} \tag{3.2}$$

To calculate the direct node uncertainty *dt_u*, which is the likelihood that the node's reliability in packet transmission cannot be predicted, the expected value of the Beta distribution function can be determined using Equation 3.3. Equation 3.4 is used to calculate the direct node reliability value *dt_r*, which is the probability that a node offers reliable packet transmission service. Finally, Equation 3.5 is used to calculate the direct node unreliability expectation *dt_n* , which is the probability that a node does not offer a reliable packet transmission service.

Node uncertainty *dt_u* is calculated as follows:

$$dt\_u = \frac{12\alpha\beta}{(\alpha+\beta)^2(\alpha+\beta+1)} \tag{3.3}$$

In above equation numerator is multiplied by a constant factor 12, it makes $u = 1$ when value of α is 1 and value of β is also 1. The node reliability expectation dt_r is calculated as below:

$$dt\_r = \frac{\alpha}{\alpha+\beta}(1-u) \tag{3.4}$$

And the node unreliability expectation dt_n is calculated as:

$$dt\_n = \frac{\beta}{\alpha+\beta}(1-u) \tag{3.5}$$

The value of dt_rnu_i represents the reliability, unreliability, and uncertainty of node i as calculated using direct observations. It is important to note that these Equations are based on direct observations and hence are called direct *rnu* values. However, indirect trust observations can also be used to calculate *rnu* values. These indirect observations are obtained from the synthesis of observations received from neighbouring nodes, as discussed in the next chapter.

3.2.3 Integration of Direct Trust Mechanisms into the AODV Protocol

In the conventional AODV routing protocol, hop count is the primary metric used in determining routing decisions [26]. When a node intends to send a packet to another node, it searches for the shortest path available based on the minimum number of hops in order to facilitate efficient packet transfer [27]. This method is effective when all nodes within the network are reliable and carry out their routing functions as intended.

However, the presence of malicious nodes within the network can compromise its efficiency and security. To address this challenge, the AODV protocol has been modified in this study to integrate trust considerations into routing decisions. This enhanced version, called DTAODV (Direct Trust AODV), takes into account the trustworthiness of nodes when selecting routes.

In DTAODV, each node calculates a value of trustworthiness for every potential packet-forwarding node. This trust value, which is denoted as i, is computed using various parameters such as direct trust and/or indirect trust and the node's history of past interactions. In this way, the aim of the protocol is to choose more reliable routes, reducing the risk of the compromised network performance caused by malicious nodes.

Equation 3.6 represents the formula for the calculation of trust that takes these factors into account. As a result, DTAODV offers improved security and reliability compared to the standard AODV protocol. This makes it more resilient against potential attacks and ensures better overall network performance.

$$Trustworthiness\_value_i = \frac{\rho}{\text{No. of Hops to Destination}} + (1-\rho) * dt\_rnu_i \quad (3.6)$$

During the experimental evaluation process, a range of values of ρ was tested in order to assign different weights to two key factors: the proximity of a hop to the destination and the reliability of individual nodes. The goal of this approach was to determine the peak performance of the trust management mechanism and to identify the most effective performance scenario that results in optimal network efficiency and security. In order to thoroughly analyse the performance of the trust-based routing protocol, various performance metrics were considered, such as packet delivery ratio, throughput, end-to-end delay, and routing overhead. These metrics provided valuable insights into the protocol's effectiveness in different network conditions and situations.

Additionally, the experiments were conducted for various network scenarios, including different node densities and mobility patterns and the presence of malicious nodes using specific attack strategies. This comprehensive analysis facilitated the evaluation of the adaptability and robustness of the proposed trust management mechanisms under a wide array of circumstances.

The results obtained from these experiments, including the impact of different weight values assigned to hop proximity and node reliability, as well as the outcomes of the detailed analysis of various performance metrics and network scenarios, are presented in the forthcoming sections. This analysis can provide valuable information for the refinement of the trust management mechanism, ultimately allowing the performance and security of the routing protocol to be enhanced.

3.3 Research Methodology

Wireless network modelling encompasses various methods such as Simulations, Emulations, and the establishment of test beds, each offering distinct benefits and drawbacks. Among these approaches, simulations stand out as a widely employed method for exploring and evaluating Mobile Ad-hoc Networks (MANETs). This is particularly evident in the context of existing research where the majority of MANET studies are conducted through simulation techniques. In line with this prevalent practice, the current research work leverages two prominent open-source simulators, namely NS2 and NS3, to validate the proposed wireless network modelling.

The use of simulations holds several advantages. It provides a controlled and reproducible environment to test network scenarios, algorithms, and protocols. Simulators allow researchers to assess the performance and behaviour of complex network systems

without the cost and logistical challenges associated with physical test beds. They enable the study of a wide range of scenarios, including various network sizes, mobility patterns, and environmental conditions, while also facilitating the collection of detailed data for analysis.

Choosing an appropriate research technique is a crucial component of any study since it gives a systematic and structured approach to answering research questions and achieving research objectives. In this study, which evaluates the impact of trust management techniques on the performance, security, and efficiency of the AODV protocol in MANETs, a rigorous research approach has been developed and implemented.

This study employs a mix of theoretical and empirical methodologies, with a primary focus on comprehending the current literature, implementing and assessing trust management mechanisms, and analysing the outcomes to make relevant conclusions. This multi-step procedure ensures that the research is founded on prior knowledge and contributes new insights to the field.

It is anticipated that the incorporation of trust management mechanisms into the AODV protocol will enhance the dependability and security of routing processes in MANETs. Nonetheless, it is essential to comprehend the potential effects of these mechanisms on the performance of the AODV protocol and to examine the connections between the trust mechanisms and various network scenarios and characteristics.

This work seeks to give a detailed assessment of the influence of trust management techniques on the AODV protocol in MANETs by adopting a comprehensive research methodology that includes a literature review, implementation, simulation, data analysis, and evaluation.

The research methodology for this study can be described as follows:

1. Literature review: Conduct a comprehensive review of the existing literature on trust management mechanisms, MANETs, and AODV protocol to gain a deep understanding of the current state of knowledge in these fields.

2. Selection of trust mechanisms: Identify and select three different types of trust management mechanisms that have the potential to enhance the performance, security, and efficiency of the AODV protocol in MANETs.

3. Implementation: Incorporate the selected trust management techniques into the AODV protocol while developing a modified version of the protocol that includes these trust mechanisms.

4. Simulation and testing: Using network simulators NS-2 and NS-3 to create various network scenarios and configurations for evaluating the performance of AODV and the modified AODV protocol.

5. Data analysis: Analyse the results obtained from the simulations to assess the impact of the implemented trust management mechanisms on the performance, security, and efficiency of the AODV protocol, considering different network scenarios and parameters.

6. Evaluation and comparison: Evaluate the accuracy, efficiency, and adaptability of the trust management mechanisms in the modified AODV protocol and compare their performance to that of the original protocol under diverse scenarios and conditions.

The extreme cases that could serve to validate the modelling approach are scenarios where the outcomes are intuitively predictable, and the modelling should corroborate this intuition. For instance, a case where there are no malicious nodes present should intuitively lead to improved network performance, and the modelling should indeed confirm this by showcasing higher packet delivery ratios, enhanced throughput, lower end-to-end delays, and reduced routing overhead. On the contrary, a scenario with a high density of malicious nodes should logically result in deteriorated network performance, and the modelling should align with this expectation by demonstrating decreased packet delivery ratios, lowered throughput, increased end-to-end delays, and escalated routing overhead.

3.3.1 Network simulator NS-2

The Network Simulator version 2 (NS-2) is an open-source platform that supports the design, implementation, and testing of various network protocols and algorithms [91]. It is a widely-used simulator which is particularly popular for studying MANETs as it provides a controlled environment for evaluating routing protocols and trust management mechanisms. Developed in C++ and Tcl (Tool Command Language), NS-2 offers a modular architecture and an event-driven simulation engine, ensuring accurate and realistic results [92]. NS-2 features include the ability to simulate different network types, an extensive library of network protocols, extensible for custom protocols, and a rich set of visualisation and analysis tools.

Furthermore, the Scenarios Generator 2 (NSG-2) tool was employed, which is a network simulator based on the Java programming platform for NS-2. NSG-2 have the capability to generate both wired and wireless TCL scripts for NS-2 automatically [91]. NSG-2 tool is used to create a TCL script that combined a range of parameters, which will be elaborated on in the simulation setup section, specifically tailored to the experimental simulation at hand.

3.3.2 Network simulator NS-3

The discrete-event network simulator NS-3 was created primarily for the modelling and research of internet networks. It is a very popular and extremely advanced network simulator. In addition, it is particularly popular for studying MANETs due because of its ability to provide a controlled and realistic environment for evaluating routing protocols and trust management mechanisms. In order to replicate the behaviour of a variety of protocols, including TCP/IP, routing formulas, and wireless communication technologies, it offers a complete library of programmable network components [93]. Researchers may simulate the behaviour of these protocols using the NS-3 simulation engine, which enables the study of these protocols' performance under various scenarios and the creation of new and enhanced algorithms.

In comparison, the Network Simulator version 2 (NS-2) is another widely-used open-source network simulator that also allows for the study of MANETs. Though, it has some differences in terms of features, architecture, and ease of use. Developed primarily in C++ with Python scripting capabilities, NS-3 offers a modular architecture and a discrete-event simulation engine, ensuring accurate and high-performance results [94]. On the other hand, NS-2 is developed in C++ and Tcl (Tool Command Language), which can make it more challenging to work with for some users.

NS-3 features include the ability to simulate different network types, an extensive library of network protocols, an extensible for custom protocols, and a rich set of visualisation and analysis tools. In comparison, NS-2 also supports a wide range of network types and provides a comprehensive protocol library which may not have as extensive a collection of visualisation and analysis tools as NS-3. The NS-3 simulator was mostly used for the analysis and evaluation throughout the thesis.

In summary, both NS-3 and NS-2 are powerful network simulators for studying MANETs and their trust management mechanisms. However, NS-3 offers a more modern architecture, Python scripting capabilities, and a more extensive set of visualisation and analysis tools, making it a popular choice among researchers for evaluating the performance, efficiency, and security of trust management mechanisms in MANETs.

3.3.3 Confidence Interval

A confidence interval, in statistics, is a range that a population parameter is expected to fall within given a specific degree of confidence [95]. It is used to estimate the true value of an unknown population parameter, such as a mean or proportion, based on a sample taken from that population. Confidence intervals provide a measure of the uncertainty associated with an estimate, as well as an indication of the precision and reliability of the estimate. A confidence interval is usually defined as a range with an associated confidence level.

The confidence level usually denoted as a percentage (e.g., 95% or 99%). It indicates the degree of certainty that the true population parameter lies within the specified interval [95]. A higher confidence level represents a higher degree of certainty, but it also results in a wider interval, thus potentially reducing the precision of the estimate.

In this thesis, a confidence interval of 95% was used for the simulation results to improve the reliability of the results. In a MANET, a confidence interval of 95% provides a range within which the true population average lies with a 95% probability.

3.3.4 Performance Scenarios

Performance scenarios in MANETs play a vital role in understanding the effectiveness of various protocols, algorithms, and security mechanisms in real-world situations. These scenarios are crucial for testing the adaptability of protocols to dynamic network conditions, ensuring network stability and efficient communication, and validating the effectiveness of proposed solutions. In the thesis, the employed different scenarios, including variations in node movement and mobility speed, variations in the number of nodes, and variations in the number of malicious nodes.

3.3.4.1 Variation in Node Movement Speed

Node mobility and movement speed are important factors that can significantly influence the performance of MANETs. Moreover, in MANETs, nodes are free to move arbitrarily, causing the network topology to change dynamically. The movement speed of nodes and their mobility pattern play a critical role in determining the efficiency and effectiveness of routing protocols and other network operations.

In the context of evaluating the performance of trust management mechanisms in MANETs, the node mobility and movement speed scenario helps in understanding how well these mechanisms adapt to dynamic network conditions. By analysing the performance metrics, it is possible to identify the robustness and effectiveness of the trust management mechanisms under varying node mobility speeds. It is essential to determine the applicability of these mechanisms in real-world situations where node mobility and movement speed may vary significantly.

3.3.4.2 Variation in Node Density

Variation in the number of nodes is a critical scenario to consider when evaluating the performance of MANETs. As the number of nodes in the network increases or decreases, it can directly impact factors such as network density, connectivity, routing overhead, and resource consumption. Studying the performance of MANETs under varying node

densities is essential to understand the scalability of routing protocols and trust management mechanisms. By analysing the impact of different node numbers on network performance, it is possible to identify potential bottlenecks and limitations. Also, it can be possible to subsequently develop more scalable and efficient solutions that cater to the diverse needs of real-world MANET deployments.

3.3.4.3 Variation in Malicious Nodes

In the performance evaluation of MANETs, the variation in malicious nodes scenario is an important aspect to consider. This scenario involves analysing the impact of different numbers of malicious nodes on the performance of the network. Malicious nodes intentionally disrupt the network's normal functioning by launching attacks, dropping packets, or propagating false routing information. In this thesis, the black hole attack was employed to investigate the performance of MANETs when faced with malicious nodes.

The primary purpose of studying the variation in malicious nodes scenario is to assess the resilience and robustness of the network and its protocols in the presence of adversaries. By simulating different levels of malicious node presence, researchers can better understand the vulnerabilities of the network and identify potential countermeasures to improve security.

3.3.5 Performance Metrics

The importance of performance metrics in MANETs lies in their ability to assess the effectiveness, efficiency, and overall performance of various routing protocols and network configurations. MANETs are characterised by dynamic network typologies, frequent link failures, and limited resources. Therefore, having suitable performance metrics is crucial for understanding the behaviour and performance of these networks under various conditions.

3.3.5.1 Packet Delivery Ratio (PDR)

Packet Delivery Ratio (PDR) is an essential performance metric in MANETs. It represents the ratio of successfully delivered data packets to the total number of data packets sent within the network. PDR is expressed as a percentage and is used to evaluate the effectiveness and reliability of a routing protocol or network configuration.

It is calculated as the ratio of the number of data packets successfully delivered to their intended destination nodes to the total number of data packets generated for those destinations. PDR serves as a measure of the packet loss rate, which impacts the overall throughput of the network. The higher the PDR, the better the performance of the routing

protocol. It represents the proportion of data successfully delivered to the destination in comparison to the data sent out by the source. The determination of PDR is crucial in evaluating the effectiveness of data transmission in a network. PDR is determined using the Equation:

$$PDR = \frac{Received\ Packets}{Sent\ Packets} * 100 \tag{3.7}$$

3.3.5.2 Throughput

Throughput is an indicator of the efficiency and capacity of a routing protocol as it shows the volume of data that can be transmitted within a given time frame. From Equations 3.8 and 3.9, throughput is defined as the ratio of the total data successfully received by a receiver from a sender over a certain period of time which is usually expressed in bytes or bits per second (bps). There are several factors that can impact the throughput in a network, including frequent changes in network topology, unreliable communication between nodes, limited bandwidth availability, and limited energy. High throughput is desirable in all networks because it represents a high rate of effective data transfer. The mathematical representation of throughput can be expressed as the number of packets received by the destination within a given time interval. It serves as a means of evaluating the performance of a routing protocol.

$$Transmission\ Time(bps) = \frac{Packet\ Size}{Bandwidth(sec)} \tag{3.8}$$

$$Throughput = \frac{Packet\ Size}{Transmission\ Time(bps)} \tag{3.9}$$

3.3.5.3 Routing Overhead

Routing overhead refers to the additional resources required by the routing protocol to perform its functions. These responsibilities include maintaining an up-to-date knowledge of the network's topology, creating and maintaining routes between nodes, and carrying out any other essential routing-related operations. In a MANET, the routing overhead can consume critical network resources such as bandwidth, processing power, memory consumption, and energy.

The influence of routing overhead on the performance of a MANET must be carefully considered. A high amount of routing overhead can lower network capacity and increase

energy usage, especially in areas with limited resources. In light of this, it is crucial to adopt a routing protocol that strikes a balance between routing overhead and routing efficiency to ensure optimal performance for a particular MANET application.

Routing overhead is the ratio or fraction of the total number of control messages transmitted in the network to the total number of data packets transmitted in the network. The Equation can be represented as:

$$Routing\ Overhead = \frac{Number\ of\ Control\ Messages}{Number\ of\ Data\ Packets} \tag{3.10}$$

3.3.5.4 End-to-End Delay (E2E Delay)

End-to-End Delay (E2E Delay) is the time it takes for a data packet to transfer from a source node to a destination node. This metric is essential for real-time applications that demand minimal delay and latency. Several factors impact E2E Delay, including network congestion, routing protocol, node mobility, and transmission error rate. In general, a lower E2E Delay indicates improved performance and more network efficiency, whereas a greater E2E Delay may indicate network congestion, node mobility, or other variables influencing network performance.

The Equation for End-to-End Delay (E2E Delay) is the sum of the processing delay, transmission delay, queuing delay, and propagation delay. The Equation can be represented as:

$$E2E\ Delay = Processing\ \ Delay\ \ + Transmission\ \ Delay + Queuing\ \ Delay + Propagation\ \ Delay \tag{3.11}$$

Where:

- Processing Delay is the time taken by the nodes to process and forward the data packets.
- Transmission Delay is the time taken for a data packet to be transmitted from one node to another.
- Queuing Delay is the time spent by the data packets in a queue waiting for transmission.
- Propagation Delay is the time taken for a data packet to travel from one node to another through the network.

3.4 Performance Evaluation and Analysis using *NS-2*

The objective of this section is to assess the performance of the proposed direct trust mechanism incorporated into the AODV routing protocol by examining its security and efficiency. To achieve this, a comparison is made between AODV and DTAODV under various node scenarios and mobility speeds. The performance evaluation is based on several metrics, such as packet delivery ratio, throughput, end-to-end delay, and routing overheads. The resulting insights will shed light on the benefits and constraints of the implementation of direct trust management within the AODV routing protocol for mobile ad-hoc networks.

Different weights were assigned to the number of hops to the destination and node reliability in order to gain a deeper understanding of the impact of direct trust. In this analysis, we got better results with value of ρ as 30%; it means a weight of 70% is allocated to node reliability and 30% to hop counts when calculating the trustworthiness value for the DTAODV protocol. This approach helps to illustrate the influence of direct trust on the protocol's performance.

To carry out the simulations, Network Simulator version 2 (NS-2.35) was used. The findings obtained from this comparative study will contribute to a better understanding of the advantages and limitations of the incorporation of direct trust assessments into the AODV routing protocol, ultimately informing further enhancements in security and efficiency for mobile ad-hoc networks.

3.4.1 Performance with Variations in Node Movement Speed

This evaluation involves an assessment of the behaviour of the AODV and DTAODV protocols under various node mobility speeds while keeping other simulation parameters constant, as specified in Table 3.2. The values of simulation parameters used in the table are inspired from [96] and [97]. The simulations were run ten times for each mobility speed, and the mean value was calculated. Additionally, a 95% confidence interval was calculated to further increase confidence in the results. The simulations were performed to study the impact of node mobility on the network and to evaluate the performance of the protocols in different mobility scenarios ranging from a minimum speed of 10 m/s to a maximum speed of 50 m/s. The evaluation metrics include packet delivery ratio, throughput, routing overheads, and end-to-end delay. Network Simulator version 2.35 (NS-2.35) software was used as the simulation tool.

Table 3.2 Simulation Parameters

Routing protocols	AODV, DTAODV
Packet Size	512 *Bytes*
Simulation Time	360 *Seconds*
Simulation Area	1000 * 1000 m^2
Number of Nodes	20
Node Movement Speed	10,20,30,40,50 *m/s*
Node Movement	Random Way Point
MAC Protocol	IEEE 802.11b
Transmission Range	250 *metres*
Number of Simulation Runs	10
Confidence Interval	95%
Traffic Type	UDP

3.4.1.1 Packet Delivery Ratio and Throughput Versus Node Mobility Speed

Figures 3.3 and 3.4 illustrate the relationship between node mobility speed, packet delivery ratio (PDR), and throughput. Figure 3.3 shows that PDR decreases for both the AODV and DTAODV protocols as mobility speed increases. However, the DTAODV protocol consistently outperforms AODV in terms of PDR. The PDR for AODV starts at 82.71% at a mobility speed of 10 m/s and decreases to 60.93% at a mobility speed of 50 m/s. In contrast, the PDR for DTAODV starts at 91.77% at a mobility speed of 10 m/s and decreases to 72.92% at a mobility speed of 50 m/s. The decrease in PDR for both protocols can be attributed to an increase in link breakages caused by the rapid movement of nodes. Due to these link breakages route maintenance activity need to be initiated which has negative impact on packet delivery ratio and throughput. On the other hand, Figure 3.4 shows that DTAODV has a higher throughput value than the default AODV. In both AODV and DTAODV, throughput decreases as mobility speed increases.

Moreover, the decreases in PDR and throughput are likely to be also due to the increased rate of link breakages that occur as nodes move more quickly. As a result, the routing protocol must spend more time in establishing new routes and re-transmitting lost packets, reducing the network's overall efficiency and resulting in a lower PDR and throughput. Thus we can see that DTAODV performs better than AODV, where the latter depends only on the shortest hop to the destination. At the same time, DTAODV uses the direct trust mechanisms with a 30% weighting for hop count and 70% for the reliability of the route. The inclusion of the confidence interval further reinforces the differences in PDR and throughput between AODV and DTAODV.

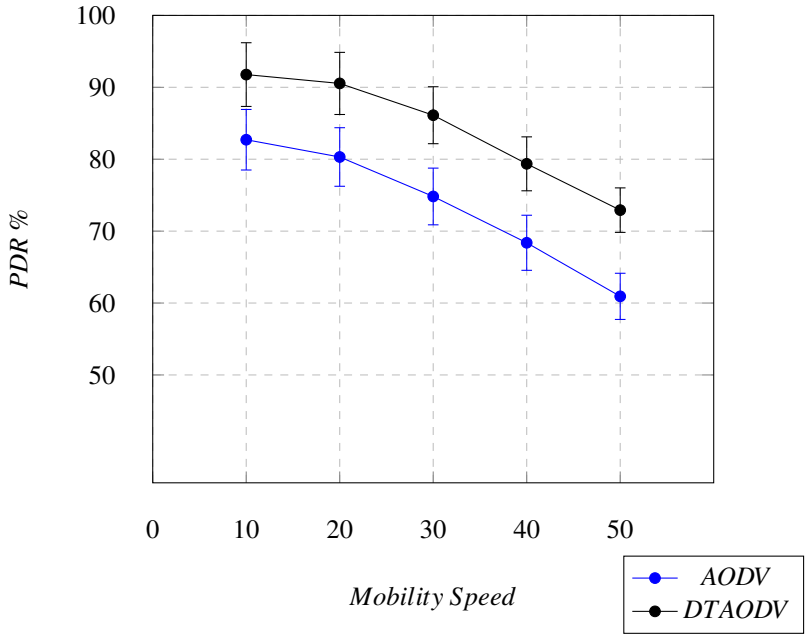

Figure 3.3 PDR vs. Mobility Speed with 95% Confidence Intervals

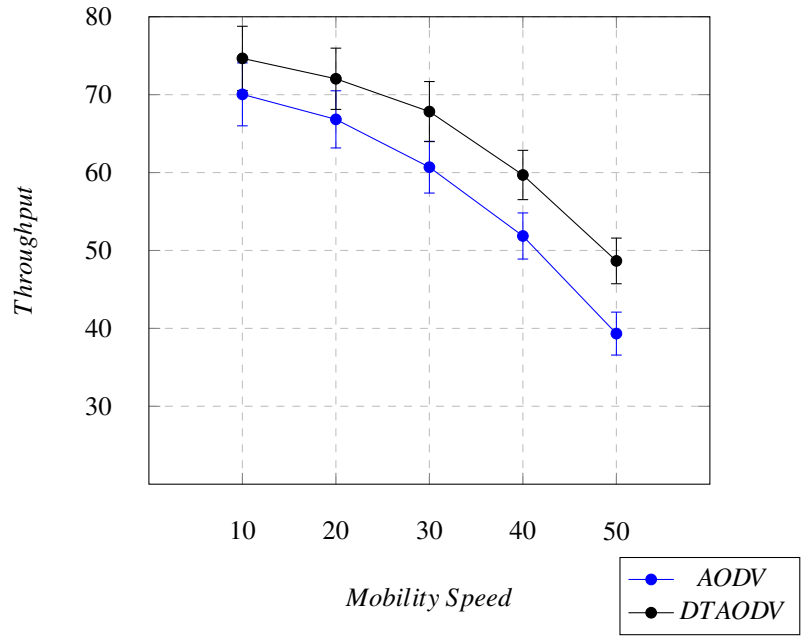

Figure 3.4 Throughput vs. Mobility Speed with 95% Confidence Intervals

3.4.1.2 End-to-End Delay and Routing Overheads Versus Node Mobility Speed

Figures 3.5 and 3.6 show performance in terms of end-to-end delay and routing overheads under different mobility speeds. We can observe that, as mobility speed increases, the delay and routing overheads increase for both AODV and DTAODV. The AODV performs

better since it only uses hop count as a criterion to send a packet from a source node to a destination node. On the other hand, DTAODV uses a weighting of 30% for hop count and 70% for the trustworthiness and reliability of a route, which ensures packet delivery but with a trade-off with delay and routing overheads.

In addition, there are several factors that can contribute to increased delay and routing overheads when node mobility speed increases. Firstly, an increased frequency of link breakages can result in the routing protocol having to more regularly re-establish new routes, leading to increased delays and routing overheads. Also, nodes may need to update their routing tables more often, resulting in a further increase in delays and routing overheads. These factors can reduce the efficiency and performance of the network.

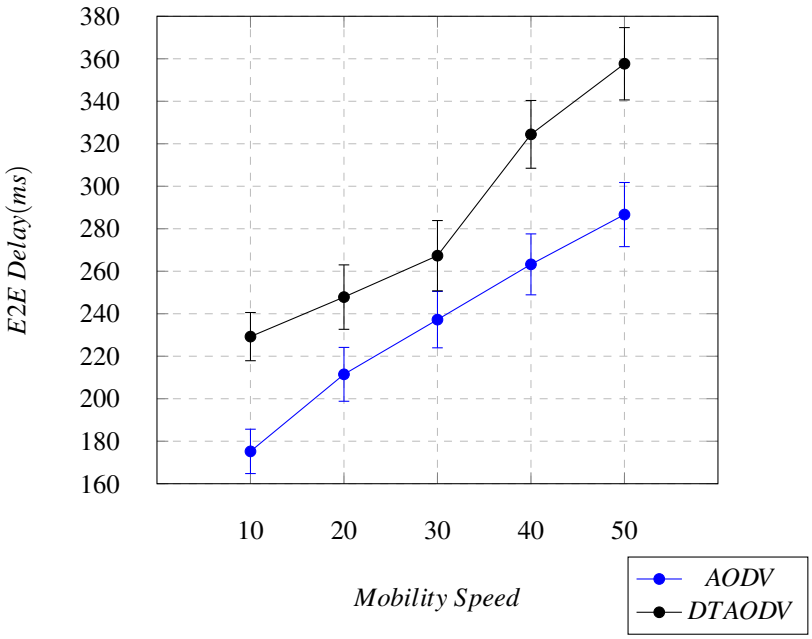

Figure 3.5 E2E Delay vs. Mobility Speed with 95% Confidence Intervals

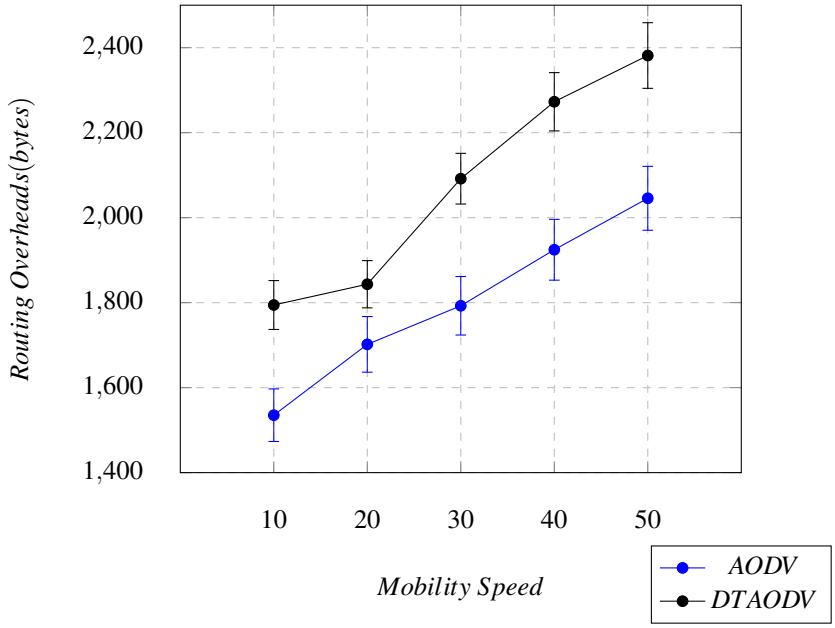

Figure 3.6 Routing Overheads vs. Mobility Speed with 95% Confidence Intervals

3.4.2 Performance With Variations in Node Density

In order to examine the performance of the AODV and DTAODV protocols, simulations were conducted with varying numbers of nodes while keeping the other simulation parameters fixed, as specified in Table 3.3. The objective of the simulations was to evaluate the behaviour of both protocols under different network conditions. To obtain reliable results, the simulations were run ten times for each number of nodes and the mean value was taken. To ensure the validity of the results, a 95% confidence interval was also calculated. The performance of the protocols was evaluated using key metrics, which are packet delivery ratio, throughput, routing overhead and end-to-end delay.

Table 3.3 Simulation Parameters

Routing protocols	***AODV, DTAODV***
Packet Size	512 *Bytes*
Simulation Time	360 *Seconds*
Simulation Area	1000 * 1000 m^2
Number of Nodes	20,40,60,80,100
Node Movement Speed	5 *m/s*
Node Movement	Random Way Point
MAC Protocol	IEEE 802.11b
Transmission Range	250 *Meter*
Number of Simulation Runs	10
Confidence Interval	95%
Traffic Type	UDP

3.4.2.1 Packet Delivery Ratio and Throughput Versus Number of Nodes

The results of the simulations of PDR and throughput when varying the number of nodes in AODV and DTAODV protocols are shown in Figures 3.7 and 3.8. It is evident that DTAODV exhibits better performance than AODV in terms of PDR and throughput as the number of nodes increases. However, as the number of nodes increases, the likelihood of interference among nodes also increases. This can result in reduced throughput due to dropped packets and re-transmissions. Nevertheless, increasing the number of nodes can also lead to a more efficient utilisation of resources, such as an increase in the number of available transmission paths, thereby resulting in improved PDR because more data can be transmitted concurrently. The use of direct trust has improved the AODV protocol, as we can see from the results for DTAODV, since it reduces the likelihood of congestion and dropped packets and improves the overall PDR and throughput.

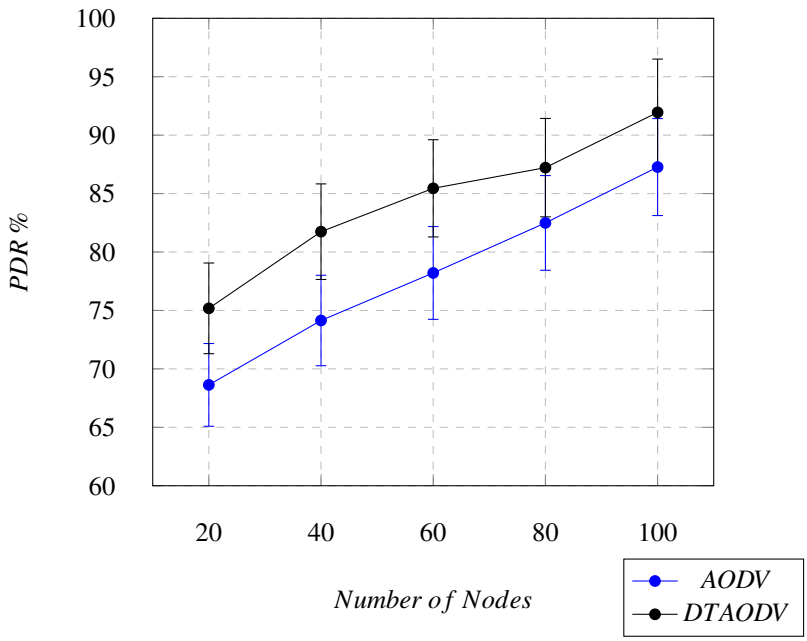

Figure 3.7 PDR vs. Number of Nodes with 95% Confidence Intervals

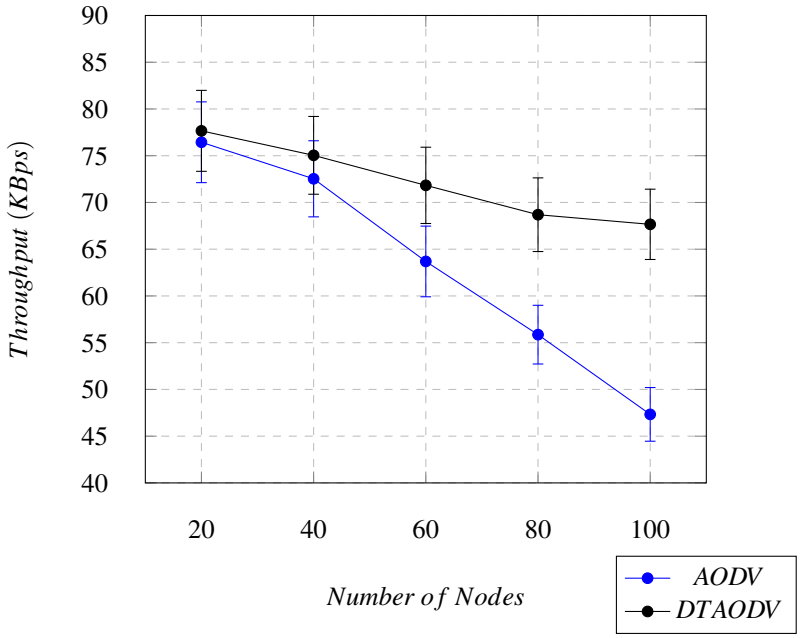

Figure 3.8 Throughput vs. Number of Nodes with 95% Confidence Intervals

3.4.2.2 End-to-End Delay and Routing Overheads Versus Number of Nodes

The results presented in Figures 3.9 and 3.10 demonstrate that as the number of nodes in the network increases, the end-to-end delay and routing overheads also increase. This is primarily due to the increase in network congestion as the nodes compete for available bandwidth and resources. As the number of nodes grows, the number of routing messages exchanged also increases, leading to the rise in routing overheads. This can result in reduced network capacity since more bandwidth is consumed by the transmission of routing messages, and increased processing time as nodes devote more resources to the processing of routing messages. However, it can be observed that the AODV protocol performs better than DTAODV, and this is because the latter uses a 70% weighting for the measure of direct trust and 30% for the shortest hop count, which leads to additional processing time and overheads for nodes in the calculation and exchange of trust information, thereby increasing end-to-end delays and routing overheads. On the other hand, the AODV protocol uses the shortest path to send a packet from a source node to a destination node, which entails the use of fewer network resources.

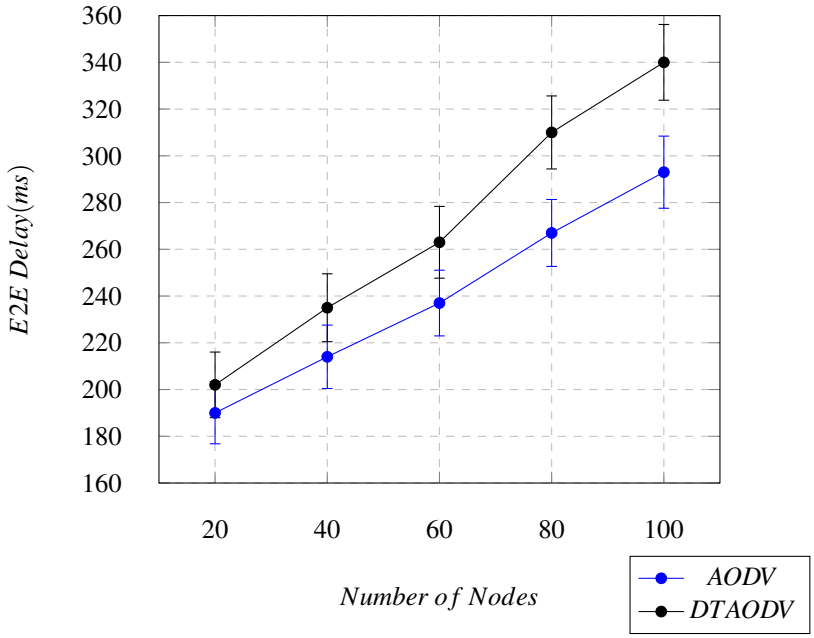

Figure 3.9 E2E Delay vs. Number of Nodes with 95% Confidence Intervals

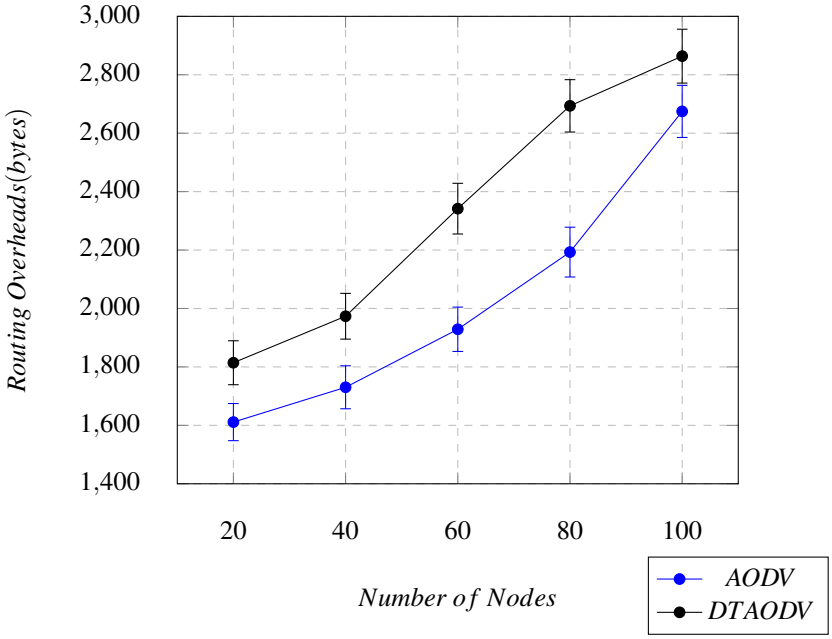

Figure 3.10 Routing Overheads vs. Number of Nodes with 95% Confidence Intervals

3.5 Performance Evaluation and Analysis using *NS-3*

In evaluating the direct trust mechanism integrated into AODV, the more advanced network simulation software NS-3 was used to validate the earlier simulation results obtained

using NS-2, as reported in Section 3.4. The NS-3 software offers more accurate and realistic simulations due to its incorporation of information about the latest advances in networking and communication technologies [94]. Therefore, the AODV and direct trust AODV (DTAODV) were compared in terms of different scenarios of mobility speed and the number of nodes. The performance evaluation is based on the key metrics of packet delivery ratio, throughput, end-to-end delay, and routing overheads.

