Context Aware Monitoring Scheme for Detecting Malicious Nodes in Mobile Ad hoc Networks

Master of Science in Technology Thesis
University of Turku
Department of Information Technology
Networked Systems Security
2013
Salman Manzoor

Examiners
Seppo Virtanen
Antti Hakkala

UNIVERSITY OF TURKU

Department of Information Technology

Salman Manzoor: Context Aware Monitoring Scheme for Detecting Malicious Nodes in Mobile Ad hoc Networks

Master of Science in Technology Thesis, 60 pp

Networked Systems Security

August 2013

In Mobile Ad-hoc Networks (MANETs), nodes communicate with each other without connection to a central access point. Thus they rely on intermediate nodes to send packets to a destination which is multiple hops away from the source. This along with other unique features of MANETs such as dynamic topology, distributed cooperation and constraint capability make them vulnerable to multiple types of security attacks including Denial of Service (DoS). Many applications of MANETs such as disaster monitoring and management require them to be vigilant especially against DoS attacks. Some common DoS attacks include blackhole, wormhole link and forging identities. In blackhole attack, the malicious node advertises itself as having the optimal path to the destination. In wormhole link attack, two nodes make a private tunnel in the network and relay messages to each other through the tunnel. In this thesis, an efficient, robust and distributed context aware monitoring scheme (CAMS) is proposed, to detect and mitigate DoS attacks. CAMS can efficiently detect the presence of blackhole attack and wormhole link attack in MANETs. The proposed scheme exploits the promiscuous mode of the nodes. Simulation results are very promising as the packet delivery ratio for CAMS is more than or equal to 95%. Moreover, CAMS maintains high throughput and the node mobility has very little impact on its behavior.

Keywords - MANETS; Blackhole attack; AODV; Routing Protocols; Denial of Service (DoS);

ACKNOWLEDGEMENTS

I am fortunate to receive the supervision and help from Dr. Seppo Virtanen. I greatly appreciate his generosity in devoting his time to help me in this Master's thesis. In completing this thesis, I also acknowledge the valuable suggestions and support from Mr. Antti Hakkala. University of Turku has provided me with a stimulating environment for research throughout a my degree and has provided significant encouragement and support for this thesis.

I feel extremely fortunate to have guidance from my brothers Kamran Manzoor and Umar Manzoor. Their encouragement and support provided for this thesis enhanced the gratification of completing this thesis. Finally I express thanks to my parents who always inspire and motivate me to take the challenges.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

LIST OF ACRONYMS

AODV Ad hoc On Demand Distance Vector

ARAN Authenticated Routing for Ad hoc Networks

CA Certification Authority

CAMS Context Aware Monitoring Scheme

CREP Route Confirmation Reply

CREQ Route Confirmation Request

DoS Denial of Service

DSR Dynamic Source Routing

DSDV Dynamic Destination-Sequenced Distance Vector Routing

ID Identity

MANETs Mobile Ad hoc Networks

MPRs Multipoint Relays

MITM Man In The Middle

OLSR Optimized Link State Routing

RREP Route Reply

RREQ Route Request

RERR Route Error

SAM Statistical Analysis of Multipath

SEAD Secure Efficient Ad hoc Distance Vector Routing Protocol

TC Topology Control

TIK Tree Authenticated Values

ZPR Zone Routing Protocols

CHAPTER 1

Introduction

Tremendous increase of wireless devices over the last few years has highlighted the importance of Mobile Ad hoc Networks (MANETs) and ubiquitous computing. MANETs are special application of wireless networking. In MANETs, nodes communicate with each other without a centralized administration. Thus they rely on intermediate nodes to send packets to a destination which is multiple hops away from the source. On the one hand, MANETs are infrastructure less networks and thus they can be deployed rapidly at a low cost. On the other hand, network survivability depends on the behavior of nodes, since each node besides functioning as a network host also acts as a router to forward the packets.

MANETs can be characterized as self configurable network with dynamic network topology. Nodes are free to move across the network and this random mobility of nodes causes frequent topology changes in MANETs [1]. The dynamic behavior of topology makes routing in MANETs, a very challenging task as compared to conventional networks. Several routing protocols have been proposed in the literature which can be broadly categorized as: reactive routing protocols, proactive routing protocols and hybrid routing protocols.

MANETs do not rely on predefined infrastructure, thus they are very attractive for mission critical applications. The various situations in which MANETs can be applied include disaster management, military operations, emergency services, maritime communication

and robotics. Obviously, providing security is critical for proper operation of these applications.

1.1 Motivation

The goal of routing protocols is to discover optimal routes from source to destination to deliver packets. Due to lack of central administration, routing protocols rely on cooperation among the nodes to discover routes. This in turn makes MANETs vulnerable as any node can disrupt routing operation and launch diverse attacks against the network including Denial of Service (DoS) attack.

The basic routing protocols for MANETs lack security mechanisms. The sole purpose of routing protocols is to discover routes, and thus they cannot detect and mitigate routing misbehaviors in the network. Attacks such as blackhole [12], grayhole [13] and wormhole link [16], [17] can severely degrade the performance of MANETs. These DoS attacks are killer attacks for MANETs. The motivation behind this thesis is to devise a mechanism to counter DoS attacks without modifying the existing routing protocols.

1.2 Contribution of the Thesis

Previously researchers have mainly focused on providing preventive schemes to protect routing protocols in MANETs. Most of these schemes are based on encryption techniques to limit unauthorized node from joining the network. The motivation behind these schemes is to prevent attack from occurring rather than countering the attack after it has occurred. The main drawback of preventive schemes is the additional traffic introduced due to exchange of encryption/decryption keys. The studies presented in this thesis focus on reactive mechanism rather than preventive mechanism. Thus the scheme presented in this thesis detects the presence of attack in the network and mitigates it.

In this thesis, an efficient, robust and distributed monitoring scheme is proposed, to detect and mitigate routing misbehaviors in MANETs. The proposed context aware monitoring scheme (CAMS) exploits the promiscuous mode of a node to overhear the traffic of its neighboring nodes. The scheme is thoroughly explained in Chapter 5. The proposed

methodology can work with all routing protocols; however, in this thesis the design of CAMS is presented for AODV routing protocol [2].

The research presented in this thesis contributes in formulating a distributed monitoring scheme to assess the performance of each node in MANETs. The monitoring scheme is fault tolerant that is, all neighbors of a node collaboratively monitor its behavior and increment or decrement its trust value. Traffic sniffing is the basis of monitoring scheme which is used to detect the presence of malicious node in the network. After the misbehavior is detected from a node, local decision process is initiated to investigate the malicious activity. Local decision process reduces false positives by considering trust values of each neighbor of the malicious node. Based on the accumulative trust value, local decision process takes a decision regarding the isolation of the malicious node from the network. Thus local decision process reduces the dependency on a single node to declare another node as malicious. The monitoring scheme enforces cooperation among the nodes and detects selfish nodes in the network. Selfish nodes are detected through the use of trust value. Selfish nodes will have lower trust values and thus network services are reduced accordingly. The proposed scheme is simulated in Qualnet 5.0 based on the methods introduced in this thesis.

