CHAPTER I

INTRODUCTION
1 INTRODUCTION

In this chapter, Section 1.1 introduces security issues in Mobile Adhoc Networks and discuss regarding role of Intrusion detection techniques for secure routing. Section 1.2 introduces Black Hole Attack problems in MANETs and its impact on AODV protocol. Section 1.3 introduces the different defense mechanisms for Black Hole Attack detection. Section 1.4 presents challenges for MANET security. Section 1.5 presents scopes and motivations. Section 1.6 lists problem statements. The scopes and objectives of this thesis are explained in Section 1.7. Section 1.8 presents the main contributions of the proposed research work. Finally, Section 1.9 outlines the organization of this thesis.

1.1 SECURITY IN MANET

As Mobile Adhoc Network (MANET) has evolved as a key enabling technology, and there is an emerging trend towards improving the security [1]. The MANET consists of a collection of wireless mobile nodes which can communicate with other in the transmission range without the use of a network infrastructure. The routing plays a significant role in the security of MANET communication. The mobile nodes in MANET also function as intermediate routers that involve in the data forwarding for other nodes [2]. The primary objective of a MANET routing protocol is to establish an efficient path between the communicating nodes. The multiple intermediate
nodes need to co-operate in establishing the routing path for wireless communication among far away nodes through multiple hops. There is a need for some distributed algorithms to organize the network topology in the routing process. Routing represents the moving data from a source to a destination, and it includes the activities of optimal path determination and data transfer. The determination of optimal path between two nodes becomes quite complicated due to the unpredictable movement of the nodes in the network. The optimal path determination is difficult in the dynamic network topology. The crucial factors such as link quality, dynamic topology, and energy consumption are the significant issues in MANET. Another concern that significantly impacts the MANET is the security of the routing process [3]. The lack of centralized administration and constrained battery power, dynamic network topology and lack of physical security of the mobile nodes are the primary factor for the vulnerability in MANET. If the malicious activities misdirect routing, the complete routing can be paralyzed. Thus, securing the routing activity plays a vital role in establishing secure communication among mobile nodes [4]. However, the fundamental characteristics of MANET such as open wireless medium, dynamic network, distributed cooperation, and constrained resources make it inherently vulnerable.

1.1.1 INTRUSION DETECTION IN ROUTING

Intrusion detection has gained more importance in secure routing. The characteristics of MANET are susceptible to different intrusions. The security in MANET implies the identification and elimination of routing attacks from the network [5][6]. Several types of intrusions are being carried out against the routing activity in MANET. The intrusions in routing can be categorized into passive and active intrusions. A passive intrusion aims at discovering the valuable information by listening to traffic without disrupting the routing operation. An active intrusion improperly modifies the data, gains authentication, or disrupts the data routing flows. Active intrusions are further divided into internal and external intrusions. The nodes belonging to the network are likely to cause routing disruption with malign intent. The internal intruders are already authorized in the network, and so they typically create a severe impact before getting detected by the network. Therefore, detecting such malicious node is the primary function of an effective Intrusion Detection Systems (IDS). It is necessary that the design of an IDS has to be efficient to detect the intrusion activities continuously in the network. An IDS includes the process of monitoring the node activities in a system or network. Designing an IDS in MANET is a challenging task due to the open characteristics of MANET [5]. The lack of infrastructure in
MANET necessitates the design of intrusion detection system as distributed and cooperative. The IDS can be categorized into two different types such as centralized IDS and distributed IDS. In centralized IDS, a centralized monitor is employed to monitor the whole network activities.