In addition to the evaluation of the impact of direct trust, this analysis aimed to validate the results obtained using NS-2. To do this, the newer version of the network simulation software, NS-3, was applied to the same direct trust mechanism. The weights assigned to node reliability and hop counts were also varied when calculating values of trustworthiness in the DTAODV protocol. Two different weight combinations: 70% node reliability and 30% hop counts; and 30% node reliability and 70% hop counts. These variations allowed deeper insights to be gained into the influence of direct trust in the performance of the DTAODV protocol. Additionally, a comparison was conducted of the outcomes obtained through the use of NS-2 and NS-3 when node reliability was given a weighting of 70% and hop count of 30%. The examination revealed that the overall performance according to the NS-3 analysis significantly exceeded that of NS-2, leading to the use of NS-3 only for all subsequent simulations.

3.5.1 Higher Weight Assigned to Node Reliability

3.5.1.1 Performance With Variation in Node Movement Speed

The evaluation of the Ad-hoc On-demand Distance Vector (AODV) and the Direct Trust AODV (DTAODV) protocols involved a thorough assessment of their behaviour under various node mobility speeds while keeping other simulation parameters constant, as outlined in Table 3.4. To ensure the validity of the results, the simulations were repeated ten times for each mobility speed, and the mean value was calculated. Further, to increase the confidence in the results, a 95% confidence interval was calculated. These simulations aimed to examine the impact of node mobility on the network and to assess the performance of the protocols in mobility scenarios which ranged from a minimum speed of 10 m/s to a maximum speed of 50 m/s. The performance metrics used in evaluating the protocols included packet delivery ratio, throughput, routing overheads, and end-to-end delay. Furthermore, the results using the NS-2 and NS-3 simulation tools as mobility speed increases were compared. The impact of node reliability and hop count parameters as the number of nodes increases was also investigated, with weightings for node reliability and hop count of 70% and 30%, respectively.

Table 3.4 Simulation Parameters

Routing protocols	AODV, DTAODV
Packet Size	512 *Bytes*
Simulation Time	360 *Seconds*
Simulation Area	1000 * 1000 m^2
Number of Nodes	20
Node Movement Speed	10,20,30,40,50 *m/s*
Node Movement	Random Way Point
MAC Protocol	IEEE 802.11b
Transmission Range	250 *Meter*
Number of Simulation Runs	10
Confidence Interval	95%
Traffic Type	UDP

3.5.1.2 Packet Delivery Ratio and Throughput Versus Node Mobility Speed

Figures 3.11 and 3.12 demonstrate the correlation between node mobility speed and packet delivery ratio (PDR), and throughput. As the mobility speed increases, it is observed that the PDRs for both AODV and DTAODV protocols decrease in both the NS-2 and NS-3 simulations. However, the PDR and throughput results of simulations carried out in NS-3 are more accurate and stable due to the incorporation of information from the latest advances in networking and communication technologies in the NS-3 software [94]. A decrease in throughput is observed as mobility speed increases, which is primarily due to an increase in the rate of link breakages as nodes move more quickly. This leads to a decrease in the network's overall efficiency, causing the routing protocol to spend more time on the establishment of new routes and retransmission of lost packets, resulting in lower throughput. However, it can be seen that the performance of DTAODV in the NS-3 simulator is robust, and the drop in the throughput is minimal compared to the other protocol.

It can also be observed that DTAODV outperforms AODV, where the latter relies only on the shortest hop to the destination. DTAODV integrates direct trust mechanisms, giving a weighting of 70% to reliable routes and 30% to hop counts. Using the direct trust mechanisms, the DTAODV protocol has a positive impact on the network. The confidence intervals further accentuate the differences in PDR and throughput performance between AODV and DTAODV.

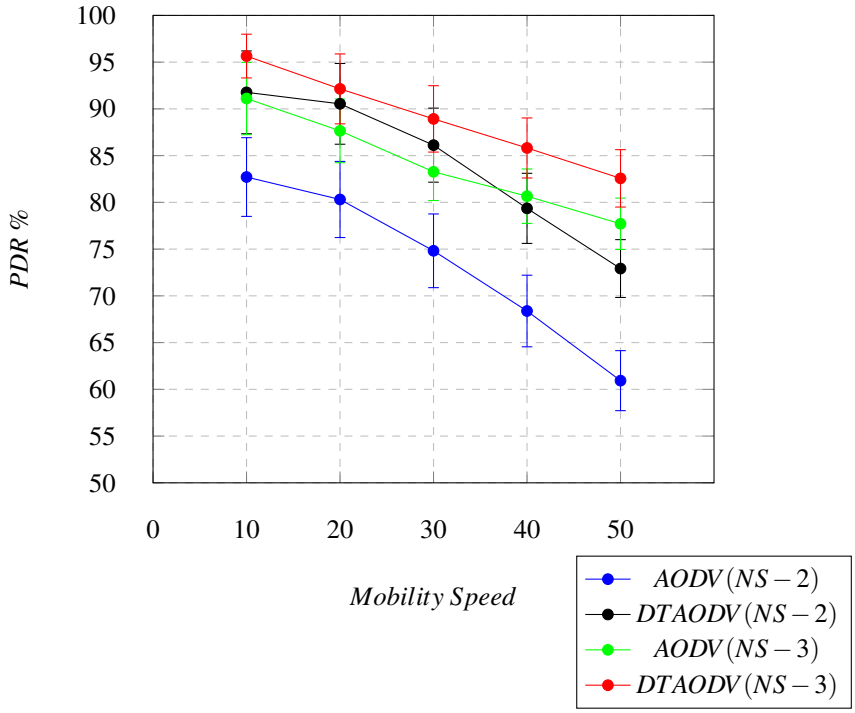

Figure 3.11 PDR vs. Mobility Speed with 95% Confidence Intervals for NS2 and NS3

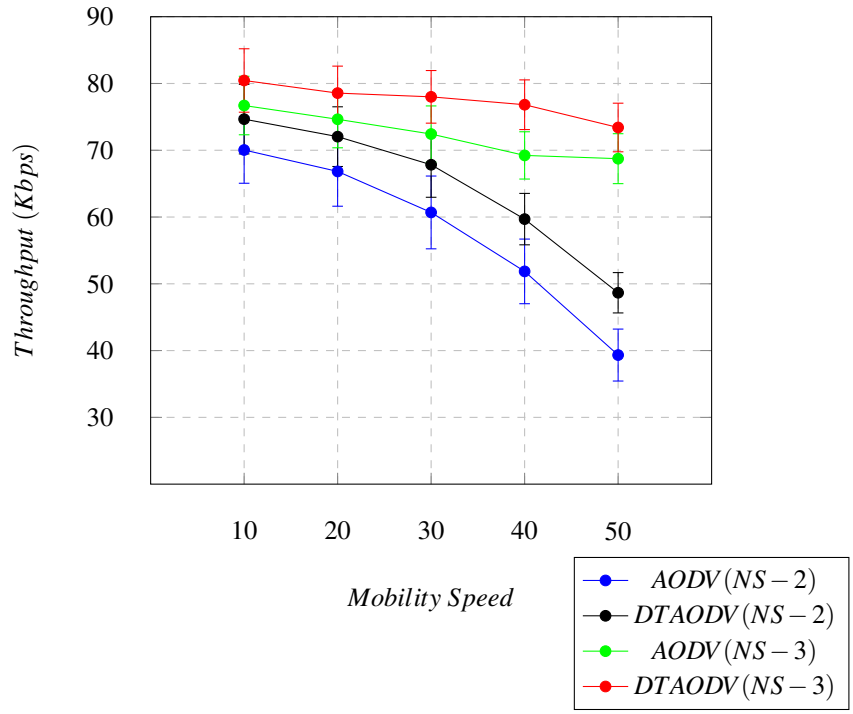

Figure 3.12 Throughput vs. Mobility Speed with 95% Confidence Intervals for NS2 and NS3

3.5.1.3 End-to-End Delay and Routing Overheads Versus Node Mobility Speed

The performance of end-to-end delay and routing overheads for both AODV and DTAODV protocols under different mobility speeds are demonstrated in Figures 3.13 and 3.14. As mobility speed increases, the end-to-end delay and routing overheads increase for both protocols, as observed in the results of both NS-2 and NS-3 simulations. AODV performs better due to its simpler methodology of routing packets based solely on hop count. On the other hand, DTAODV uses a composite metric taking into account both hop count and the trustworthiness of the route in order to ensure reliable packet delivery, but at the cost of increased delays and routing overheads.

These increased delay and routing overheads at higher mobility speeds can be attributed to several factors, including the need for more frequent updates to routing tables, which results in higher overheads and delay. However, the use of the NS-3 simulator offers better and more stable performance than NS-2, with the AODV and DTAODV protocols both exhibiting higher stability, reliability, and accuracy in their performance.

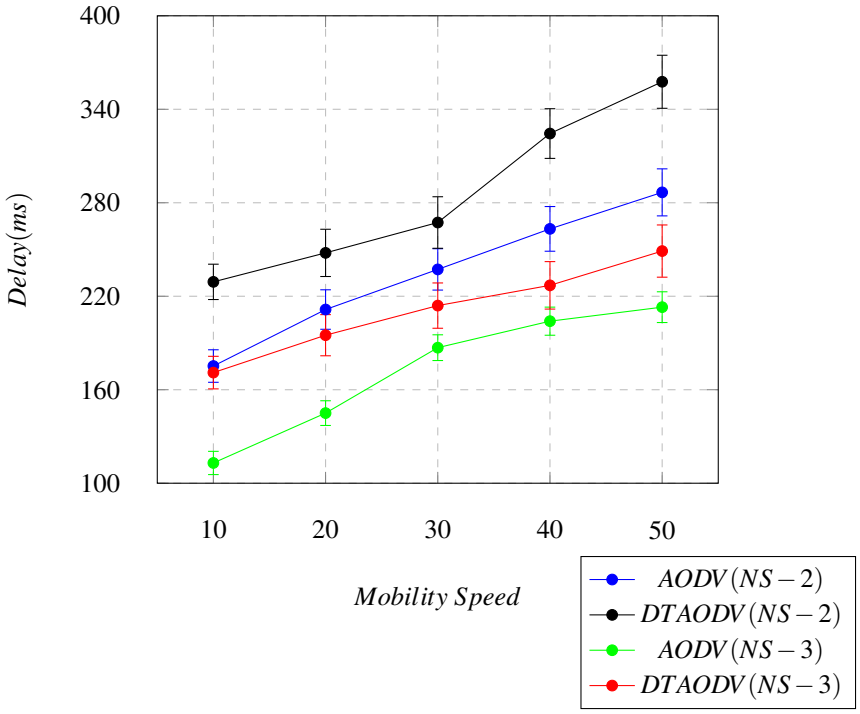

Figure 3.13 End-to-End Delay vs. Mobility Speed with 95% Confidence Intervals for NS2 and NS3

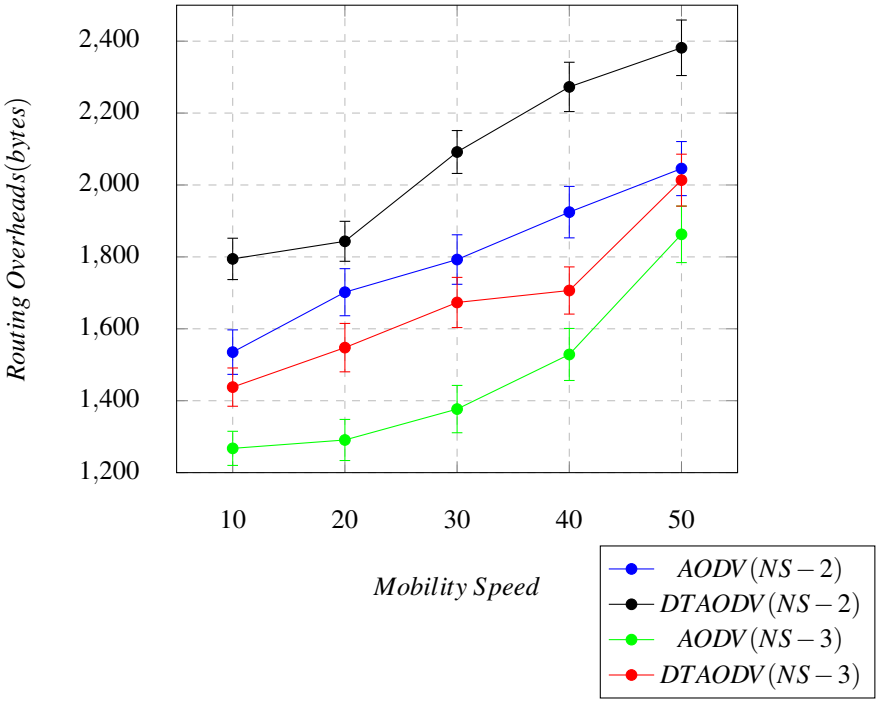

Figure 3.14 Routing Overheads vs. Mobility Speed with 95% Confidence Intervals for NS2 and NS3

3.5.1.4 Performance With Variation in Node Density

Simulations were performed to evaluate the performance of the AODV and DTAODV protocols with changes in the number of nodes in the network while maintaining constant simulation conditions as specified in Table 3.5. The aim of the simulations was to investigate the behaviour of both protocols in various network scenarios. To ensure the validity of the results, the simulations were repeated ten times for each different number of nodes and the average value was calculated. Additionally, a 95% confidence interval was calculated to increase confidence in the results. The performance of the protocols was assessed using important metrics such as packet delivery ratio, throughput, routing overheads, and end-to-end delay.

Table 3.5 Simulation Parameters

Routing protocols	***AODV, DTAODV***
Packet Size	512 *Bytes*
Simulation Time	360 *Seconds*
Simulation Area	1000 * 1000 m^2
Number of Nodes	20,40,60,80,100
Node Movement Speed	5 *m/s*
Node Movement	Random Way Point
MAC Protocol	IEEE 802.11b
Transmission Range	250 *Meter*
Number of Simulation Runs	10
Confidence Interval	95%
Traffic Type	UDP

3.5.1.5 Packet Delivery Ratio and Throughput Versus Number of Nodes

The impact on the AODV and DTAODV protocols of varying the number of nodes on the packet delivery ratio (PDR) and throughput is illustrated in Figures 3.15 and 3.16. The results indicate that DTAODV performs better than AODV in terms of PDR and throughput as the number of nodes increases. However, an increase in the number of nodes also increases the risk of interference among nodes, which can result in reduced throughput due to dropped packets and retransmissions. On the other hand, a larger number of nodes can lead to more efficient resource utilisation, such as by increasing the number of available transmission paths, resulting in improved PDR since more data can be transmitted concurrently. The use of direct trust in AODV has improved its performance, as seen with DTAODV, by reducing the chances of congestion and dropped packets and improving overall PDR and throughput. As shown in the figures, the results for NS-2 and NS-3 when the number of nodes increases are also compared.

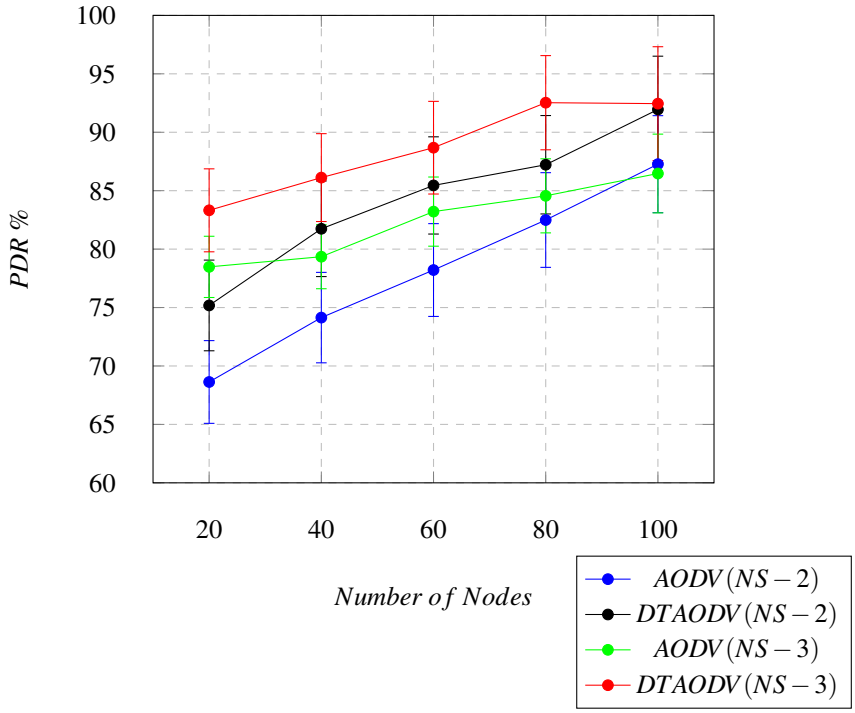

Figure 3.15 PDR vs. Number of Nodes with 95% Confidence Intervals for NS2 and NS3

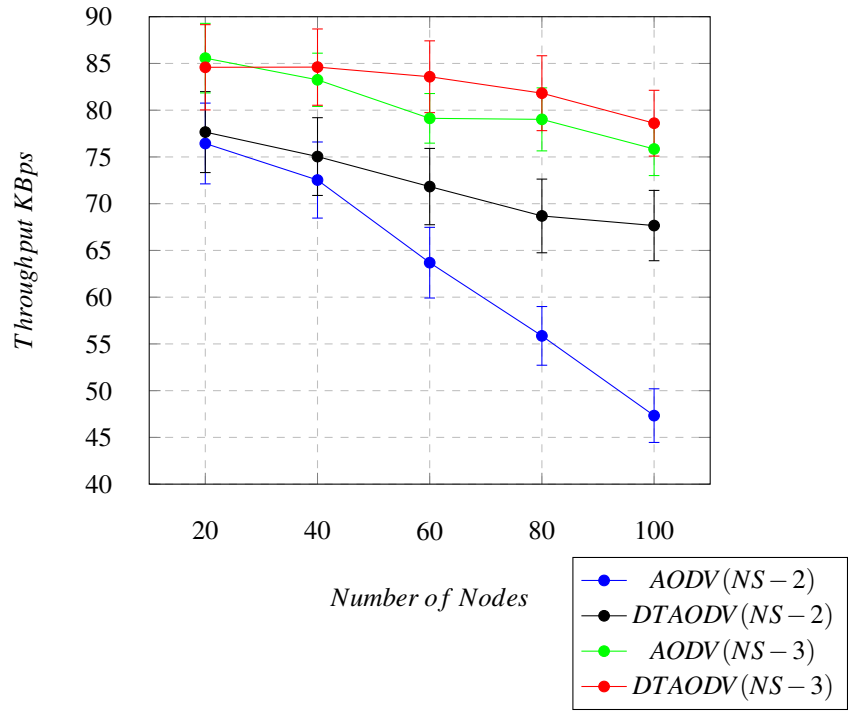

Figure 3.16 Throughput vs. Number of Nodes with 95% Confidence Intervals for NS2 and NS3

3.5.1.6 End-to-End Delay and Routing Overheads Versus Number of Nodes

The results displayed in Figures 3.17 and 3.18 highlight the correlation between the number of nodes in the network and the end-to-end delay and routing overheads. As the number of nodes increases, the network becomes congested because nodes compete for limited bandwidth and resources. This leads to a higher frequency of the exchange of routing messages, resulting in increased routing overheads. This can diminish network capacity since more bandwidth is consumed in the transmission of routing messages, resulting in longer processing times as nodes dedicate more resources to processing these messages.

Nevertheless, the results demonstrate that the AODV protocol outperforms the DTAODV protocol with regard to end-to-end delay and routing overheads. The DTAODV protocol employs a direct trust-based mechanism which requires additional processing time and overheads for the nodes to calculate and exchange trust information. This leads to higher end-to-end delay and routing overheads. On the other hand, the AODV protocol utilises only the shortest path for the transmission of packets, leading to the lower utilisation of network resources and lower end-to-end delay and routing overheads. Furthermore, both AODV and DTAODV perform significantly better when using the NS-3 simulator compared to the NS-2 simulator. One of the main reasons for this is the more efficient, process-oriented simulation architecture of NS-3, which reduces the routing overheads for AODV. Additionally, NS-3's more modular and extensible architecture enables the more effective optimisation of the implementation of the routing protocol.

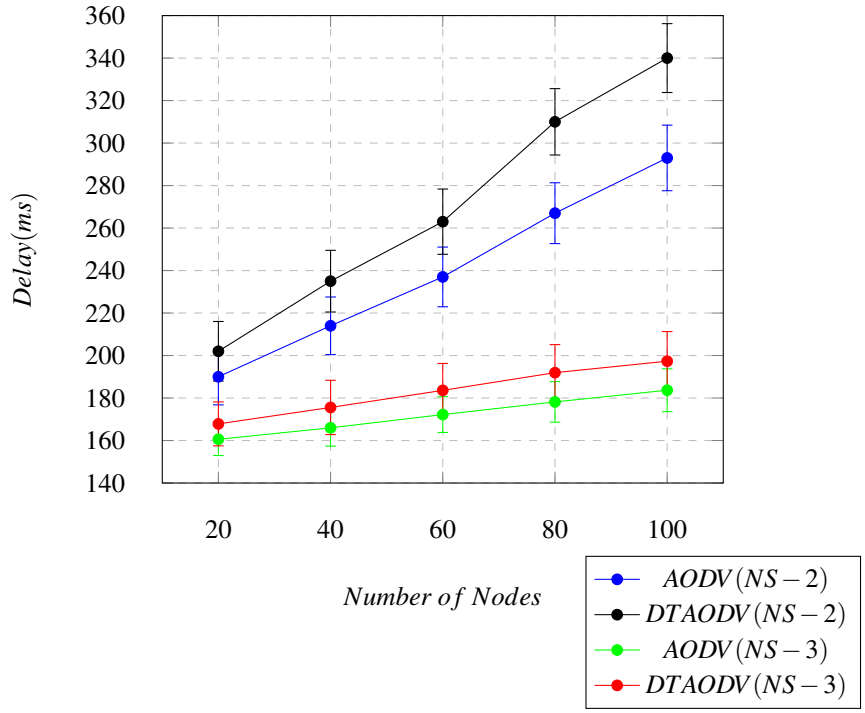

Figure 3.17 End-to-End Delay vs. Number of Nodes with 95% Confidence Intervals for NS2 and NS3

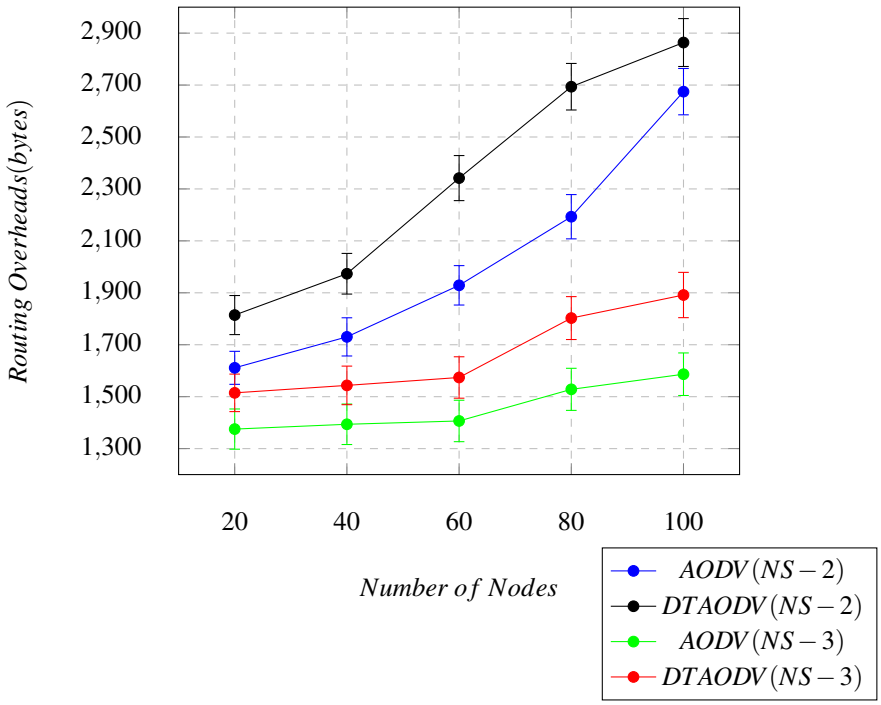

Figure 3.18 Routing Overheads vs. Number of Nodes with 95% Confidence Intervals for NS2 and NS3

3.5.2 Higher Weight Assigned to Hop Count

3.5.2.1 Performance With Variation in Node Movement Speed

A comprehensive evaluation of the Ad hoc On-demand Distance Vector (AODV) and Direct Trust Ad hoc On-demand Distance Vector (DTAODV) protocols was conducted in order to assess their behaviour when exposed to different node mobility speeds. The simulation parameters, as outlined in Table 3.6, were kept constant throughout the evaluation process so as to ensure consistent results. The simulation was repeated ten times for each mobility speed in order to validate the findings, and the mean value was calculated. Furthermore, a 95% confidence interval was calculated to show the variation in the results.

These simulations aimed to examine the effect of node mobility on the network and determine the performance of the protocols under varying mobility conditions. The mobility speeds ranged from 10 m/s to 50 m/s. The protocols were evaluated using performance metrics such as packet delivery ratio, throughput, routing overheads, and end-to-end delay. The simulation results provide valuable insights into the impact of node mobility on the network and the performance of the protocols in different mobility scenarios.

In the previous section, the impact was studied of node reliability and hop count parameters on the performance of the AODV and DTAODV protocols where the weighting assigned to node reliability was higher. This section considers the effect of node reliability and hop count when the weighting for hop count is higher. The simulations were executed using Network Simulator version 3 (NS-3.33) software. AODV relies on the shortest hop count to determine the optimal route for packet transmission, while DTAODV employs both direct trust and hop count mechanisms. By comparing the results obtained here with those of the previous section, where AODV and DTAODV were evaluated with weightings of 70% for node reliability and 30% for hop count, a more comprehensive understanding can be gained of the behaviour of these protocols in different network scenarios.

Table 3.6 Simulation Parameters

Routing protocols	AODV, DTAODV
Packet Size	512 *Bytes*
Simulation Time	360 *Seconds*
Simulation Area	1000 * 1000 m^2
Number of Nodes	20
Node Movement Speed	10,20,30,40,50 *m/s*
Node Movement	Random Way Point
MAC Protocol	IEEE 802.11b
Transmission Range	250 *Meter*
Number of Simulation Runs	10
Confidence Interval	95%
Traffic Type	UDP

3.5.2.2 Packet Delivery Ratio and Throughput Versus Node Mobility Speed

The correlation between node mobility speed and packet delivery ratio (PDR) and throughput is demonstrated in Figures 3.19 and 3.20. As mobility speed increases, it can be observed that the PDRs for both AODV and DTAODV protocols decrease with both combinations of weightings for trust value and hop count. This is due to the increasing likelihood of nodes moving out of range or encountering significant changes in their environment. These changes can result in alterations to network topology, such as the formation of new links or the disruption of existing links, leading to the need for more frequent updating of routing information.

The AODV protocol relies on the shortest path for packet transmission from a source node to a destination node. It may not be able to adjust quickly enough to these network changes, thus reducing its PDR and throughput performance. The DTAODV protocol, on the other hand, utilises a direct trust-based mechanism in addition to the shortest path for packet transmission, which may provide better performance in high-mobility environments, as shown in Figures 3.17 and 3.18. This approach reduces the frequency of occurrence of congestion and dropped packets, thereby improving the overall PDR and throughput.

It can also be noted that DTAODV, with weightings of 70% for trust value and 30% for hop count, outperforms the same protocol with weightings of 30% for trust and 70% for hop count in terms of both PDR and throughput. The confidence intervals further highlight the differences in PDR and throughput between AODV and DTAODV.

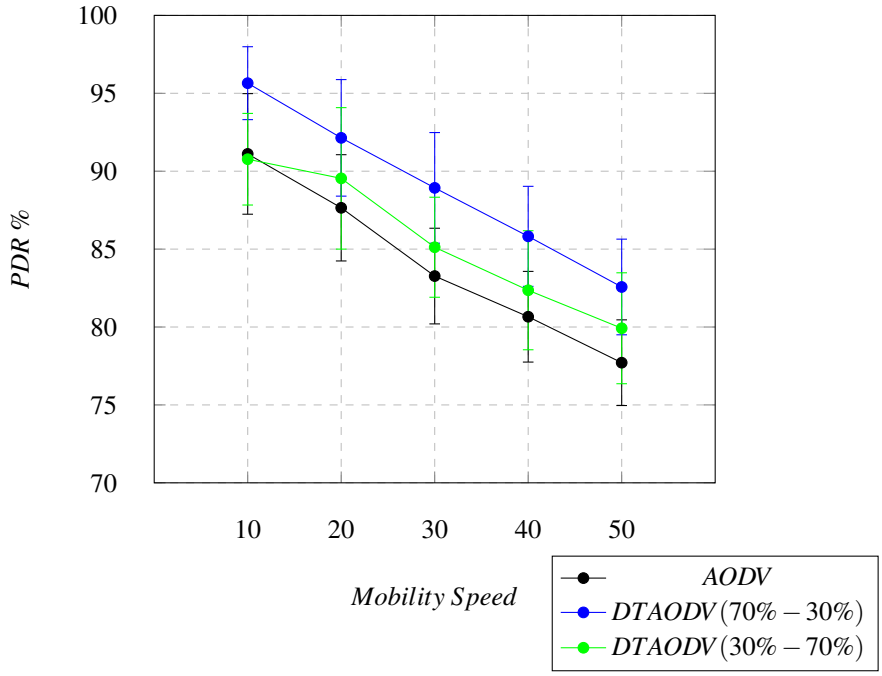

Figure 3.19 PDR vs. Mobility Speed with 95% Confidence Intervals

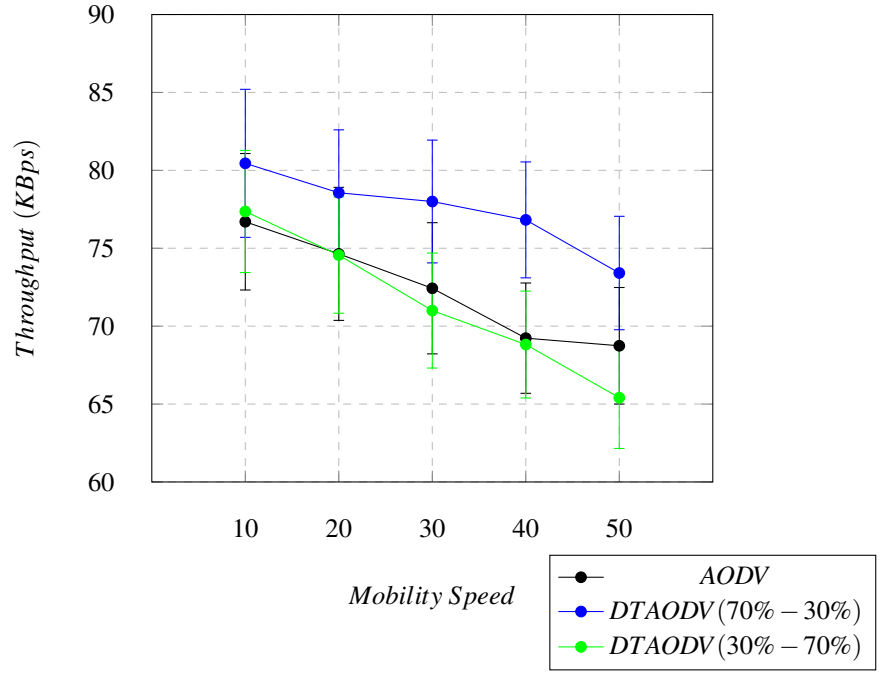

Figure 3.20 Throughput vs. Mobility Speed with 95% Confidence Intervals

3.5.2.3 End-to-End Delay and Routing Overheads Versus Node Mobility Speed

The impact of node mobility on the end-to-end delay and routing overheads of the Ad hoc On-demand Distance Vector (AODV) and Direct Trust Ad-hoc On-demand Distance

Vector (DTAODV) protocols are depicted in Figures 3.21 and 3.22. As the mobility speed increases, both end-to-end delay and routing overheads increase. The AODV protocol, which relies only on hop count for decisions on the routing of packets, performs better in terms of delay and routing overheads due to its straightforward methodology. On the other hand, the DTAODV protocol utilises a combination of hop count and the trustworthiness of the route, resulting in more reliable packet delivery but at the cost of increased delays and routing overheads. The results show that DTAODV, with weightings of 30% for trust and 70% for hop count, performs better in terms of end-to-end delay and routing overheads compared to weightings of 70% for trust and 30% for hop count. The higher delay and routing overheads at higher mobility speeds can be attributed to the need for more frequent updates to routing tables.

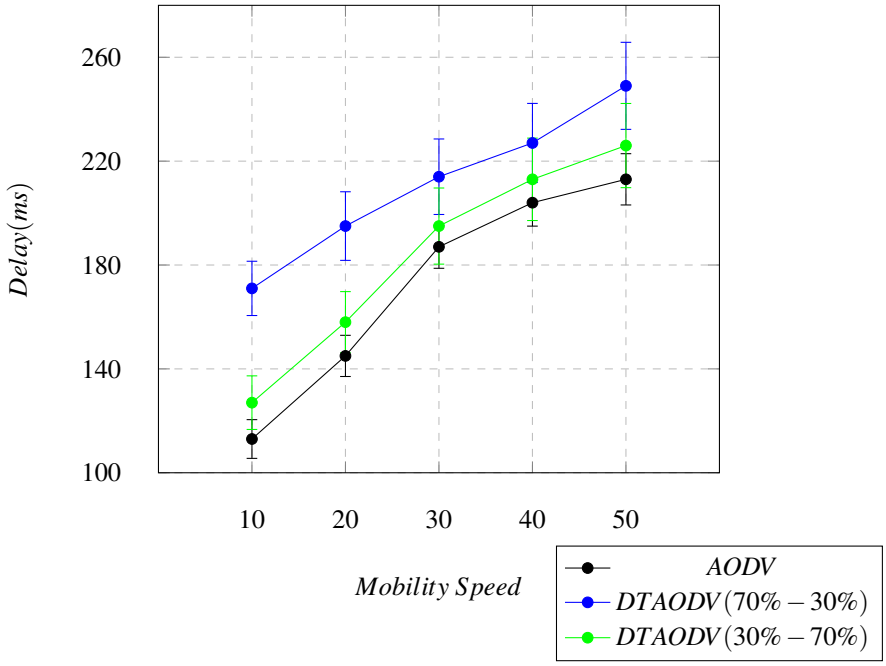

Figure 3.21 End-to-End Delay vs. Mobility Speed with 95% Confidence Intervals

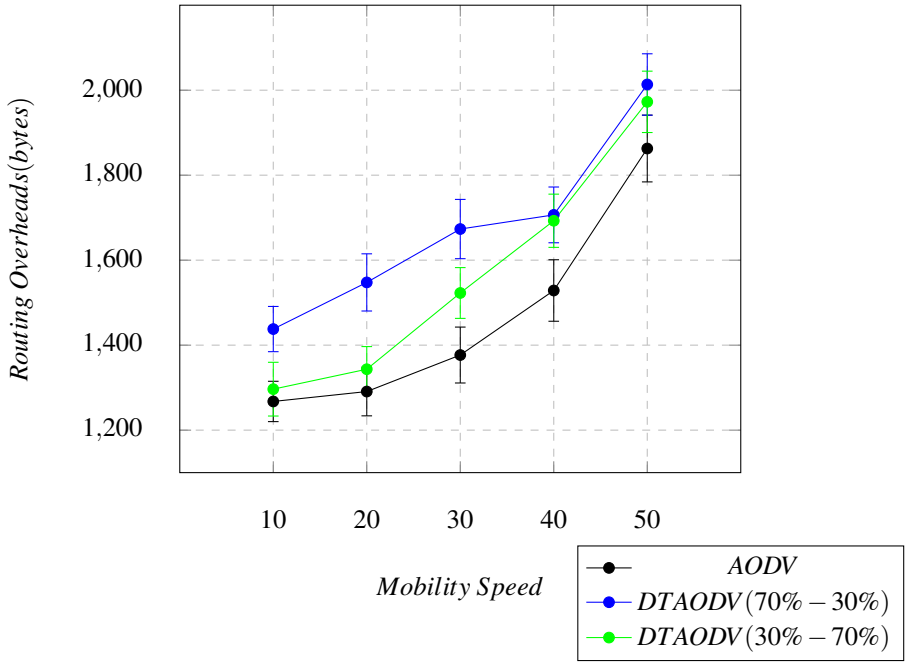

Figure 3.22 Routing Overheads vs. Mobility Speed with 95% Confidence Intervals

3.5.2.4 Performance With Variation in Node Density

The simulation-based assessment of the Ad hoc On-demand Distance Vector (AODV) and Direct Trust Ad-hoc On-demand Distance Vector (DTAODV) protocols involved a comprehensive examination of their behaviour as the number of nodes in the network varied to start from 20 nodes, and the maximum is 100 nodes in the network. As outlined in Table 3.7, the simulation parameters were kept constant throughout the evaluation process. To ensure the robustness of the results, the simulations were repeated ten times for each different number of nodes and the mean value was calculated. To further reinforce the validity of the results, a 95% confidence interval was also computed. These simulations aimed to study the impact of different network scenarios on the protocols and to evaluate their performance in terms of the key metrics of packet delivery ratio, throughput, routing overheads, and end-to-end delay.