1.3 Structure of the Thesis

The remainder of the thesis is organized as follows. In the next chapter, routing protocols of MANETs are reviewed. Categories of routing protocols are also presented in this chapter. Reactive as well as proactive routing protocols are described along with their examples. Reactive routing protocol for example, AODV is described in detail, since it is used for testing the performance of the proposed scheme. In chapter 3, node misbehaviors against each layer of TCP/IP reference model are reviewed. Since network layer is responsible for routing, thus chapter 3 focuses on node misbehaviors that exploit routing protocols. This chapter explains attacks such as blackhole, grayhole and wormhole link along with their affects on routing protocols. This chapter also introduces selfishness and impersonation attack against the network layer. Chapter 4 describes literature regarding countermeasures of the attacks against network layer. This chapter also introduces secure routing protocols for MANETs. Chapter 5 deals with the design and technical detail of proposed Context

Aware Monitoring Scheme (CAMS). This chapter thoroughly explains CAMS and its related mechanisms. For example traffic overhearing mechanism and key assumptions for CAMS are described before technical detail of CAMS is presented. Detection and mitigation of different attacks through CAMS is described in this chapter. In chapter 6 performance analysis of CAMS is presented. To estimate the performance of CAMS, this chapter compares network scenarios with and without CAMS in presence of attacks. In this chapter networks running on default AODV and AODV with CAMS are used, to estimate the performance of proposed scheme. The results will be discussed in chapter 6, while chapter 7 concludes the thesis.

CHAPTER 2

Routing in MANETs

Routing is essential for proper operation of MANETs. The goal of routing protocols is to discover the latest and optimal route from source to destination to deliver packets. Many routing protocols have been proposed for MANETs which can be categorized as: reactive routing protocols (demand driven), proactive routing protocols (table driven) and hybrid routing protocols. On the one hand, in reactive routing protocols, for instance Ad hoc On Demand Distance Vector (AODV) [2], routes are discovered when requested by the sender. On the other hand, in proactive routing protocols for example Optimized Link State Routing (OLSR) [7], nodes exchange routing information periodically. Hybrid routing protocols such as Zone Routing Protocols (ZPR) [9], combine good characteristics of both reactive and proactive routing protocols. In next sections each category of routing protocol is briefly described.

2.1 Reactive Routing Protocols

Protocols that discover routes when requested by the sender fall under the category of reactive routing protocols. These protocols are also known as source initiated or on demand routing protocols. Reactive routing protocols do not exchange periodic routing messages, thus they reduce total traffic overhead in the network. Examples of reactive routing protocols include AODV [2], DSR [3], TORA [4] and DYMO [5]. AODV and DSR will be described as an example, since they are most commonly used in MANETs.

2.1.1 Ad hoc On Demand Distance Vector

Ad hoc On Demand Distance Vector (AODV) is a reactive routing protocol, thus nodes do not require maintaining routes for destinations that are not in an active communication. However each node using AODV, maintains routing table entry for each destination of interest. As long as the communication is active and the route is valid between end points, AODV does not play any role. AODV is initiated when routes are required for new destinations or when the link between communicating nodes is broken. AODV protocol uses three control messages to discover and maintain routes. These control messages are: Route REQuest (RREQ), Route REPly (RREP) and Route ERRor (RERR). Sender broadcasts RREQ packet, when it needs to find a route to a new destination. This message contains source address, source sequence number, broadcast identity, destination sequence number and hop count. Source address and broadcast identity, together make each RREQ packet unique. RREP is a reply sent back to the sender from a node which has a fresh route to the destination. The RREP packet contains source address, destination sequence number, hop count and lifetime. RERR message is used to inform the sender about link breakages in the route. When a node is unable to forward the RREQ packet, it generates RERR packet.

Suppose source has a packet that it needs to send to a destination. Source node checks its routing table for a path to the destination node. If there is no entry for that specific destination then source node initiates route discovery. For route discovery, source node broadcasts a route request packet. When an intermediate node receives a route request packet, it either forwards the packet or prepares a route reply, if it has a valid route to the destination.

Figure 2.1 illustrates route discovery process in AODV by considering a simple network scenario. Suppose node S wants to establish a connection with node D. Source node S broadcasts RREQ packet. Upon receiving RREQ packet, intermediate node 1 checks its routing table for a route to destination D. If there is no entry for node D, then node 1 forwards the RREQ packet to node 2, which further propagates it to node 3 and node 4. Each node increments broadcast id of the RREQ packet before forwarding it. Upon receiving RREQ through node 3 and node 4, destination node D prepares a RREP packet. Since each node records the address of the node from where it has received RREQ packet,

thus it can send RREP packet using the reverse path of the RREQ packet. When node 2 receives RREP, it enters a route to node D, and unicasts RREP to node 1. When node S receives RREP, the connection is established between source and destination. In case node S receives multiple RREP packets then RREP packet with largest destination sequence number is selected. Destination sequence number is used to evaluate freshness of the route. If the destination sequence number is same then route with least number of hops is selected for data transmission.

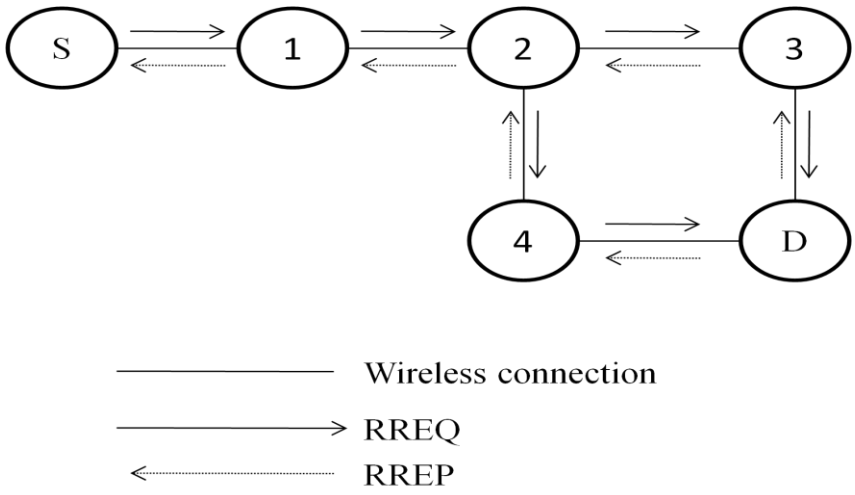

Figure 2.1: Route discovery in reactive routing protocols

2.1.2 Dynamic Source Routing

Dynamic Source Routing (DSR) also belongs to reactive routing protocol category and initiated only when a route to new destinations needs to be discovered. The underlying phenomenon in DSR is source routing that is, source mentions the complete and ordered list of nodes that each packet must traverse to reach the destination.

The basic operation of DSR is as follows: Suppose source node has a packet for a destination node. Source node searches its route cache for a path to the destination. In DSR the routes to all known destinations are stored in a route cache. If source node does not find a route to the destination, it broadcasts a RREQ packet to initiate route discovery process. The RREQ packet contains source address, destination address, a unique request id, and a route record field. Each intermediate node appends its own address to the route record field

before forwarding the RREQ packet. Consider the network scenario shown in Figure 2.1, and suppose node 2 has a valid path to the destination. When the intermediate node that is node 1 receives RREQ packet from source node S, it checks RREQ packet for duplication. If node1 has already received RREQ packet with the same source address and request id, it discards the RREQ packet. Otherwise, node 1 appends its own address to the route record field and then forwards it to node 2. Since node 2 has a path to destination D, it sends back RREP packet containing the complete route to reach node D. Upon receiving RREP packet, source node S stores the route to node D in its cache and writes the complete route to each packet's header while sending it. Each node en route to node D uses the path recorded in packet's header to determine the next hop of the packet. The packet always traverses through the recorded list in the header of the packet to reach the destination.