1.2 THE BLACK HOLE PROBLEM IN MANET ROUTING PROTOCOLS

The black hole is the most destructive threat in MANET. The black hole nodes utilize the routing protocol functionalities to advertise themselves as the shortest path to the destination [5]. The black-hole node drops all the data packets, by proclaiming as the nearest route to the destination. Moreover, the black hole attacker can observe the network traffic and trace the activity of each node in the network. The impact of the black hole attack varies for different routing protocols. Conventionally, the routing protocols are classified into proactive and reactive routing. The proactive routing protocol always enables each node to maintain the up-to-date routing information in their routing table, for instance, Destination Sequence-based Distance Vector (DSDV) routing. However, the reactive routing protocols are designed to discover the route to the destination, only when it is needed, for instance, Dynamic Source Routing (DSR) and AdHoc On-demand Distance Vector (AODV) routing. The DSR follows a source routing, but AODV uses a table-driven routing with destination sequence numbers. The primary way of a black hole to enter into the routing path using destination sequence number, which represents the fresh or recent route to the destination. Thus, the black hole impact on AODV and DSDV is high, compared to the DSR. Moreover, an efficient operation of a reactive routing is due to the nature of route discovery on demand. However, as there is no security considered in currently used routing protocols, the routing protocol is an easy target for malicious nodes. Although the reactive routing protocols aim at increasing the reliability of wireless communication by initiating the route discovery on demand, the black hole downgrades the routing protocol performance. Several defense systems have been proposed in the literature to detect and terminate the impact of black hole nodes on conventional routing protocols. The routing layer attackers are gaining advantage day by day due to continuous improvements in the advanced technology. It is paramount to focus on significant security obstacles in reactive routing protocols as well. Most reactive routing protocols operate according to the strong assumption that all nodes are benign and cooperate during data forwarding. This assumption is not suitable for real scenarios, where the mobile nodes can be compromised for launching adversarial activities.
1.2.1 CATEGORIES OF BLACK-HOLE ATTACK

The black hole attack can be classified as individual and collaborative black-hole attack [7]. The former performs an attack individually and establishes a new and shortest route to the destination. The latter enables two or more nodes to cooperate with the intent of malign. In the individual black hole, a single node misuses the route discovery process to claim it as the shortest path to the destination. After receiving the data packets from the source node, it starts to drop the routing packets without forwarding it to its next-hop node. A single black hole attack happens easily in the MANET routing protocols. Compared to the individual black hole attack, the collaborative black hole attack is more robust to identify. The single or collaborative black-hole nodes disrupt the routing function of the communicating nodes and create damage to the network resources. The destination or legitimate intermediate nodes that initially have a route to the destination may reply the Route REQuest (RREQ) packet. If the Route REPLY (RREP) packet is received from a normal node, the routing protocol functions well. However, in the case of receiving the RREQ through the malicious node, it could not check its routing table. It generates the fake RREP with the intention of reaching the source node first. When the source node receives the fake RREP, it presumes that the route discovery process is complete and ignores all other RREP messages. As a result, the source node sends all the packets to the malicious node. In this way, the malicious node can easily mislead or drop the data packets and possibly cause damage to the network resources.

1.2.2 VARIANTS OF BLACK HOLE ATTACK AND ITS IMPACT ON REACTIVE ROUTING PROTOCOLS

A black-hole is a most severe attack in MANET. The variants of the black-hole attack are gray-hole and worm-hole, regarding routing in MANET [6][7]. The black-hole attack attempts to advertise false information in the network to attract network traffic as possible towards itself, and the absorbed traffic is dropped, whereas the wormhole attackers located in different regions collude with each other to receive the network traffic. The gray-hole attack is also a different version of the black hole attack, and in contrast to the black-hole attack, it selectively drops the data packets. Due to the gray-hole attack that switches its behavior from being malevolent and benevolent, is tough to discover in MANET [8].

Most reactive routing protocols initiate the route discovery process when a node demands
communication with another node. It broadcasts an RREQ packet to its neighbors [9-12]. The RREQ receiving nodes rebroadcast the packets until either the destination or an intermediate node with a fresh route to the destination is identified. When the destination or an intermediate node with a fresh route receives the RREQ, it responds by unicasting an RREP packet back to the sender node through the intermediate neighbors from which it received the RREQ. It creates a fresh and shortest path between the source and destination nodes. From the route discovery process of routing protocols, the black-hole attack could easily attack the MANET. According to the original activities of routing protocols, any intermediate node may respond to the RREQ message if it has a fresh route to the destination. The new route is ensured by the large destination sequence number contained in the RREQ packet. This process is implemented for reducing the usage of stale routes and routing delay. However, this process may ease the Black-hole and its variants to involve in the routing path. Either the black-hole or its variants uses the feature by immediately responding the sender using a malicious RREP, having largest destination sequence number and minimum hop count set to the minimum to claim that it has the freshest and shortest route to the destination. On receiving this RREP, the source node forwards the data packets through the claimed path, and subsequently, the malicious node drops all the received packets immediately.

1.3 DEFENSE MECHANISM FOR BLACK-HOLE ATTACK DETECTION

Several defense schemes have been suggested against black-hole attack in MANET. It can be classified into IDS techniques, Trust measurement, and sequence-based methods [12-17].