In the previous investigation of node reliability and hop count parameters described in Section 3.5.1, the weights assigned to node reliability and hop count were 70% and 30%, respectively, as the node mobility speed was varied. This presents findings concerning the impact of these parameters when the weighting of node reliability is changed to 30%, and that of hop count is increased to 70. The simulations were once again executed using Network Simulator version 3 (NS-3.33). The AODV protocol relies on hop count in determining the shortest route for the transmission of packets from a source node to a destination. Conversely, the DTAODV protocol utilises the direct trust and shortest hop

count mechanisms. The results obtained from the previous examination of AODV and DTAODV shown in Section 3.5.1 with a 70% weighting assigned to node reliability and a 30% weighting assigned to hop count are combined with the results obtained in this section for DTAODV with a weighting of 30% assigned to node reliability and a 70% weighting assigned to hop count.

Table 3.7 Simulation Parameters

Routing protocol	***AODV, DTAODV***
Simulator	***NS-3.33***
Packet Size	512 *Bytes*
Simulation Time	360 *Seconds*
Simulation Area	1000 * 1000 m^2
Number of Nodes	20,40,60,80,100
Node Speed	5 *m/s*
Node Movement	Random Way Point
Mac Protocol	IEEE 802.11b
Transmission Range	250 *Meter*
Number of Simulation Runs	10
Confidence Interval	95%
Traffic Type	UDP

3.5.2.5 Packet Delivery Ratio and Throughput Versus Number of Nodes

The impact of the increase in the number of nodes in a network on the AODV and DTAODV protocols is depicted in Figures 3.23 and 3.24, respectively, with respect to the PDR and throughput metrics. As the number of nodes increases, the PDR also tends to increase owing to the availability of more transmission paths, thereby enhancing network efficiency. However, an increase in the number of nodes can lead to decreased throughput due to several factors, such as an increase in collisions among nodes. From Figure 3.23, it can be observed that the DTAODV protocol with weightings of 70% for node reliability and 30% for hop count exhibits the best performance since it incorporates direct trust mechanisms which ensure the delivery of packets from a source node to a destination node. Meanwhile, Figure 3.24 shows that the DTAODV with a weighting of 70% for node reliability and 30% for hop count performs worse when the number of nodes is 20 nodes. However, it performs slightly better than the other protocols as the number of nodes increases.

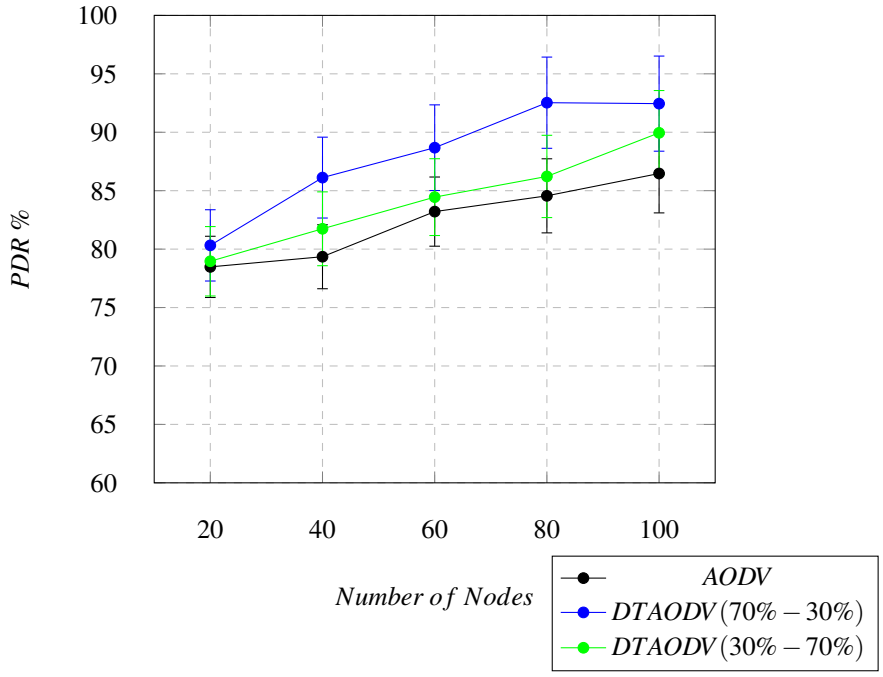

Figure 3.23 PDR vs. Number of Nodes with 95% Confidence Intervals

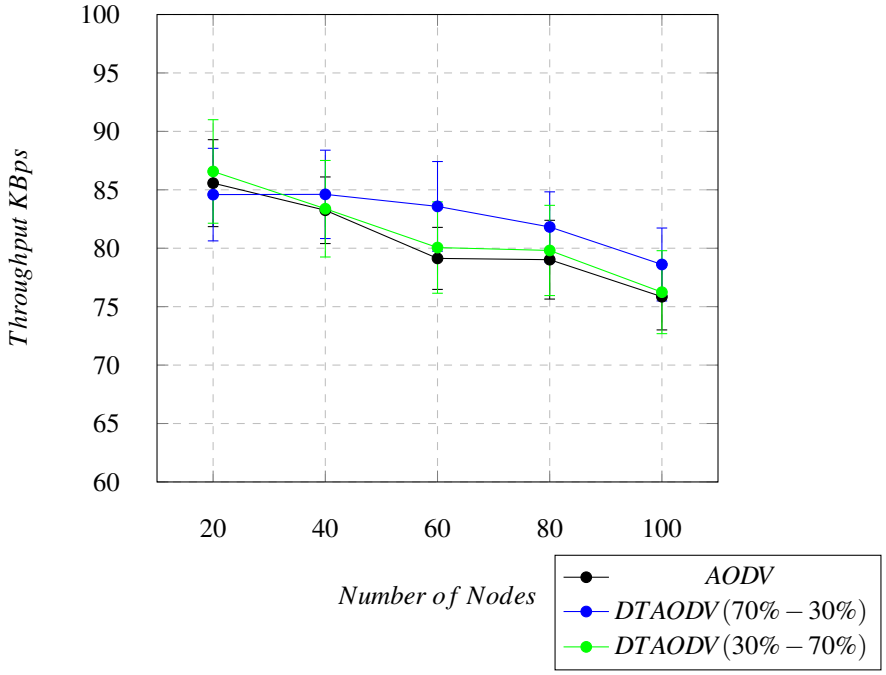

Figure 3.24 Throughput vs. Number of Nodes with 95% Confidence Intervals

3.5.2.6 End-to-End Delay and Routing Overheads Versus Number of Nodes

The simulation outcomes can be seen in Figures 3.25 and 3.26, which show the comparison between the AODV and DTAODV protocols in terms of end-to-end delay and routing

overheads. The results indicate that AODV outperforms both DTAODV protocols with different weightings of node reliability and hop counts in terms of end-to-end delay and overheads. Moreover, the DTAODV protocol with weightings of 30% for hop counts and 70% for node reliability exhibits better performance than its counterpart with 70% hop counts and 30% node reliability in terms of end-to-end delay and routing overheads. This is due to the fact that the DTAODV protocol employs a direct trust-based mechanism along with the calculation of the shortest path, leading to an increase in processing time and overheads for nodes to determine and exchange trust information, thereby contributing to a higher end-to-end delay and routing overheads. Hence, we can see that the DTAODV protocol with weightings of 70% for node reliability and 30% for hop count incurs higher end-to-end delay and routing overheads.

Furthermore, as the number of nodes in the network increases, there is a heightened likelihood of congestion and processing overheads, causing an escalation in end-to-end delay and routing overheads. Overall, the outcomes indicate that AODV exhibits superior performance in terms of end-to-end delay and routing overheads compared to both DTAODV protocols. However, DTAODV with weightings of node reliability at 70% and hop count at 30% demonstrate better results in terms of packet delivery ratio (PDR) and throughput.

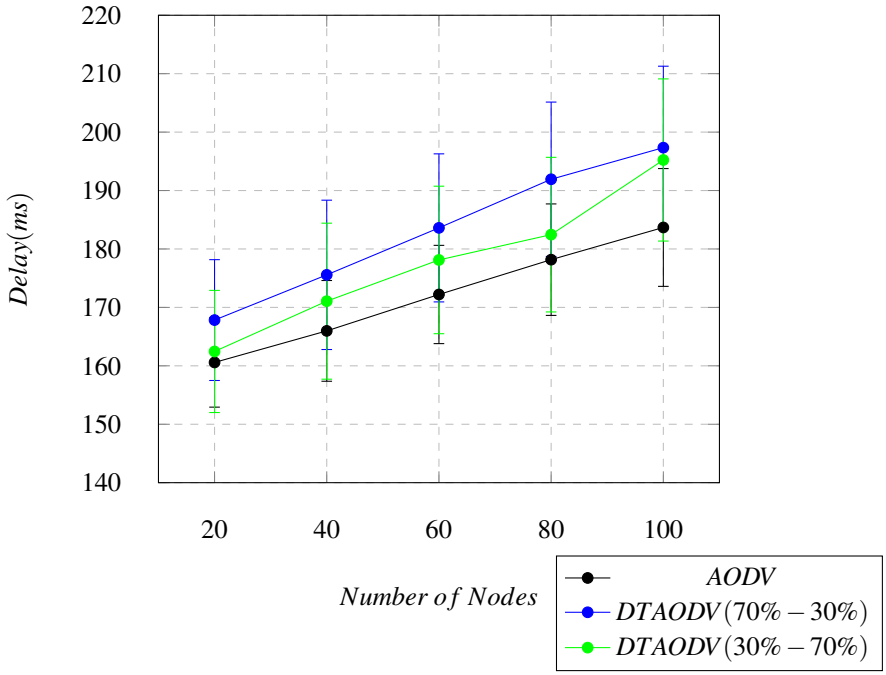

Figure 3.25 E2E Delay vs. Number of Nodes with 95% Confidence Intervals

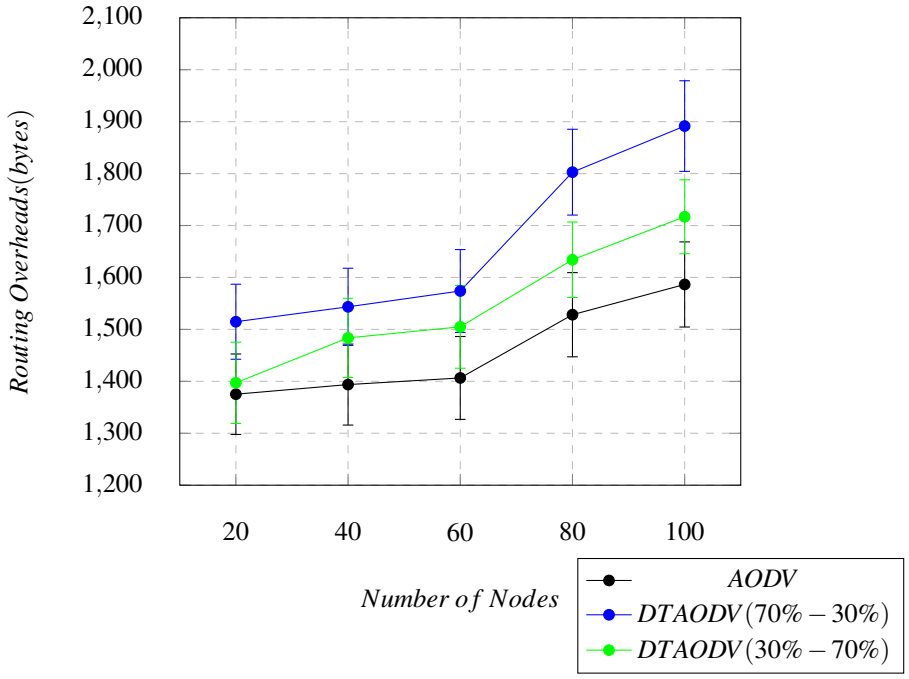

Figure 3.26 Routing Overheads vs. Number of Nodes with 95% Confidence Intervals

3.6 Performance Evaluation of AODV and DTAODV in the Presence of a Black hole Attack

This section explores the influence of security breaches on both the AODV and DTAODV protocols. The consequences of executing a black hole attack in these protocols are evaluated and analysed.

A black hole attack is a network attack that can occur when a malicious node advertises itself as having the shortest path to a destination node, causing other nodes to route their traffic through the malicious node [37]. This can result in dropped or modified packets. To defend against such attacks, direct trust mechanisms were implemented, as explained in depth in Section 3.2. Moreover, the efficiency of the implementation of a direct trust mechanism in the default AODV protocol can be tested. In AODV, when a source node wants to send data to a destination node, it broadcasts a route request (RREQ) message to all nodes within its radio range [83]. The RREQ message is then forwarded by intermediate nodes towards the destination node until the destination node is reached or a node with a sufficiently fresh route to the destination node is found. Once such a route is established, data packets can be transmitted along it. On the other hand, in a black hole attack, a malicious node intercepts the RREQ message and responds with a false route reply (RREP) message that claims to have the shortest path to the destination node [98]. Other nodes in the network will then use this false route and send their data packets through the malicious

node, causing packets to be dropped or even modified [99]. This can cause packets to be dropped or altered.

3.6.1 Experimental Set-up

In this section, the performance of the AODV and DTAODV protocols in the presence of a black hole attack is evaluated. PDR, throughput, end-to-end delay, and routing overheads were used as performance metrics, and the protocols were evaluated using the fixed simulation parameters shown in Table 3.8 while the number of malicious nodes was varied.

The simulations were run ten times on each different number of malicious nodes so as to increase the reliability of the results, with the calculation of means and 95% confidence intervals. The simulations were carried out to investigate the effect of the increase in the number of malicious nodes in the network. The simulations were carried out to check the behaviour of the default AODV and the proposed DTAODV under a black hole attack when the number of malicious nodes inside the network was increased from 5 to 25.

Table 3.8 Simulation Parameters

Routing protocols	***AODV, DTAODV***
Type of Threat	***Black hole Attack***
Packet Size	512 *Bytes*
Simulation Time	360 *Seconds*
Simulation Area	1000 * 1000 m^2
Number of Nodes	100
Number of Malicious Nodes	5,10,15,20,25
Node Movement Speed	10 *m/s*
Node Movement	Random Way Point
MAC Protocol	IEEE 802.11b
Transmission Range	250 *Meter*
Number of Simulation Runs	10
Confidence Interval	95%
Traffic Type	UDP

3.6.1.1 Evaluation of Packet Delivery Ratio and Throughput With Varying Numbers of Malicious Nodes

The simulation results presented in Figures 3.27 and 3.28 show the packet delivery ratio and throughput, respectively, when the number of malicious nodes in the network varied from 5 to a maximum of 25. In contrast, the overall number of network nodes was fixed at one hundred, as seen in Table 3.8. The PDR and throughput of AODV and DTAODV decreased as the number of malicious nodes increased in the network. The black hole

attack is one of the most dangerous threats to any MANET protocols, leading to poor performance in the network.

It can be observed from Figures 3.27 and 3.28 that the performance of AODV was negatively affected by the black hole attack, and the PDR decreased significantly from 53% with five malicious nodes in the network to 34% with 25 malicious. Moreover, the throughput decreased from 79 to 39 Kbps. The black hole attack on an AODV can significantly affect the PDR and throughput of the network. This is because a black hole node drops or modifies data packets that are being routed through it, causing them to be lost or delayed. This results in fewer successfully delivered packets per unit of time, which reduces the PDR and throughput of the network.

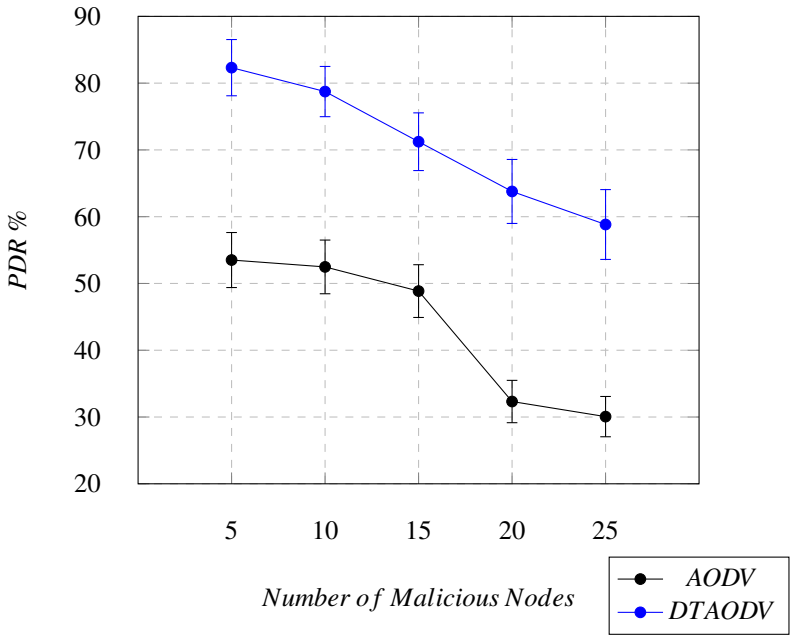

Figure 3.27 PDR vs. Number of Malicious Nodes with 95% Confidence Intervals

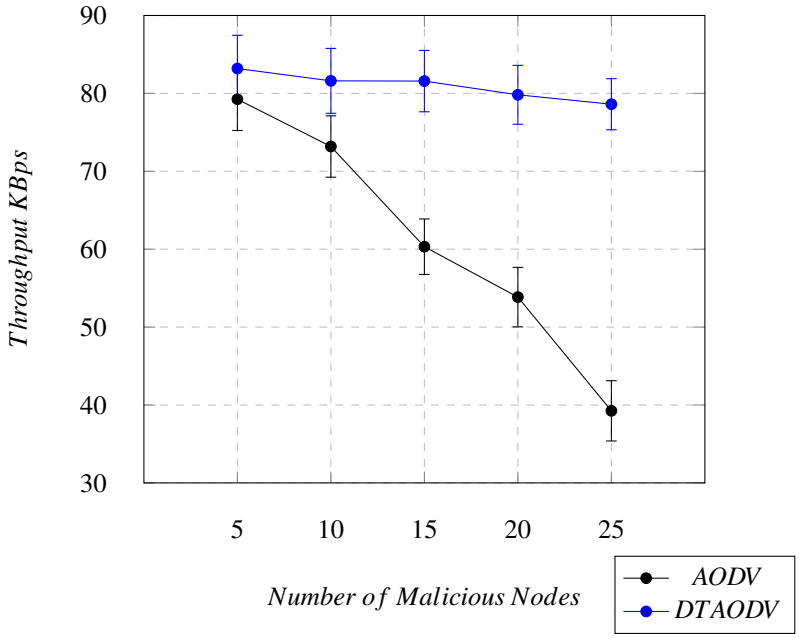

Figure 3.28 Throughput vs. Number of Malicious Nodes with 95% Confidence Intervals

3.6.1.2 Evaluation of End-to-End Delay and Routing Overheads With Varying Numbers of Malicious Nodes

The results of the simulation are presented in Figures 3.29 and 3.30, which provide a comparison of the AODV and DTAODV routing protocols in terms of their end-to-end delay and routing overheads under the influence of a black hole attack. As expected, the black hole attack negatively impacts both AODV and DTAODV, with increases in end-to-end delay and routing overheads as the number of malicious nodes in the network increases.

A black hole attack is particularly harmful to network performance since it causes disruptions to the normal routing path to the destination node, resulting in increased delays as the protocol attempts to locate an alternate path. This often results in repeated route discovery processes, which further exacerbates the issues of routing overheads and end-to-end delay. Moreover, a black hole node can selectively target and drop specific types of packets, leading to increased delays and potential data loss. This type of targeted attack can have a devastating impact on specific traffic flows, further impacting end-to-end delay and routing overheads.

However, Figures 3.29 and 3.30 demonstrate that the DTAODV protocol performs better than AODV in the presence of a black hole attack. This can be attributed to the direct trust mechanisms that have been implemented in DTAODV, which help to reduce the impact of attacks such as the black hole attack on end-to-end delay and routing overheads. In DTAODV, when a node detects a malicious node, it can reduce the trust level of that

node in its trust table and avoid selecting it for routing. This creates a more secure routing process, which leads to a more efficient path selection that ultimately reduces end-to-end delay and routing overheads. By incorporating trust management mechanisms, DTAODV can more effectively defend against malicious nodes and reduce the negative impact of black hole attacks on network performance.

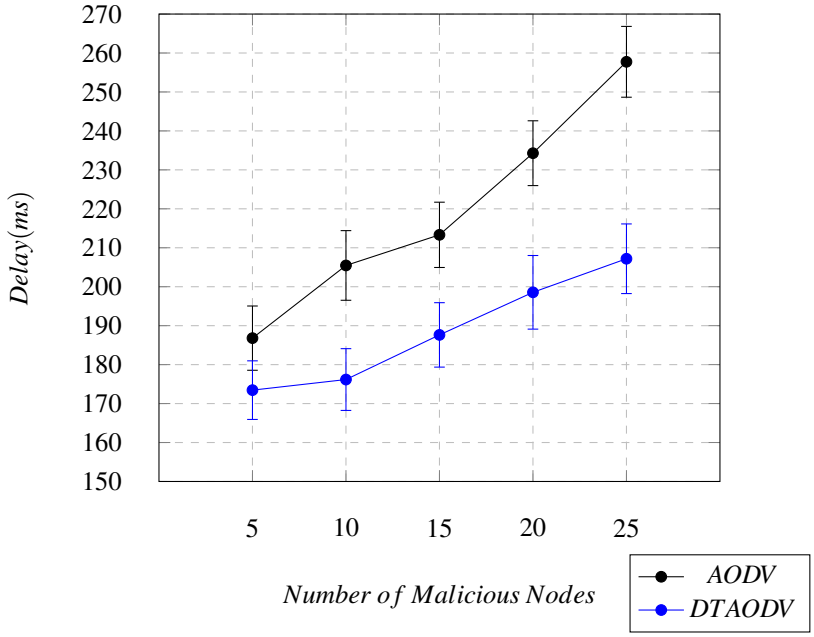

Figure 3.29 End-to-End Delay vs. Number of Nodes with 95% Confidence Intervals

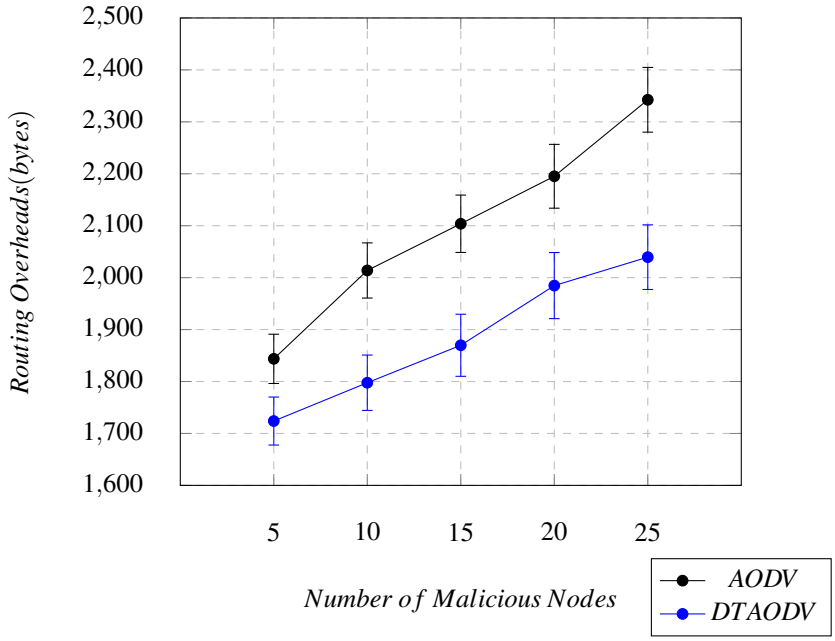

Figure 3.30 Routing Overheads vs. Number of Malicious Nodes with 95% Confidence Intervals

3.7 Summary and Discussion

This chapter has presented the proposed DTAODV protocol, which uses assessments of direct trust to improve the performance of the routing process in MANETs. The DTAODV protocol is an extension of the traditional AODV protocol, which is designed to use parameters such as packet forward rate, node battery power availability, battery drain rate, and congestion around a node to calculate a node's reliability value. The calculated value of reliability is used to determine the trustworthiness of each node in the network.

The chapter aimed to evaluate the performance of two different routing protocols, AODV and DTAODV, using advanced simulation techniques implemented with the NS-2 and NS-3 simulators. Moreover, the effectiveness of the direct trust mechanism, which uses the node reliability mechanism, and the default AODV protocol mechanism, which uses the number of hops to the destination node as the primary factor to determine trustworthiness, were compared. Measures of node reliability mechanisms and the shortest route to the destination were employed to examine the protocols operating in various scenarios. Different combinations of weightings of 70% and 30% were assigned to node reliability, and the number of hops to the destination, and the goal was to investigate the impact of the direct trust mechanism on the metrics of PDR, throughput, end-to-end delay, and routing overheads, while also testing the effect of different mobility speeds and various numbers of node scenarios.

The study further evaluated the efficiency and effectiveness of the implementation of trust management mechanisms, particularly the direct trust mechanism, in the AODV protocol by assessing the impact of a black hole attack on the AODV and DTAODV protocols. The research used NS-3 simulators to carry out this evaluation. The black hole attack is a malicious attack in which a node falsely advertises itself as having the shortest path to a destination node, causing other nodes to route their traffic through the malicious node. This action leads to dropped or modified packets and disrupts the normal path to the destination node. The study found that the direct trust mechanism in the DTAODV protocol helped in reducing the impact of such attacks since it could identify and reduce the trust level of malicious nodes in the network. This process allowed the protocol to avoid malicious nodes during the selection of a route, leading to a more efficient and secure routing process.

In general, the findings of this study of direct trust indicate that the DTAODV protocol outperforms the AODV protocol in terms of both PDR and throughput in scenarios of increased mobility speed and higher numbers of nodes. However, the performance of both protocols in the presence of a specific network threat, namely a black hole attack, was also evaluated by increasing the number of malicious nodes in the network. The results indicate that the DTAODV protocol performs significantly better than the AODV protocol in terms of PDR, throughput, end-to-end delay, and routing overheads under these conditions. This suggests that the implementation of the direct trust mechanisms in the AODV protocol has led to an improvement in overall performance in the presence of network threats and attacks. As discussed in Table 2.1 MANET has applications in various domains like Tactical networks, Emergency services, Sensor networks, Education, Conferences, Events, and various commercial places. There is always possibility of security attacks in MANETs which are deployed in commercial places, events, and tactical networks. Even in MANETs deployed in educational premises are prone to security attacks launched by the students for various purposes. The proposed trust mechanism is useful to overcome Black-hole attacks and selfish behaviour of the nodes in all such circumstances.

Chapter 4

Indirect Trust Management in AODV Routing Protocol

The previous chapter discussed the direct trust management mechanism and its integration into the Ad-hoc On-demand Distance Vector (AODV) protocol. Then the AODV and Direct Trust AODV (DTAODV) protocols were evaluated using various scenarios and performance metrics.

This chapter presents the integration of an indirect trust management mechanism into the AODV protocol, with the aim of enhancing its security and reliability. The modified protocol, which is called the Indirect Trust AODV (ITAODV), and AODV protocols are evaluated using the Network Simulator version 3 (NS-3). Different simulation scenarios and performance metrics were used to evaluate the performance of both the ITAODV and AODV protocols. Various different values of node movement speed and node density were used in the simulation scenarios to evaluate the packet delivery ratio, throughput, end-to-end delay and routing overhead performance metrics. The findings of this study are expected to demonstrate the superior performance of ITAODV in achieving improved security and reliability compared to the original AODV protocol. This chapter includes the use of indirect trust mechanisms and some results that were previously published [3, 4].

The chapter is structured as follows. Section 4.1 explains the proposed indirect trust management mechanisms. The performance evaluation and analysis of AODV and ITAODV with varying node movement speed and node density are discussed in Section 4.2, and Section 4.3 investigates the performance of AODV and ITAODV in the presence of a black hole attack. Finally, Section 4.4 summarises and discusses the finding of the chapter.

4.1 Proposed Indirect Trust Management Mechanism for AODV Protocol

4.1.1 Indirect Trust Mechanism

Direct trust is when a node determines its own trust value based on its assessments of other nodes in the network [4]. This type of trust is beneficial if the node has sufficient information about every other node in the network. However, in larger networks where nodes may not have direct contact with each other, it is more practical to rely on recommendations about the target node from other nodes. The node combines these recommendations with its own observations to calculate an overall trust value. This is called indirect trust.

Indirect trust, which is also known as reputation, refers to a type of trust that is based on a transitive property. In other words, if node A trusts node B, and node B trusts node C, then node A may indirectly trust node C based on its trust in node B. In Mobile Ad- hoc Networks (MANETs), indirect trust refers to the trust that is established between nodes through a series of intermediate nodes rather than through direct interactions between the nodes themselves [46]. In MANETs, nodes may have limited communication ranges and may only be able to communicate with nodes in their immediate vicinity. As a result, nodes may not be able to establish direct trust relationships with all other nodes in the network. Indirect trust can be particularly useful in situations where there are many nodes in a network, and it is difficult or impractical to establish direct relationships of trust between all of them. By relying on indirect trust, nodes can still make informed decisions about whether or not to trust others, even if they have not had direct interactions or experience with them. This work proposes the Indirect Trust AODV (ITAODV) protocol, which is an extension of the AODV routing protocol. ITAODV uses indirect trust management mechanisms to improve the performance and security of the protocol.

Indirect trust management mechanisms in MANETs aim to assess the trustworthiness of nodes based on the recommendations or experiences of other nodes within the network. This approach complements direct trust mechanisms, explained in Section 3.2.1, by providing additional information about a node's behaviour, even in cases where there has been no direct interaction. The following is an overview of how indirect trust management mechanisms work in MANETs:

1. Recommendation Gathering: A node requests trust information about a specific node from its neighbours. The neighbours share their trust evaluations or experiences with the target node, which can be based on their direct observations or previous indirect trust information.

2. Recommendation Aggregation: The requesting node collects trust recommendations from multiple neighbours and aggregates the data to form an indirect trust value. Various algorithms and techniques can be employed for aggregation, such as Dempster-Shafer theory which was used in this research. The aggregation process may also consider the trustworthiness of the recommending nodes to mitigate the risk of false recommendations.

3. Trust Threshold (δ): Similar to direct trust management, the network sets a trust threshold value indicated by δ, determining the minimum trust value required for a node to be considered trustworthy. Nodes with trust values below this threshold may be excluded from certain routing or communication processes.

4. Decision Making: When a node needs to select a route or a neighbour to forward a packet, it combines the direct and indirect trust values to make an informed decision. This process ensures that the overall trustworthiness of the candidate nodes is taken into account, improving network security and resilience against malicious nodes.

5. Trust Update: As nodes continue to interact and communicate, they may update their indirect trust values based on new recommendations or experiences. This dynamic trust evaluation allows the network to adapt to changing conditions and maintain an up-to-date view of each node's trustworthiness.

By implementing indirect trust management mechanisms in MANETs, the network can leverage the collective knowledge and experiences of multiple nodes to enhance trust evaluation accuracy. This approach helps mitigate the risk of malicious nodes, reduce the impact of attacks, and improve overall network performance and reliability. ITAODV is explained in detail in the rest of the sections in this chapter.

4.1.2 Overview of Proposed Indirect Trust Protocol

The proposed method uses indirect trust to evaluate the reliability and trustworthiness of nodes in the packet routing process. The level of indirect trust is calculated by combining recommendations made by neighbouring nodes. These recommendations simply represent their own direct trust observations about other nodes. The process adopted for the calculation of direct trust is explained in detail in Chapter 4, and this process is briefly described in Section 4.1.2.1 below.

The Indirect Trust AODV (ITAODV) is a modified version of the AODV routing protocol which incorporates trust mechanisms to improve the security and performance of routing in MANETs. Trust mechanisms help in the evaluation of the network nodes'

reliability, allowing the protocol to avoid the inclusion of potentially malicious or compromised nodes in the routing paths. The example below elaborates on how ITAODV works in a simple ad-hoc network with the six nodes A to F. Figure 4.1 illustrates a simple ad-hoc network diagram to show the connectivity between the nodes.

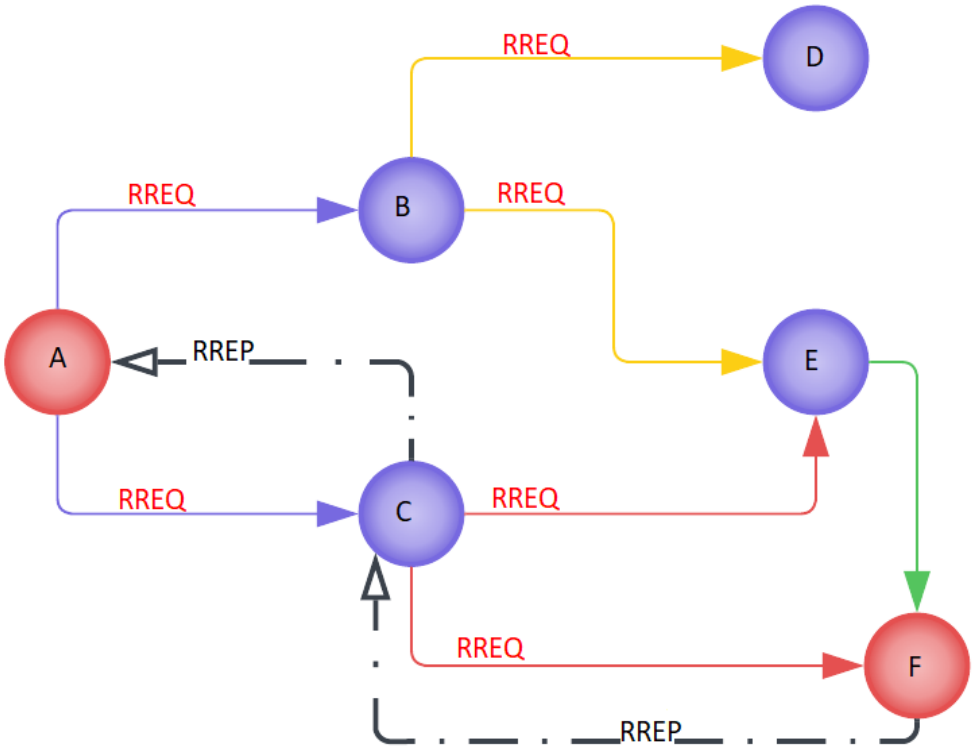

Figure 4.1 Diagram of ITAODV nodes Connectivity

1. Trust Initialisation: When a node joins the network, it is assigned an initial trust value. In this example, the trust values for the nodes are as follows:

   - A: 0.9
   - B: 0.8
   - C: 0.7
   - D: 0.6
   - E: 0.5
   - F: 0.9

2. Route Discovery: Node A wants to send a packet to node F but does not know the route to F. Node A broadcasts a Route Request (RREQ) packet to its neighbours B

and C. The RREQ contains the source (A) and destination (F) addresses, a sequence number, and the trust value of A (0.9).

3. Trust Calculation: Nodes B and C receive the RREQ from A. They update their routing tables with an entry for node A and calculate their trust values based on the trust value received from A and their own trust evaluations. For example, node B can calculate its trust value as (0.9 * 0.8) = 0.72, and node C can calculate its trust value as (0.9 * 0.7) = 0.63.

4. RREQ Propagation: Nodes B and C forward the RREQ to their neighbours, updating the trust value in the RREQ packet. It is supposed that node B is connected to nodes D and E, while node C is connected to nodes E and F.

    - Node B forwards the RREQ with a trust value of 0.72 to nodes D and E.
    - Node C forwards the RREQ with a trust value of 0.63 to nodes E and F.

5. Trust Evaluation at Destination: Nodes D, E, and F receive the RREQ from B and C. They update their routing tables with entries for nodes B and C and calculate their trust values based on the received trust values and their own trust evaluations.

    - Node D receives RREQ from B with a trust value of 0.72. It calculates its trust value as (0.72 * 0.6) = 0.432.
    - Node E receives RREQ from B with a trust value of 0.72 and from C with a trust value of 0.63. It selects the RREQ with the highest trust value (0.72) and calculates its trust value as (0.72 * 0.5) = 0.36.
    - Node F receives RREQ from C with a trust value of 0.63. It calculates its trust value as (0.63 * 0.9) = 0.567.

6. Route Reply (RREP) Generation: Node F, being the destination, sends a Route Reply (RREP) packet back to the node from which it received the RREQ with the highest trust value (in this case, node C). The RREP packet contains the source (F) and destination (A) addresses, a sequence number, and the calculated trust value (0.567).

7. RREP Propagation: The RREP is forwarded back through the network along the established route (F -> C -> A). Intermediate nodes update their routing tables with the route to F and the associated trust value (0.567).

8. Route Establishment: Node A receives the RREP, updates its routing table with the route to node F and the associated trust value (0.567), and begins sending data packets to node F via the established route (A -> C -> F).

By incorporating trust values in the routing process, ITAODV enhances the security and performance of ad hoc networks, making them more resilient against malicious or compromised nodes. The trust values help nodes to select routes with higher reliability, reducing the chances of the inclusion of malicious nodes in the route. Trust values are updated periodically based on the node's experiences and recommendations from neighbouring nodes, making the protocol adaptable to the dynamic nature of MANETs. Table 4.1 displays the parameters used for node monitoring.