2.2 Proactive Routing Protocols

Proactive routing protocols are also known as periodic protocols as each node broadcasts route updates to its neighbors periodically. Each node maintains a table with routing information to all destinations and next hop to each destination. This routing table is used to make decisions regarding the selection of a route from source to destination. The most prominent examples of proactive routing protocol are Dynamic Destination Sequenced Distance Vector Routing (DSDV) [6] and Optimized Link State Routing Protocol (OLSR) [7]. These protocols minimize data latency introduced due to route discovery but provoke large signaling overhead each time the topology is modified.

2.2.1 Dynamic Destination Sequenced Distance Vector Routing

Dynamic Destination Sequenced Distance Vector Routing (DSDV) is based on distance vector routing algorithm. Like in distance vector algorithm each node in DSDV also maintains distances to all destinations and the next hop to each destination. The distance is interpreted as the number of hops to the destination. Each node broadcasts route advertisements periodically and especially, when the topology is modified or when a new node joins the network.

The advantage of DSDV over distance vector algorithm is that DSDV guarantees loop freedom. DSDV uses sequence number to tag each advertised route. This sequence number

is useful in determining the freshness and validity of the route. The route with higher sequence number is preferred. If the sequence number is same then decision of choosing specific route depends on the number of hops to reach destination.

The proper operation of DSDV depends on up to date route advertisements from each node. The route is advertised when a link is broken or when a node has an alternative path to a destination with less number of hops. DSDV protocol requires that for each new route advertisement, advertising node must broadcast the packet containing destination address, number of hops from the source to destination and sequence number of the route. This information is stored in the routing table of each node. When a source node has a packet to send to a destination it checks the route for the destination in its routing table and sends the packet to next hop from where the destination can be reached.

Since mobility of nodes is high in MANETs, DSDV is tailored to suit frequent topology changes by using triggered updates. Triggered updates are initiated with the help of two update messages: full and incremental dump. The full dump carries all the routing information where as the incremental dump contains only that information which has changed since the last full dump.

2.2.2 Optimized Link State Routing Protocol

Optimized Link State Routing Protocol (OLSR) belongs to the class of proactive routing protocols and thus information is exchanged periodically during the network operation. OLSR is an optimization of link state routing protocol and tailored to suit the requirement for MANETs. OLSR is based on the concept of multipoint relays (MPRs) [8]. MPRs are nodes in wireless network that relay messages between nodes during the flooding process. The advantage of using MPRs is reduced control traffic in the network, since control traffic from node is forwarded only by its MPRs. Figure 2.2 shows MPRs of node m. Control traffic from node m is forwarded by its MPRs and node m shares MPRs with its neighbors in route advertisements.

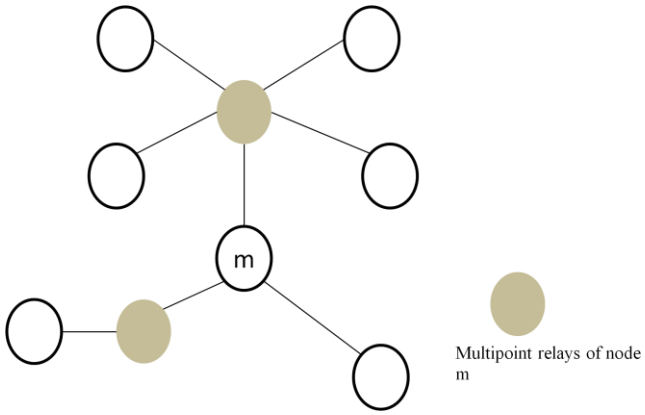

Figure 2.2: Multipoint Relays of node m

OLSR uses two special messages to discover and share link information with the neighbors. To detect the direct neighbors, each node broadcasts hello message periodically to known neighbors with their link status. The link status can be symmetric, asymmetric, multi point relay or lost. In symmetric link, nodes can communicate in both directions while in asymmetric, communication is possible only in one direction. If the link between nodes is symmetric and hello message sender has selected this node as MPR, then link status between the nodes is multi point relay. Link status is lost if communication channel between the nodes is broken.

Upon receiving hello message, neighbors do not propagate it further; but instead they broadcast it after a refreshing period. Each node can get first and second hop neighborhoods information through the exchange of hello messages. On the basis of first and second hop neighborhoods, each node selects its MPRs to cover communication range up to its second hop neighbors. Each node maintains its MPRs list and it is updated whenever a change in the first hop or second hop neighborhoods is detected.

Topology Control (TC) message is used to update each node regarding the topological changes in the network. The purpose of TC message is to update each node regarding latest topology for better calculation of the routes. TC messages are broadcasted by nodes that have been elected as MPRs to minimize retransmission of control packets. The node can be reached directly or via its MPRs. The topology information is exchanged periodically and routes are recalculated if the neighboring node or topological information is changed.

2.3 Hybrid Routing Protocols

In MANETs due to frequent mobility of nodes, proactive routing protocols introduce large control traffic which utilizes excessive bandwidth. The general disadvantage of reactive routing protocols is longer route discovery delay. Hybrid routing protocols combine good characteristics of both reactive and proactive routing protocols. Hybrid routing protocols for example, Zone Routing Protocols (ZRP) [9]-[11] divide the network into multiple zones to effectively discover routes to destinations.

2.3.1 Zone Routing Protocols

Zone Routing Protocols (ZPR) combines proactive and reactive routing protocols by dividing the network into multiple zones. Each zone can either utilize reactive routing protocol or proactive routing protocol to discover routes. Since in MANETs maximum traffic is exchanged between nearby nodes and thus this intra zone utilizes proactive routing protocol to discover routes. Each node stores the routes to all destinations within intra zone to avoid route discovery delay. When a node needs to transmit data to destination outside the intra zone it broadcasts a route request packet to discover route. Thus reactive routing is utilized for route discovery outside the intra zone.

Figure 2.3 depicts a network division using ZPR. The network is divided into two zones: zone for S and zone for D. Zones are divided on the basis of first hop information. In zone for S all nodes that can be directly accessed by node S is included, where as zone for D includes all the first hop neighbors of D. For intra zone routing, proactive routing protocol is utilized to avoid route discovery delay while reactive routing protocol is utilized for inter zone communication. For example, suppose node 4 has a packet for node 3, since both nodes are in the same zone, thus node 4 checks routing table entry for node 3 and sends the packet through the path found in its routing table. However if node S has packet for node D, which is in the other zone then reactive routing protocol is used. Node S broadcasts a RREQ packet to its boundary nodes that is node 2 and node 4, which further propagate RREQ packet to node 5 and 6. Since both these nodes have a fresh route to node D, so they send RREP packet to node 2 and 4. Node S receives RREP packet from node 2 and node 4, and this concludes route establishment between node S and node D.