1.3.1 IDS TECHNIQUES

In a MANET, any unauthorized activity is referred as an intrusion. An intrusion detection system, IDS is a process of monitoring the node activities in a system or network and the mechanism that performs the intrusion detection process is named as IDS [18][19]. Ids can be implemented either in centralized or distributed manner. In centralized IDS, a centralized monitor is used to monitor the whole network activities. In distributed IDS, each node has a separate IDS to monitor the behavior, and it also monitors the one-hop neighbors’ activities. The conventional IDS can be categorized into the anomaly, misuse, and specification-based IDS. The anomaly-based IDS models the legitimate node behavior to decide the routing profiles. The training phase examines the payload and then collects them from different nodes to generate
profiles. They check the legitimate routing patterns with an anomalous payload to detect the back hole attackers in the testing phase. The Misuse-based IDS learns the well-known attack profiles and considers it as a signature. To detect attacks, the signature is matched with the detected routing activity. However, the detection of new attacks is still a question of misuse based IDS. In contrast, the specification-based IDS learns both the normal and abnormal behaviors. While monitoring the network, the normal behavior is differentiated from the malicious activities. However, it is a time-consuming task, and the normal profiles may include errors.

1.3.2 TRUST MEASUREMENT

The trust-based defense models observe the routing behavior of MANET nodes in the past communications. The trust refers the faith on the routing behavior of a node. Most of the reactive defense systems maintain a counter for each neighbor to count the failure rate of packet transmissions. The count of a node increases, only when its next hop refuses to route the data packets through a discovered path [20-22]. This scheme can identify the black-hole attack straightforwardly. The trust management scheme maintains and updates the trust values by observing the neighbor activities continuously. There are three types of trust values used such as direct, indirect, and accumulated path trust. Most trust models derive trust of a node based on its historical routing activities. The trust relationship does not always reflect the actual relationship. However, when the network traffic is low, the neighboring nodes are often unrelated to each other and have no trust information on a node behavior. This tends the system to fail in MANET, especially in the highly mobile environment. The reputation-based mechanism fuses the direct trust values that are collected from neighboring nodes. In some cases, the attackers provide false evidence for the neighboring nodes to escalate the attack detection failure. The most commonly used indirect trust models are a Bayesian and Dempster-Shaffer theory. The Bayesian theory lacks in explicitly handling the ignorance, which is a lack of knowledge on a node whether to trust or distrust. Even though the Dempster-Shaffer theory solves this problem, the opinion consensus rule is fundamentally flawed. The third trust factor is path trust, which is an accumulation of routing cooperation of nodes in a path. However, most of the trust-based defense techniques have failed due to the lack of considering network collision, limited transmission range, false misbehavior, and selective forwarding nature of the attack.
1.3.3 BASED ON SEQUENCE NUMBER

The destination sequence number plays a vital role in launching Black-hole attack in MANET. Most of the defense schemes utilize the factor of a sequence number to detect and eliminate the black-hole attackers from the network [22][23]. The most well-known technique is sequence number accumulation, wherein the sequence number of the received RREP packets is accumulated to compare the sequence number of black-hole attack. When receiving the RREP packet with the largest sequence number compared to the accumulated value, the presence of an attacker is confirmed. There is a need for maintaining a table to store the sequence number, in addition to the routing information. The other significant concept of detecting malicious nodes using sequence number is by setting Timer Expired Table for all the identified routing paths to the destination. The sequence number of every received RREP packets is stored along with the received time of RREP in collecting route reply table. According to the stored sequence number, the malicious RREP with largest sequence number can be identified. This table is also used to eliminate the stale routes, concerning the time value stored in the table. The sequence number threshold based black-hole attack detection is also widely utilized in a MANET to eliminate the attackers in the route discovery phase itself [24][25]. The average value of the stored sequence number over a period is considered as a reference to detect the malicious nodes. According to the updation of sequence number threshold based on the network environment, the defense scheme provides secure routing in MANET. However, when a small change has occurred in the sequence number of the malicious node, the sequence number based defense scheme fails.

1.3.4 INTRUSION DETECTION SYSTEM

In a MANET, any unauthorized activity is referred as an intrusion. An intrusion detection system IDS is a process of monitoring the node activities in a system or network and the mechanism that performs the intrusion detection process is named as IDS [18]. Ids can be implemented either in centralized or distributed manner. In centralized IDS, a centralized monitor is used to monitor the whole network activities. In distributed IDS, each node has a separate IDS to monitor the behavior itself, and it also monitors the one-hop neighbors’ activities. The conventional IDS can be categorized into the anomaly, misuse, and specification-based IDS. The anomaly-based IDS models the legitimate node behavior to decide the routing profiles [9]. The training phase examines the payload and then collects them from different nodes to generate profiles. They check the legitimate routing patterns with an anomalous payload to detect the
Back-hole attackers in the testing phase. The Misuse-based IDS learns the well-known attack profiles and considers it as a signature. To detect attacks, the signature is matched with the detected routing activity. However, the detection of novel attacks is guaranteed in misuse based IDS. In contrast, the specification based IDS learns both the normal and abnormal behaviors. While monitoring the network, the normal behavior is differentiated from the malicious activities. However, it is a time-consuming task, and the normal profiles may include errors.