Table 4.1 Trust Observation Parameters

Sr.	**Observation Parameter**	**Frequency of Recording the Observation**	**Positive Observation (α)**	**Negative Observation (β)**
1	Packet forwarding ability	For each observed data packet	α++ for each data packet forward	β++ for each data packet drop
2	Node Battery	At beginning of a new data transmission session	α++ if node's Battery Power > MBT	β++ if node's Battery Power <= MBT
3	Node's participation in network routing activities	For each observed RREP packet	α++ for the node which initiated control packet	β++ for the node which dropped a control packet. Also, β++ for a node caused a route error.
4	Node's packet forwarding queue capacity	At beginning of a new data transmission session	α++ if more than MQE of queue capacity is empty	β++ if available queue capacity is less than equal to MQE

4.1.2.1 Calculation of a Node's *rnu* using Direct Observations (dt_rnu_i)

To determine the direct trust, each node in the network monitors its neighbouring nodes for specific events that are indicative of the reliability of their packet forwarding ability. These observations are recorded as positive (α) or negative (β) observations of the neighbour node. Bayesian Inference is then used to calculate the reliability and value of the trustworthiness of each neighbour node. Bayesian Inference is a statistical method that uses Bayes' theorem to update the probability of a hypothesis as further evidence or information becomes available [90].

In wireless networks, cooperation between nodes is essential for reliable packet transmission. To evaluate the potential for successful cooperation between two nodes, a Beta distribution function can be used to represent the posterior distribution. The density func-

tion of the Beta distribution function is given in Equations 4.1 and 4.2, which is determined according to the two parameters, α and β.

Equation 4.3 can be used to calculate the direct node uncertainty (dt_u), which is the likelihood that the node's reliability for packet transmission cannot be predicted. In this equation numerator is multiplied by a constant factor 12, it makes $u = 1$ when value of α is 1 and value of β is also 1. The value of uncertainty ranges between 0 and 1 where 0 indicates fully certain and 1 indicates complete uncertainty. In order to calculate the direct node reliability expectation (dt_r), which is the probability that a node offers a reliable packet transmission service, the expected value of the Beta distribution function needs to be determined using Equation 4.4. Similarly, the direct node unreliability expectation (dt_n), which is the probability that a node does not offer a reliable packet transmission service, can be calculated using Equation 4.5.

$$Beta(T_{old}|\alpha,\beta) = \frac{\tau(\alpha+\beta+2)}{\tau(\alpha+1)\tau(\beta+1)} T_{old}^{\alpha}(1-T_{old})^{\beta} \tag{4.1}$$

In the mentioned equation, T_{old} represents the previous trust value of node x for y. The updated trust value, T_{new}, is then computed as follows:

$$T_{new} = E(Beta(T_{old}|\alpha,\beta)) = \frac{\alpha}{\alpha+\beta} \tag{4.2}$$

Node uncertainty dt_u is calculated as follows:

$$dt\_u = \frac{12\alpha\beta}{(\alpha+\beta)^2(\alpha+\beta+1)} \tag{4.3}$$

Node reliability expectation dt_r is calculated as follows:

$$dt\_r = \frac{\alpha}{\alpha+\beta}(1-u) \tag{4.4}$$

Node unreliability expectation dt_n is calculated as follows:

$$dt\_n = \frac{\beta}{\alpha+\beta}(1-u) \tag{4.5}$$

The dt_rnu_i signifies the reliability, unreliability, and uncertainty of node i, as determined through direct observations.

It is important to note that the Equations above are based on direct observations and are therefore referred to as direct *rnu* values. However, it is also possible to calculate the *rnu* values using indirect observations, which are obtained by combining the observations received from neighbouring nodes. The determination of indirect trust is discussed next.

4.1.2.2 Calculating Node's *rnu* using Indirect Observations

The nodes in the network continually exchange their direct trust observations about the reliability of other neighbouring nodes. The indirect trust is calculated by combining these direct trust observations, which are given by the neighbouring nodes. Here, each node disseminates calculated dt_rnu_i values to all neighbouring nodes at regular intervals. Upon reception, each node processes these observations and synthesises them to calculate its indirect trust (it_rnu_i) values, representing the node's reliability, unreliability, and uncertainty. These values are derived from both direct and indirect observations and are calculated using a weighted average method. Equation 4.6 outlines the calculation of node reliability using indirect observations (it_r_i), while Equation 4.7 outlines the calculation of node unreliability using indirect observations (it_n_i). Lastly, Equation 4.8 illustrates the calculation of node uncertainty using indirect observations (it_u_i).

$$it\_r_i = \frac{\sum_{0<j<=N} r_{ji} * w_j}{W} \tag{4.6}$$

$$it\_n_i = \frac{\sum_{0<j<=N} n_{ji} * w_j}{W} \tag{4.7}$$

$$it\_u_i = 1 - (it\_r_i + it\_n_i) \tag{4.8}$$

where, N is number of nodes in the network, r_{ji} is indirect reliability of node i which is reported by node j, n_{ji} is indirect unreliability of node i which is reported by node j. w_j is the weight assigned to node j depending on past interactions and W is the cumulative weight. The value of w_j is calculated using the following Equations :

$$\alpha\_sum_j = \sum_{i=1}^{N} \alpha_{i,j} \tag{4.9}$$

$$\beta\_sum_j = \sum_{i=1}^{N} \beta_{i,j} \tag{4.10}$$

$$w_j = \sum_{j=1}^{N} \alpha\_sum_j + \beta\_sum_j \tag{4.11}$$

where $\alpha_{i,j}$ is α reported by node i about node j and $\beta_{i,j}$ is β reported by node i about node j.

4.1.3 Integration of Direct and Indirect Trust in the ITAODV Routing Protocol

Direct trust is beneficial if the node has sufficient observations about every other node in the network. However, this is difficult to achieve in larger networks where nodes may not have direct contact with each other. In such situations it is more practical to rely on recommendations about the target node from other nodes. The node combines these recommendations with its own observations to calculate an overall trust value. This is called indirect trust.Thus indirect trust management mechanism extends the direct trust approach by considering recommendations from neighbouring nodes to establish trust among nodes that have not previously interacted. This mechanism fosters cooperation among nodes and mitigates the impact of malicious or compromised nodes in the network. In the proposed method, direct and indirect trust mechanisms are integrated into the Ad hoc On-Demand Distance Vector (AODV) protocol. The modified AODV protocol is referred to as the Indirect Trust AODV (ITAODV).

In the proposed ITAODV routing protocol, a node's ability to provide reliable packet routing service is represented by (r), which denotes the probability of dependable packet service offered by a node. Conversely, the probability that a node's packet routing service is not reliable is termed as its unreliability (n). Additionally, the likelihood that the node's reliability for packet routing cannot be predicted is referred to as node uncertainty (u). These three values collectively constitute the *rnu* (denoting its reliability, unreliability, and uncertainty) metric. This metric is computed using a weighted average method taking into account both direct and indirect observations. In order to determine the *rnu* values of neighbouring nodes, each node performs the following actions:

- The values of α_i and β_i for every neighbouring node i. are consistently observed.
- Each node computes the direct trust dt_rnu_i for the neighbouring node i using its α_i and β_i values. This process is explained in detail in Chapter 3.
- At periodic intervals, each node transmits computed dt_rnu_i values to all neighbouring nodes.
- Each node combines the received direct trust observations (dt_rnu_i) and computes the indirect trust it_rnu_i for each node in the network.

The AODV protocol uses hop count as a metric for routing decisions, which is suitable for reliable networks with trustworthy nodes. However, the protocol is vulnerable to many unique attacks, such as the black hole attack. Therefore, to overcome this issue, the Indirect Trust AODV (ITAODV) protocol is proposed as a modification to the AODV protocol so

as to overcome vulnerability issues and enhance the performance of the protocol under different conditions. In ITAODV, each node utilises combined reliability values to make routing decisions. The reliability value of each neighbour node is calculated using direct and indirect observations, and the node with the highest reliability value that is closer to the destination is preferred as the node to forward the next packet to. This method enhances the security and efficiency of the routing protocol compared to the default AODV protocol.

$$Trust\_value_i = \frac{\rho}{\text{No. of Hops to Destination}} + (1-\rho) * Node\ Reliability\ Value\ (it\_r_i) \tag{4.12}$$

As in Chapter 3, various values of ρ were used to assign varying weights, firstly to hop count from a source node to the destination node and secondly to node reliability, with the aim to optimise the performance of the trust mechanism and to identify the best performance scenario. The results of this experimentation led to the conclusion that the optimal weight to be used in modifying the standard AODV protocol is 70% for node reliability and 30% for hop count. Consequently, in this chapter, ρ is set to 0.30, signifying that 70% weight is assigned to node reliability, and a weight of 30% is assigned to hop count. Finally, the above mechanism was implemented in AODV, which then becomes the Indirect Trust AODV (ITAODV) protocol. The ITAODV protocol employs a technique where a packet is forwarded from a source node to a destination node through a neighbour node that has the highest trust value. This mechanism ensures that the packet is routed through a more reliable node, which improves the security and efficiency of the network. By using trust values to determine the forwarding node, the ITAODV protocol can mitigate attacks such as a black hole attack as well as other security threats.

4.2 Performance Evaluation and Analysis of Proposed Protocol

The aim of this section is to evaluate the effectiveness and efficiency of the implementation of the indirect trust mechanism in the AODV protocol. The performance of the AODV and ITAODV protocols is compared based on different scenarios and metrics. To do this, experiments were conducted using the NS-3 simulator. The performance metrics used were Packet Delivery Ratio (PDR), throughput, end-to-end delay, and routing overhead. The performance of the two protocols was evaluated under two different test conditions involving the variation of values of node movement speed and node density in the network.

An in-depth explanation of these testing conditions and their corresponding assessments can be found below.

4.2.1 Performance Evaluation When Varying Node Movement Speed

Increasing node mobility can make the network more challenging to manage, and adjustments to the trust mechanisms and protocol design may be required in order to ensure optimal performance. Therefore, it is important to evaluate the performance of these protocols under different mobility scenarios so as to determine the best option for a given network. This study aims to evaluate the performance of the AODV and ITAODV protocols at different node movement speeds. Table 4.2 specifies the simulation parameters that are kept constant during the evaluation. To ensure the accuracy of the results, each simulation was run ten times, and the mean value was computed. A 95% confidence interval was also calculated. The simulations were conducted to analyse the impact of node mobility on the network and to assess the performance of the protocols in various mobility scenarios ranging from 10 m/s to 50 m/s. The evaluation metrics used in this study include packet delivery ratio, throughput, routing overhead, and end-to-end delay. The simulation tool used is the Network Simulator version 3 (NS-3.33).

Table 4.2 Simulation Parameters

Routing protocols	AODV, ITAODV
Packet Size	512 *Bytes*
Simulation Time	360 *Seconds*
Simulation Area	1000 * 1000 m^2
Number of Nodes	20
Node Movement Speed	10,20,30,40,50 *m/s*
Node Movement	Random Way Point
MAC Protocol	IEEE 802.11b
Transmission Range	250 *Meter*
Number of Simulation Runs	10
Confidence Interval	95%
Traffic Type	UDP

4.2.1.1 Packet Delivery Ratio and Throughput Versus Node Movement Speed

The impact of node movement speed on PDR and throughput in ITAODV and AODV is complex and depends on a variety of factors, including the density of the network, the mobility patterns of the nodes and the level of trust established between them. However, in general, higher node movement speeds can lead to a longer time to establish trust relationships, and a higher potential for packet loss and collisions, all of which can result

in decreased PDR and throughput. However, it is found here that ITAODV performs better than AODV in terms of both PDR and throughput.

Figures 4.2 and 4.3 shows the correlation between node movement speed and PDR and throughput metrics. It can be seen that ITAODV exhibits better performance than AODV in both metrics. As shown in Figure 4.2, ITAODV has a PDR of 94.87% when the mobility speed is at 10 metres, and this declines to a PDR of 88.73% when the mobility speed is at 50 metres. On the other hand, AODV has a lower PDR of 91.11% when the mobility speed is 10 metres which falls to a PDR of 77.71% when the mobility speed is at 50 metres. Values for both ITAODV and AODV decrease as node movement speed increases. High PDR and throughput are generally desirable in AODV because faster transmission of data is enabled, and more efficient communication among nodes is supported [100]. This can be especially important in applications such as emergency response scenarios that require real-time communication or the transfer of large amounts of data. However, the achievement of high PDR and throughput is challenging when the movement speed of the nodes is high; therefore, the use of indirect trust management mechanisms in these conditions has improved the stability and improvement of PDR and throughput. Using ITAODV in situations when the movement speed of nodes is increasing would be better than using the standard AODV protocol.

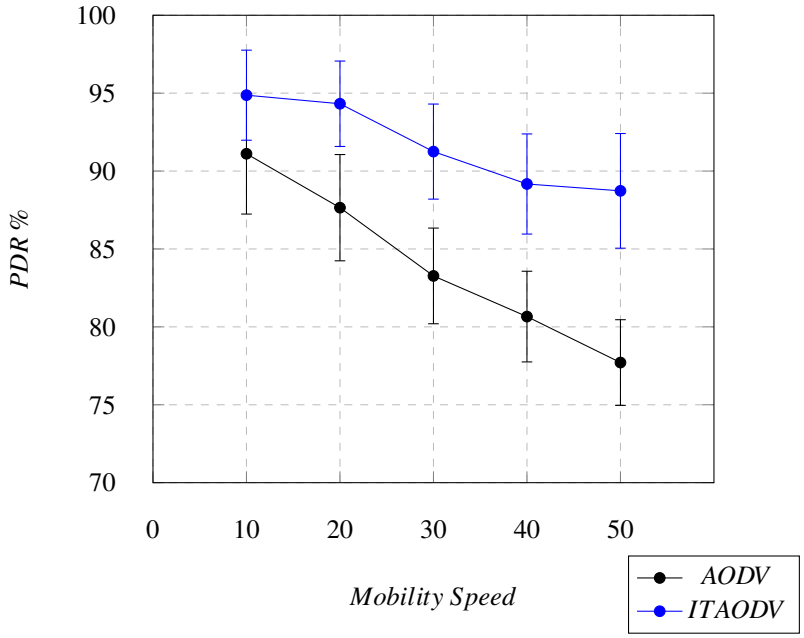

Figure 4.2 PDR vs. Node Movement Speed with 95% Confidence Intervals

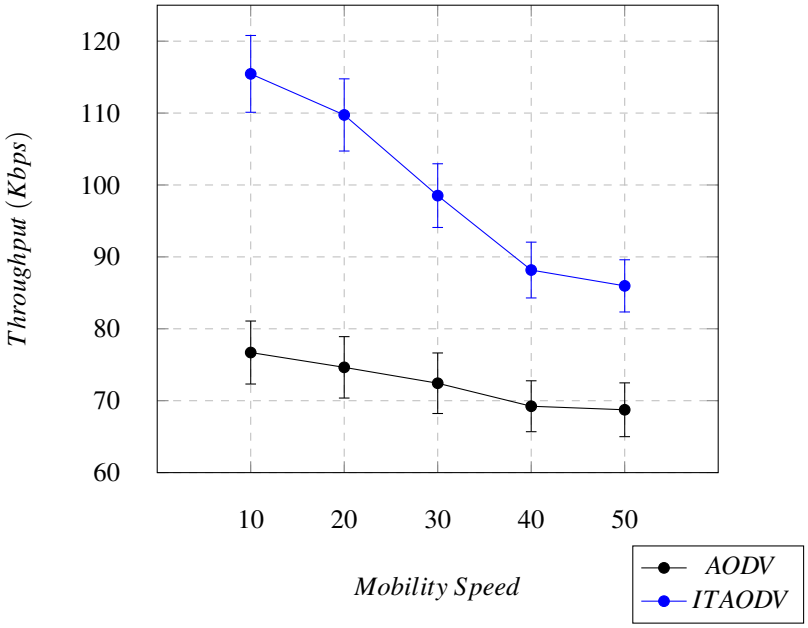

Figure 4.3 Throughput vs. Node Movement Speed with 95% Confidence Intervals

4.2.1.2 End-to-End Delay and Routing Overhead Versus Node Mobility Speed

The performance of end-to-end delay and routing overheads for both AODV and ITAODV protocols under different mobility speeds are shown in Figures 4.3 and 4.4. As the mobility speed increases, the end-to-end delay and routing overheads increase for both protocols. AODV performs better due to its simpler methodology of packet routing, which is based only on hop count. On the other hand, ITAODV uses a composite metric which takes into account both hop count and the direct trust mechanisms, which ensure reliable packet delivery and throughput, but at the cost of increased delay and routing overheads. The cause of higher end-to-end delay and routing overheads could be the higher frequency of update requests to the routing table. In addition, as the movement speed of nodes increases, the network topology changes rapidly, and this leads to a higher frequency of route discovery and maintenance processes, which cause higher end-to-end delays and routing overheads.

It can be seen from Figures 4.3 and 4.4 that AODV exhibits better performance than ITAODV in this respect. With the ITAODV protocol, each node maintains a trust table that contains information about the trustworthiness of other nodes in the network. This information is used to make routing decisions based on the trust level of the nodes. The trust level of each node is calculated based on the feedback received from other nodes in the network, causing higher end-to-end delay and routing overheads than AODV. Moreover, when nodes move faster, the network topology changes more frequently, and the routing protocols need to exchange more control messages so as to adapt to these changes [101].

This results in higher routing overheads, which can consume more network resources and increase the delay in delivering packets.

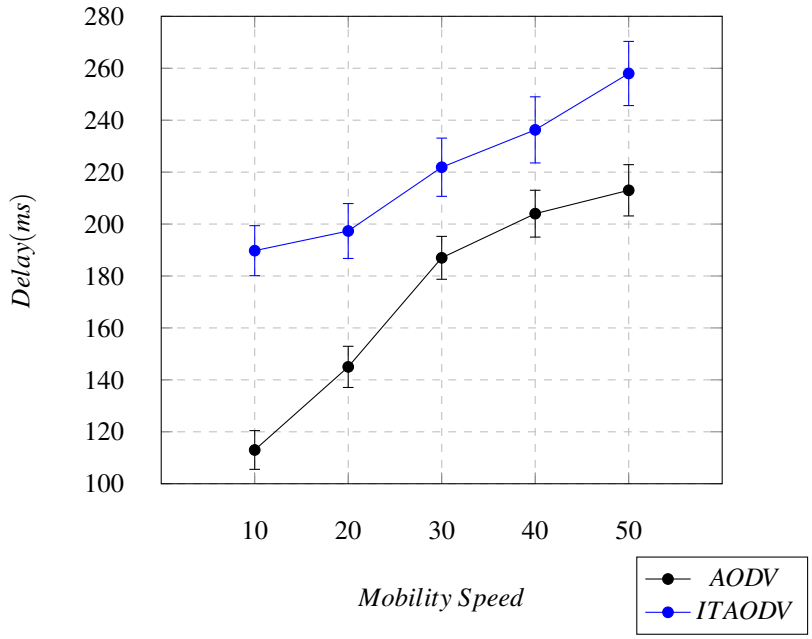

Figure 4.4 End-to-End Delay vs. Mobility Speed with 95% Confidence Intervals

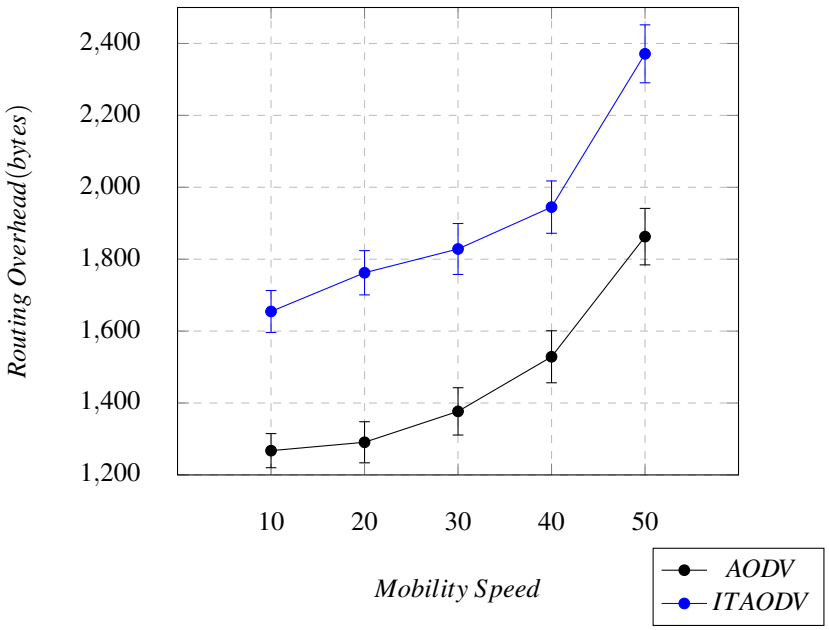

Figure 4.5 Routing Overhead vs. Mobility Speed with 95% Confidence Intervals

4.2.2 Performance Evaluation When Varying Node Density

In order to evaluate the efficacy of the AODV and ITAODV protocols, a series of simulations were conducted in which the number of nodes in the network was varied while keeping other simulation conditions constant, as defined in Table 4.3. The aim was to examine the behaviour of these protocols under different network scenarios. To ensure the accuracy and statistical significance of the results, the simulations were repeated ten times for each node count, and the mean value was calculated. A 95% confidence interval was also computed to provide a level of assurance and confidence in the findings. The performance of the protocols was assessed using critical metrics, including packet delivery ratio, throughput, routing overheads, and end-to-end delay, in order to provide a comprehensive understanding of their performance under various network scenarios.

Table 4.3 Simulation Parameters when Varying Node Density

Routing protocols	***AODV, ITAODV***
Packet Size	512 *Bytes*
Simulation Time	360 *Seconds*
Simulation Area	1000 * 1000 m^2
Number of Nodes	20,40,60,80,100
Node Movement Speed	5 *m/s*
Node Movement	Random Way Point
MAC Protocol	IEEE 802.11b
Transmission Range	250 *Meter*
Number of Simulation Runs	10
Confidence Interval	95%
Traffic Type	UDP

4.2.2.1 Packet Delivery Ratio and Throughput Versus Node Density

Figures 4.6 and 4.7 show the impact on PDR and throughput of varying the number of nodes. Figure 4.6 shows the better performance of the ITAODV, as the PDR of the ITAODV protocol is 87.75% when the number of nodes is 20 and increases with the number of nodes to 96.04% when there are 100 nodes in the network. On the other hand, the AODV protocol has a PDR of 78.48% when the number of nodes is 20, which increases to 86.47% when there are 100 nodes in the network. An increasing number of nodes in the network has a positive effect on the PDRs of AODV and ITAODV. One main reason for this is that the network becomes denser as the number of nodes increases, which provides more routing options and paths for packets to reach their destination [102]. This can result in the more efficient use of network resources and an increase in the PDR. Additionally, the probability of multiple routes to the same destination also increases with the number of

nodes [103]. This redundancy can help to improve the robustness and reliability of the network and can lead to an increase in the PDR. Another factor that may contribute to the increase in PDR is the effect of signal strength. As the number of nodes increases, the probability of there being more nodes within the communication range of a given node also increases [26]. This can lead to stronger signal strength and better link quality, which can also result in an increase in the PDR. Moreover, using the indirect trust mechanism increases the probability of delivering packets from a source node to a destination node.

Figure 4.7 displays significant differences in the throughput of AODV and ITAODV protocols. The AODV protocol exhibited a lower throughput compared to ITAODV, with a value of 85 KBps when the network had 20 nodes, whereas, for ITAODV, the corresponding value is 126 KBps. As the number of nodes increased, the ITAODV protocol displayed a better and more stable throughput, while the throughput of the AODV protocol was negatively impacted. An increase in the number of nodes in a wireless network can lead to congestion and contention for shared resources, which can have an adverse effect on network throughput [104]. Additionally, in a highly populated network, nodes may need to compete for limited available bandwidth, resulting in lower throughput [105]. However, the negative impact of these factors was more pronounced in the AODV than in the ITAODV protocol, which used indirect trust mechanisms to ensure packet delivery, resulting in a more stable throughput and packet delivery ratio.

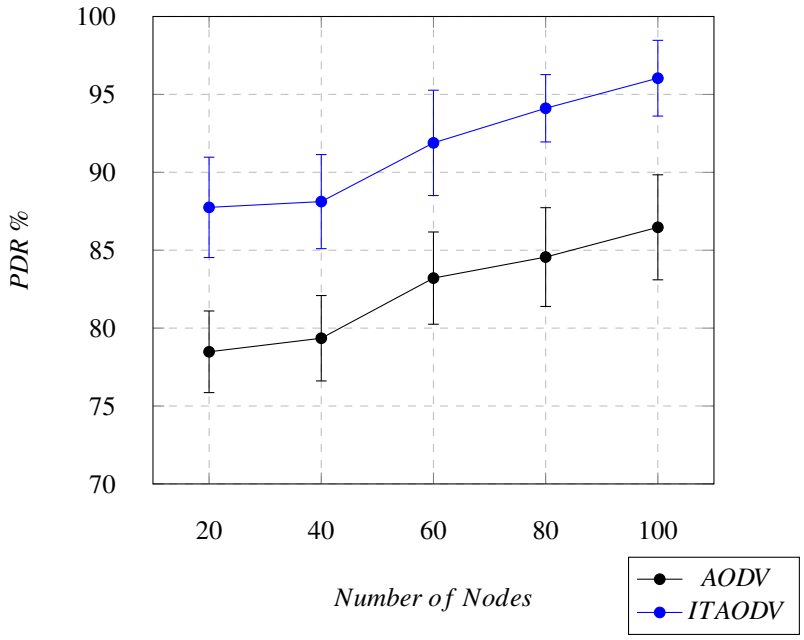

Figure 4.6 PDR vs. Number of Nodes with 95% Confidence Intervals

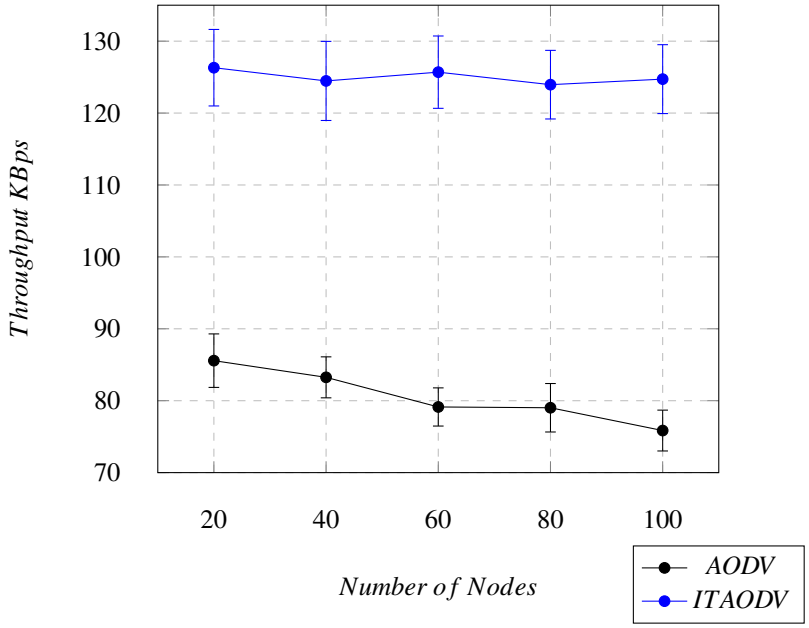

Figure 4.7 Throughput vs. Number of Nodes with 95% Confidence Intervals

4.2.2.2 End-to-End Delay and Routing Overhead Versus Node Density

Figures 4.7 and 4.8 present the relationship between the number of nodes and the end-to-end delay and routing overhead metrics in the network. The performance of AODV and ITAODV is affected negatively as the number of nodes increases. However, ITAODV exhibits worse performance than AODV in terms of end-to-end delay and routing overheads. This is because ITAODV uses indirect trust mechanisms, which require more time to determine the most reliable route for the sending of a packet from a source to a destination node. Consequently, there is a higher frequency of the exchange of routing messages, leading to increased end-to-end delay and routing overheads [44]. In contrast, AODV uses a simple approach to manage routing in the network, which is based on the shortest hop [26]. Therefore, AODV performs better in terms of end-to-end delay and routing overheads.

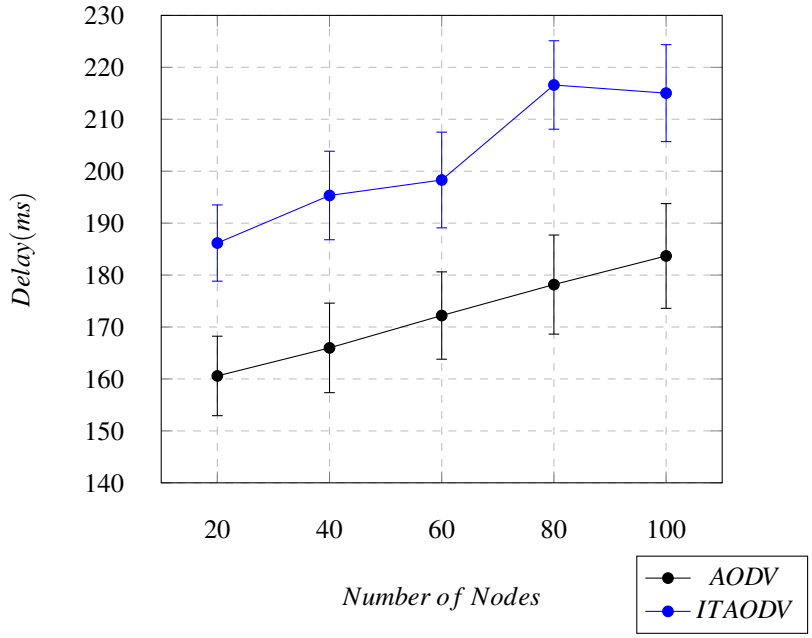

Figure 4.8 End-to-End Delay vs. Number of Nodes with 95% Confidence Intervals

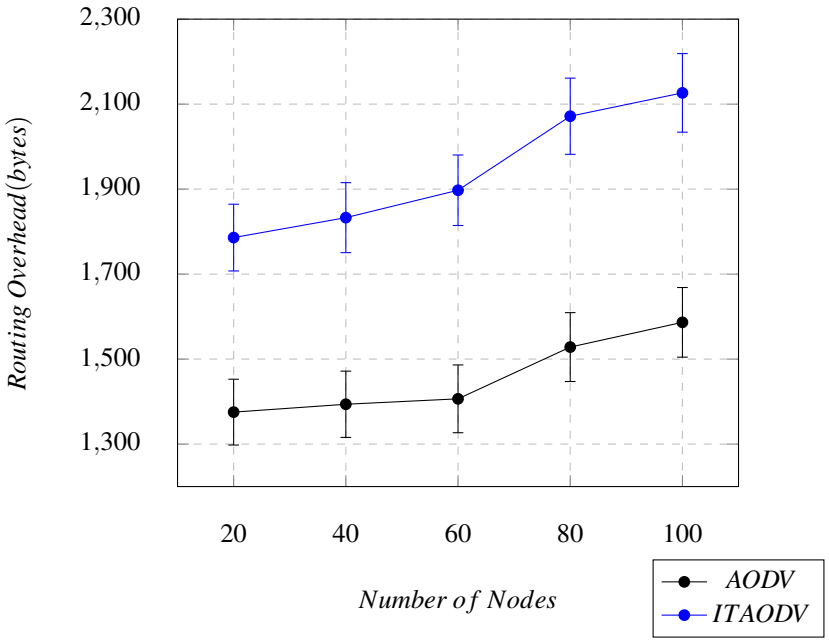

Figure 4.9 Routing Overhead vs. Number of Nodes with 95% Confidence Intervals

4.3 Performance Evaluation and Analysis in the Presence of a Black hole Attack

The effects of a notorious security threat known as a black hole attack on the two MANET routing protocols, AODV and ITAODV are thoroughly investigated in this section. A black hole attack is a pernicious type of attack that occurs when a malicious node, referred to as a black hole node, falsely claims to have the shortest path to the destination node [106]. The black hole node intercepts data packets from the source node and drops them, failing to forward them to the next hop [98]. This malicious behaviour tricks the source node into believing that the destination node is unreachable, leading to a severe denial-of-service attack. During a black hole attack, the malicious node captures the RREQ message and responds with a false route reply (RREP) message that claims to have the shortest path to the destination node [107]. This fraudulent route attracts other nodes in the network to send their data packets through the malicious node, causing those packets to be dropped or even altered.

An investigation was therefore conducted into the impact and behaviour of a black hole attack when implemented in the AODV and ITAODV protocols. This section examines the effect of the security threat and attack on the indirect trust approach, which should perform effectively in the presence of an attack due to its use of reputation and appropriate behaviour to calculate the most reliable route for packet transmission.

4.3.1 Experimental Set-up

This section explains the performance evaluation of the AODV and ITAODV protocols in the presence of the black hole attack. To assess the impact of increasing the number of malicious nodes on crucial performance metrics like PDR, throughput, end-to-end delay, and routing overhead, the number of malicious nodes in the network was varied. The fixed simulation parameters illustrated in Table 4.4 were used, while the number of malicious nodes was incrementally increased. In order to ensure the accuracy and reliability of the simulation results, ten simulations were conducted for each different number of malicious nodes, and the average values of the performance metrics were calculated. In addition, a 95% confidence interval was determined to increase the confidence in the simulation results. The simulation's primary objective was to investigate the effect of the introduction of increasing numbers of malicious nodes on the network's performance.

The simulation aims to explore how the default AODV and ITAODV protocols perform in the presence of a black hole attack as the number of malicious nodes in the network increases from 5 to 25. By incrementally increasing the number of malicious nodes in the network, the robustness and resilience of the protocols against black hole attacks, which are

common types of malicious attacks in ad hoc networks, could be evaluated. Furthermore, this investigation allows the effectiveness of the indirect trust mechanism used in ITAODV in combating black hole attacks to be assessed.

Table 4.4 Simulation Parameters

Routing protocols	***AODV, ITAODV***
Type of Threat	***Black hole Attack***
Packet Size	512 *Bytes*
Simulation Time	360 *Seconds*
Simulation Area	1000 * 1000 m^2
Number of Nodes	100
Number of Malicious Nodes	5,10,15,20,25
Node Movement Speed	10 *m/s*
Node Movement	Random Way Point
MAC Protocol	IEEE 802.11b
Transmission Range	250 *Meter*
Number of Simulation Runs	10
Confidence Interval	95%
Traffic Type	UDP

4.3.2 Evaluating Packet Delivery Ratio and Throughput

Figures 4.10 and 4.11 show the comparison of the PDR and throughput of the two different routing protocols, AODV and ITAODV, as the number of malicious nodes increases. The x-axis represents the number of malicious nodes in the network. In contrast, the y-axis represents the PDR percentage in Figure 4.10 and throughput in KBps in Figure 4.11 with 95% confidence intervals for both AODV and ITAODV. The results show that both protocols experience a decrease in PDR and throughput as the number of malicious nodes increases. However, the ITAODV protocol generally outperforms AODV in terms of PDR and throughput, especially when the number of malicious nodes is high. For example, when there are 25 malicious nodes, the PDR of ITAODV is around 64.83%, while that of AODV is only around 34.76%. Also, when there are 25 malicious nodes, the throughput of AODV drops to 39.25 KBps while that of ITAODV drops only to 88.62 KBps. It is also worth noting that the confidence intervals of ITAODV are generally narrower than those of AODV, which suggests that the network is more consistent in its performance. This could be attributed to the fact that ITAODV incorporates an indirect trust-based mechanism that helps to identify and avoid malicious nodes, thereby improving the reliability of data transmission in the network. Overall, these results demonstrate the effectiveness of ITAODV in mitigating the impact of malicious nodes on PDR and throughput in the MANET routing protocol.

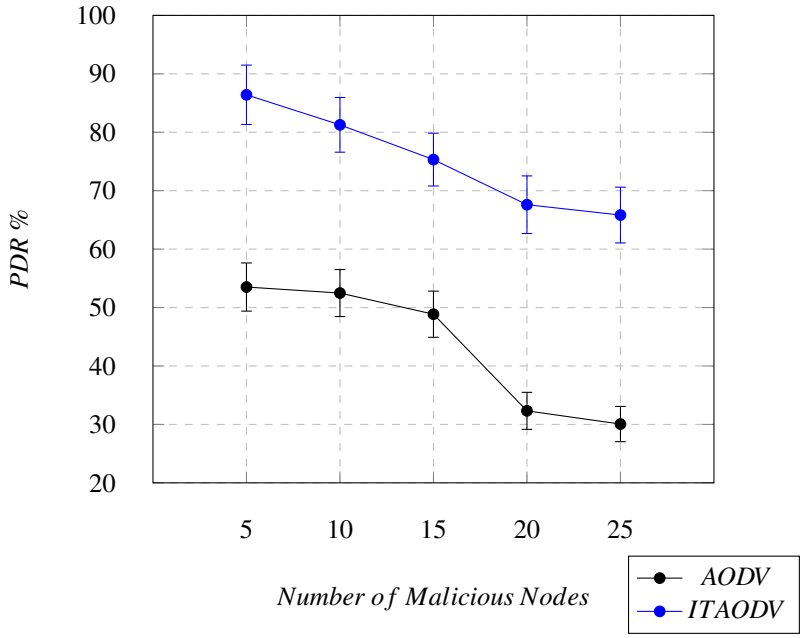

Figure 4.10 PDR vs. Number of Malicious Nodes with 95% Confidence Intervals

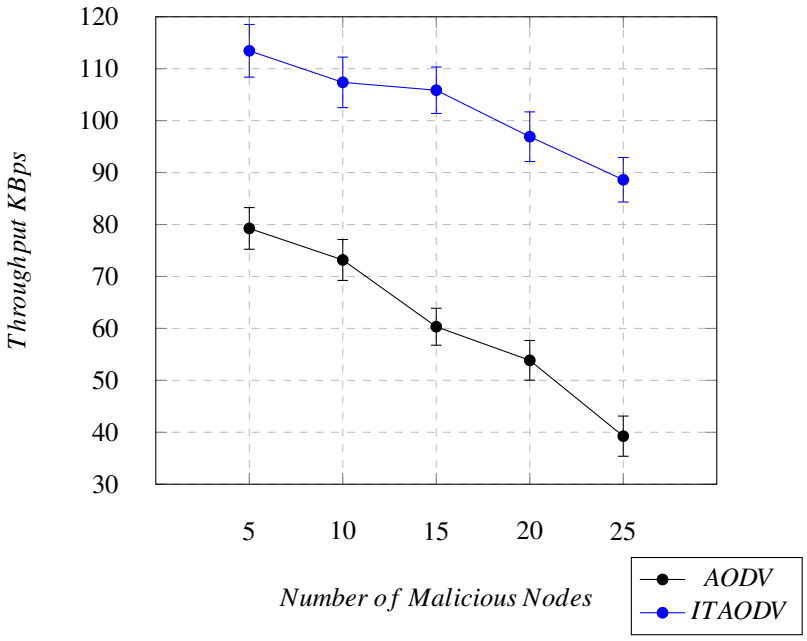

Figure 4.11 Throughput vs. Number of Malicious Nodes with 95% Confidence Intervals

4.3.3 Evaluating End-to-End Delay and Routing Overheads

Figures 4.12 and 4.13 show the comparison between the two routing protocols, AODV and ITAODV, in terms of end-to-end delay and routing overheads with the presence of varying numbers of malicious nodes in a wireless network.