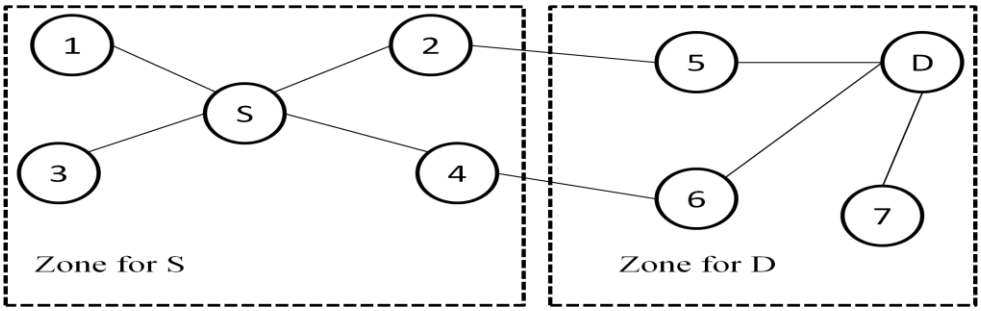

Figure 2.3: Network division using ZRP

Hybrid protocols overcome disadvantages of both reactive and proactive routing protocols. On the one hand, proactive routing protocols introduce large overhead due to frequent route updates. ZPR overcomes this by dividing the network into smaller zones and restricting control packets inside the zone. On the other hand, reactive routing protocol has the disadvantage of route discovery delay. ZPR overcomes this limitation by using reactive routing protocol only for a route establishment between nodes of different zones.

2.4 Summary

This chapter presented routing protocols for MANETs. The goal of routing protocol is to discover an optimal route to the destination. Different categories of routing protocols were presented. Reactive routing protocol discovers routes when requested by the sender whereas proactive routing protocol exchanges control messages periodically. Thus reactive routing protocol initiates longer route discovery delay while proactive routing protocol introduces large control traffic. To overcome these limitations hybrid routing protocol was introduced. Hybrid routing protocol divides the network into multiple zones and each zone utilizes either reactive or proactive routing protocol.

CHAPTER 3

Security Challenges in MANETs

The open medium and lack of central administration make MANETs more vulnerable to different attacks as compared to conventional networks [12]. An attacker can launch diverse attacks against MANETs including active and passive attacks [13]. Active attack such as routing misbehavior from a node severely degrades the performance of MANETs. Performance of the network can degrade up to 32% if 40% nodes start malicious activity in the network [14]. On the one hand, active attack disrupts proper operation of the network and thus it can be detected using different techniques for example, by analyzing traffic misbehaviors in the network. On the other hand, passive attack is the unauthorized monitoring or listening of the communication. Since it does not disrupt proper operation of the network, therefore detecting a passive attack is more challenging than active attack. Common example of passive attack is network traffic sniffing. Figure 3.1 shows the most common active and passive attacks against MANETs. Denial of Service (DoS) attacks falls under active attacks category, since these attacks disrupt network operation by denying specific node from legitimate traffic. The most common DoS attacks against MANETs are blackhole, grayhole and wormhole link attack. The operation of these attacks is presented in next sections.

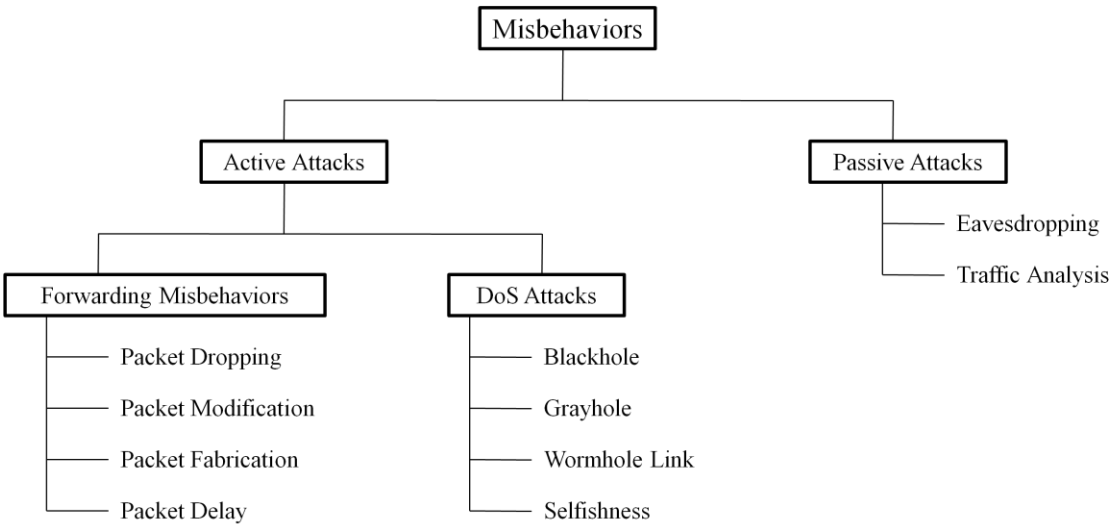

Figure 3.1: Classes of attacks in MANETs

Table 3.1 shows possible security threats against each layer of TCP/IP reference model. Attacks against application layer include repudiation and data corruption. Repudiation is a common attack against application layer. It allows malicious user to write wrong data to log files and trap legitimate users for the malicious activity. The task of the application layer is to detect and prevent repudiation attack as well as worms and viruses. Attacks that the can be successfully launched against transport layer include session hijacking and SYN flooding. SYN packet is used to start Transmission Control Protocol (TCP) connection establishment between hosts. Transport layer is responsible for providing authenticity and confidentiality between network hosts by creating secure communication sessions between them. Session hijacking is a common and dangerous attack against this layer. The most critical layer in MANETs is the network layer, which is responsible for routing packets correctly. Misbehaviors that disrupt routing are: fake route replies from a node, routing table overflow, packet replication and DoS attacks. Impersonation attack and Man in the Middle (MITM) attack are examples of multiple layer attacks.

Table 3.1: Security attacks against each layer in MANETs

Layer	Security Issue
Application Layer	Repudiation, Data corruption
Transport Layer	Session Hijacking, SYN flooding.
Network Layer	DoS attacks • Blackhole Attack • Grayhole Attack • Wormhole Link Attack Routing Misbehaviors • Routing table overflow • Routing table poisoning • Packer replication
Multiple Layer Attacks	Dos Attacks, Impersonation Attack, Device Tampering, replay attack, Man in the Middle attack.

3.1 Blackhole Attack

Blackhole attack comes under the category of active attacks. Blackhole attack characterizes two properties. A malicious node exploits routing protocols and advertises itself as having the optimal route to a destination although the route is spurious. Once the route is established, malicious node then dumps the intercepted traffic through spurious route thus causing denial of service to the destination.

An illustration of blackhole attack against AODV is depicted in Figure 3.2. Node S wants to send data packets to node D and suppose it does not have a path to node D. Consequently, node S broadcasts Route REQuest (RREQ) packet and its neighbors further propagate RREQ packet in the network. When the malicious node M receives RREQ packet, it does not forward the RREQ packet; instead it sends back false Route REPly (RREP) packet claiming that it has a fresh and optimal path to destination D. Since RREP packet from M reaches back to node S ahead of RREP from other neighbors, thus node S considers sending data packets through node M. In this way, blackhole attack is setup and node M can cause denial of service by dumping all the packets destined for D.