1.4 CHALLENGES IN MANET SECURITY

Security is a crucial concern in the MANET, and the wireless communication is more susceptible to the black hole attacks. From a security point of view, security systems in MANETs must consider the following features of MANETs [11][4].

- **The absence of centralized infrastructure:** As the centralized infrastructure is not available in MANETs, the node cooperativeness becomes a critical precondition in security systems.

- **Highly dynamic network topology:** The nodes in MANETs are free to move anywhere in the network. The unpredictable node mobility occasionally interrupts communication, resulting in packet drop.

- **Open and error-prone transmission medium:** The transmitted data via a wireless medium is susceptible to both transmission errors and collision dropping.

- **Rigorous power constraint:** Due to the limited battery power, the transmission range of a node is limited. Every node relies on the observations from other nodes to know the global network topology.

1.4.1 NODE MOBILITY AND NETWORK COLLISION

The black hole attack is the major reason for the cause of packet dropping in MANET. Another reason behind the packet loss is node mobility. The data corruption refers to errors in receiving data that occur during the access of the same medium by multiple nodes at a time. This scenario results in data loss. According to the trust measurement, the routing behavior of neighboring nodes is monitored. Hence, considering that the entire packet loss is only due to malevolent node character is not an adequate factor to precisely identify the malicious activities.
in MANET. Although the use of node mobility facilitates to describe the reality, the negative impact of node mobility is high on the accuracy of trust model. The trust model observes the network knowledge, and it can camouflage the packet dropping due to node mobility and collision under the background of malicious behavior. Decide that a packet loss is intentional or unintentional is a crucial challenge in MANET. The contextual information extracted from the network can distinguish the packet loss either due to either network conditions or malicious activities. Mostly, the node speed, mobility frequency, and the number of access nodes are considered as the primary metrics in distinguishing the malicious activities of the packet dropping due to other reasons.

1.5 SCOPE AND MOTIVATION

The emerging trend of mobile devices emphasizes the recent research on wireless communication principally. To utilize the wireless networks in emergency scenarios, the secure routing protocol is the main component to be ensured.

![Figure 1.2 MANET Applications](image)

For example, in a military environment, security is of remarkable concern. Since, belligerent country imposes virus infections, computer hacking, and unauthorized access to malicious intentions. The hackers working for the military intend to breach over the database and collect the secrets of the belligerent country. The insecure communication in military
environments probably damages critical infrastructure in the military. The business sectors need the transfer of the generated data to happen at a time. Hence, the reliability of wireless communication is crucial, since a delay in sending an error in business sectors can severely impact the customer satisfaction. For reliable communication, the popular routing protocol employed widely in MANET is AODV. A black hole attack gravely influences the reactive routing protocol AODV. The proliferation of MANET installation in different application areas demands extraordinary attention on AODV security. With the appearance of dynamic routing paths, new security complications rise the essentials of AODV routing. The conventional AODV routing protocol is designed with the strong assumption of node cooperativeness. On the other hand, secure routing techniques can handle the single Black-hole attack. Nowadays, the business competitors take into account the advanced Black-hole attack known as colluding attackers. This factor adversely affects the most secure applications of the MANET. For instance, the battlefield is a highly secured environment because little interference is impossible for the unauthorized individuals or opponent soldiers or anyone from elsewhere. So such protocols cannot support MANET principally that include the malicious nodes. Therefore, to reduce those risk factors in the applications of MANET, an extremely secure and a quite useful routing is necessary.