Figure 4.12 shows that TAODV has a higher end-to-end delay than AODV in all cases. This can be attributed to the fact that ITAODV adds an extra layer of security checks that are not present in AODV. As the number of malicious nodes in the network increases, the end-to-end delay for both protocols also increases. However, the increase in delay is more pronounced for ITAODV than for AODV. This is because ITAODV has to perform more security checks in order to detect and isolate the malicious nodes, which adds to the overall delay.

The results shown in Figure 4.13 indicate that the routing overheads of both protocols increase with the number of malicious nodes. However, ITAODV has lower routing overheads compared to AODV in the presence of malicious nodes. The difference in routing overheads between AODV and ITAODV becomes more significant as the number of malicious nodes in the network increases. ITAODV is an indirect trust-based protocol that uses a trust model to avoid routing through malicious nodes, whereas AODV does not implement any security measures to avoid malicious nodes. The lower routing overheads of ITAODV can be attributed to its trust model, which enables it to avoid malicious nodes and thus reduces the number of control packets needed for route discovery and maintenance.

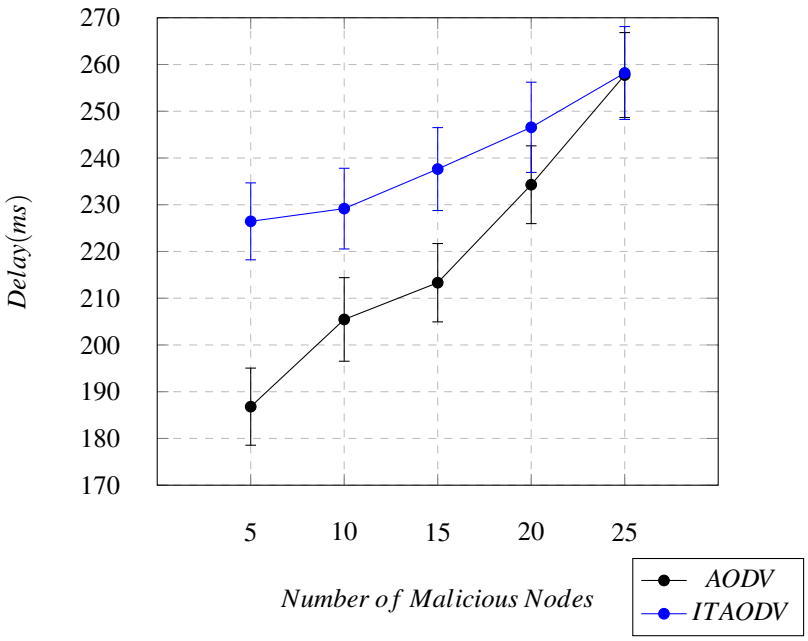

Figure 4.12 End-to-End Delay vs. Number of Nodes with 95% Confidence Intervals

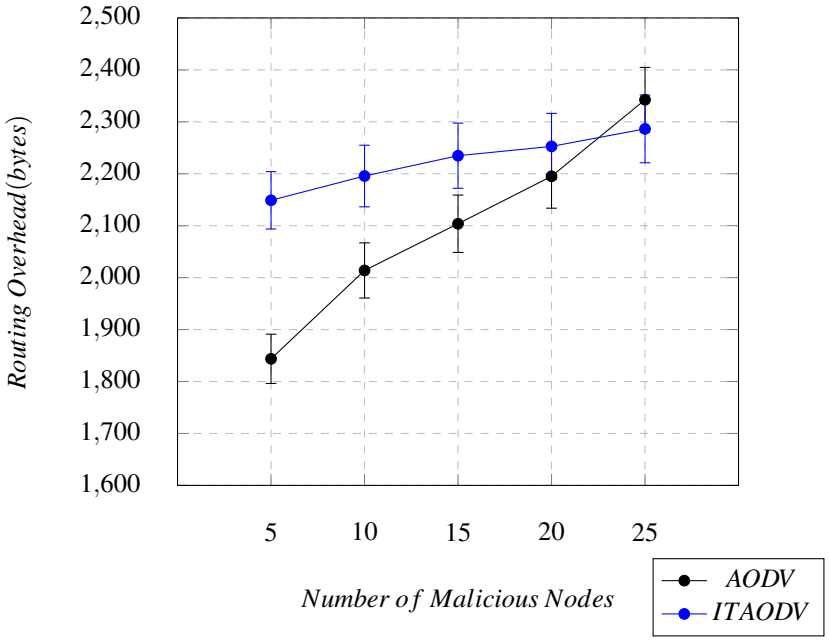

Figure 4.13 Routing Overhead vs. Number of Malicious Nodes with 95% Confidence Intervals

4.4 Summary and Discussion

This chapter has discussed the AODV protocol and the proposed ITAODV protocol, which is an extension of the AODV protocol that uses indirect trust mechanisms to improve the performance of the routing process in MANETs. The indirect trust mechanism is a method used in trust-based routing protocols for MANETs to establish trust relationships between nodes that have not directly communicated with each other. In indirect trust mechanisms, nodes gather trust information about other nodes from other trustworthy nodes in the network and use this information to make decisions about routing and forwarding packets [108]. Indirect trust mechanisms involve the exchange of recommendations or feedback between nodes about the behaviour of other nodes [4]. For example, a node may request recommendations from its neighbours about a particular node's behaviour and use this information along with its own evaluations to determine the trustworthiness of the target node. Alternatively, a node may assess the behaviour of its neighbours and use this information to infer the behaviour of other nodes in the network. ITAODV is designed to use different parameters such as packet forward rate, node battery power availability, battery drain rate, and congestion around a node in the calculation of another node's reliability. The calculated value of reliability is used to determine the trustworthiness of each node in the network, and then each node will share it with other nodes in the network.

Furthermore, the effectiveness of AODV and ITAODV protocols using the NS-3 simulator in various node mobility speed and density scenarios was assessed. Protocol performance was evaluated using several metrics, including PDR, throughput, end-to-end delay, and routing overheads. Based on the analysis of results, the ITAODV protocol exhibited superior performance compared to AODV in terms of both PDR and throughput in scenarios of increasing node mobility speed and density. However, AODV outperformed ITAODV in terms of the end-to-end delay and routing overhead metrics. This is considered to be a reasonable trade-off since ITAODV uses indirect trust mechanisms that require communication and calculations to ensure the usage of trusted nodes. At the same time, AODV employs the shortest path to transmit data packets.

Finally, the effect was investigated of a security threat and attack on the AODV and ITAODV protocols in order to test the efficiency of implementing indirect trust mechanisms in the AODV protocol. The black hole attack was used to examine the behaviour and effect of malicious nodes on AODV and ITAODV. The effect of the number of malicious nodes in the network was determined using the PDR, throughput, end-to-end delay, and routing overhead as metrics. The results show that ITAODV exhibits better performance than AODV in all performance metrics except end-to-end delay. Therefore, the study suggests that the implementation of an indirect trust mechanism in AODV has improved overall performance in the presence of network threats and attacks. The findings highlights the importance of trust mechanisms in enhancing the reliability and security of routing protocols in wireless networks.

Chapter 5

Global Trust Management in AODV Routing Protocol

The preceding chapter discussed the indirect trust management method and its incorporation into AODV, resulting in the ITAODV protocol. The performance of both AODV and ITAODV was then assessed under various scenarios, employing a range of performance metrics. Furthermore, the AODV and ITAODV protocols were analysed in the context of security challenges and attacks, specifically focusing on black hole attacks.

This chapter introduces the integration of the global trust management mechanism into the AODV protocol to improve its performance concerning security and efficiency. This modified version of AODV, which incorporates the global trust mechanism, is referred to as the GTAODV protocol. The chapter provides details of the global trust mechanism using the NS-3 simulator and compares the performance of AODV and GTAODV under different scenarios in terms of various metrics. Finally, the behaviour of AODV and GTAODV is investigated in the context of security threats, in this instance, using a black hole attack.

Moreover, this chapter includes a description of the use of direct and indirect trust mechanisms previously published [3, 4].

The chapter is organised in the following manner: Section 5.1 presents the proposed global trust management mechanism for the AODV protocol, and Section 5.2 discusses the performance assessment and analysis of AODV and GTAODV. In Section 5.3, the impact of a security threat on both AODV and GTAODV is then examined, along with a discussion of their performance in the presence of a security threat, specifically focusing on a black hole attack. Finally, Section 5.4 summarises the chapter.

5.1 Proposed Global Trust Management Mechanisms for AODV Protocol

5.1.1 Global Trust and Overview of Proposed Protocol

The global trust management mechanism in Mobile Ad-hoc Networks (MANETs) relies on a leader node. The leader node is a trusted node which is assigned a task to manage and maintain trust information for the entire network in addition to its regular functioning. This approach can help improve network security, reliability, and efficiency by centralising trust management and making informed routing decisions based on the trust values evaluated and distributed by the leader nodes.

GTAODV is an enhanced version of the AODV routing protocol, which incorporates global trust principles as the basis for routing choices. The global trust mechanism relies on a designated central or a leader node which computes trust values for each node participating in the network. Periodically, the leader node gathers reports from the participating nodes and processes them to determine the trust value of each node within the network. The leader node periodically distributes these trust values to all participating nodes. Each participating node uses these received global trust values to make routing decisions, the aim of which is to enhance the routing protocol's performance in terms of security, reliability, and efficiency.

Trust in this context is represented as a continuous value ranging between 0 and 1, where 0 signifies complete distrust, 1 indicates absolute trustworthiness, and 0.5 represents uncertainty about a node's behaviour. Using a continuous value to depict trust provides a more accurate representation of the inherent uncertainty associated with trust, as opposed to using a binary variable which could only express trust or distrust without considering varying degrees of trustworthiness.

To illustrate how the Global Trust AODV (GTAODV) works in practice, consider an example scenario where a group of mobile nodes forms a MANET for communication. In this example, the functioning of a Global Trust Ad-hoc On-Demand Distance Vector (GTAODV) is illustrated in a simple MANET environment consisting of 6 nodes (A, B, C, D, E, and F). Suppose node A wants to communicate with node F, and the GTAODV protocol is implemented in the network, with node A acting as the designated leader node that calculates global trust values.

1. Trust Initialisation:
   Initially, each node computes and maintains local trust values for its neighbours based on its own experiences. Node A, as the central node, collects reports from participating nodes and calculates global trust values for each node in the network. For simplicity, the following global trust values are assumed:

- Node A: B (0.7), C (0.8)
- Node B: A (0.7), D (0.6)
- Node C: A (0.8), D (0.9)
- Node D: B (0.6), C (0.9), E (0.5), F (0.4)
- Node E: D (0.5), F (0.8)
- Node F: D (0.4), E (0.8)

2. Route Discovery: When node A wants to communicate with node F, it initiates the route discovery process by broadcasting a Route Request (RREQ) message to its neighbours B and C. The RREQ message includes the destination node (F) and a trust threshold value, which is the minimum required global trust value for nodes to be considered for the route.

3. Global Trust-Based Routing: Upon receiving the RREQ message, nodes B and C check the trust threshold value against their global trust values for node F. In this example, the trust threshold value is assumed to be 0.6.

   - Node B forwards the RREQ message to its neighbour D, assuming its global trust value for node D (0.6).
   - Node C forwards the RREQ message to its neighbour D, assuming its global trust value for node D (0.9).

   Node D, upon receiving the RREQ message from both B and C, checks its global trust value for nodes E and F. Since the trust value for node F (0.4) is below the threshold, D forwards the RREQ message to node E (0.5).

4. Route Reply: Node E, upon receiving the RREQ message from node D, sends a Route Reply (RREP) message back to node A along the same path that the RREQ message traversed. In this case, the selected route is A -> C -> D -> E -> F.

5. Data Transmission and Trust Update: Node A can now send data packets to node F along the chosen route. As nodes in the network interact and exchange information, their local trust values are updated based on observed behaviour, such as successful packet forwarding or accurate routing information exchange. Node A, acting as the central node, periodically collects observation reports and updates global trust values accordingly.

This example demonstrates the basic functioning of the GTAODV protocol in a MANET. By incorporating global trust values into routing decisions, GTAODV can enhance the security, reliability, and efficiency of the network by selecting more trustworthy routes and avoiding potential malicious nodes.

5.1.2 Proposed Global Trust Mechanism in the AODV Protocol

The proposed method uses global trust to evaluate the reliability and credibility of nodes during the packet routing procedure. In the centralised global trust management approach, a designated central node collects observational data from participating nodes within the network. This data is indirect trust values about the other nodes, which are evaluated by the participating nodes. The indirect trust values are evaluated by combining recommendations given by the neighbouring nodes. The data received by the leader node is then processed using specific algorithms to compute the global trust value for each node in the network. Afterwards, the leader node distributes the calculated global trust values to all participating nodes periodically. Later the participating nodes use these global trust values to identify the most reliable route for transmitting packets from a source node to a destination node.

The following terminology and conventions are used during the rest of this chapter. The reliability of a node (r) signifies the probability that the node consistently provides dependable service during the packet routing process. Conversely, node unreliability (n) represents the likelihood that the packet routing service offered by the node is not reliable. Additionally, node uncertainty (u) refers to the probability that the node's reliability for packet routing cannot be definitively determined. These three values are collectively represented by the acronym (*rnu*), which stands for reliability, unreliability, and uncertainty. Direct observations are represented by *dt_rnu*, while indirect observations are indicated by *it_rnu*, and global observations are indicated by *gt_rnu*.

Each node calculates direct trust observations using various parameters. Then indirect trust measures are calculated by combining direct trust reports received from various neighbour nodes. Once the indirect (*rnu*) values are calculated using direct observations, each participating node sends the results to the designated leader node. The leader node calculates global trust values and distributes them to all participating nodes. In this way, the leader node contributes in making informed decisions about routing based on the trustworthiness and reliability of the nodes involved in the network. The objective of this method is to improve the security, efficiency, and overall performance of the packet routing process in the network.

The working of proposed Global Trust AODV (GTAODV) routing protocol is described in brief as follows:

- Each node participating in the network continuously and passively monitors its neighbouring node.
- Each node calculates direct trust dt_rnu_i of the neighbour node i using the above monitoring. This calculation is accomplished using Bayesian Inference, the details of which are explained in Section 5.1.3.
- At regular intervals, each node periodically sends dt_rnu_i values to all neighbouring nodes i.
- Every node synthesises received observations and calculates it_rnu_i. Here it_rnu_i is the node's reliability, unreliability and uncertainty, which is calculated using direct and indirect observations. This calculation is conducted using the weighted average method, the details of which are explained in Section 5.1.4.
- At regular intervals, each node periodically sends it_rnu_i values for all neighbour nodes to the leader node.
- The leader node synthesises the reports received and calculates gt_rnu_i for each node i. This synthesis is performed using Dempster–Shafer Theory (DST), the details of which are explained in Section 5.1.5.
- At periodic intervals, the leader node transmits computed gt_rnu_i values to all nodes participating in the network.
- Each node participating in the network uses global trust values sent by the leader node in choosing a reliable and optimal route to the destination. The details of this process are as explained in Section 5.1.6.

5.1.3 Calculation of a Node's *rnu* using Direct Observations (dt_rnu_i)

In order to calculate direct trust, each node in the network monitors its neighbouring nodes for specific events that indicate their packet forwarding reliability. These are recorded as either positive (α) or negative (β) observations concerning the neighbouring node. Bayesian Inference is subsequently applied to compute values of reliability and trustworthiness for each neighbouring node. Bayesian Inference is a statistical technique that utilises Bayes' theorem to update the probability of a hypothesis as additional evidence, or when further information becomes available [90]. Table 5.1 displays the parameters used for node monitoring.

Table 5.1 Trust Observation Parameters

Sr.	Observation Parameter	Frequency of Recording the Observation	Positive Observation (α)	Negative Observation (β)
1	Packet forwarding ability	For each observed data packet	α++ for each data packet forward	β++ for each data packet drop
2	Node Battery	At beginning of a new data transmission session	α++ if node's Battery Power > MBT	β++ if node's Battery Power <= MBT
3	Node's participation in network routing activities	For each observed RREP packet	α++ for the node which initiated control packet	β++ for the node which dropped a control packet. Also, β++ for a node caused a route error.
4	Node's packet forwarding queue capacity	At beginning of a new data transmission session	α++ if more than MEQ of queue capacity is empty	β++ if available queue capacity is less than equal to MEQ

Due to the fact that only two parameters in Table 5.1 are taken into consideration, the Beta distribution function is chosen in modelling the behaviour of the nodes. Let x and y be two neighbouring nodes in the network, and node textitx has made a total of textitn reports about node textity. Let T_{new} represents the likelihood that node y will exhibit positive behaviour at time $n+1$. The posterior distribution of successful collaboration between nodes x and y can then be depicted by a Beta distribution function, with the density function provided in Equation 5.1:

$$Beta(T_{old}|\alpha,\beta) = \frac{\tau(\alpha+\beta+2)}{\tau(\alpha+1)\tau(\beta+1)} T_{old}^{\alpha}(1-T_{old})^{\beta} \tag{5.1}$$

In this Equation, T_{old} is the old value of trust of node x on y. Then an updated value of trust T_{new} is calculated as follows:

$$T_{new} = E(Beta(T_{old}|\alpha,\beta)) = \frac{\alpha}{\alpha+\beta} \tag{5.2}$$

Using Equation 5.2 and taking into consideration the level of uncertainty u, direct node reliability (dt_r) is calculated using Equation 5.3:

$$dt\_r = \frac{\alpha}{\alpha+\beta}(1-u) \tag{5.3}$$

Using Equation 5.2 and taking into consideration the level of uncertainty, direct node unreliability expectation (dt_n) is calculated using Equation 5.4:

$$dt\_n = \frac{\beta}{\alpha+\beta}(1-u) \tag{5.4}$$

Here the direct node uncertainty (dt_u) is calculated using Equation 5.5:

$$dt\_u = \frac{12\alpha\beta}{(\alpha+\beta)^2(\alpha+\beta+1)} \tag{5.5}$$

The value of dt_rnu_i represents the combined reliability, unreliability, and uncertainty of node i calculated using direct monitoring.

5.1.4 Calculation of a Node's *rnu* using Indirect Observations (it_rnu_i)

The nodes in the network continually exchange their direct trust reports about the reliability of neighbouring nodes. Indirect trust is calculated by combining these direct trust reports, which are communicated by the neighbouring nodes. Here, each node disseminates calculated dt_rnu_i values to all neighbouring nodes at regular intervals. Upon reception, each node processes these reports and synthesises them to calculate its indirect trust (it_rnu_i) values which represent the node's reliability, unreliability, and uncertainty. These values are derived from both direct and indirect reports and are calculated using a weighted average method. Equation 5.6 shows the calculation of node reliability using indirect reports (it_r_i), while Equation 5.7 shows the calculation of node unreliability using indirect reports (it_n_i). Then, Equation 5.8 illustrates the calculation of node uncertainty using indirect reports (it_u_i).

$$it\_r_i = \frac{\sum_{0<j<=N} r_{ji} * w_j}{W} \tag{5.6}$$

$$it\_n_i = \frac{\sum_{0<j<=N} n_{ji} * w_j}{W} \tag{5.7}$$

$$it\_u_i = 1 - (it\_r_i + it\_n_i) \tag{5.8}$$

where N is number of nodes in the network, r_{ji} is the indirect reliability of node i which is reported by node j, n_{ji} is the indirect unreliability of node i which is reported by node j. w_j is the weight assigned to node j depending on past interactions and W is the cumulative weight. The value of w_j is calculated using the following Equations 5.9-5.11:

$$\alpha\_sum_j = \sum_{i=1}^{N} \alpha_{i,j} \tag{5.9}$$

$$\beta\_sum_j = \sum_{i=1}^{N} \beta_{i,j} \tag{5.10}$$

$$w_j = \sum_{j=1}^{N} \alpha\_sum_j + \beta\_sum_j \tag{5.11}$$

where $\alpha_{i,j}$ is the value of α reported by node i about node j and $\beta_{i,j}$ is the value of β reported by node i about node j.

5.1.5 Calculation of a Node's *rnu* using Global Trust Observations (gt_rnu_i)

The leader node collects it_rnu_i reports from all participating nodes in the network. Then these observations are synthesised and gt_rnu_i is calculated using Dempster-Shafer Theory (DST). The leader node uses DST to synthesise the evidence received from different nodes in the network.

Let

r_1(i)= basic probability value indicating node 1's reliability value for a target node i;
r_2(i) = basic probability value indicating node 2's value of reliability for the target node i;
n_1(i)= basic probability value indicating node 1's unreliability value for a target node i;
n_2(i) = basic probability value indicating node 2's unreliability value for the target node i;
u_1(i)= basic probability value indicating node 1's uncertainty value for a target node i;
u_2(i) = basic probability value indicating node 2's uncertainty value for the target node i.

The updated values of reliability, unreliability and uncertainty for target node i, which are calculated using the above terms and Dempster–Shafer theory (DST) are as follows:

$$\text{gt\_r}_i = \text{r}_1(i) \oplus \text{r}_2(i) = \frac{1}{C}\{r_1(i) * r_2(i) + r_1(i) * r_2(u) + r_1(u) * r_2(i)\} \tag{5.12}$$

$$\text{gt\_n}_i = \text{n}_1(i) \oplus \text{n}_2(i) = \frac{1}{C}\{n_1(i) * n_2(i) + n_1(i) * n_2(u) + n_1(u) * n_2(i)\} \tag{5.13}$$

$$\text{gt\_u}_i = \text{u}_1(i) \oplus \text{u}_2(i) = \frac{1}{C}\{u_1(i) * u_2(i)\} \tag{5.14}$$

where $\text{C} = \text{r}_1(i) * r_2(i) + r_1(i) * u_2(i) + u_1(i) * r_2(i) + n_1(i) * n_2(i) + n_1(i) * u_2(i) + u_1(i) * n_2(i) + u_1(i) * u_2(i)$

5.1.6 Integration of Global Trust in the AODV Protocol

In the proposed method, direct, indirect, and global trust mechanisms are integrated into the Ad-hoc On-Demand Distance Vector (AODV) protocol. The modified AODV protocol is referred to as Global Trust AODV (GTAODV). The process of making routing decisions in GTAODV is explained next.

In the proposed GTAODV routing protocol, a node's ability to provide a reliable packet routing service is represented by r, which denotes the probability of a dependable packet service offered by a node. Conversely, the probability that a node's packet routing service is not reliable is termed as its unreliability, n. Additionally, the likelihood that the node's reliability in packet routing cannot be predicted is referred to as node uncertainty, u. These three values collectively constitute the *rnu* (reliability, unreliability, and uncertainty) metric. This metric includes node reliability, unreliability, and uncertainty and is computed by each node participating in the network using a weighted average method taking into consideration both direct and indirect observations.

In order to determine the *rnu* values of neighbouring nodes, each node continuously observes the values of α_i and β_i for every neighbouring node i. Each node computes the direct trust dt_rnu_i for neighbouring node i using its α_i and β_i values. At periodic intervals, each node transmits computed dt_rnu_i values to all of its neighbouring nodes. Each node combines the received direct trust reports (dt_rnu_i) and computes a value of indirect trust it_rnu_i for each node in the network. Again at periodic intervals, each node also transmits computed it_rnu_i values to the leader node. The leader node synthesises the received indirect trust reports (it_rnu_i) and computes a value of global trust gt_rnu_i for each node in the network. At periodic intervals, the leader node then transmits computed gt_rnu_i values to all nodes participating in the network.

The AODV protocol uses hop count as a metric for routing decisions, which is suitable for reliable networks with trustworthy nodes. However, the protocol is vulnerable to many unique attacks, such as the black hole attack. Therefore, to overcome this issue, the Global Trust AODV (GTAODV) protocol is proposed as a modification to the AODV protocol so as to overcome vulnerability issues and enhance the performance of the protocol under different conditions. In GTAODV, each node uses reliability values computed and distributed by the leader node in making routing decisions. Here, the central node computes a reliability value for each node in the network by synthesising indirect trust reports received from participating nodes. A node with the highest reliability value that is closer to the destination is preferred as the node to forward the next packet to. This method enhances the security and efficiency of the routing protocol compared to the default AODV protocol.

$$Trust\_value_i = \frac{\rho}{\text{No. of Hops to Destination}} + (1-\rho) * Node\ Reliability\ Value\ (gt\_r_i) \tag{5.15}$$

As in Chapters 4 and 5, various values of ρ were used to assign varying weights: firstly to hop count from a source node to the destination node; and secondly to node reliability. The aim of this process is to optimise the performance of the trust mechanism and to identify the best performance scenario. The results of this experimentation led to the conclusion that the optimal weightings to be used in the modification of the standard AODV protocol are 70% for node reliability and 30% for hop count. Consequently, in this chapter, ρ is set to 0.30, which signifies that a weight of 70% is assigned to node reliability, and a weight of 30% is assigned to hop count. Finally, this mechanism was implemented in AODV, which then becomes the Global Trust AODV (GTAODV) protocol. The GTAODV protocol employs a technique where a packet is forwarded from a source node to a destination node through a neighbouring node that has the highest trust value. This mechanism ensures that the packet is routed through a maximally reliable node, which improves the security and efficiency of the network. By using trust values to determine the node the packet is forwarded to, the GTAODV protocol can guard against attacks such as a black hole attack as well as other security threats.

5.2 Performance Evaluation and Analysis

A performance evaluation allows the AODV and GTAODV to be subjected to a systematic comparison in terms of their efficiency and effectiveness in a variety of network conditions. This assessment can provide insights into the performance of each protocol in terms of routing overheads, end-to-end delay, packet delivery ratio, and throughput. In addition, the evaluation of GTAODV is crucial if an understanding of the impact of incorporating trust mechanisms into the standard AODV protocol is to be achieved. The objectives of the evaluation include an analysis of how trust-based routing decisions affect network performance and security, as well as determining the effectiveness of the use of trust. Finally, a key objective of the performance evaluation of the two protocols is to determine their scalability in the context of different node mobility speeds and a variety of numbers of nodes in the network. By comparing their performance in these diverse network conditions, the limits and challenges associated with each protocol can be identified and potential improvements proposed.

Experiments were carried out using the NS-3 simulator to compare the performance of the AODV and GTAODV protocols. The performance metrics employed include

packet delivery ratio (PDR), throughput, end-to-end delay, and routing overheads. The performance of both protocols was assessed for two distinct testing scenarios where the speed of node movement and then the density of nodes within the network were varied. Comprehensive information on these testing conditions and the corresponding results are provided in the following sections.

5.2.1 Performance Evaluation when Varying Node Movement Speed

The primary aim of performance evaluation when varying node movement speed in AODV and Global Trust AODV (GTAODV) is to understand how these routing protocols react to different mobility scenarios and the resulting network dynamics. The results of this evaluation will help to identify the strengths and weaknesses of the protocols and guide future research and development to enhance their performance, security, and adaptability in MANETs. Moreover, an analysis of the performance of AODV and GTAODV at varying node movement speeds can provide insights into the behaviour of the protocols, including how they react to rapid changes in network topology, maintain routes, and adapt to different network conditions.

Hence, the assessment of the performance of these protocols in diverse mobility scenarios is crucial for the most suitable choice for a specific network to be identified. Table 5.2 outlines the simulation parameters that remain constant during the evaluation process. In order to ensure the reliability of the results, each simulation was executed ten times and the average performance values computed and 95% confidence intervals were also determined to enhance the credibility of the findings. The simulations were carried out to explore the influence of node mobility on the network and to evaluate the effectiveness of the protocols in various mobility situations ranging from 10 m/s to 50 m/s. The assessment metrics employed in this research are packet delivery ratio, throughput, routing overheads, and end-to-end delay. The Network Simulator version 3 (NS-3.33) served as the simulation tool for this study.

Table 5.2 Global Trust Simulation Parameters

Routing protocols	AODV, GTAODV
Packet Size	512 *Bytes*
Simulation Time	360 *Seconds*
Simulation Area	1000 * 1000 m^2
Number of Nodes	20
Node Movement Speed	10,20,30,40,50 *m/s*
Node Movement	Random Way Point
MAC Protocol	IEEE 802.11b
Transmission Range	250 *Meter*
Number of Simulation Runs	10
Confidence Interval	95%
Traffic Type	UDP

5.2.1.1 Packet Delivery Ratio and Throughput Versus Node Movement Speed

Figures 5.1 and 5.2 show that, as the node movement speed increases, the PDR and throughput for both protocols decrease due to more frequent breaks in links between nodes and increased numbers of route discoveries and dropped packets. The higher likelihood of links breaking between nodes forces both AODV and GTAODV to more frequently rediscover routes, which can result in higher numbers of dropped packets and lower PDR. More frequent link breaks can thus lead to more time spent on route discovery and maintenance, reducing the time available for actual data transmission and thereby decreasing throughput. Furthermore, at higher node movement speeds, the stability of the routes which are discovered decreases for both AODV and GTAODV. This may again lead to more frequent route breaks and packet drops, resulting in lower PDR. However, GTAODV has higher PDR and throughput compared to AODV, since it takes into account trust metrics during route discovery and maintenance which helps in the selection of more reliable and stable routes. The better route stability of GTAODV compared to AODV due to the trust-based mechanism means that routes are more likely to be selected which involve nodes with a higher likelihood of maintaining connectivity.

Figures 5.1 and 5.2 illustrate the correlation between node mobility speed and the PDR and throughput metrics. The performance of GTAODV is better than AODV in regards to PDR and throughput even as node mobility speed increases. Figure 5.1 shows that GTAODV has a highly stable PDR with a percentage of no less than 90% at all node movement speeds. On the other hand, the AODV protocol exhibits a dramatic decrease in PDR from 91.11% to 77.71% as the mobility speed increase from 10 metres to 50 metres. Figure 5.2 shows the throughput for the GTAODV and AODV protocols. GTAODV has a very high throughput in the range of 153.82 KBps to 147.34 KBps with stable performance

as the node movement speed increases. On the other hand, the AODV protocol has a very low throughput in a range from 76.70 KBps to 68.74 KBps.

In summary, as node movement speed increases, PDR and throughput for both AODV and GTAODV decline, but GTAODV consistently outperforms AODV. The difference in PDR between the two protocols ranges from 5.25% to 13.33%, with GTAODV providing better and more consistent performance. This can be attributed to the trust mechanism in GTAODV that allows for the selection of more reliable and stable routes.

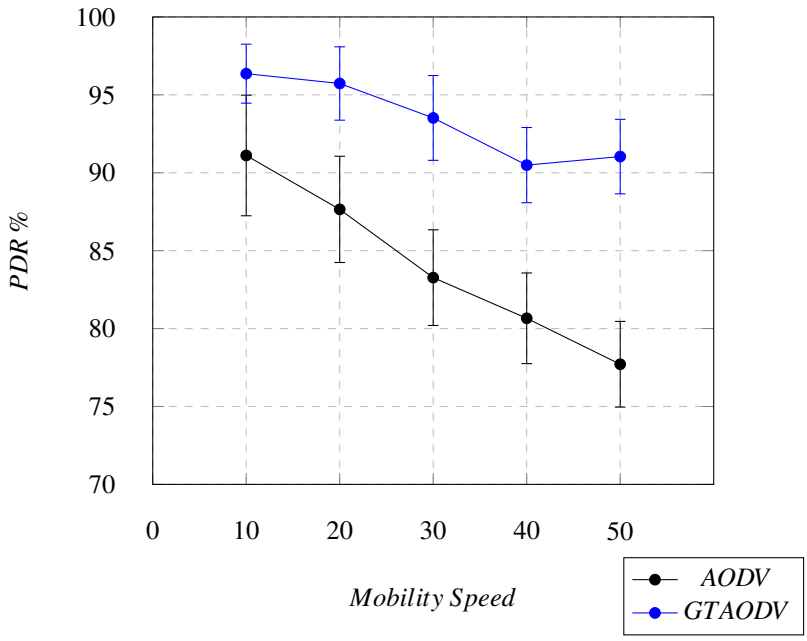

Figure 5.1 PDR vs. Node Movement Speed with 95% Confidence Intervals

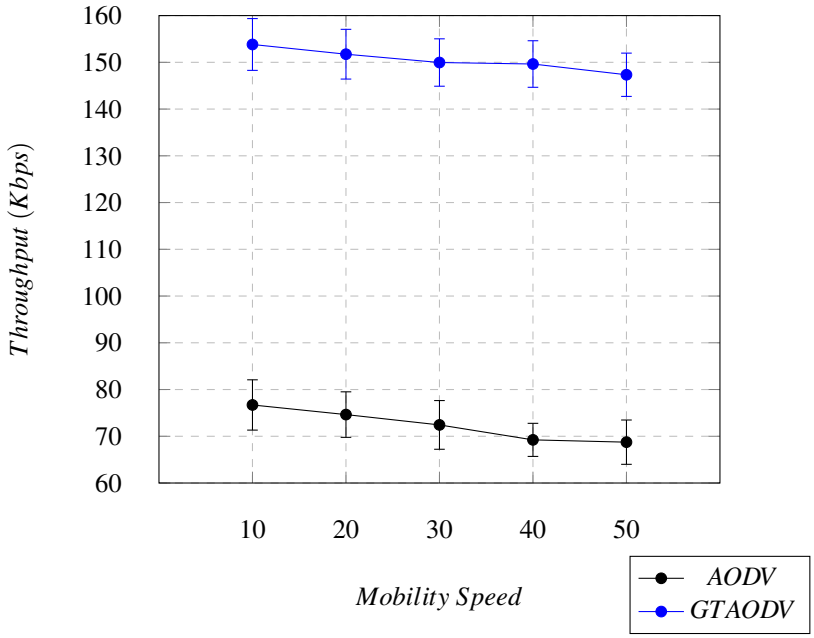

Figure 5.2 Throughput vs. Node Movement Speed with 95% Confidence Intervals

5.2.1.2 End-to-End Delay and Routing Overheads Versus Node Mobility Speed

Figures 5.3 and 5.4 show performance in terms of end-to-end delay and routing overheads for the AODV and GTAODV protocols as the node movement speed increases. From Figure 5.3 it can be seen that, as node movement speed increases, the end-to-end delay for both AODV and GTAODV increases. This is expected since higher movement speeds result in more frequent link breaks and route discoveries, which contribute to the overall delay. Nevertheless, GTAODV consistently has higher end-to-end delays compared to AODV across all node movement speeds. This can be attributed to the additional processing overheads introduced by the operation of the trust mechanism in GTAODV.

From Figure 5.4 it is clear that, as node mobility speed increases, the routing overheads for both AODV and GTAODV protocols also increase. This is due to the increased frequency of route breakages due to faster movements of the nodes which increases frequency of route maintenance operations. For AODV, the routing overheads increase moderately as node mobility speed increases due to conventional route discovery and maintenance mechanisms. On the other hand, for GTAODV, the routing overheads increase more significantly because of the additional overheads introduced by the trust mechanism. Indirect trust and Global trust mechanisms use additional control packets for its functioning. Trust-based route selection and maintenance require more control packets, which increases the overall routing overheads. Due to this higher increase in routing overhead is observed in GTAODV as compared with AODV.

In summary, although GTAODV has better PDR and throughput performance than AODV, as shown in Figures 5.1 and 5.2, this comes at the cost of increased end-to-end delays and routing overheads as shown in Figures 5.3 and 5.4.

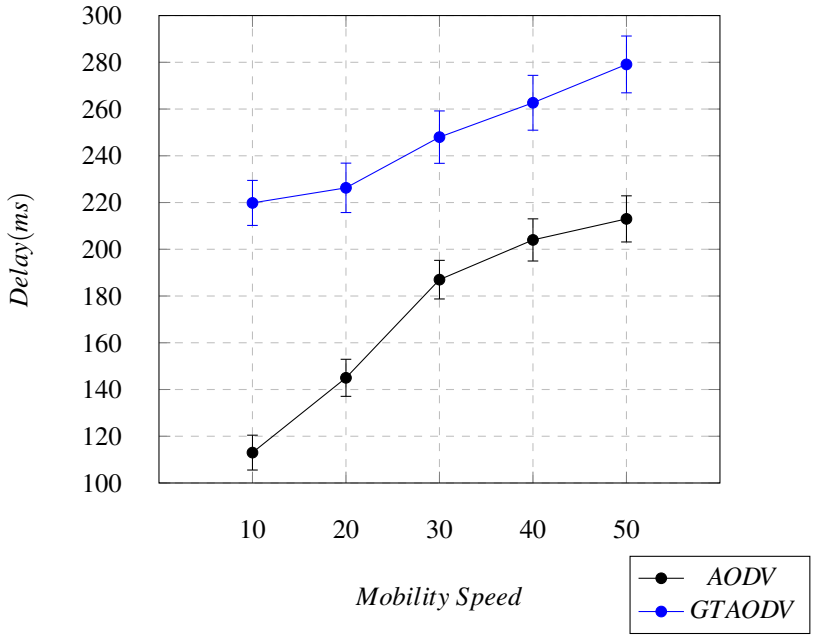

Figure 5.3 End-to-End Delay vs. Mobility Speed with 95% Confidence Intervals

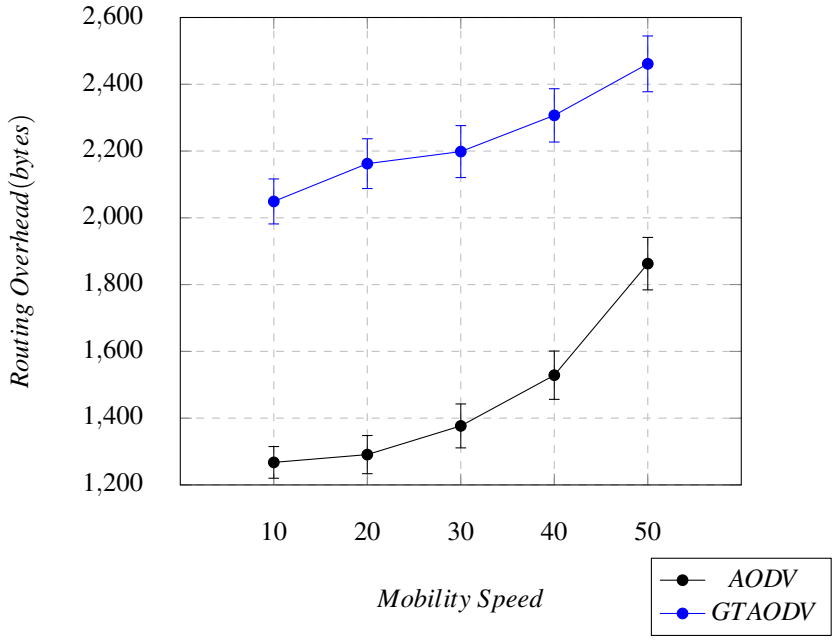

Figure 5.4 Routing Overheads vs. Mobility Speed with 95% Confidence Intervals

5.2.2 Performance Evaluation when Varying Node Density

In order to evaluate the efficacy of the AODV and GTAODV protocols, a series of simulations were conducted with varying numbers of nodes in the network while other simulation conditions were kept constant, as defined in Table 5.3. The analysis of the performance of these protocols at different node densities helps in assessing their scalability, and it is crucial to understand how these protocols can cope with increasing network size and whether or not their performance is degraded significantly as the number of nodes increases. Moreover, varying node density enables an examination of the efficiency of route discovery and maintenance as well as the mechanisms of trust evaluation in both AODV and GTAODV. A comparison of their performance helps in identifying their strengths and weaknesses and provides insights into the potential for further improvements and the optimisation of these protocols.