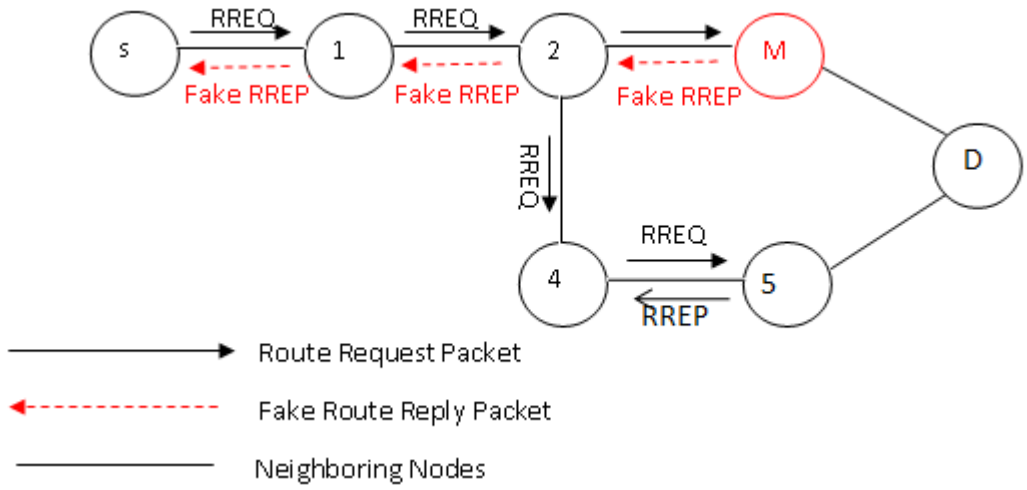

Figure 3.2: Operation of Blackhole attack

3.2 Grayhole Attack

Grayhole attack is a variation of blackhole attack in which behavior of the malicious node is unpredictable. The malicious node may behave as a normal node and later it starts malicious activity. This unpredictability makes detection of grayhole attack more challenging than blackhole attack. There are three types of grayhole attack [15]. In the first type, malicious node denies specific node from the services while it behaves like a normal node for other nodes. The motivation behind this type of attack is to reduce the possibility of malicious behavior detection. The second type of grayhole attack involves certain timings of the malicious activity. The malicious node drops packets from all nodes but after a certain time, the malicious node behaves like a normal node and starts forwarding the

packets. The third type is a combination of first and second type. The malicious node drops packets of a specific node for certain duration and later it behaves like a normal node and forwards the packets. Due to these variations, detecting and preventing grayhole attack is more challenging than blackhole attack.

The operation of grayhole attack is illustrated in Figure 3.3. Figure 3.3(a) shows the network scenario when the malicious node that is, node 5 acts as a normal node. Suppose node S needs to send the packets to destination D. Node S selects the route S-2-5-D since it has minimum hops as shown in Figure 3.3(a). Initially malicious node 5 behaves like a normal node and forwards the packets destined for D. After certain time node 5 starts malicious activity and drops the packets destined for node D, thus causing denial of service for node D. This malicious activity is shown in Figure 3.3(b).

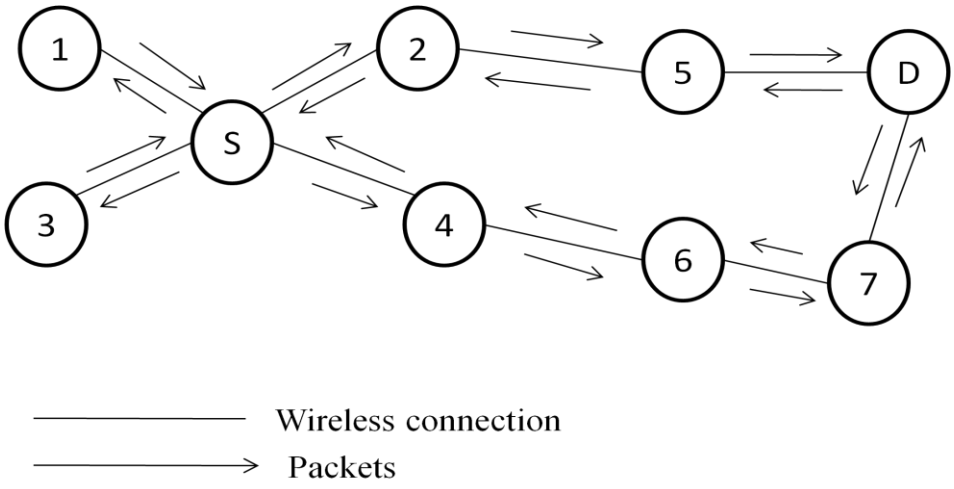

Figure 3.3a: Malicious node acting as a normal node

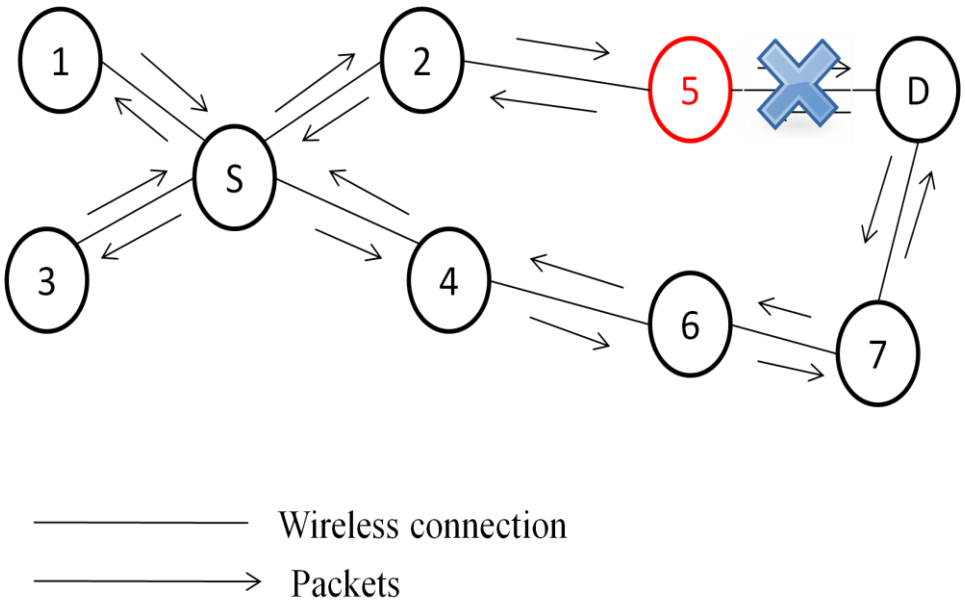

Figure 3.3b: Malicious activity by node 5

3.3 Wormhole Link Attack

Wormhole link attack [16] [17] is a kind of tunneling attack where two colluding nodes (worms) make their private tunnel in the network and exchange data packets through the tunnel. One worm peer records packet at one location relays it to the other worm peer through the tunnel, giving impression that they are immediate neighbors [18]. Malicious nodes are placed at optimal positions in the network and use high speed wired or wireless link for their private tunnel. Both worms can use packets to analyze traffic flow and then drop these packets, thus causing a denial of service to a legitimate node.