1.6 PROBLEM STATEMENT

Most of the current defense mechanisms assume that the AODV routing protocol is affected by the single black hole attack. These works are inefficient in responding to multiple black hole attacks and in providing secure wireless communication. It emphasizes the defense system to focus on both single and multiple black hole attack and extend the conventional systems to mitigate these attacks in MANET. Therefore, little attention has been given to examine and implement the secure routing against multiple black hole attacks. Furthermore, it is essential to focus on secure communication without affecting the performance of the AODV routing protocol. Most conventional defense systems for preventing single/multiple black hole attack in MANET applying AODV routing protocol are evaluated in terms of detection accuracy, packet delivery ratio, throughput, average packet delay, and normalized control overhead. Although the detection accuracy is a fair metric, the throughput and packet delivery ratio is significantly lower due to the unnecessary overhead induced by the control packets. Moreover, the high false rate removes the legitimate nodes as malicious and makes the network as intermittent. At the end of this investigation, it is highlighted that the defense system has considerably reduced the impact of
multiple black hole attacks as well as show best performance in terms of the high packet delivery ratio, low packet loss, low average end-to-end delay, and less routing overhead.

1.7 AIM AND OBJECTIVES

The main aim and objectives of the work are as follows.

- To analyze the working nature of AODV and the impact of the black hole attack on the AODV routing protocol under different MANET environments.
- To survey the existing defense systems against the black hole attacks in MANET.
- To evaluate the existing BDAODV system against the black hole attack in MANET using the NS2 simulator.
- To evaluate the comparative result analysis of MANET security in presence and absence of malicious nodes (Black-hole nodes) activity.
- To detect the Black-hole nodes and determine the most trustworthy routing path for data transmission using the 2-Tier Trust Model
- To design detection algorithm in the network to avoid attacks and secure data transmission.
- To implement an experimental evaluation of the 2-Tier Trust-based model by the innovative approach like NTPTSAODV secure routing protocol.
- To mitigate the impact of node mobility on secure routing and demonstrated how the performance is better in terms of high packet delivery ratios, throughput and end-to-end delay QoS parameters using the weighted trust model.
1.8 CONTRIBUTIONS OF THE PROPOSED WORK

The main contributions of the proposed research work are as follows.

- The performance of an AODV routing protocol under Black-hole malicious scenarios is analyzed in detail.

- The proposed 2-Tier trust model, named as Node Trust Path Trust Secure AODV routing protocol (NTPTSAODV) considerably improves the security of AODV in MANET environment using multi-dimensional trust parameters.

- The trust model integrates historical trust and node mobility in current trust estimation. This scheme effectively balances the attack detection overhead and routing performance.

- To minimize the impact of node mobility and to enhance the routing performance of secure AODV routing protocol, the proposed NTPTSAODV executes weighted trust model regarding routing behavior and node mobility.

Figure 1.2 Research Methodology
• The performance evaluation of the proposed secure routing is simulated using the extensive NS2 simulator. The simulation result demonstrates that the proposed approach delivers secure and efficient routing performance.

• An APP Tool – GUL based Evaluation Tool is very useful and efficient tool for post-performance evaluation comparative results. Using this tool, we can analyze different aspects of network packets delivery ratio, packets drops rate, throughput, delay time etc. also plot graphs based on the python-matplotlib package.

1.9 THESIS OUTLINE

Chapter 2 provides a background on various types of black hole attacks and defense schemes in a MANET environment. It discusses the challenges in MANET routing security. The types of trust and intrusion detection systems against the black hole attacks are analyzed with their limitations.

Chapter 3 discusses the related works. This chapter explains various defense models for single and multiple black hole attacks. The intrusion detection systems such as anomaly, misuse, and specification based models are reviewed. The work which has conducted the performance evaluation of the AODV protocol under various malicious environments is discussed in detail.

Chapter 4 discusses the AODV routing protocol and the impact of the black hole attack on AODV routing performance. The security holes in AODV route discovery and data forwarding phases are discussed in detail. Using NS 2.34, the AODV is analyzed by varying the number of black-hole nodes, the number of connections, and simulation time. This shows the vulnerability of Black-Hole attack under AODV over MANET environment.

Chapter 5 illustrates the issues in existing defense systems against black hole attacks and presents the secure AODV routing, Node Trust Path Trust Secure AODV (NTPTSAODV). The trust information is calculated for control and data packet forwarding individually. The accumulated trust value is used to evaluate the trust of a routing path. Moreover, this work has discussed the importance of node stability to utilize the advantage of secure AODV. Thus, it applies a weighted average of trust and node stability to decide the path trust.

Chapter 6 demonstrates the impact of the number of connections, simulation time, and
malicious nodes on the performance of AODV, Black-hole Detection AODV (BDAODV) and NTPTSAODV. From the scenarios explored, this chapter shows how that the performance of NTPTSAODV has been considerably better, compared to others in MANET environment.

Chapter 7 concludes the work. Moreover, this chapter illustrates the simulation results of the proposed NTPTSAODV under various simulation scenarios and overall performance of the proposed scheme.