In order to maintain the precision and statistical significance of the outcomes, the simulations were performed ten times for every node count and the average value was determined. Additionally, 95% confidence intervals were calculated so as to offer a degree of certainty and trust in the results. The performance of the protocols was evaluated using the key metrics of packet delivery ratio, throughput, routing overheads, and end-to-end delay, in order to attain a thorough comprehension of their performance in diverse network situations.

Table 5.3 Simulation Parameters for Varying Node Density

Routing protocols	***AODV, GTAODV***
Packet Size	512 *Bytes*
Simulation Time	360 *Seconds*
Simulation Area	1000 * 1000 m^2
Number of Nodes	20,40,60,80,100
Node Movement Speed	5 *m/s*
Node Movement	Random Way Point
MAC Protocol	IEEE 802.11b
Transmission Range	250 *Meter*
Number of Simulation Runs	10
Confidence Interval	95%
Traffic Type	UDP

5.2.2.1 Packet Delivery Ratio and Throughput Versus Node Density

Figures 5.5 and 5.6 present the performance comparison of AODV and GTAODV protocols based on packet delivery ratio (PDR) and throughput as the number of nodes in the network increases. The results are displayed with 95% confidence intervals to provide assurance in the findings. Figure 5.5 shows how the PDR performance of the AODV and GTAODV

protocols changes as the number of nodes in the network increases from 20 to 100. The PDR of AODV increases from 78.48% to 86.47%, while that of GTAODV remains consistently high, ranging from 94.18% to 97.26%. The results show that GTAODV consistently outperforms AODV in terms of PDR across different node densities, indicating its higher reliability and robustness in delivering packets. Figure 5.6 presents the comparison of the throughput performance of AODV and GTAODV as the number of nodes in the network varies from 20 to 100. The throughput of AODV decreases from 85.57 KBps to 75.85 KBps, while that of GTAODV remains relatively stable, ranging from 154.65 KBps to 149.64 KBps. GTAODV demonstrates significantly higher throughput performance than AODV across all node densities, indicating its superior efficiency in the utilisation of network resources and delivery of data

In summary, with the GTAODV protocol, as the number of nodes in the network increases, there is a higher likelihood of multiple trusted paths between the source and the destination. This redundancy can lead to improved PDR and throughput since the leader node in the GTAODV protocol has more options in the selection of a suitable path. Therefore, in the case of a link failure, an alternative path can be quickly established. Also, GTAODV uses the global trust mechanism explained earlier and, as the number of nodes increases, there is a higher possibility of load balancing across multiple paths [109]. Load balancing can help to alleviate congestion and reduce packet losses, leading to an increase in PDR and throughput [110].

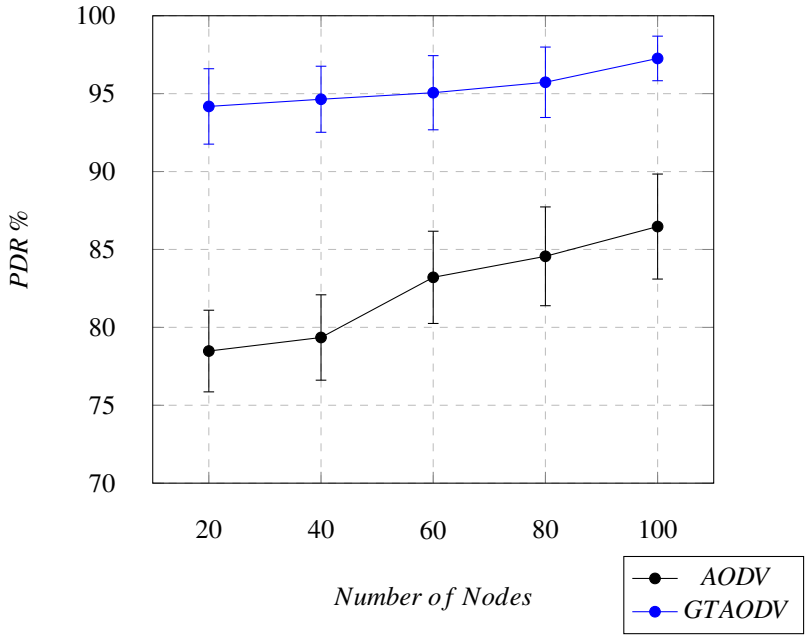

Figure 5.5 PDR vs. Number of Nodes with 95% Confidence Intervals

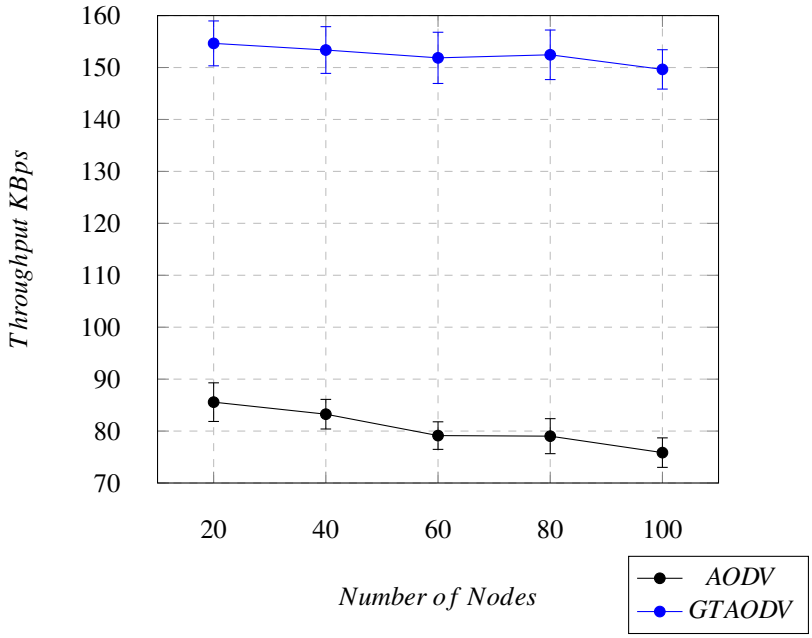

Figure 5.6 Throughput vs. Number of Nodes with 95% Confidence Intervals

5.2.2.2 End-to-End Delay and Routing Overheads Versus Node Density

Figures 5.7 and 5.8 illustrate the relationship between the end-to-end delay and routing overheads metrics with the increase in the number of nodes in the network. The overall performance of GTAODV and AODV is impacted negatively by the increase in the number of nodes in the network in terms of end-to-end delay and routing overheads. As shown in Figure 5.7, the end-to-end delay in AODV increases with the number of nodes. This can be attributed to the presence of more alternate paths in denser networks, which reduces the average distance between nodes and results in shorter hops between them. Consequently, the transmission time and the chances of packet loss, collisions, and interference are reduced. However, beyond a certain point, the network may become congested, causing an increase in end-to-end delay. Meanwhile, in the case of GTAODV, the end-to-end delay also increases as the node density grows. The trust-based mechanisms in GTAODV contribute to this trend because this protocol leads to the avoidance of malicious or poorly performing nodes, thereby establishing more reliable paths. This reduces the likelihood of retransmissions and delays caused by extra route discovery or link failures. However, as with AODV, network congestion may arise in highly dense networks, thus leading to increased end-to-end delay.

From Figure 5.8, the routing overheads for the AODV protocol exhibit a rising trend as node density increases. This is a result of the higher number of nodes, which leads to a greater frequency of route discovery and route maintenance messages, thereby increasing the overheads. Nevertheless, the presence of more alternate paths and improved spatial

reuse in denser networks can potentially reduce the number of route discovery attempts and the overall routing overheads. On the other hand, in the GTAODV protocol, routing overheads also increase with node density. While the trust-based mechanisms in GTAODV contribute to this increase by necessitating the exchange and processing of trust information, they can also help to establish more reliable paths. This may, in turn, reduce the frequency of route discoveries and maintenance, offsetting the overheads caused by the exchange of trust information. The net impact on routing overheads is dependent on the network conditions and the efficiency of the trust-based mechanisms in GTAODV.

In summary, the end-to-end delay and routing overheads in both AODV and GTAODV are significantly influenced by node density. The impact of node density on these performance metrics is complex and contingent upon various factors, including network congestion, path redundancy, spatial reuse, and the efficiency of the trust-based mechanisms in GTAODV. The figures illustrate these trends and demonstrate the importance of taking into account node density when evaluating the performance of routing protocols in mobile ad-hoc networks.

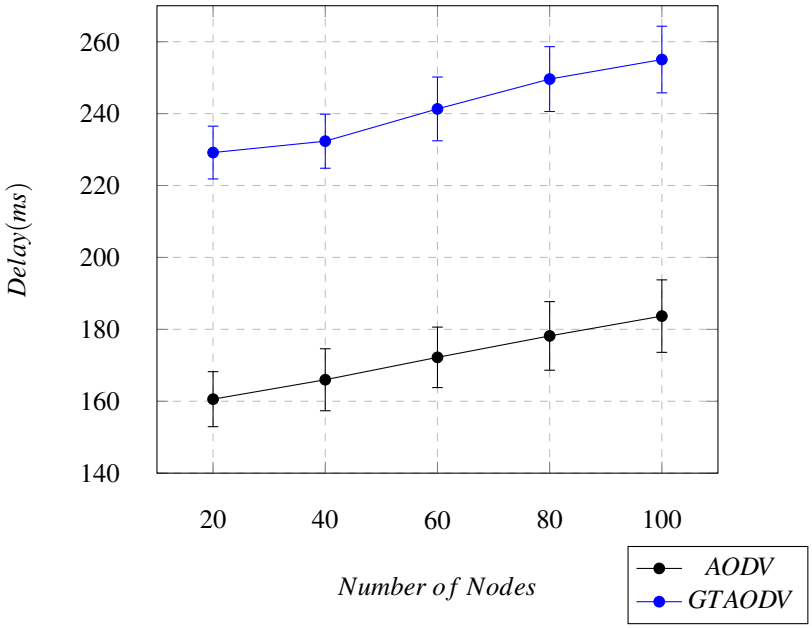

Figure 5.7 End-to-End Delay vs. Number of Nodes with 95% Confidence Intervals

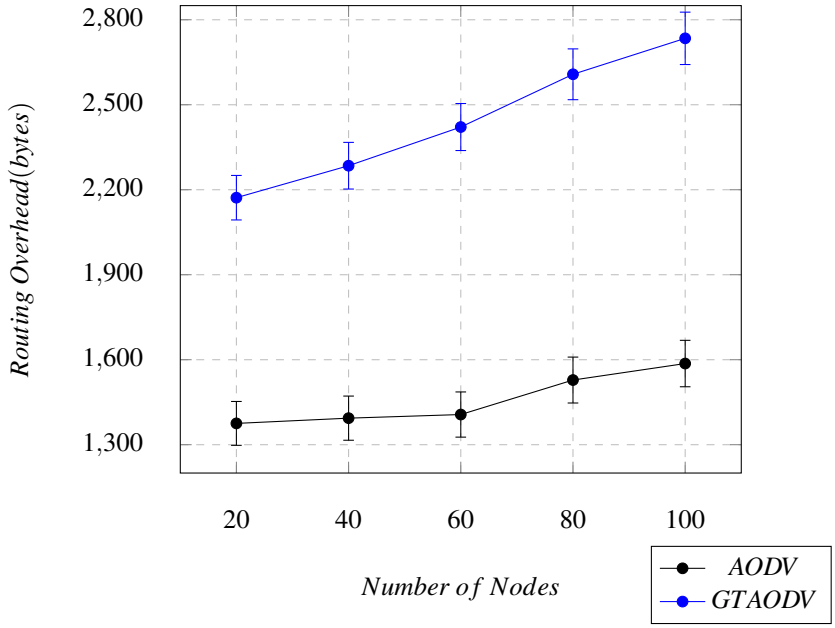

Figure 5.8 Routing Overheads vs. Number of Nodes with 95% Confidence Intervals

5.3 Performance Evaluation of AODV and GTAODV in the Presence of a Black hole Attack

A black hole attack is a type of network security breach in which a malicious node disrupts the normal functioning of a routing protocol by falsely claiming to have the shortest path to the destination [111]. This attack is particularly common in MANETs using the AODV routing protocol due to its automatic reliance on the trustworthiness of nodes, which makes it more vulnerable to such attacks [112].

An investigation of the impact of a security threat, in this case, a black hole attack, on the AODV and GTAODV protocols is essential for several reasons. Firstly, MANETs are inherently vulnerable to security threats due to their dynamic topology, lack of centralised infrastructure, and reliance on cooperative behaviour among nodes [5]. As a widely-used routing protocol in MANETs, AODV is particularly susceptible to black hole attacks [112]. An understanding of the impact of black hole attacks on AODV will help in identifying security weaknesses to allow the design of better countermeasures to mitigate such attacks. Moreover, GTAODV is an enhanced version of the AODV protocol that incorporates centralised trust-based mechanisms in order to improve the security of the routing process. The evaluation of the impact of black hole attacks on GTAODV helps in the assessment of the effectiveness of these trust-based mechanisms in detecting and isolating malicious nodes and, subsequently, preventing an attack from compromising the network.

Finally, a comparison of the performance of AODV and GTAODV in the presence of black hole attacks can reveal the advantages and disadvantages of each protocol. An understanding of how these attacks affect various performance metrics such as packet delivery ratio, throughput, end-to-end delay, and routing overheads can help network designers and administrators make informed decisions in the selection of the most suitable routing protocol for their specific network requirements.

5.3.1 Experimental Set-up

This section explains the set-up which provided a comprehensive and controlled environment in which to assess the performance and robustness of the AODV and GTAODV routing protocols under varying conditions where malicious nodes were executing black hole attacks. The parameters listed in Table 5.4 were chosen in the simulation of a realistic and complex wireless ad-hoc network environment.

The simulations were run multiple times with different numbers of malicious nodes so as to examine the impact of the attack on overall network performance. The results can be used to determine which routing protocol is more resilient against black hole attacks and may help inform future protocol improvements or network configurations aiming to more effectively mitigate the effects of such attacks.

The use of 95% Confidence Intervals enhances the results of the analysis, providing a clear understanding of the differences between the two protocols under the conditions described. By using UDP traffic, the simulations focus on the routing aspects of the protocols without the added complexity of managing connections and error handling such as are found when other transport layer protocols like TCP are used.

To summarise, this experimental set-up reflects a structured and detailed approach to the evaluation of the performance of the AODV and GTAODV routing protocols dealing with black hole attacks. The findings allow for a better understanding of their strengths and weaknesses and contribute valuable insights which will be useful in future research and development in the field of wireless ad-hoc network security.

Table 5.4 Simulation Parameters

Routing protocols	***AODV, GTAODV***
Type of Threat	***Black hole Attack***
Packet Size	512 *Bytes*
Simulation Time	360 *Seconds*
Simulation Area	1000 * 1000 m^2
Number of Nodes	100
Number of Malicious Nodes	5,10,15,20,25
Node Movement Speed	10 *m/s*
Node Movement	Random Way Point
MAC Protocol	IEEE 802.11b
Transmission Range	250 *Meter*
Number of Simulation Runs	10
Confidence Interval	95%
Traffic Type	UDP

5.3.2 Evaluation of Packet Delivery Ratio and Throughput when Varying the Number of Malicious Nodes

The performance results for the AODV and GTAODV routing protocols in the presence of black hole attacks can be seen in Figures 5.9 and 5.10, which provide valuable insights into the robustness and efficiency of the protocols when faced with an increasing number of malicious nodes in the network.

Figure 5.9 depicts PDR as a function of the number of malicious nodes in the network, and compares the performance of the AODV and GTAODV routing protocols. PDR is shown with 95% Confidence Intervals for both protocols. The AODV protocol exhibits a significant decline in PDR as the number of malicious nodes increases. This degradation in performance can be attributed to the lack of an effective mechanism to identify and avoid malicious nodes, leading to more dropped or lost packets [113]. On the other hand, GTAODV maintains a relatively high PDR despite the increasing number of malicious nodes. This can be attributed to the trust-based mechanism incorporated in GTAODV, which allows the protocol to assess the trustworthiness of nodes based on the monitoring of the parameters mentioned above. By identifying and avoiding malicious or less reliable nodes, GTAODV can maintain a higher PDR, thus ensuring more efficient and reliable data transmission.

Moreover, as shown in Figure 5.9, the PDR for AODV with 5 malicious nodes is 53.51% with a confidence interval of ±4.12%. This means that we can be 95% confident that the true PDR value for AODV in this scenario lies between 49.39% and 57.63%. In contrast, the PDR for GTAODV is 91.21% with a confidence interval of ±3.08%, indicating

a range of 88.13% to 94.29%. As the number of malicious nodes increases to 25, the PDR for AODV drops to 30.06% (±3.017%), while the decline for GTAODV is only relatively small in falling to 84.83% (±3.27%). These values demonstrate the superior performance of GTAODV in maintaining a higher PDR in the presence of malicious nodes.

Figure 5.10 presents the results for throughput in KBps as a function of the number of malicious nodes in the network in a comparison of the performance of the AODV and GTAODV routing protocols. Throughput measures the rate of successful data packet delivery across the network. Higher throughput implies better network performance and utilisation of available resources. The throughput is shown with 95% confidence intervals for both protocols. The throughput of the AODV protocol drops significantly as the number of malicious nodes increases, indicating this protocol's vulnerability to black hole attacks. The decline in throughput can be attributed to the fact that AODV is unable to distinguish between malicious and non-malicious nodes, leading to inefficient routing and reduced data transmission rates. In contrast, the throughput of the GTAODV protocol remains relatively stable and significantly higher than that of the AODV protocol, even with an increasing number of malicious nodes. The trust-based mechanism in GTAODV allows the protocol to identify and avoid malicious nodes effectively, resulting in more efficient routing and better utilisation of network resources. This leads to a higher throughput which is crucial in ensuring optimal network performance.

As shown in Figure 5.10, the throughput for AODV with 5 malicious nodes is 79.251 KBps with a confidence interval of ±3.91 KBps, indicating a range of 75.341 to 83.161 KBps. Meanwhile, the throughput for GTAODV is 134.27 KBps with a confidence interval of ±5.07 KBps, suggesting a range of 129.20 to 139.34 KBps. As the number of malicious nodes increases to 25, the throughput for AODV drops significantly to 39.25 KBps (±3.87 KBps), while that for GTAODV decreases only slightly to 117.89 KBps (±4.28 KBps). These values show that the GTAODV protocol is more successful in sustaining higher throughput rates even in the presence of an increasing number of malicious nodes.

In conclusion, the comparison of AODV and GTAODV protocols based on PDR and throughput demonstrates that the trust-based mechanism employed in GTAODV offers significant advantages in terms of network performance and resilience against black hole attacks. By incorporating trust evaluation in the routing process, GTAODV can effectively identify and avoid malicious nodes, ensuring higher PDR and throughput, thereby ultimately contributing to more robust and efficient mobile ad-hoc networks.

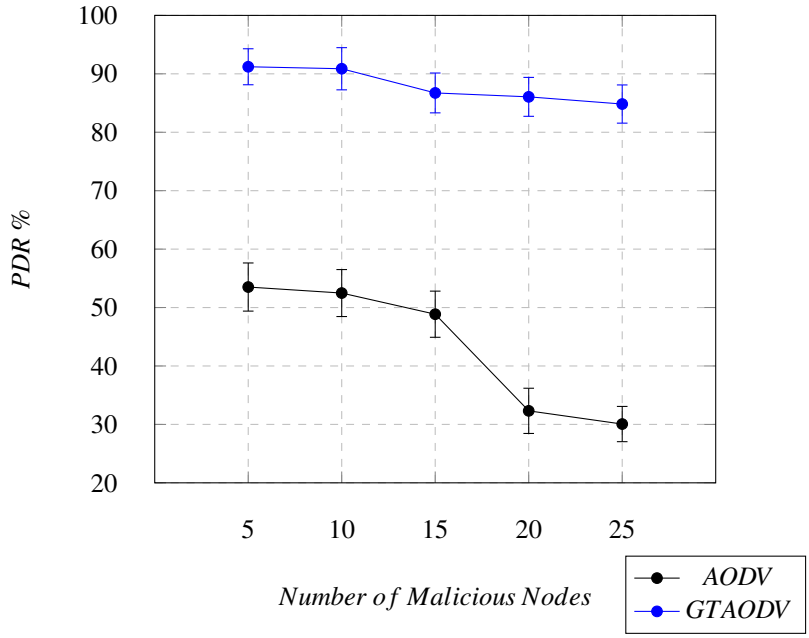

Figure 5.9 PDR vs. Number of Malicious Nodes with 95% Confidence Intervals

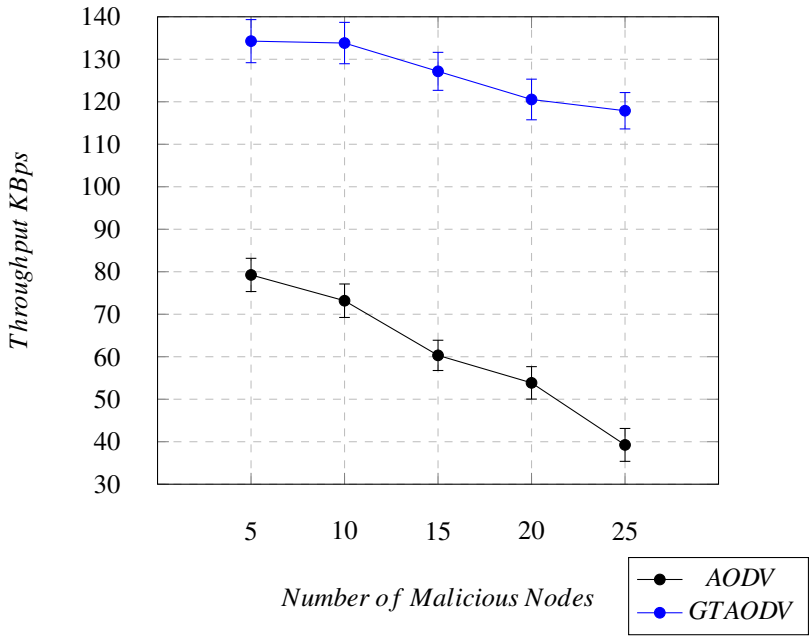

Figure 5.10 Throughput vs. Number of Malicious Nodes with 95% Confidence Intervals

5.3.3 Evaluation of End-to-End Delay and Routing Overheads when Varying the Number of Malicious Nodes

Figures 5.11 and 5.12 represent the results for the end-to-end delay and routing overheads respectively for AODV and GTAODV in the presence of varying numbers of malicious nodes, along with their 95% confidence intervals.

As shown in Figure 5.11, the end-to-end delay for AODV with 5 malicious nodes is 186.80 ms with a confidence interval of ±8.25 ms, indicating a range of 160.55 ms to 177.05 ms. For GTAODV, the delay is 261.846 ms with a confidence interval of ±10.23 ms, suggesting a range of 251.616 ms to 272.076 ms. As the number of malicious nodes increases to 25, the delay for AODV increases to 257.74 ms (±9.09 ms), while that for GTAODV also increases to 319.972 ms (±11.94 ms). These values show that, while GTAODV outperforms AODV in PDR and throughput, it experiences higher end-to-end delays with any number of malicious nodes. This can be attributed to the costs of the additional trust mechanism incorporated into the GTAODV protocol. This mechanism increases the processing time at each node during route discovery and packet forwarding, resulting in longer delays. However, the trade-off for higher delays is improved security and performance in terms of PDR and throughput.

In Figure 5.12, the routing overheads for AODV with 5 malicious nodes amount to 1843.64 bytes with a confidence interval of ±47.43 bytes, indicating a range of 1796.21 bytes to 1891.07 bytes. In contrast, the routing overheads for GTAODV reach 2403.876 bytes with a confidence interval of ±93.230 bytes, suggesting a range of 2310.646 bytes to 2497.106 bytes. As the number of malicious nodes increases to 25, the routing overheads for AODV rise to 2342.436 bytes (±62.32 bytes), while those for GTAODV also increase to 3074.435 bytes (±103.217 bytes). These values indicate that, compared to AODV, GTAODV incurs higher routing overheads in the presence of any number of malicious nodes. This can also be explained by the added trust mechanism in GTAODV, which requires additional control packets and processing during route discovery and maintenance. Although this results in increased overheads, the improved security and performance reflected in the PDR and throughput results make it a worthwhile trade-off in environments where security is a primary concern.

In conclusion, while GTAODV experiences higher end-to-end delays and routing overheads than AODV, it demonstrates superior resilience against black hole attacks, maintaining higher PDRs and throughput with varying numbers of malicious nodes. Therefore, the choice between AODV and GTAODV should be made based on the network's specific requirements, with a focus on balancing security, performance, and resource usage.

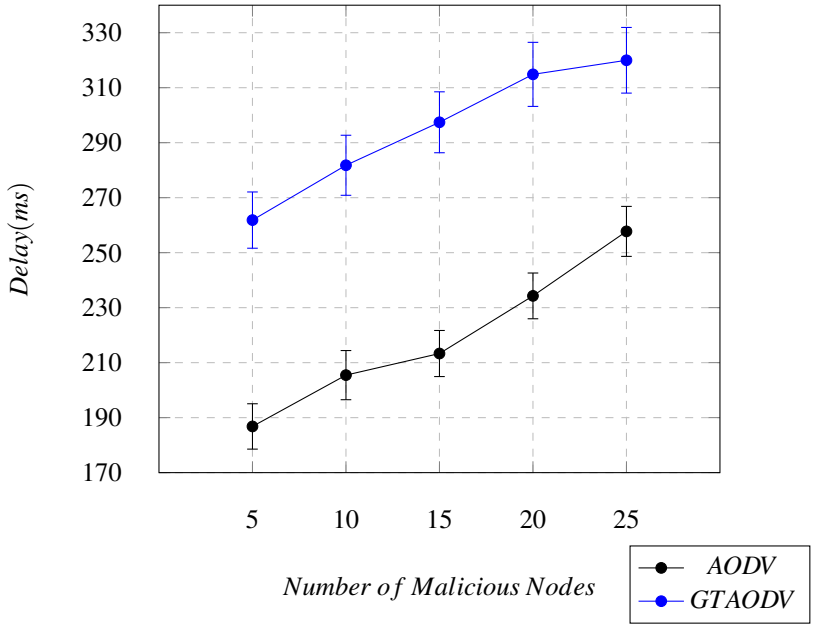

Figure 5.11 End-to-End Delay vs. Number of Nodes with 95% Confidence Intervals

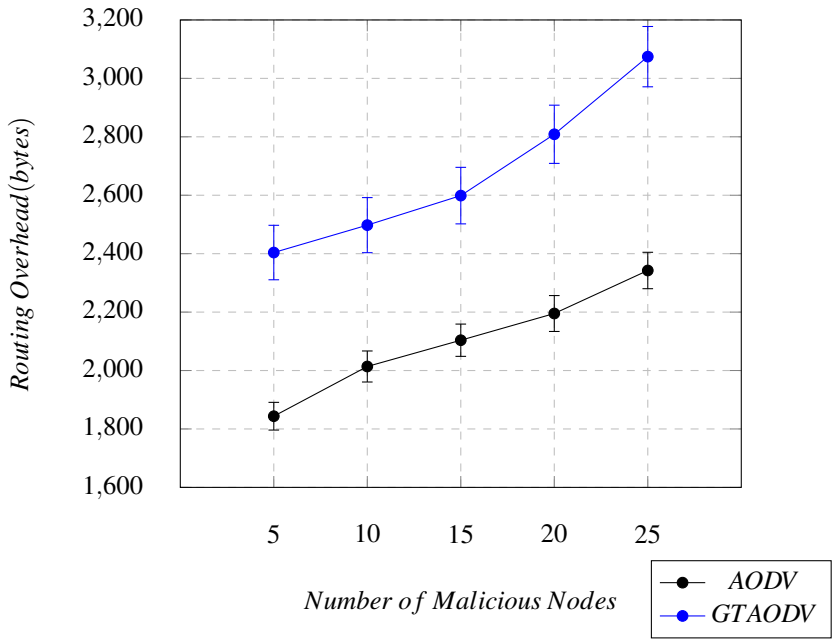

Figure 5.12 Routing Overhead vs. Number of Malicious Nodes with 95% Confidence Intervals

5.4 Summary and Discussions

This chapter considers the integration of a global trust management mechanism into the AODV routing protocol, aiming to enhance its security and efficiency attributes. The

modified AODV protocol featuring the global trust mechanism is designated as the Global Trust AODV (GTAODV) protocol. The chapter provides a thorough analysis of the global trust mechanism, elaborating on its core principles, architecture, and the rationale behind its implementation.

An extensive comparison of the conventional AODV and advanced GTAODV protocols is then conducted, examining their performance under a variety of circumstances and using multiple performance metrics. This comparison is facilitated by the Network Simulator-3 (NS-3), which is a state-of-the-art simulation tool that enables accurate evaluation and quantification of the behaviour of the protocols in terms of packet delivery ratio, end-to-end delay, and other relevant parameters.

In the latter part of this chapter, an in-depth investigation is carried out into the resilience of the AODV and GTAODV protocols when confronted with security threats and attacks, specifically focusing on the black hole attack. This type of attack involves one or more malicious nodes that falsely advertise themselves as having the shortest path to the destination, resulting in the interception and dropping of data packets. The analysis encompasses the detection and mitigation strategies employed in both protocols, highlighting the potential benefits of the global trust mechanism in terms of improving the ability to withstand such attacks.

By providing a comprehensive exploration of the global trust management mechanism's integration into the AODV protocol, this chapter aims to offer valuable insights and an in-depth understanding of the advantages and limitations of the GTAODV protocol. The findings presented here can serve as a foundation for future research in the realm of secure and efficient ad-hoc networking, ultimately contributing to the development of more robust and reliable ad-hoc network protocols.

Chapter 6

Comparative Analysis of Direct, Indirect, and Global Trust Mechanisms

The previous chapters discussed the direct, indirect, and global trust management mechanism and its integration into the Ad-hoc On-demand Distance Vector (AODV) protocol, in which each mechanism is evaluated against AODV protocols in its own chapter.

This chapter is focused on comparing the performance of direct, indirect, and global trust mechanisms in Mobile Ad-hoc Networks (MANETs) against each other. The chapter is organised in the following manner: Section 6.1 presents an overview of direct (DTAODV), indirect (ITAODV), and global (GTAODV) trust management mechanisms. In Section 6.2, the performance evaluation when varying node movement speed of DTAODV, ITAODV, and GTAODV is discussed and compared. In Section 6.3, the performance evaluation when varying number of nodes of DTAODV, ITAODV, and GTAODV is discussed and compared. In Section 6.4, the impact of malicious nodes on DTAODV, ITAODV and GTAODV is discussed and compared. Section 6.5 discusses the strengths and limitations of each trust management mechanism. Finally, Section 6.5 summarises this chapter.

6.1 Overview of Direct, Indirect, and Global Trust Management Mechanisms

Direct, indirect, and global trust management mechanisms are different approaches to establishing and maintaining trust relationships among nodes in a Mobile Ad-hoc Network (MANET). These mechanisms serve to improve the network's overall performance and security by assessing the trustworthiness of nodes during communication and data transmission. The following is a brief explanation of each mechanism.

6.1.1 Direct Trust Management Mechanism

The direct trust management mechanism is based on first-hand experiences and direct interactions between nodes in a MANET. In this approach, a node evaluates the trustworthiness of another node based on its history of interactions with that specific node. The trust value is calculated using metrics such as the number of successful transactions, packet delivery ratio, or other relevant criteria. This trust value is then used to make decisions regarding future interactions, such as choosing the best route for data transmission. The main advantage of the direct trust is its simplicity and the fact that it relies on actual experiences between nodes. However, it may not be as effective in large networks where nodes have limited direct interactions. Chapter 3 explained the direct trust management mechanisms in detail.

6.1.2 Indirect Trust Management Mechanism

Indirect trust management mechanisms rely on gathering trust information from neighbouring nodes or third parties rather than relying solely on direct experiences. In this approach, a node obtains trust information about another node from its neighbours who have had interactions with the target node. This is particularly useful when a node has little or no direct experience with the target node. By aggregating the trust information from multiple sources, the indirect trust mechanism can provide a more comprehensive view of the target node's trustworthiness. However, this approach may be susceptible to false or misleading trust information from malicious or compromised nodes.

6.1.3 Global Trust Management Mechanism

The global trust management mechanism combines both direct and indirect trust information to form a more comprehensive trust assessment. This approach aims to leverage the strengths of both direct and indirect trust mechanisms while mitigating their weaknesses. In this mechanism, a leader node calculates the trustworthiness of all other nodes by combining its direct trust information with the indirect trust information gathered from neighbouring nodes. The global trust mechanism can provide a more accurate and reliable trust assessment, as it incorporates information from multiple sources and considers both first-hand experiences and the experiences of other nodes in the network. However, it may be more complex to implement and can require more computational resources than the other mechanisms.

6.2 Performance Evaluation when Varying Node Movement Speed

6.2.1 Packet Delivery Ratio and Throughput

Figures 6.1 and 6.2 illustrate the relationship between PDR, throughput and node movement speed in a MANET for the three different trust-based AODV routing protocols: Direct Trust AODV (DTAODV), Indirect Trust AODV (ITAODV), and Global Trust AODV (GTAODV). The graph includes 95% confidence intervals to indicate that there is a 95% probability that the true value of the results lies within the specified range.

- DTAODV shows the PDR and throughput performance of the Direct Trust AODV routing protocol as the mobility speed increases. It can be observed that the PDR and throughput tend to decrease as the mobility speed increases.
- ITAODV the performance of the Indirect Trust AODV routing protocol. Similar to DTAODV, the PDR and throughput decrease as the mobility speed increases, but the decrease is less pronounced in comparison to DTAODV.
- GTAODV routing protocol shows the PDR performance as the mobility speed increases. The PDR decreases with increasing mobility speed, but the decrease is less significant compared to both DTAODV and ITAODV. However, GTAODV's throughput remains relatively stable, with only a slight decrease as mobility speed increases, outperforming both DTAODV and ITAODV.

In summary, the figures illustrate the performance of three trust-based AODV routing protocols in terms of PDR and throughput as the mobility speed increases in a MANET. The graph shows that the PDR and throughput generally decrease with increasing mobility speed for all three protocols, with GTAODV having a comparatively less pronounced decrease. GTAODV performs better in PDR and throughput compared to DTAODV and ITAODV due to several factors. One reason is that GTAODV uses a comprehensive trust evaluation, combining direct and indirect trust information, which leads to more informed routing decisions and, ultimately, better PDR and throughput. GTAODV's trust management mechanism enables it to adapt efficiently to changes in the network. As the network topology changes due to node mobility, GTAODV can quickly identify reliable routes and avoid faulty ones by leveraging both direct and indirect trust information, allowing it to maintain better PDR and throughput in dynamic network environments.