Wormhole link attack is among the most sophisticated and severe attacks in MANETs. The effectiveness of this attack depends on the number of packets passed through the tunnel. Wormhole link attack can cause route discovery disruption and could lead to all packets being sent through the wormhole link for all destinations. It is relatively easy to deploy a tunnel in the network and launch attack but extremely difficult to detect it. Wormhole link attack can be used against all communications irrespective of links providing confidentiality through encryption.

An illustration of wormhole link attack for AODV routing protocol is shown in Figure 3.4. M1 and M2 are malicious nodes that have formed their private tunnel in the network, and node D is the target. Node S has to establish a route to node D to transmit data. Node S checks its routing entry for node D and if there is a path for node D, node S takes the same path otherwise AODV is initiated to discover the fresh path to node D.

For route discovery, node S broadcasts RREQ packet to its neighbors that is, node 1 and node A. Both these nodes check their routing table for node D entry and further propagate RREQ packet if they do not have a path to destination D. However if any of the neighbor has a path to node D, it sends back RREP packet. When the malicious node M1 receives RREQ packet, it forwards the packet to M2 through high speed tunnel. M2 further propagates the RREQ packet to node B which sends it to node D. Node D receives RREQ packet, through the tunnel faster than any other alternate path so node D unicasts RREP back to node S through the route D-B-M2-M1-A-S. Since node S receives RREP from D, so it considers sending packets through the route S-A-M1-M2-B-D. However the valid routes from node S to node D are through nodes 1-2-3-4-5-6-D and 1-2-3-4-5-B-D. Since these routes have higher number of hops thus source node S selects the route involving the wormhole link.

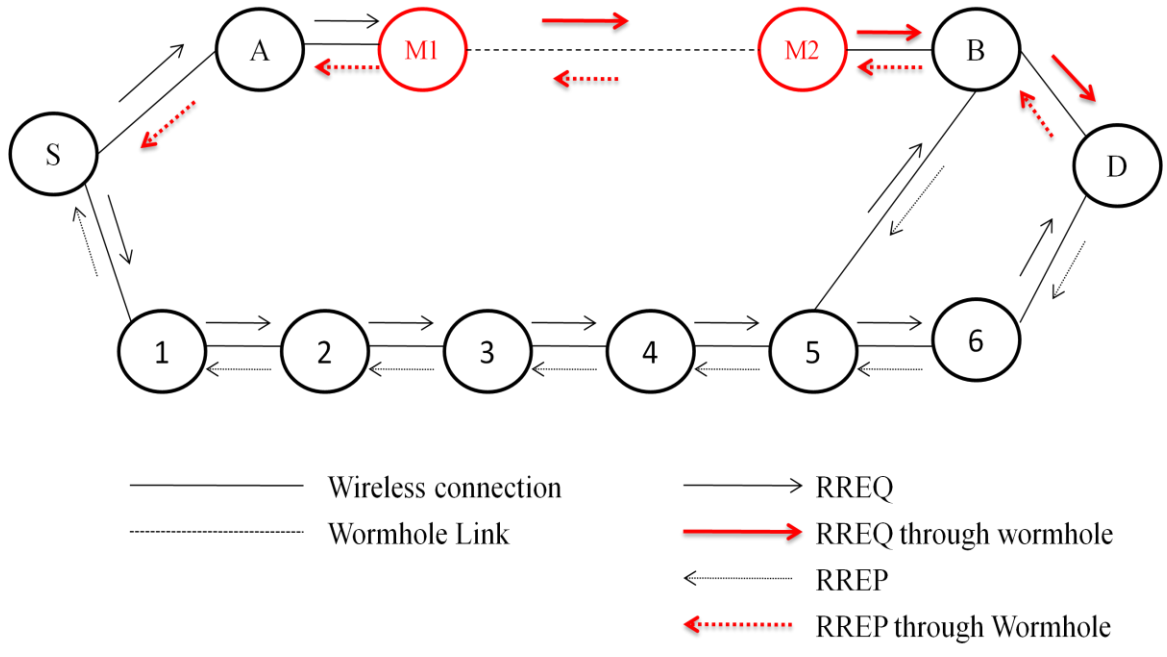

Figure 3.4: Operation of Wormhole Link attack

3.4 Impersonation

In impersonation attack, an attacker steals the identity of other node and uses network resources through the stolen identity. Impersonation is usually the first step in most attacks and used to launch further sophisticated attacks. An attacker impersonates Internet Protocol (IP) or Media Access Control (MAC) address of a legitimate node, and launches further attacks through the stolen identity.

In a wired or wireless network involving central authority, impersonating a node's identity can be prevented by authenticating each node. For example, in Wi-Fi, which is a wireless network, access point authenticates each node before it can use network services. Since MANETs are infrastructure less networks and do not have a central authority, authenticating nodes is a challenge in these networks.

3.5 Sybil Attack

Sybil attack [16] is an attempt from a malicious node to acquire multiple identities in the network. The additional identities of the malicious nodes are referred as sybil nodes. The purpose of sybil nodes is to use more network resources and control network traffic. An attacker can get identities for sybil nodes by stealing or fabricating identities.

3.5.1 Fabricated Identities

In some cases an attacker can fabricate the identity if it knows the algorithm for creating identity. For instance if a node is identified by a 16 bit integer, the attacker can arbitrary create and assign each sybil node, a 16 bit number. However this mechanism will fail if the identities are authenticated or verified through a central station.

3.5.2 Stolen Identities

In most of the cases when an attacker cannot fabricate the identity due to verification algorithm, it steals the identity of other legitimate node. For instance if the identity space is limited, then the attacker needs to steal identities of other legitimate nodes and assign them to sybil nodes. The stealing identity attack is also known as impersonation. If the attacker disables impersonated nodes from accessing the network then this impersonation cannot be detected.

An attacker can use identities either stolen or fabricated in multiple ways to launch sybil attack. It can use sybil nodes simultaneously or non-simultaneously. In simultaneous approach, the attacker uses all sybil nodes in network at once. In non-simultaneous approach, the attacker uses a subset of sybil nodes to participate in the network while preserving the rest of the identities. Through this approach, the attacker is able to leave the network at one place and join the network at another.

3.6 Selfishness

The proper operation of MANETs lies in cooperation among the nodes. However all nodes may not be cooperative and this non cooperative behavior is termed as selfishness. Selfishness is not a malicious activity. Selfish nodes do not have intent to damage the network whereas malicious node damages and degrades the performance of the network. Selfish nodes use the network for their own communication but do not participate otherwise, to save power and energy. Selfish nodes utilize resources of the network to send their own packets but do not make available their own resources to help others.

3.7 Summary

In this chapter security threats against MANETs were presented. This chapter classified attacks on the basis of the TCP/IP model layer, they target. Application layer is vulnerable to data corruption, while session hijacking attack can be launched against transport layer. The primary focus of the chapter was Denial of Service (DoS) attacks. These attacks are killer attacks for the network since they disrupt the proper operation of routing protocols. The attacks that kill MANETs include blackhole, grayhole and wormhole link attack. Under the presence of any of these attacks, the network fails to operate properly and thus these attacks limit the applications of MANETs.