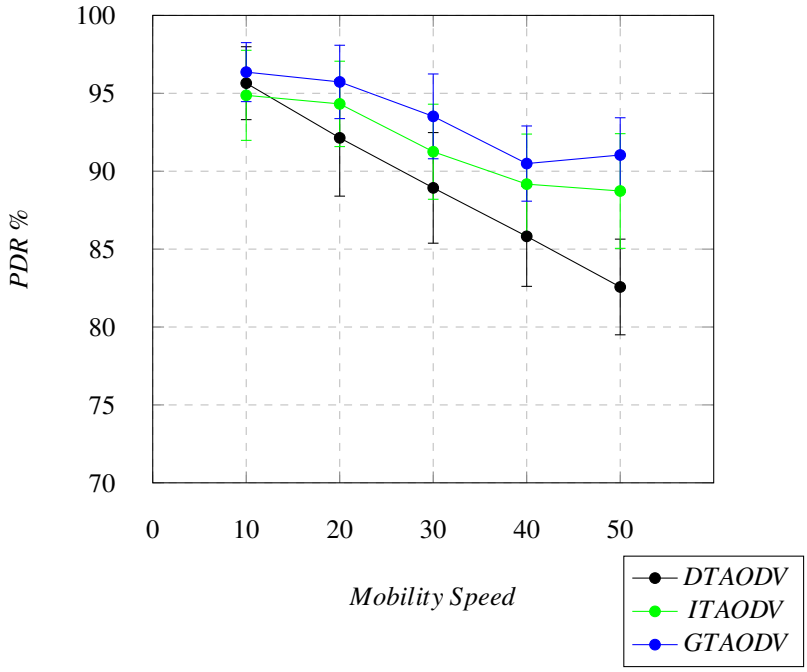

Figure 6.1 PDR vs. Mobility Speed with 95% Confidence Intervals

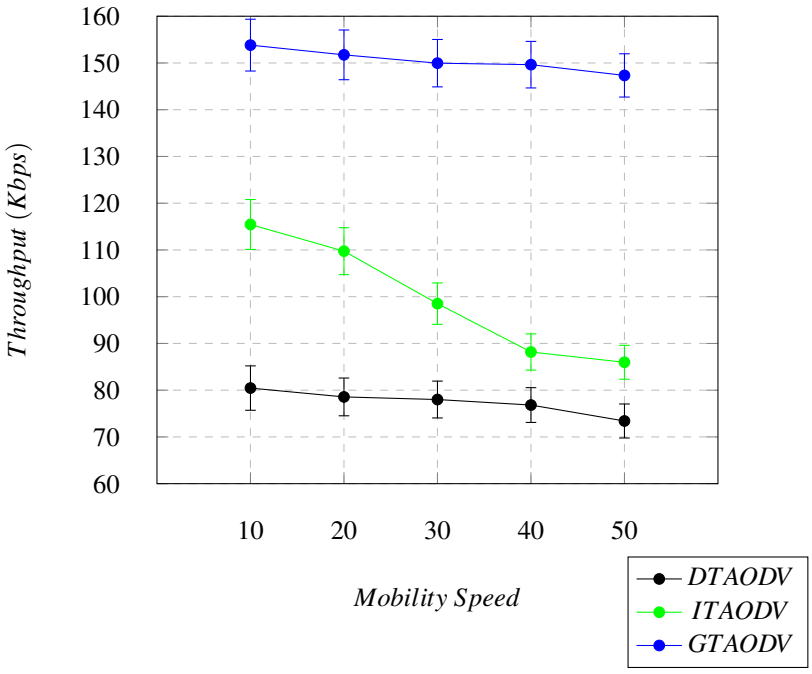

Figure 6.2 Throughput vs. Mobility Speed with 95% Confidence Intervals

6.2.2 End-to-End Delay and Routing Overheads

Figures 6.3 and 6.4 represent the performance of three routing protocols: DTAODV, ITAODV, and GTAODV, in terms of end-to-end delay and routing overheads as a function of mobility speed.

Figure 6.3 shows the end-to-end delay versus mobility speed with 95% confidence intervals. End-to-end delay is an essential metric to evaluate the performance of routing protocols, as low delays are generally preferred. In this figure, it is observed that as mobility speed increases, end-to-end delay also increases for all three protocols. However, the delay for GTAODV is consistently higher than that of DTAODV and ITAODV. This increase in delay could be attributed to the additional processing time and complexity required for trust evaluation and management mechanisms employed by GTAODV.

Figure 6.4 displays the routing overheads versus mobility speed. Routing Overheads represent the additional bytes or packets transmitted in the network for routing purposes. Lower overhead is generally preferred as it indicates more efficient use of network resources. In this figure, it is observed that as mobility speed increases, routing overheads also increase for all the three protocols. GTAODV has higher routing overheads compared to DTAODV and ITAODV. The increased overheads in GTAODV could be due to the exchange of trust information and additional control messages needed to maintain its trust management system.

In summary, the figures show that while GTAODV outperforms DTAODV and ITAODV in terms of packet delivery ratio and throughput; however, it has higher end-to-end delay and routing overheads. The increased delay and overheads in GTAODV are likely due to the additional complexity and processing time required for its trust management mechanisms. Moreover, GTAODV tends to perform better than ITAODV and DTAODV because it incorporates a more comprehensive trust evaluation mechanism. While ITAODV and DTAODV rely on direct and indirect trust evaluations, respectively, GTAODV combines both direct and indirect trust information, allowing for more informed routing decisions. In scenarios with high mobility speed, GTAODV is particularly beneficial for the many reasons. For example, it has a robust trust evaluation. As nodes frequently change their positions in high mobility environments, the trust relationships between them may fluctuate. GTAODV's global trust mechanism can adapt more effectively to such changes, ensuring that the most reliable routes are selected. In addition, it has enhanced route stability. Due to its comprehensive trust evaluation, GTAODV is more likely to select stable routes in dynamic environments. This leads to fewer route failures and reduces the need for frequent route rediscovery, ultimately improving network performance.

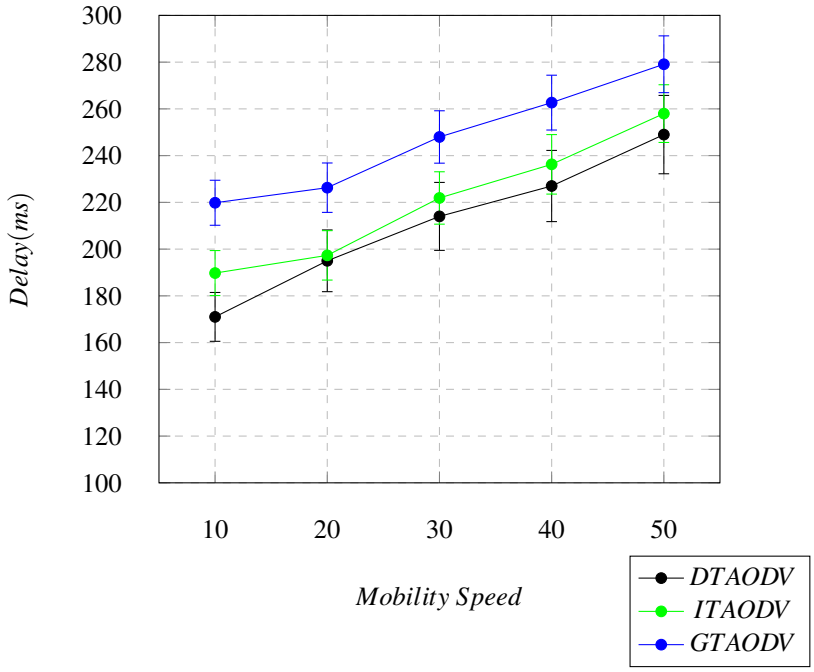

Figure 6.3 End-to-End Delay vs. Mobility Speed with 95% Confidence Intervals

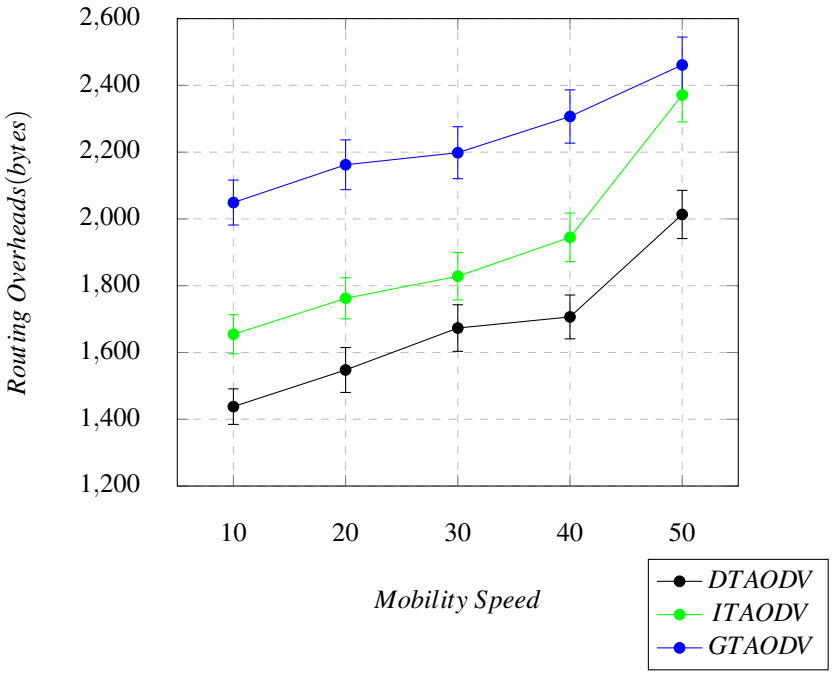

Figure 6.4 Routing Overheads vs. Mobility Speed with 95% Confidence Intervals

6.3 Performance Evaluation when Varying Node Density

6.3.1 Packet Delivery Ratio and Throughput Versus Number of Nodes

Figures 6.5 and 6.6 represent the performance of the three routing protocols: DTAODV, ITAODV, and GTAODV, in terms of PDR and throughput as a function of the number of nodes in the network.

From Figure 6.5, it can be observed that as the number of nodes increases, PDR for all three protocols also increases. However, GTAODV consistently outperforms DTAODV and ITAODV across all node counts. For example, at 100 nodes, the PDR values for DTAODV, ITAODV, and GTAODV are 92.45%, 96.04%, and 97.26%, respectively, with GTAODV showing the highest PDR.

In Figure 6.6, it can be seen that as the number of nodes increases, the throughput for DTAODV decreases, whereas ITAODV and GTAODV maintain relatively stable throughput values. GTAODV outperforms both DTAODV and ITAODV in terms of throughput. For instance, at 100 nodes, the throughput values for DTAODV, ITAODV, and GTAODV are 78.61 KBps, 124.72 KBps, and 149.64 KBps, respectively, with GTAODV achieving the highest throughput.

In summary, the figures demonstrate that GTAODV consistently outperforms DTAODV and ITAODV in terms of PDR and throughput across varying numbers of nodes in the network. This superior performance can be attributed to the trust-based mechanisms employed by GTAODV, which help improve the reliability and efficiency of data packet delivery in the network.

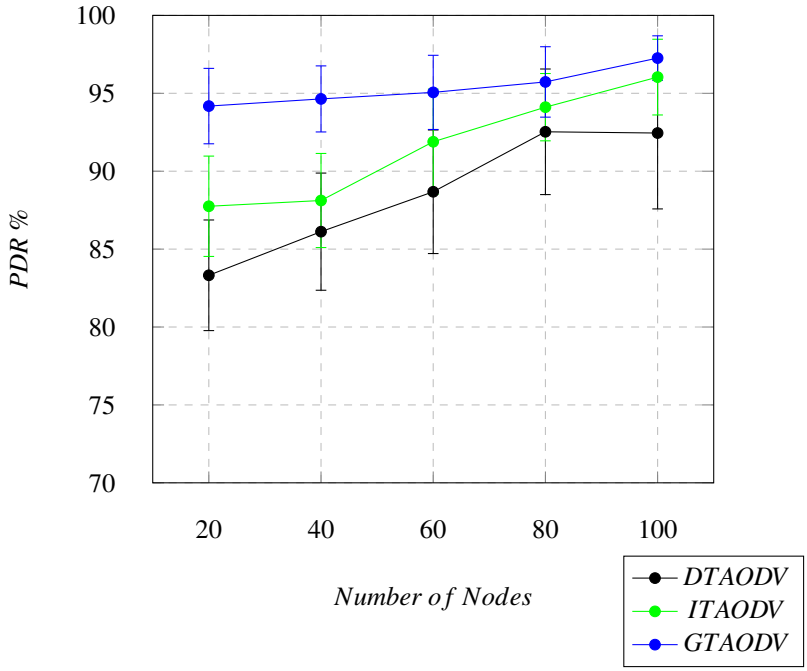

Figure 6.5 PDR vs. Number of Nodes with 95% Confidence Intervals

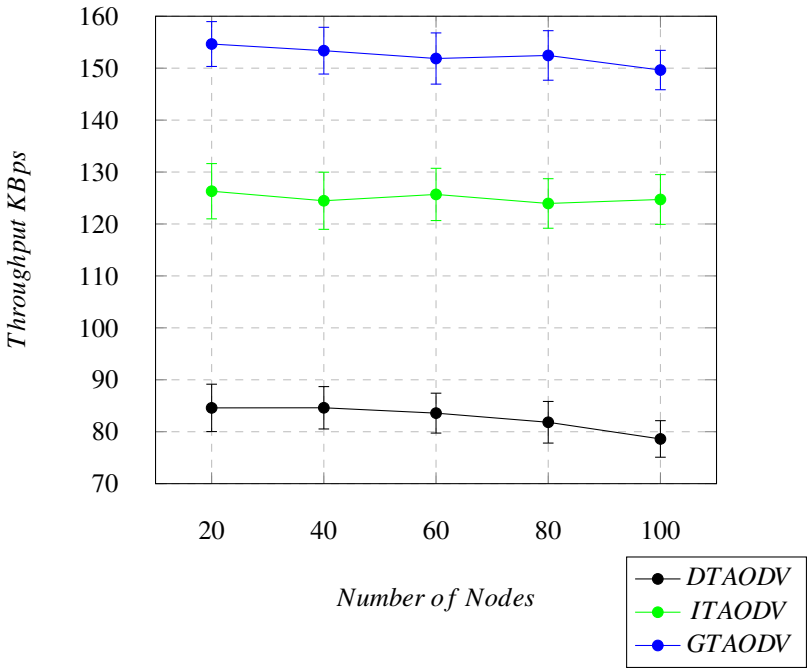

Figure 6.6 Throughput vs. Number of Nodes with 95% Confidence Intervals

6.3.2 End-to-End Delay and Routing Overhead Versus Number of Nodes

Figures 6.7 and 6.8 provide a comparison of DTAODV, ITAODV, and GTAODV in terms of end-to-end delay and routing overheads as the number of nodes in the network increases. The data points in these figures are accompanied by 95% confidence intervals.

The Figures show how the end-to-end delay and the routing overheads vary with the number of nodes for the three protocols. As the number of nodes increases, the end-to-end delay and routing overheads for DTAODV, ITAODV, and GTAODV also increase. However, GTAODV consistently exhibits higher delays and overheads compared to DTAODV and ITAODV across all node counts.

From the presented data, it can be observed that GTAODV has higher end-to-end delays and routing overheads compared to DTAODV and ITAODV. However, as discussed in the previous section, GTAODV outperforms the other two protocols in terms of PDR and throughput. The reason for the higher end-to-end delay and routing overheads in GTAODV is that it uses a more comprehensive trust evaluation mechanism, which takes into account both direct and indirect trust information. This approach provides more reliable routes and better overall network performance, but it comes at the cost of increased delay and overheads.

In summary, while GTAODV has higher end-to-end delays and routing overheads than DTAODV and ITAODV, its superior performance in terms of PDR and throughput makes it a better choice for scenarios where trust evaluation and network reliability are of higher importance. Moreover, GTAODV may be more suitable than ITAODV or DTAODV in some scenarios due to its trust evaluation approach. GTAODV computes trust by considering both direct and indirect trust values, which helps in creating a more comprehensive and accurate trust assessment. However, it is important to note that GTAODV's performance might come at the cost of higher end-to-end delay and routing overheads, as observed in the presented graphs. As the number of nodes increases in the MANET environment, GTAODV could be better suited in scenarios where the emphasis is on network size and robustness and where slightly higher delays and overheads are acceptable trade-offs. On the other hand, if minimising delay and routing overheads are the primary concern, DTAODV or ITAODV might be more appropriate choices, depending on the specific network conditions and trust requirements. The selection of a suitable trust-based routing protocol depends on the particular scenario and the priorities of the network, such as security, robustness, delay, and overheads.

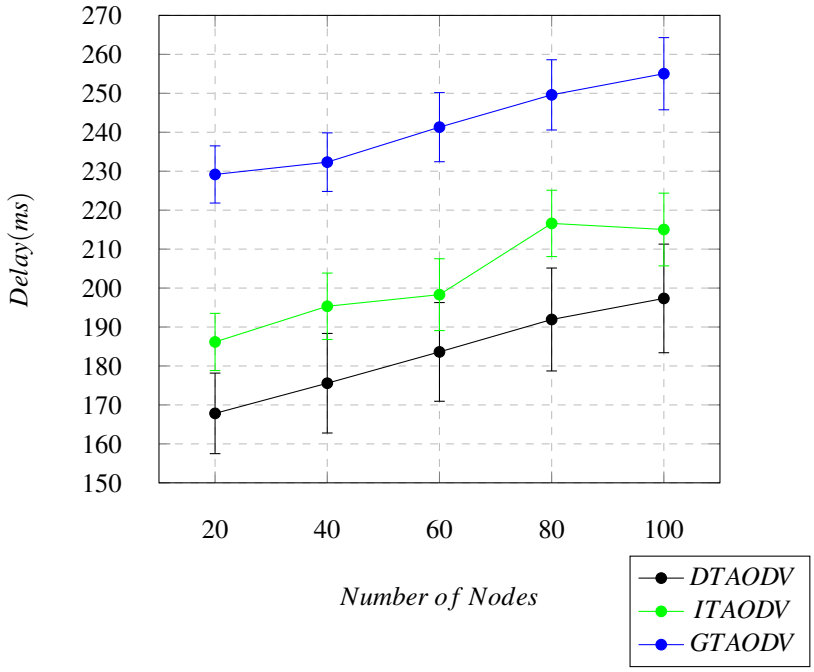

Figure 6.7 End-to-End Delay vs. Number of Nodes with 95% Confidence Intervals

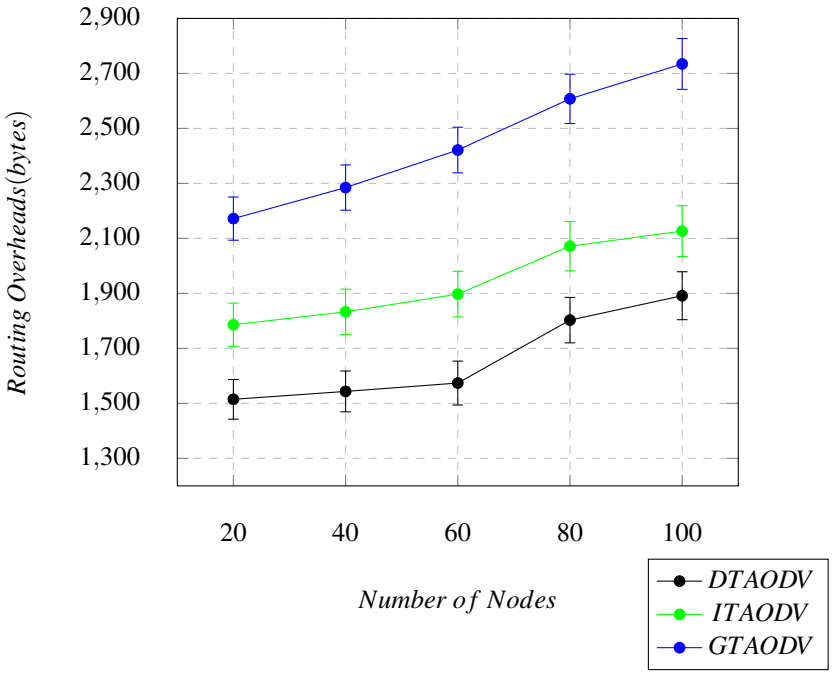

Figure 6.8 Routing Overheads vs. Number of Nodes with 95% Confidence Intervals

6.4 Performance Evaluation in the Presence of a Black hole Attack

A black hole attack is a type of network attack in which a malicious node falsely claims to have the shortest path to a destination, causing data packets to be redirected to the attacker. This results in the loss of data packets and the degradation of network performance. To evaluate the performance of routing protocols in the presence of a black hole attack, several metrics are used, which are PDR, throughput, end-to-end delay and routing overheads.

To evaluate the performance of different routing protocols in the presence of a black hole attack, the NS-3 simulator was used with varying numbers of malicious nodes. The results are compared across the three different protocols to determine their resilience against black hole attacks.

GTAODV, ITAODV, and DTAODV routing protocols are designed to be more resilient against such attacks. By incorporating trust values into the routing process, these protocols can help identify and avoid malicious nodes, mitigating the impact of a black hole attack on the network performance. The performance evaluation in the presence of a black hole attack can help identify which trust-based routing protocol offers the best balance between security and performance in different network scenarios.

6.4.1 Evaluation of Packet Delivery Ratio and Throughput when Varying the Number of Malicious Nodes

Figures 6.9 and 6.10 present a comparison between the performance of DTAODV, ITAODV, and GTAODV in the presence of varying numbers of malicious nodes in the network. The performance is measured in terms of PDR and throughput.

Figure 6.9 shows the PDR as a percentage for each of the three routing protocols, plotted against the number of malicious nodes in the network.

- DTAODV: As the number of malicious nodes increases from 5 to 25, the PDR decreases from 82.32% to 58.83
- ITAODV: The PDR decreases from 86.41% to 65.83% as the number of malicious nodes increases from 5 to 25.
- GTAODV: This protocol shows a relatively stable PDR as the number of malicious nodes increases. The PDR ranges from 91.21% to 84.83% with the increasing number of malicious nodes.

Figure 6.10 compares the throughput of the three routing protocols as the number of malicious nodes increases.

- DTAODV: The throughput ranges from 83.19 KBps to 78.61 KBps as the number of malicious nodes increases from 5 to 25.
- ITAODV: As the number of malicious nodes increases from 5 to 25, the throughput decreases from 113.45 KBps to 88.62 KBps.
- GTAODV: This protocol has the highest throughput among the three. The throughput ranges from 134.27 KBps to 117.89 KBps as the number of malicious nodes increases from 5 to 25.

In summary, GTAODV demonstrates better resilience against malicious nodes, maintaining a higher PDR and throughput compared to DTAODV and ITAODV. As the number of malicious nodes increases in the network, GTAODV consistently outperforms the other two protocols, making it a more suitable choice for networks with a higher likelihood of encountering malicious nodes.

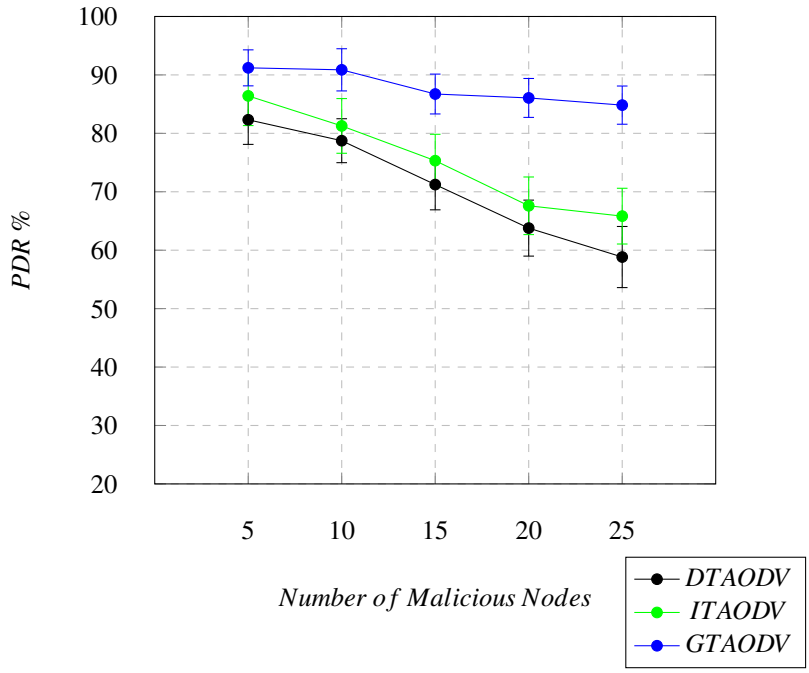

Figure 6.9 PDR vs. Number of Malicious Nodes with 95% Confidence Intervals

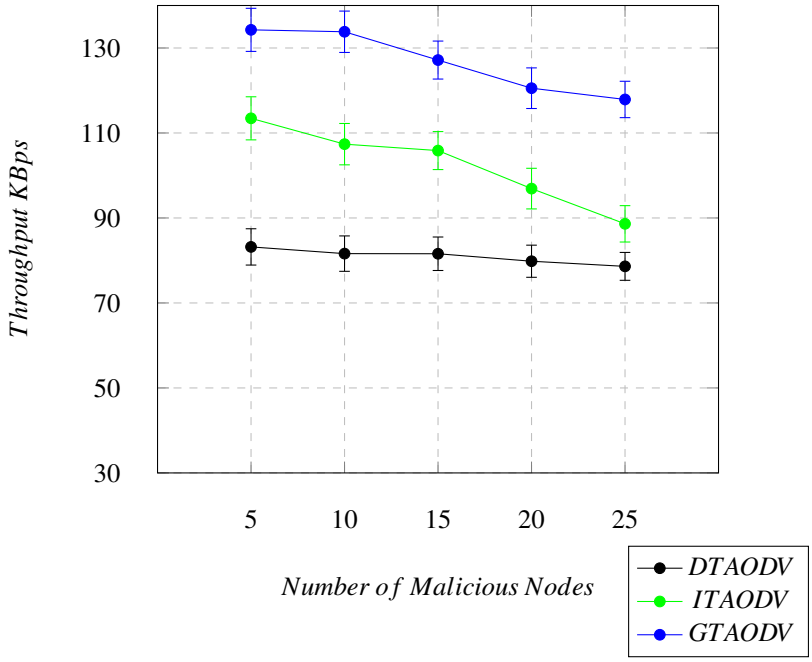

Figure 6.10 Throughput vs. Number of Malicious Nodes with 95% Confidence Intervals

6.4.2 Evaluation of End-to-End Delay and Routing Overheads when Varying the Number of Malicious Nodes

Figures 6.11 and 6.12 present a comparison between the performance of DTAODV, ITAODV, and GTAODV in the presence of varying numbers of malicious nodes in the network. The performance is measured in terms of end-to-end delay and routing overheads.

Figure 6.11 shows the end-to-end delay when the malicious nodes in the network increase. The following is observed from the figure results.

- DTAODV's delay increases from 173.45 ms (5 malicious nodes) to 207.18 ms (25 malicious nodes)
- ITAODV's delay increases from 226.45 ms (5 malicious nodes) to 258.18 ms (25 malicious nodes)
- GTAODV's delay increases from 261.846 ms (5 malicious nodes) to 319.972 ms (25 malicious nodes)

End-to-End Delay Difference:

- The difference in end-to-end delay between DTAODV and ITAODV increases from 53 ms (5 malicious nodes) to 51 ms (25 malicious nodes)

- The difference in end-to-end delay between DTAODV and GTAODV increases from 88 ms (5 malicious nodes) to 113 ms (25 malicious nodes)

In Figure 6.12, it can be seen that as the number of malicious nodes increases, the routing overheads for DTAODV, ITAODV and GTAODV increase. From the figure, the following is observed.

- DTAODV's overhead increases from 1723.876 bytes (5 malicious nodes) to 2039.435 bytes (25 malicious nodes)
- ITAODV's overhead increases from 2148.876 bytes (5 malicious nodes) to 2286.435 bytes (25 malicious nodes)
- GTAODV's overhead increases from 2403.876 bytes (5 malicious nodes) to 3074.435 bytes (25 malicious nodes)

Routing Overhead Difference:

- The difference in routing overhead between DTAODV and ITAODV decreases from 425 bytes (5 malicious nodes) to 247 bytes (25 malicious nodes)
- The difference in routing overhead between DTAODV and GTAODV increases from 680 bytes (5 malicious nodes) to 1035 bytes (25 malicious nodes)

By examining these specific values, we can gain a deeper understanding of the trends and patterns observed in the figures. As the number of malicious nodes increases, the performance gap between the protocols tends to widen. This is evident in the growing difference in end-to-end delay and routing overheads between DTAODV and GTAODV.

In summary, the trust-based protocols, such as GTAODV, ITAODV, and DTAODV, are designed to enhance the security and performance of mobile ad hoc networks (MANETs) by incorporating trust mechanisms into the routing process. These trust mechanisms help to identify and isolate malicious nodes in the network, thereby improving overall network performance, particularly when the number of malicious nodes increases.

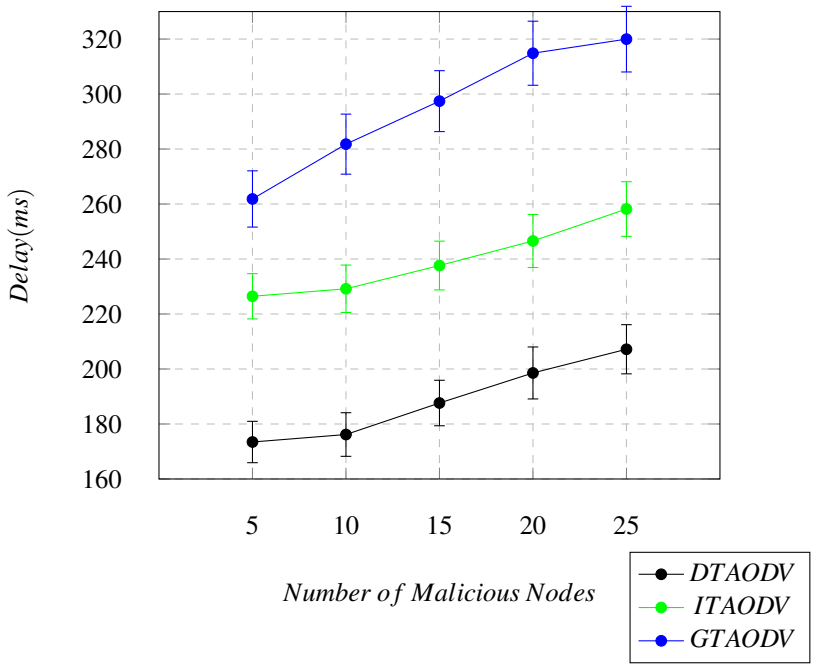

Figure 6.11 End-to-End Delay vs. Number of Nodes with 95% Confidence Intervals

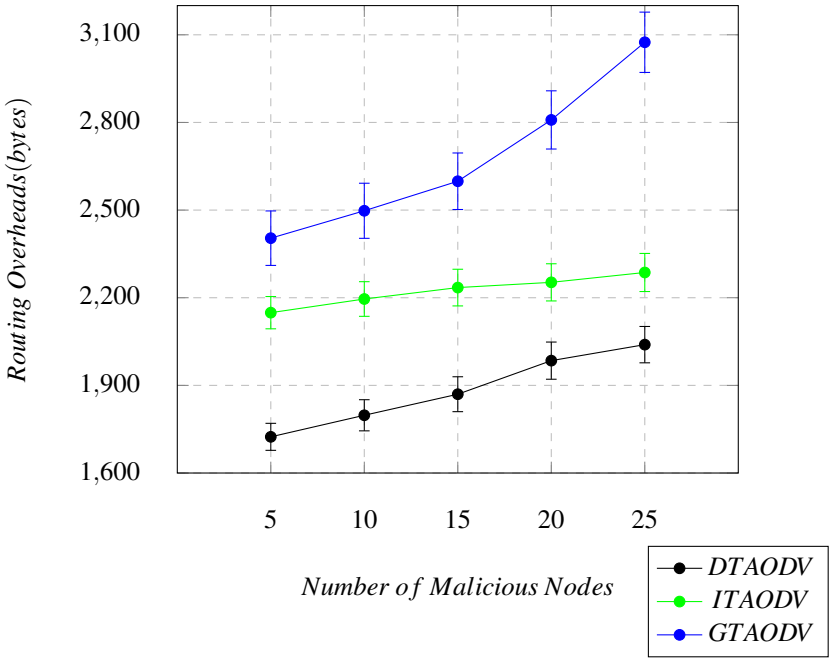

Figure 6.12 Routing Overheads vs. Number of Malicious Nodes with 95% Confidence Intervals

6.5 Comparitive Analysis of Different Trust Approaches

This research work explored Direct, Indirect and Global Trust to identify their usefulness to overcome Black hole security attacks. Based on various experimental setup and observations noted from each one the research work identified strengths and weaknesses for each trust based protocol. This section summarises strengths and weaknesses of each type of trust based routing protocol.

Chapter 3 explored concept of direct trust routing protocol using proposed DTAODV protocol. DTAODV protocol is an extension of the traditional AODV protocol, which is designed to use parameters such as packet forward rate, node battery power availability, battery drain rate, and congestion around a node to calculate a node's reliability value. The calculated value of reliability is used to determine the trustworthiness of each node in the network. Performance evaluation of DTAODV is done with help of NS2 and NS3 simulators under varying conditions of mobility, node density and attacking nodes. Experimental results given in Chapter 3 and Chapter 6 show that DTAODV protocol outperforms the AODV protocol in terms of both PDR and throughput in scenarios of increased mobility speed and higher numbers of nodes. The performance of both protocols in the presence of black hole attack was evaluated by increasing the number of malicious nodes in the network. The results indicate that the DTAODV protocol performs significantly better than the AODV protocol in terms of PDR, throughput, end-to-end delay, and routing overheads under these conditions. This suggests that the implementation of the direct trust mechanisms in the AODV protocol has led to an improvement in overall performance in the presence of network threats and attacks. In the DTAODV routing protocol, the mechanism is simple and effective. The strength lies in its dependence on prior experience, which ensures that the trust value is based on direct interactions. Therefore, it is less likely to be manipulated. It is ideal for environments where nodes have frequent direct interactions, leading to robust and reliable communication.

Chapter 4 explored concept of indirect trust routing protocol using proposed ITAODV protocol. ITAODV protocol is an extension of the traditional AODV protocol. The indirect trust mechanism is a method used in trust-based routing protocols for MANETs to establish trust relationships between nodes that have not directly communicated with each other. In indirect trust mechanisms, nodes gather trust information about other nodes from other trustworthy nodes in the network and use this information to make decisions about routing and forwarding packets. Indirect trust mechanisms involve the exchange of recommendations or feedback between nodes about the behaviour of other nodes. ITAODV is designed to use different parameters such as packet forward rate, node battery power availability, battery drain rate, and congestion around a node in the calculation of another node's reliability. Performance evaluation of ITAODV is done

with help of NS2 and NS3 simulators under varying conditions of mobility, node density and attacking nodes. Experimental results given in Chapter 4 and Chapter 6 show that ITAODV protocol outperforms the AODV protocol in terms of both PDR and throughput in scenarios of increased mobility speed and higher numbers of nodes. The performance of both protocols in the presence of black hole attack was evaluated by increasing the number of malicious nodes in the network. The results show that ITAODV exhibits better performance than AODV in all performance metrics except end-to-end delay. This suggests that the implementation of the indirect trust mechanisms in the AODV protocol has led to an improvement in overall performance in the presence of network threats and attacks. In the ITAODV routing protocol, the mechanism capitalises on the collective data of the network. Incorporating recommendations from neighbouring nodes can provide a more comprehensive view of a node's trustworthiness. This could be particularly useful in large networks where direct interactions may not be feasible for all node pairs.

Chapter 5 explored concept of global trust routing protocol using proposed GTAODV protocol. In Chapter 5 and Chapter 5 an extensive comparison of the conventional AODV and advanced GTAODV protocols is conducted, examining their performance under a variety of circumstances and using multiple performance metrics. This comparison is facilitated by the Network Simulator-3 (NS-3), which is a state-of-the-art simulation tool that enables accurate evaluation and quantification of the behaviour of the protocols in terms of packet delivery ratio, end-to-end delay, and other relevant parameters.GTAODV protocol is an extension of the traditional AODV protocol. In the GTAODV routing protocol, the strength of its mechanism lies in its hybrid approach. Using a centralised node to combine both direct and indirect trust evaluations offers a more balanced and accurate trust assessment. The mechanism can adapt to various network conditions and scales depending on the size of the network.

6.5.1 Key Points about Different Trust-based Routing Protocols

After performing comparative analysis of DTAODV, ITAODV, and GTAODV following key points are observed in this research work.

1. Figures given in section 6.2.1 illustrate the performance of three trust-based AODV routing protocols in terms of PDR and throughput as the mobility speed increases in a MANET. The graph shows that the PDR and throughput generally decrease with increasing mobility speed for all three protocols, with GTAODV having a comparatively less pronounced decrease. Compared with other two variants GTAODV's trust management mechanism enables it to adapt efficiently to changes in the network.

2. Figures given in section 6.2.2 illustrate that while GTAODV outperforms DTAODV and ITAODV in terms of packet delivery ratio and throughput; however, it has higher end-to-end delay and routing overheads. The increased delay and overheads in GTAODV are likely due to the additional complexity and processing time required for its trust management mechanisms.

3. Figures given in section 6.3.1 demonstrate that GTAODV consistently outperforms DTAODV and ITAODV in terms of PDR and throughput across varying numbers of nodes in the network. This superior performance can be attributed to the trust-based mechanisms employed by GTAODV, which help improve the reliability and efficiency of data packet delivery in the network.

4. Figures given in section 6.3.2 illustrate that while GTAODV has higher end-to-end delays and routing overheads than DTAODV and ITAODV, its superior performance in terms of PDR and throughput makes it a better choice for scenarios where trust evaluation and network reliability are of higher importance. However, it is important to note that GTAODV's performance might come at the cost of higher end-to-end delay and routing overheads, as observed in the graphs.

5. Figures given in section 6.4 illustrate that GTAODV demonstrates better resilience against malicious nodes, maintaining a higher PDR and throughput compared to DTAODV and ITAODV. As the number of malicious nodes increases in the network, GTAODV consistently outperforms the other two protocols, making it a more suitable choice for networks with a higher likelihood of encountering malicious nodes.

6.6 Summary and Discussions

This chapter summarises and compares the performance of direct, indirect, and global trust management mechanisms in MANETs. The chapter provided an overview of these trust mechanisms, focusing on their unique characteristics and functioning. Direct trust management mechanism relies on first-hand observations, while indirect trust management gathers recommendations from neighbouring nodes, and global trust management considers a combination of both direct and indirect trust values using a leader node for the routing decision.

The performance of these trust mechanisms was compared and evaluated under different network conditions, such as varying node movement speed, node density, and in the presence of a black hole attack. The evaluation focused on key performance metrics, including packet delivery ratio, throughput, end-to-end delay, and routing overheads.

When varying node movement speed, the analysed results of DTAODV, ITAODV, and GTAODV were compared, using the impact on PDR, throughput, end-to-end delay, and routing overheads. The results showed that trust-based mechanisms could maintain good performance even under high mobility conditions. Moreover, the results showed the GTAODV has an overall better performance in the PDR and throughput while having a high delay and overheads.