In blackhole attack, malicious node falsely claims to have an optimal path to a destination. When data is transmitted through the advertised path, malicious node simply dumps the packets, thus causing the denial of service. Grayhole attack is a variation of blackhole, characterizing unpredictability. In grayhole attack, behavior of the malicious node is unpredictable. This unpredictability makes detection of grayhole harder than blackhole attack. Wormhole link is among the most sophisticated attack against MANETs. In this

attack, two malicious nodes form their private tunnel in the network and exchange messages through the tunnel. If an attacker is able to position the worms at critical locations then packets to all destinations may be sent through the tunnel. Wormhole link attack can be launched against any wireless channel irrespective of channels providing authentication and confidentiality. The ultimate purpose of blackhole, grayhole and wormhole link attacks is to deny legitimate users from getting the desired network services. These attacks are big hurdle for widespread of MANETs. Finally the chapter focused on sybil attack which allows an attacker to use network resources more than the allocated resources. To achieve this, an attacker impersonates legitimate nodes identities and assigns these identities to sybil nodes. Through the use of multiple identities the attacker can leave network at one place and join the network at another.

CHAPTER 4

Security Attacks Countermeasures

Chapter 3 introduced most common attacks that kill the proper operation of MANETs. In chapter 3, the attacks were classified based on the layer of TCP/IP reference model. Most of the common misbehaviors are due to lack of security mechanisms in routing protocols. Thus these attacks are the biggest hurdle for widespread of MANETs. Passive attacks against the network can be countered by encrypting the data. However more sophisticated approaches are required for detecting and mitigating active attacks.

Recently researchers have proposed several techniques to counter attacks in MANETs. Mostly these techniques have focused on providing preventive mechanism rather than reactive mechanism. The motivation behind preventive schemes is to prevent attack from occurring by using techniques such as node authentication. In preventive schemes nodes cannot join the network unless it is authenticated by a central authority. Most of these schemes use encryption techniques to prevent unauthorized node from joining the network. Since encryption (decryption) algorithm requires key to encrypt (decrypt) data packets, this in turn introduces heavy traffic load due to exchange of keys. In reactive schemes, detecting attack is focused rather than preventing it. Nodes are not authenticated through a central party, but once the misbehavior is detected from a node, it is isolated from the network. The general advantage of reactive schemes over preventive schemes is the reduced control traffic in the network.

4.1 Network Layer Defense

Routing in MANETs is based on cooperation among the nodes of the network. Possibility of misbehaviors from a node was not considered in designing the routing protocols. Routing protocols of MANETs were designed solely to route data packets, thus they lack security mechanisms. In next sections, existing defense mechanisms against network layer attacks are described in detail.

4.1.1 Defense against Blackhole Attack

Many approaches have been proposed in the literature to detect and mitigate blackhole attack in MANETs. The most common countermeasures are: source node waits for multiple route replies before selecting a particular route [19], common neighbor acting as watchdog [20] and route request confirmation method [21].

Al-Shurman et al. [19] proposed a solution that requires source node to wait for multiple route replies. Source node verifies authenticity of replying nodes by sending a ping packet through these routes. Upon receiving an acknowledgement from the destination, source node decides which route is safe for data transmission. The disadvantage of this scheme is longer time delay since source node must wait for multiple route replies.

Peng et al. [20] proposed blackhole detection based on traffic listening by a common neighbor. A node is a common neighbor if it is in between radio range of two different nodes. In this scheme common neighbor acts as a watchdog to detect misbehaviors from a node and discover new route in presence of blackhole attack. The drawback of this scheme is the new route discovery by a common neighbor, which is a routing overhead.

Lee et al. [21] introduced the concept of route Confirmation REQuest (CREQ) and route Confirmation REPly (CREP). In this approach, the node between source and destination sends a CREQ packet to its next hop towards the destination. Upon receiving a CREQ packet, the node prepares CREP packet if it has a valid route to the destination. When the CREQ packet sender, receives CREP, it sends both the CREP and RREP to source node. Upon receiving RREP and CREP source node determines the validity of the route by comparing both CREP and RREP. However, this scheme cannot detect blackhole attack if two consecutive nodes are cooperating in malicious activity.

Kurosawa et al. [22] showed that malicious node has to increase destination sequence number sufficiently to convince the source node to send packets through it. Destination sequence number is checked for freshness of the route and higher the destination sequence number more fresh is the route. The scheme proposed by Kurosawa et al. analyzes RREP packet and destination sequence number statistically to detect blackhole attack. This scheme compares sequence number in RREP with statistically calculated sequence number. If the sequence number in RREP is greater than the statistically calculated sequence number, then the node is concluded as malicious. This scheme generates no additional traffic but has the disadvantage of higher false positives.

Tamilselvan et al. [23] used response table for detecting blackhole attack. In this approach, authors also introduced the detection of cooperating malicious nodes based on the same response table. Source node collects route replies in a response table till the timer expires. The selection of a particular route is based on the fidelity level of the participating nodes. The fidelity level is updated each time acknowledgement of data packet is received from the destination. Source node updates the fidelity level of the participating nodes and thus the route is considered safe. When the fidelity level of a node drops to 0, it means that node is not forwarding the packet and hence alarm packets are generated to remove it. The drawback of this scheme is longer transmission delay.

Ameza et al. [24] detected blackhole attack through the use of two additional fields in RREQ packet. First field is used to record all the intermediate nodes addresses between source and destination. This field is used to detect the address of the malicious node. Each node uses second field to keep sequence number of the destination node. When a node receives back RREP, it verifies the address of the sender in its table of addresses. If the address does not match then the node is concluded as malicious. The disadvantage of this scheme is delay in route discovery.

Raj et al. [25] proposed blackhole detection scheme based on checking sequence number against a threshold sequence number. The threshold sequence number is calculated after specific interval of time and it is checked against the sequence number of RREP. If the sequence number in RREP has higher value than threshold sequence number value, the

node is considered as malicious. The disadvantage of this scheme is increased end to end delay in packet transmission and higher false positives.

4.1.2 Defense against Grayhole Attack

As mentioned in section 3.3, detection of grayhole attack is more challenging than blackhole attack, due to unpredictable behavior of the malicious node. However many approaches have been proposed to detect malicious node and mitigate grayhole attack. Common countermeasures of grayhole attack include: end to end path checking [27] and use of postlude and prelude message for the start and end of data transmission [28].

Xiaopeng et al. [26] proposed a solution that is based on three algorithms; creating proof, check up and diagnosis algorithm. Each node involved in the communication session must create proof that it has received the packet. Source and intermediate nodes need to store information on the forwarded packet. This information is the evidence that the node has forwarded the packet. When source node suspects packet dropping or destination reports loss of packets to the sender, it initiates check up algorithm. Check up algorithm determines the misbehavior in the network by checking each node along the path to the destination. After check up algorithm, source node initiates diagnosis algorithm which traces malicious node based on the findings of check up algorithm. Diagnosis algorithm checks the forwarded evidence of each node and if a node fails to provide forwarded evidence it is accused to be malicious. The disadvantage with this approach is the routing overhead and it may not detect cooperating malicious nodes.