In the case of varying node density, the PDR, throughput, end-to-end delay, and routing overheads were assessed in relation to the number of nodes. The performance of trust-based mechanisms demonstrated resilience to fluctuations in node density, ensuring efficient and reliable communication in the network.

The performance of trust mechanisms was also evaluated in the presence of a black hole attack, where packets are deliberately dropped by malicious nodes. The analysis showed that trust-based protocols could effectively detect and isolate malicious nodes, improving the packet delivery ratio, throughput, end-to-end delay, and routing overheads in the presence of such attacks. Furthermore, when comparing the three protocols, DTAODV, ITAODV, and GTAODV, it is observed that GTAODV protocol outperformed DTAODV and ITAODV as it has a higher PDR and throughput when the malicious nodes increase.

In summary, direct, indirect, and global trust management mechanisms offer significant benefits for MANETs, including enhanced security, reliability, robustness, and resilience. By incorporating trust evaluation and adaptive behaviour, these mechanisms can maintain network performance under various conditions and protect against attacks and malicious activities.

In addition, the benefits of trust-based protocols include improved security, reliability, robustness, resilience, and reduced overhead. By evaluating the trustworthiness of nodes and updating trust values based on observed behaviour, these protocols can adapt to changing conditions and maintain network performance even in the presence of increasing malicious nodes. Trust-based protocols contribute to more efficient use of network resources, better overall performance, and increased resilience against coordinated attacks or exploitation of network vulnerabilities.

Chapter 7

Conclusions and Future Work

This thesis aimed to explore applications of trust in MANET routing protocols to overcome security attacks and improve reliability of the routing process. In this thesis, numerous aspects of MANETs were investigated, encompassing their uses and applications. Detailed discussions of direct, indirect, and global trust management mechanisms were provided. Each mechanism was incorporated into the AODV protocol to evaluate their performance and behaviour under different conditions and performance metrics.

Each trust management mechanism was explored in details in separate chapters 3, 4, and 5. Each different trust based variant compared with the AODV protocol. Moreover, the implications of security attacks on both AODV and the protocols associated with each trust management mechanism were explored, with a specific emphasis on the outcomes of black hole attacks.

This chapter is a summary of every chapter in the thesis and concludes the thesis. Also, it outlines and discusses potential pathways for advancing the field and future work.

7.1 Thesis Summary

Chapter 1: Chapter 1 serves as the Introduction to the thesis and begins by presenting the problem statement and research questions. The problem statement highlights the issues being addressed in the thesis, while the research questions guide the investigation throughout the study. The research aims, and objectives are then detailed to outline the main goals of the research and the specific objectives that must be achieved to fulfil the aims. The motivation behind the thesis and its contributions are explained, emphasising the importance of the study and its impact on the field. Following this, the structure of the thesis is outlined, providing an overview of the organisation of the chapters and their respective content. Lastly, Chapter 1 concludes with a chapter summary, offering a concise recap of the key points presented in the introduction.

Chapter 2: This chapter covers the literature survey and background and explains various aspects of Mobile Ad-hoc Networks (MANETs). It begins with an introduction to MANET routing, followed by a classification of MANET routing protocols. The chapter also explores diverse applications and uses of MANETs and provides an in-depth analysis of the Ad-hoc On-Demand Distance Vector (AODV) protocol. Security issues in MANETs are examined, including the importance of addressing these issues and the various security attacks that can occur. Techniques to overcome these security attacks are also discussed. The chapter then moves on to the concept of trust in MANET routing protocols, exploring the features of trust management systems, parameters used in trust score derivation, and trust mechanisms using node reputation and characteristics. Furthermore, trust management mechanisms are explored, such as fuzzy theory, game theory, and reputation and probability techniques. The application of trust is discussed in various contexts like e-business, peer-to-peer (P2P) networks, and MANETs. Finally, the chapter addresses the limitations of existing trust-based routing protocols and known countermeasures before concluding with a summary of the key points covered.

Chapter 3: Chapter 3 of this thesis focuses on direct trust management in the AODV routing protocol. It starts with an overview of AODV routing and discusses the need for trust in the AODV protocol, covering topics such as the route discovery process, route maintenance, and route deletion. The chapter then introduces the proposed direct trust management mechanisms for the AODV Protocol, providing an overview of the protocol, the proposed direct trust routing protocol, and the integration of direct trust mechanisms into the AODV protocol. Next, the chapter presents a performance evaluation and analysis using NS-2, including the effects of variations in node movement speed and node density. Then, the performance evaluation continues with the use of NS-3 software. Furthermore, the chapter explores the performance evaluation of AODV and DTAODV in the presence of a black hole attack, detailing the experimental setup and performance measurement parameters. Finally, the chapter concludes with a summary and discussion of the key findings and their implications.

Chapter 4: This chapter focuses on indirect trust management in the AODV routing protocol. The chapter begins with the proposal of an indirect trust management mechanism for the AODV protocol. Also, it discuses the indirect trust mechanism by providing an overview of the proposed indirect trust protocol, and explaining the integration of direct and indirect trust in the AODV protocol to become the ITAODV routing protocol. Afterword, the chapter discuss the performance evaluation and analysis of the proposed protocol by examining the effects of varying node movement speed and node density on the performance of the ITAODV routing protocol. The chapter then investigates the performance evaluation and analysis in the presence of a black hole attack. It presents the experimental setup and evaluates the packet delivery ratio, throughput, end-to-end delay,

and routing overheads under the black hole attack scenario. Finally, the chapter concludes with a summary and discussion of the main findings, offering insights into the effectiveness of the proposed indirect trust management mechanism in the AODV routing protocol.

Chapter 5: Chapter 5 of the thesis is centred on global trust management in the AODV routing protocol. The chapter starts by proposing Global Trust Management Mechanisms for the AODV Protocol, presenting an overview of the global trust and the proposed protocol, discussing the proposed global trust mechanism in the AODV protocol, and explaining the integration of global trust in the AODV protocol. The chapter proceeds with the performance evaluation and analysis of the proposed global trust management mechanism. It investigates the performance of the protocol under varying node movement speeds and node densities, evaluating the impact of these variations on the AODV protocol with global trust management. Next, the chapter examines the performance of AODV and GTAODV protocols in the presence of a black hole attack. The experimental setup is detailed, followed by an evaluation of the packet delivery ratio, throughput, end-to-end delay, and routing overheads when the number of malicious nodes is varied. Finally, Chapter 5 concludes with a summary and discussion of the findings, highlighting the effectiveness and implications of the proposed global trust management mechanism in the AODV routing protocol.

Chapter 6: This chapter focuses on providing an in-depth comparison of direct, indirect, and global trust management mechanisms in MANETs. It begins with an overview of these three mechanisms, detailing their distinctive operational mechanisms. Comparisons of performance evaluations were carried out considering various network conditions such as node movement speed and node density. The results highlighted the significant impact of these trust management mechanisms on key network performance metrics, including packet delivery ratio, throughput, end-to-end delay, and routing overheads. Also, the chapter compared the investigated performance of these mechanisms in the presence of black hole attacks, with a specific focus on varying the number of malicious nodes. The results underscored the importance of trust-based protocols in maintaining the performance and security of MANETs, even in adverse conditions. Finally, the strengths of these mechanisms include their potential to enhance the security and performance of MANETs, particularly in challenging network conditions. However, limitations were also noted, such as the reliance on the honesty of nodes in ITAODV and the resource-intensity of GTAODV.

7.2 Future Work

This section of the thesis will explore possible opportunities for additional research and development in the field MANETs and trust management mechanisms. Some prospective areas for future exploration may consist of the following.

7.2.1 Development of New Security Countermeasures

With the ongoing evolution of security threats in MANETs, it is essential to continuously develop innovative countermeasures that can effectively protect against emerging attacks. Such advancements may include the following:

- Advanced encryption techniques: As cryptographic techniques progress, new encryption methods can be developed to better secure data transmitted over MANETs. This could involve the use of lightweight encryption algorithms to provide increased security without significantly impacting network performance.
- Privacy-preserving techniques: In addition to securing data, preserving user privacy is a critical aspect of MANET security. Researchers can explore new privacy-enhancing technologies, such as anonymous communication protocols, differential privacy, and secure multi-party computation, to ensure the confidentiality of user data and communications while maintaining network functionality.

7.2.2 Evaluation in Different Scenarios and Environments

Conducting performance assessments and evaluations of trust management mechanisms across a wide range of scenarios and conditions can be crucial for determining their practical applicability and effectiveness in diverse real-world contexts. Some examples of these scenarios include:

- Disaster recovery scenarios: In disaster-stricken areas, MANETs can play a critical role in supporting rescue and recovery operations. Assessing trust management mechanisms in such scenarios will help determine their ability to maintain secure and resilient communication under extreme conditions, including network fragmentation, resource scarcity, and the presence of malicious nodes.
- IoT and edge computing: With the growth of the Internet of Things (IoT) and edge computing, MANETs can become increasingly relevant for enabling device-to-device communication and distributed processing. Evaluating trust management mechanisms in IoT and edge computing scenarios can help identify their suitability

for securing communication among a diverse array of devices, including sensors, actuators, and edge servers.

7.2.3 Comparison with other Routing Protocols

A comprehensive analysis of trust management mechanisms involves comparing their performance and security when integrated with various MANET routing protocols. It can help identify the most effective solutions based on specific network conditions and requirements. Some of the other routing protocols that can be considered for comparison with the AODV protocol are:

- Dynamic Source Routing (DSR): DSR is an on-demand, source-based routing protocol that uses source routing to discover and maintain routes in the network. Investigating the integration of trust management mechanisms with DSR can provide insights into their effectiveness in networks where the source node has more control over the routing decisions, and how this affects overall security and performance.
- Optimised Link State Routing (OLSR): OLSR is a proactive, table-driven routing protocol that relies on a periodic exchange of link-state information to maintain up-to-date routing tables. By examining trust management mechanisms within the context of OLSR, researchers can explore their performance in networks where routes are pre-established and continuously updated, and how this approach impacts the ability to detect and mitigate security threats and enhance the performance.

Trust-based security systems are poised to revolutionise future security strategies by focusing on behavioural aspects. These systems go beyond traditional methods, adapting to real-time behaviour patterns and environmental context. Trust metrics can optimise resource allocation, enhancing system performance by prioritising trusted entities. They harness collective intelligence to share threat information and improve overall system knowledge. Machine learning integration enables adaptive learning from experiences, leading to a constantly improving trust system. Advanced hardware capabilities support the deployment of complex trust models, even on resource-constrained devices in IoT and edge computing environments. However, ethical considerations and user privacy must be central to the implementation of these systems to ensure responsible and effective adoption.

References

[1] A. Alzahrani, H. Jari, and N. Thomas, "Analysing the effect of mobility on the performance of MANET routing protocols," *Proceedings of the 35th Annual UK Performance Engineering Workshop (UKPEW 2019)*, vol. 35, pp. 1 – 11, 12 2019.

[2] H. Jari, A. Alzahrani, and N. Thomas, "Performance evaluation of manet trust-based AODV protocol in the presence of black hole attacks," *Proceedings of the 36th Annual UK Performance Engineering Workshop (UKPEW 2020)*, vol. 36, pp. 30 – 40, 12 2020.

[3] H. Jari and N. Thomas, "Performance evaluation of indirect trust management in MANET routing protocols," *Proceedings of the 38th Annual UK Performance Engineering Workshop (UKPEW 2022)*, vol. 38, pp. 79 – 89, 12 2022.

[4] H. Jari, A. Alzahrani, and N. Thomas, "A novel indirect trust mechanism for addressing black hole attacks in MANET," *DIVANet 2021 - Proceedings of the 11th ACM Symposium on Design and Analysis of Intelligent Vehicular Networks and Applications*, pp. 27–34, 2021.

[5] C. P. Subir Kumar Sarkar, T.G. Basavaraju, *Ad hoc mobile wireless networks principles, protocols, and applications*, 2nd ed. CRC Press, New York, 2016.

[6] J. Hoebeke, I. Moerman, B. Dhoedt, and P. Demeester, "An overview of mobile ad hoc networks: Applications and challenges," *Journal Communications Network*, vol. 3, pp. 60–66, 07 2004.

[7] N. I. S. Ramli, S. I. Hisham, N. S. N. Ismail, and M. Ramalingam, "Performance comparison between AODV and DSR in mobile ad-hoc network (MANET)," in *2021 International Conference on Software Engineering Computer Systems and 4th International Conference on Computational Science and Information Management (ICSECS-ICOCSIM)*, 2021, pp. 217–221.

[8] D. Ramphull, A. Mungur, S. Armoogum, and S. Pudaruth, "A review of mobile ad hoc network (MANET) protocols and their applications," in *2021 5th International Conference on Intelligent Computing and Control Systems (ICICCS)*, 2021, pp. 204–211.

[9] J. H. Cho, A. Swami, and I. R. Chen, "A survey on trust management for mobile ad hoc networks," *IEEE Communications Surveys and Tutorials*, vol. 13, pp. 562–583, 2011.

[10] H. Yu, Z. Shen, C. Miao, C. Leung, and D. Niyato, "A survey of trust and reputation management systems in wireless communications," *Proceedings of the IEEE*, vol. 98, pp. 1755 – 1772, 10 2010.

[11] S. A. K. Omari and P. Sumari, "An overview of mobile ad hoc networks for the existing protocols and applications," *International Journal on Applications of Graph Theory In Wireless Ad Hoc Networks And Sensor Networks*, vol. 2, pp. 87–110, 3 2010.

[12] S. Patnaik, *Recent development in wireless sensor and ad-hoc networks*. Springer, 2015.

[13] Z. Ismail and R. Hassan, "A performance study of various mobility speed on AODV routing protocol in homogeneous and heterogeneous manet," 2011, pp. 637–642.

[14] S. Purbey, "A Review on MANET (Mobile Ad Hoc Network)," *International Journal of Emerging Trends in Engineering and Development*, vol. 1, no. 9, pp. 7–12, 2018.

[15] U. Srilakshmi, N. Veeraiah, Y. Alotaibi, S. A. Alghamdi, O. I. Khalaf, and B. V. Subbayamma, "An improved hybrid secure multipath routing protocol for MANET," *IEEE Access*, vol. 9, pp. 163 043–163 053, 2021.

[16] V. N. Talooki and J. Rodriguez, "Quality of service for flat routing protocols in mobile ad hoc networks," in *Proceedings of the 5th International ICST Mobile Multimedia Communications Conference*. Brussels, BEL: ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering), 2009. [Online]. Available: https://doi.org/10.4108/ICST.MOBIMEDIA2009.7334

[17] X. Hong, K. Xu, and M. Gerla, "Scalable routing protocols for mobile ad hoc networks," *IEEE Network*, vol. 16, no. 4, pp. 11–21, July 2002.

[18] P. Arce, J. C. Guerri, A. Pajares, and O. Lázaro, "Performance evaluation of video streaming over ad hoc networks using flat and hierarchical routing protocols," *Mobile Networks and Applications*, vol. 13, pp. 324–336, 2008.

[19] D. P. I. I. Ismail and M. H. F. Ja'afar, "Mobile ad hoc network overview," in *2007 Asia-Pacific Conference on Applied Electromagnetics*, 2007, pp. 1–8.

[20] S. Singh, A. Pise, O. Alfarraj, A. Tolba, and B. Yoon, "A cryptographic approach to prevent network incursion for enhancement of QoS in sustainable smart city using MANET," *Sustainable Cities and Society*, vol. 79, p. 103483, 2022. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2210670721007423

[21] V. K. Quy, V. H. Nam, D. M. Linh, and L. A. Ngoc, "Routing algorithms for MANET-IoT networks: A comprehensive survey," *Wireless Personal Communications*, vol. 125, pp. 3501–3525, 8 2022.

[22] M. Maad Hamdi, L. Audah, S. Abduljabbar Rashid, A. Hamid Mohammed, S. Alani, and A. Shamil Mustafa, "A review of applications, characteristics and challenges in vehicular ad hoc networks (VANETs)," in *2020 International Congress on Human-Computer Interaction, Optimization and Robotic Applications (HORA)*, 2020, pp. 1–7.

[23] S. Goumiri, M. A. Riahla, and M. Hamadouche, "Security issues in self-organized ad-hoc networks (MANET, VANET, and FANET): A survey," in *Artificial Intelligence and Its Applications*, B. Lejdel, E. Clementini, and L. Alarabi, Eds. Cham: Springer International Publishing, 2022, pp. 312–324.

[24] G. Kaur and P. Thakur, "Routing protocols in MANET: An overview," in *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, vol. 1, 2019, pp. 935–941.

[25] H. Jhajj, R. Datla, and N. Wang, "Design and implementation of an efficient multi-path AODV routing algorithm for MANETs," in *2019 IEEE 9th Annual Computing and Communication Workshop and Conference (CCWC)*, 2019, pp. 0527–0531.

[26] V. Sahu, P. K. Maurya, G. Sharma, A. Roberts, and M. Srivastava, "An overview of AODV routing protocol," *International Journal of Modern Engineering Research (IJMER) www.ijmer.com*, vol. 2. [Online]. Available: https://www.researchgate.net/publication/252068339

[27] T. K. Saini and S. C. Sharma, "Recent advancements, review analysis, and extensions of the AODV with the illustration of the applied concept," *Ad Hoc Networks*, vol. 103, p. 102148, 2020.

[28] S. R. Das, C. E. Perkins, and E. M. Belding-Royer, "Ad hoc On-Demand Distance Vector (AODV) Routing," RFC 3561, Jul. 2003. [Online]. Available: https://www.rfc-editor.org/info/rfc3561

[29] M. A. Abdelshafy and P. J. King, "Analysis of security attacks on AODV routing," *2013 8th International Conference for Internet Technology and Secured Transactions, ICITST 2013*, pp. 290–295, 2013.

[30] N. Khanna and M. Sachdeva, "A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in MANETs," *Computer Science Review*, vol. 32, pp. 24–44, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1574013718301862

[31] F. Abdel-Fattah, K. A. Farhan, F. H. Al-Tarawneh, and F. AlTamimi, "Security challenges and attacks in dynamic mobile ad hoc networks MANETs," in *2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT)*, 2019, pp. 28–33.

[32] N. Khanna and M. Sachdeva, "A comprehensive taxonomy of schemes to detect and mitigate blackhole attack and its variants in manets," *Computer Science Review*, vol. 32, pp. 24–44, 2019. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1574013718301862

[33] M. Karthigha, L. Latha, and K. Sripriyan, "A comprehensive survey of routing attacks in wireless mobile ad hoc networks," in *2020 International Conference on Inventive Computation Technologies (ICICT)*, 2020, pp. 396–402.

[34] B. Banerjee and S. Neogy, "A brief overview of security attacks and protocols in MANET," in *2021 IEEE 18th India Council International Conference (INDICON)*, 2021, pp. 1–6.

[35] O. Fasunlade, S. Zhou, and D. Sanders, "Comprehensive review of collaborative network attacks in MANET," in *2020 IEEE 44th Annual Computers, Software and Applications Conference (COMPSAC)*, 2020, pp. 1542–1545.

[36] F. C. Korir and W. Cheruiyot, "A survey on security challenges in the current manet routing protocols," *Global Journal of Engineering and Technology Advances*, vol. 12, pp. 078–091, 7 2022.

[37] D. Khan and M. Jamil, "Study of detecting and overcoming black hole attacks in MANET: A review," in *2017 International Symposium on Wireless Systems and Networks (ISWSN)*, 2017, pp. 1–4.

[38] Z. A. Zardari, J. He, N. Zhu, K. H. Mohammadani, M. S. Pathan, M. I. Hussain, and M. Q. Memon, "A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in MANETs," *Future Internet*, vol. 11, 2019.

[39] M. Tahboush and M. Agoyi, "A hybrid wormhole attack detection in mobile ad-hoc network (MANET)," *IEEE Access*, vol. 9, pp. 11 872–11 883, 2021.

[40] P. Sen and M. Rahman, "Investigating the performance of MANET routing protocols under jamming attack," in *Innovations in Computer Science and Engineering*, H. S. Saini, R. Sayal, A. Govardhan, and R. Buyya, Eds. Singapore: Springer Singapore, 2021, pp. 251–258.

[41] R. L. Raju and C. R. Reddy, "Node activity based trust and reputation estimation approach for secure and QoS routing in MANET," *International Journal of Electrical and Computer Engineering*, vol. 9, no. 6, pp. 5340–5350, 2019.

[42] Y. Kumar and S. Ravichandran, "Secure data transfer in manet with key calculator and key distributer using cryptography methods," *International Journal of Safety and Security Engineering*, vol. 10, pp. 567–572, 10 2020.

[43] M. Islabudeen and M. K. K. Devi, "A smart approach for intrusion detection and prevention system in mobile ad hoc networks against security attacks," *Wireless Personal Communications*, vol. 112, pp. 193–224, 5 2020.

[44] N. Khanna and M. Sachdeva, "Study of trust-based mechanism and its component model in manet: Current research state, issues, and future recommendation," *International Journal of Communication Systems*, vol. 32, no. 12, p. e4012, 2019, e4012 IJCS-18-0575.R2. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/dac.4012

[45] A. Singh, M. Maheshwari, Nikhil, and N. Kumar, "Security and trust management in MANET," in *Information Technology and Mobile Communication*, V. V. Das, G. Thomas, and F. Lumban Gaol, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2011, pp. 384–387.

[46] M. K. Deno and T. Sun, "Probabilistic trust management in pervasive computing," in *2008 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing*, vol. 2, 2008, pp. 610–615.

[47] J. Sen, P. Chowdhury, and I. Sengupta, "A distributed trust mechanism for mobile ad hoc networks," 12 2006, pp. 62 – 67.

[48] S. Nageswararao and S. Chigarapalle, "Weightage based trusted QoS protocol in mobile adhoc networks," *Proceedings - 2014 IEEE Global Conference on Wireless Computing and Networking, GCWCN 2014*, pp. 283–287, 02 2015.

[49] S. Mostafavi, V. Hakami, and F. Paydar, "A QoS-assured and mobility-aware routing protocol for MANETs," *International Journal on Informatics Visualization*, vol. 4, 02 2020.

[50] V. L. S. S. Kasa, C. S. Bindu, and N. Sirisala, "Trusted quality of service routing protocol in mobile ad-hoc networks," *2018 3rd IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology, RTEICT 2018 - Proceedings*, pp. 2269–2273, 2018.

[51] L. Zadeh, "Fuzzy sets," *Information and Control*, vol. 8, no. 3, pp. 338–353, 1965. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S001999586590241X

[52] A. Jøsang, R. Ismail, and C. Boyd, "A survey of trust and reputation systems for online service provision," *Decision Support Systems*, vol. 43, no. 2, pp. 618–644, 2007, Emerging Issues in Collaborative Commerce. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0167923605000849

[53] Z. Wei, L. Lu, and Z. Yanchun, "Using fuzzy cognitive time maps for modeling and evaluating trust dynamics in the virtual enterprises," *Expert Systems with Applications*, vol. 35, no. 4, pp. 1583–1592, 2008. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S095741740700382X

[54] H. Chen and Z. Ye, "Research of P2P trust based on fuzzy decision-making," vol. 2, 2008, pp. 793–796.

[55] D. Helen and D. Arivazhagan, "A stable routing algorithm for mobile ad hoc network using fuzzy logic system," *International Journal of Advanced Intelligence Paradigms*, vol. 14, no. 3-4, pp. 248–259, 2019. [Online]. Available: https://www.inderscienceonline.com/doi/abs/10.1504/IJAIP.2019.103412

[56] W. Saad, Z. Han, M. Debbah, A. Hjorungnes, and T. Basar, "Coalitional game theory for communication networks," *IEEE Signal Processing Magazine*, vol. 26, no. 5, pp. 77–97, 2009.

[57] L. I. Li, "Reputation, trust, and rebates: How online auction markets can improve their feedback mechanisms," *Journal of Economics & Management Strategy*, vol. 19, no. 2, pp. 303–331, 2010. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1530-9134.2010.00253.x

[58] M. Harish, G. Mahalakshmi, and T. Geetha, "Game theoretic model for p2p trust management," in *International Conference on Computational Intelligence and Multimedia Applications (ICCIMA 2007)*, vol. 1, 2007, pp. 564–566.

[59] K. lu, J. Wang, and M. Li, "An eigentrust dynamic evolutionary model in P2P file-sharing systems," *Peer-to-Peer Networking and Applications*, vol. 9, 05 2016.

[60] V. Srivastava, J. Neel, A. Mackenzie, R. Menon, L. Dasilva, J. Hicks, J. Reed, and R. Gilles, "Using game theory to analyze wireless ad hoc networks," *Communications Surveys Tutorials, IEEE*, vol. 7, pp. 46– 56, 03 2006.

[61] B. Khan, F. Anwar, R. Olanrewaju, B. Rasool, and R. Mir, "A game theory-based strategic approach to ensure reliable data transmission with optimized network operations in futuristic mobile ad hoc networks," *IEEE Access*, vol. PP, pp. 1–1, 06 2020.

[62] W. Yu and K. R. Liu, "Game theoretic analysis of cooperation stimulation and security in autonomous mobile ad hoc networks," *IEEE Transactions on Mobile Computing*, vol. 6, no. 5, pp. 507–521, 2007.

[63] W. T. Teacy, J. Patel, N. R. Jennings, and M. Luck, "TRAVOS: Trust and reputation in the context of inaccurate information sources," *Autonomous Agents and Multi-Agent Systems*, vol. 12, no. 2, p. 183–198, mar 2006. [Online]. Available: https://doi.org/10.1007/s10458-006-5952-x

[64] F. N. Nwebonyi, R. Martins, and M. E. Correia, "Reputation based approach for improved fairness and robustness in P2P protocols," *Peer-to-Peer Networking and Applications*, vol. 12, pp. 951–968, 7 2019.

[65] J. Mundinger and J.-Y. Le Boudec, "Analysis of a reputation system for mobile ad-hoc networks with liars," *Performance Evaluation*, vol. 65, no. 3, pp. 212–226, 2008. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S016653160700048X

[66] R. Varadarajan and M. Yadav, "Marketing strategy and the internet: An organizing framework," *Journal of The Academy of Marketing Science - J ACAD MARK SCI*, vol. 30, pp. 296–312, 10 2002.

[67] S. Stieglitz, C. Fuchb, and C. Lattemann, "A business model for mobile ad-hoc communities," *2009 IEEE Conference on Commerce and Enterprise Computing, CEC 2009*, pp. 252–257, 2009.

[68] Y. Zhang, K.-J. Lin, and R. Klefstad, "Direct: A robust distributed broker framework for trust and reputation management," in *Eighth IEEE International Conference on E-Commerce Technology (CEC 2006) / Third IEEE International Conference on Enterprise Computing, E-Commerce and E-Services (EEE 2006) and Workshops, 26-29 June 2006, Palo Alto, California*. IEEE Computer Society, 2006, p. 21. [Online]. Available: http://doi.ieeecomputersociety.org/10.1109/CEC-EEE.2006.35

[69] X. Lin, X. Wang, and N. Hajli, "Building e-commerce satisfaction and boosting sales: The role of social commerce trust and its antecedents," *International Journal of Electronic Commerce*, vol. 23, no. 3, pp. 328–363, 2019. [Online]. Available: https://doi.org/10.1080/10864415.2019.1619907

[70] R. Li and J. Li, "Requirements and design for neutral trust management framework in unstructured networks," *Journal of Supercomputing*, vol. 64, pp. 702–716, 6 2013.

[71] Q. H. Vu, M. Lupu, and B. C. Ooi, *Peer-to-peer computing: Principles and applications*. Springer Berlin Heidelberg, 2010.

[72] F. Cornelli, E. Damiani, S. D. C. di Vimercati, S. Paraboschi, and P. Samarati, "Choosing reputable servents in a P2P network," in *Proceedings of the 11th International Conference on World Wide Web*, ser. WWW '02. New York,

NY, USA: Association for Computing Machinery, 2002, p. 376–386. [Online]. Available: https://doi.org/10.1145/511446.511496

[73] R. J. Cai, X. J. Li, and P. H. J. Chong, "An evolutionary self-cooperative trust scheme against routing disruptions in MANETs," *IEEE Transactions on Mobile Computing*, vol. 18, pp. 42–55, 2019.

[74] Q. He, D. Wu, and P. Khosla, "SORI: A secure and objective reputation-based incentive scheme for ad-hoc networks," *2004 IEEE Wireless Communications and Networking Conference, WCNC 2004*, vol. 2, pp. 825–830, 2004.

[75] S. Marti, T. J. Giuli, K. Lai, and M. Baker, "Mitigating routing misbehavior in mobile ad hoc networks," in *Proceedings of the 6th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '00. New York, NY, USA: Association for Computing Machinery, 2000, p. 255–265. [Online]. Available: https://doi.org/10.1145/345910.345955

[76] Y. L. Sun, W. Yu, and Z. Han, "Information theoretic framework of trust modeling and evaluation for ad hoc networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, pp. 305–315, 2 2006.

[77] S. Buchegger and J.-Y. Le Boudec, "A robust reputation system for mobile ad-hoc networks," 2003. [Online]. Available: http://infoscience.epfl.ch/record/486

[78] K. Govindan and P. Mohapatra, "Trust computations and trust dynamics in mobile adhoc networks: A survey," *IEEE Communications Surveys and Tutorials*, vol. 14, pp. 279–298, 2012.

[79] Y. Sun, Z. Han, and K. R. Liu, "Defense of trust management vulnerabilities in distributed networks," *IEEE Communications Magazine*, vol. 46, no. 2, pp. 112–119, 2008.

[80] J.-H. Cho and I.-R. Chen, "On the tradeoff between altruism and selfishness in manet trust management," *Ad Hoc Networks*, vol. 11, no. 8, pp. 2217–2234, 2013. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1570870513001030

[81] U. Herberg, T. H. Clausen, and C. Dearlove, "Integrity Check Value and Timestamp TLV Definitions for Mobile Ad Hoc Networks (MANETs)," Internet Engineering Task Force, Internet-Draft draft-ietf-manet-rfc6622-bis-03. [Online]. Available: https://datatracker.ietf.org/doc/draft-ietf-manet-rfc6622-bis/03/

[82] M. Singh and S. Kumar, "A survey: Ad-hoc on demand distance vector (aodv) protocol," *International Journal of Computer Applications*, vol. 161, no. 1, pp. 38–44, 2017.

[83] D. N. Patel, S. B. Patel, H. R. Kothadiya, P. D. Jethwa, and R. H. Jhaveri, "A survey of reactive routing protocols in manet," in *International Conference on Information Communication and Embedded Systems (ICICES2014)*, 2014, pp. 1–6.

[84] S. Peng, Y. Wang, H. Xiao, and B. Lin, "Implementation of an improved aodv routing protocol for maritime ad-hoc networks," in *2020 13th International Congress on Image and Signal Processing, BioMedical Engineering and Informatics (CISP-BMEI)*, 2020, pp. 7–11.

[85] V. V. Sarbhukan and L. Ragha, "Establishing secure routing path using trust to enhance security in manet," *Wireless Personal Communications*, vol. 110, pp. 245–255, 1 2020.

[86] I. Chakeres and E. Belding-Royer, "Aodv routing protocol implementation design," in *24th International Conference on Distributed Computing Systems Workshops, 2004. Proceedings.*, 2004, pp. 698–703.

[87] D. Ravilla and C. S. R. Putta, "Enhancing the security of manets using hash algorithms," *Procedia Computer Science*, vol. 54, pp. 196–206, 2015, eleventh International Conference on Communication Networks, ICCN 2015, August 21-23, 2015, Bangalore, India Eleventh International Conference on Data Mining and Warehousing, ICDMW 2015, August 21-23, 2015, Bangalore, India Eleventh International Conference on Image and Signal Processing, ICISP 2015, August 21-23, 2015, Bangalore, India. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050915013460

[88] M. S. Usha and K. C. Ravishankar, "Implementation of trust-based novel approach for security enhancements in manets," *SN Computer Science*, vol. 2, 7 2021.

[89] N. Sirisala and C. S. Bindu, "Weightage based trusted qos protocol in mobile ad hoc networks," *Proceedings - 2014 IEEE Global Conference on Wireless Computing and Networking, GCWCN 2014*, pp. 283–287, 2015.

[90] M. Yadollahzadeh-Tabari, "An Stochastic Reward net Model for Performance Analysis of Network layer in Mobile Ad Hoc Network Under the Workload of Misbehvaior Nodes," *Wireless Personal Communications*, vol. 118, no. 2, pp. 1087–1109, 2021. [Online]. Available: https://doi.org/10.1007/s11277-020-08060-0

[91] T. Issariyakul, E. Hossain, T. Issariyakul, and E. Hossain, *Introduction to network simulator 2 (NS2)*. Springer, 2009.

[92] S. Kurkowski, T. Camp, N. Mushell, and M. Colagrosso, "A visualization and analysis tool for NS-2 wireless simulations: inspect," in *13th IEEE International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems*. IEEE, 2005, pp. 503–506.

[93] G. F. Riley and T. R. Henderson, *The NS-3 Network Simulator*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010, pp. 15–34. [Online]. Available: https://doi.org/10.1007/978-3-642-12331-3_2

[94] J. L. Font, P. Iñigo, M. Domínguez, J. L. Sevillano, and C. Amaya, "Architecture, design and source code comparison of NS-2 and NS-3 network simulators," in *Proceedings of the 2010 Spring Simulation Multiconference*. San Diego, CA, USA: Society for Computer Simulation International, 2010. [Online]. Available: https://doi.org/10.1145/1878537.1878651

[95] S. F. O'Brien and Q. L. Yi, "How do I interpret a confidence interval?" *Transfusion*, vol. 56, no. 7, pp. 1680–1683, 2016. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1111/trf.13635

[96] H. Xia, "Trust management model for mobile ad hoc network based on analytic hierarchy process and fuzzy theory," *IET Wireless Sensor Systems*, vol. 1, pp. 248–266(18), December 2011. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-wss.2011.0042

[97] X. Li, "Trust-based on-demand multipath routing in mobile ad hoc networks," *IET Information Security*, vol. 4, pp. 212–232(20), December 2010. [Online]. Available: https://digital-library.theiet.org/content/journals/10.1049/iet-ifs.2009.0140

[98] N. Jaisankar, R. Saravanan, and K. D. Swamy, "A novel security approach for detecting black hole attack in MANET," *CCIS*, vol. 70, pp. 217–223, 2010.

[99] H. Moudni, M. Er-rouidi, H. Mouncif, and B. E. Hadadi, "Black hole attack detection using fuzzy based intrusion detection systems in MANET," *Procedia Computer Science*, vol. 151, pp. 1176–1181, 2019, the 10th International Conference on Ambient Systems, Networks and Technologies (ANT 2019) / The 2nd International Conference on Emerging Data and Industry 4.0 (EDI40 2019) / Affiliated Workshops. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1877050919306350

[100] J. Xie and T. Murase, "An optimal location allocation by multi-user cooperative mobility for maximizing throughput in MANETs," *IEEE Access*, vol. 8, pp. 226 089–226 107, 2020.

[101] V. S. Janani and M. S. Manikandan, "Efficient trust management with bayesian-evidence theorem to secure public key infrastructure-based mobile ad hoc networks," *Eurasip Journal on Wireless Communications and Networking*, vol. 2018, 12 2018.

[102] H. M. Haglan, S. A. Mostafa, N. Z. M. Safar, A. Mustapha, M. Z. Saringatb, H. Alhakami, and W. Alhakami, "Analyzing the impact of the number of nodes on the performance of the routing protocols in manet environment," *Bulletin of Electrical Engineering and Informatics*, vol. 10, pp. 434–440, 2 2021.

[103] G. Singal, V. Laxmi, M. S. Gaur, S. Todi, V. Rao, and A. Zemmari, "MCLSPM: Multi-constraints link stable multicast routing protocol in ad hoc networks," in *2016 Wireless Days (WD)*, 2016, pp. 1–6.

[104] B. Divecha, A. Abraham, C. Grosan, and S. Sanyal, "Impact of node mobility on MANET routing protocols models," *Journal of Digital Information Management*, vol. 5, no. 1, pp. 19–23, 2007.

[105] R. I. Al-Essa and G. A. Al-Suhail, "Mobility and transmission power of AODV routing protocol in MANET," in *2022 2nd International Conference on Computing and Machine Intelligence (ICMI)*, 2022, pp. 1–5.

[106] P. Singh and M. Khari, "Empirical analysis of energy-efficient hybrid protocol under black hole attack in manets," in *Research in Intelligent and Computing in Engineering: Select Proceedings of RICE 2020*. Springer, 2021, pp. 725–734.

[107] R. Vatambeti, K. S. Supriya, and S. Sanshi, "Identifying and detecting black hole and gray hole attack in manet using gray wolf optimization," *International Journal of Communication Systems*, vol. 33, no. 18, p. e4610, 2020.

[108] V. Alappatt and J. P. PM, "Trust-based energy efficient secure multipath routing in manet using lf-sso and sh2e," *International Journal of Computer Networks and Applications*, vol. 8, no. 4, pp. 400–400, 2021.

[109] Z. Yang, L. Li, F. Gu, X. Ling, and M. Hajiee, "TADR-EAODV: A trust-aware dynamic routing algorithm based on extended AODV protocol for secure communications in wireless sensor networks," *Internet of Things*, vol. 20, p. 100627, 2022.

[110] T. Varshney, T. Sharma, and P. Sharma, "Implementation of watchdog protocol with AODV in mobile ad hoc network," in *2014 Fourth International Conference on Communication Systems and Network Technologies*. IEEE, 2014, pp. 217–221.

[111] P. Gupta, P. Goel, P. Varshney, and N. Tyagi, "Reliability factor based aodv protocol: Prevention of black hole attack in manet," in *Smart Innovations in Communication and Computational Sciences: Proceedings of ICSICCS-2018*. Springer, 2019, pp. 271–279.

[112] R. R. Chandan and P. Mishra, "Performance analysis of AODV under black hole attack," in *Proceedings of 2nd International Conference on Advanced Computing and Software Engineering (ICACSE)*, 2019.

[113] J. R. Pullagura and V. R. Dhulipalla, "Black-hole attack and counter measure in ad hoc networks using traditional routing optimization," *Concurrency and Computation: Practice and Experience*, p. e7643, 2023.