Agrawal et al. [27] used end to end route checking for detecting malicious node. This approach is based on observing each node's behavior. Few nodes in the network observe behavior of other nodes by listening to their traffic. These observing nodes are referred as strong nodes and they are characterized as trustworthy. The strong nodes are located at different positions of the network and form a backbone network. This backbone network provides the infrastructure to the infrastructure less MANETs. The second step in this approach involves checking end to end validity of the route that is, validity of the route from source to destination. Source node sends packets to destination, after few blocks of data packets source node requests backbone network to check whether destination has

received the packets or not. If the destination has not received the packets or it is aware of a possible attack, it informs the backbone network. The backbone network initiates detection of malicious node(s) by critically observing the traffic from all nodes en route to destination. This approach detects single as well as cooperating malicious nodes assuming malicious nodes are not many in the network. The drawback of this scheme is that each node must know its position in the network at the time of joining the network. The authors did not address the possibility of misbehavior from a strong node.

Banerjee et al. [28] proposed a scheme based on prelude and postlude messaging. In this scheme the authors used prelude and postlude messages to detect grayhole attack. Total traffic is divided into small sets of blocks and grayhole attack can be detected between two blocks transmission. Before the start of a data block transmission, source node starts a timer after sending a prelude message to destination and monitor message to intermediate nodes. Prelude message alerts the destination for block reception and monitor message informs neighbors to start monitoring the flow of traffic. Once the destination receives the prelude message it starts a counter for block reception. All nodes en route to destination monitor each other's behavior for the flow of traffic. After the end of block transmission, destination node sends postlude message to the source node. The postlude message indicates number of packets received by the destination during the timer. If the destination has received the same number of packets as sent by the source and postlude message is received by the source before the timer expires, then the path is trustworthy. Otherwise source node declares the possibility of an attack. To detect malicious node(s), source node broadcasts a query message to gather the aggregate responses from the monitoring neighbors. Monitoring nodes send their responses in a result message. If the source receives a result message indicating a malicious node then that node is declared as malicious. If the source node does not receive result message from a particular node within the timer, then that node is suspected as malicious. For next data block transmission the malicious node is isolated by finding alternate path to destination. The drawback of this scheme is higher false positives and it may not detect cooperating malicious nodes.

Gonzalez et al. [29] proposed scheme based on the principle of flow conservation: all packets that are not destined for a particular node should exit from that node. Both source

and destination nodes of each transmission maintain statistics that are used to determine whether the packet was forwarded properly by the intermediate nodes or not. To declare a node as malicious the packets need to be dropped below a threshold value to accommodate the loss due to link collisions or overloaded node. Proper threshold value can discriminate misbehaving nodes from well behaved nodes. This scheme assumes all links to be bi-directional and only detects packet dropping from a node.

4.1.3 Defense against Wormhole Link Attack

In wormhole link attack, one worm records packet at one location and sends it to its peer through high speed private tunnel. The packets sent by worms are identical to packets sent by legitimate nodes, therefore detecting wormhole link poses challenge. However many efforts have been made in detecting and mitigating wormhole link attack. The most common countermeasure is by using Global Positioning System (GPS) for locating node in the network and using its location, detecting wormhole link is possible [30].

Chun Hu et al. [30] proposed a method based on packet leashes algorithm to detect wormhole link in MANETs. A leash is information that is added to the packet to restrict its transmission. In particular two types of leashes were introduced by the authors; temporal leashes and geographical leashes. To detect wormhole link through temporal leash, each node is required to compute the expiration time of the packet. This expiration time is included in the packet to limit it from traveling further than the specific distance. Each receiving node checks the expiration time included in the packet against the current time before forwarding the packet. The authors have also proposed Tree Authenticated Values (TIK) to prevent malicious node from changing expiration time in the packet. The disadvantage of using temporal leash approach is that it requires all nodes in the network to have tightly synchronized clocks. In geographical leashes, position of the source node is added in the packet. Thus this approach requires each node to know its position in the network. Sender of the packet includes its current position and time stamp in the packet. Using this information, receiver of the packet can calculate the distance between itself and the sender of the packet. The advantage of this approach over temporal leash is loosely synchronized clocks however this approach requires each node to know its position in the network.

Raffo et al. [31] proposed a scheme that uses node location for detecting tunnel in the network. The authors protected OLSR routing protocol from wormhole link attack by using node location information and deploying public key infra structure. This approach is similar to geographical leashes [30]. In this approach node sends a hello message including its current position and current time. Upon receiving hello message, the receiver computes distance between itself and its neighbors. If the distance is more than the transmission range then receiver suspects that hello message has been tunneled. The disadvantage of this scheme is that it works only with protocols that support multi hop routing.

Qian et al. [32] showed that the Statistical Analysis of Multipath (SAM) routing can be used to detect wormhole link attack in MANETs. This approach works by calculating and analyzing relative frequencies of all the links obtained through route discovery process. The route with highest relative frequency is identified as wormhole link. This approach works only for multipath routing protocols and this approach cannot identify wormhole link in non-multipath protocols such as AODV.

Detecting wormhole link through the use of directional antennas was proposed by Hu et al. [33], [34]. Each node in the network determines a relation with its neighbors through the direction of the signal. If the direction matches then the relation between the nodes is set and these nodes can start data transmission. The drawback of this scheme is the use of directional antennas. This scheme cannot work without directional antennas.

Capkun et al. [35] proposed secure tracking of node encounters in multi-hop wireless networks (SECTOR). It a set of mechanism that can be used to prevent wormhole link attack and help securing routing protocols of MANETs. The basis of SECTOR is distance bounding techniques and hash functions. Each node measures its distance with other node at the time of their encounter. SECTOR keeps track of the latest encounter of nodes and stores their mutual distances. This distance is used to track current topology of the network. SECTOR detects wormhole link attack by means of network topology information. SECTOR has advantage over other approaches as it does not require location or clock synchronization to detect wormhole link attack. However it requires secret key mechanism for mutual authentication of nodes.

4.1.4 Defense against Impersonation Attack

Sanzgiri et al. [36] proposed Authenticated Routing for Ad hoc Networks (ARAN) to prevent impersonation attack in MANETs. The security of this protocol lies in providing authentication and non repudiation. ARAN provides authentication by means of certificates issued from a trusted certificate server. These certificates are used for end to end authentication.

To discover routes for a new destination, source node broadcasts Route Discovery Packet (RDP) to its neighboring nodes which further propagate RDP in the network. Upon receiving RDP, destination node sends Route Reply Packet (REP) to the source node. Both RDP and REP are authenticated at each hop before they are further propagated in the network.

Route discovery authentication is illustrated in Figure 4.1. Source node S needs to discover route for node D, it broadcasts RDP to node 1 which further propagates the packet. RDP contains various fields such as RDP, IPD, CertS, NS, and T. RDP is packet identifier from the sender. IPD is used for destination IP address. CertS, is the certificate of the source node. NS is the nonce used by source, it can be used once only, and T indicates the time of the packet when it was sent from source node.

Each node need to sign packet before forwarding it in the network. Thus source node signs the packet [RDP, IPD, CertS, NS, t] K_S, with its own private key K_S and broadcasts it to its neighbors that is, node 1. Since node 1 is one hop away from the source node, it verifies the signature of source node and its certificate. If the signature is valid and certificate is not expired, node 1 adds its own certificate and signs the packet with its own private key [[RDP, IPD, CertS, NS, t] K_S] K_1, Cert1. Node 1 propagates this packet further in the network. Each hop verifies the signature of the previous hop and replaces the signature of previous hop with its own. Thus node 2 verifies the signature and certificate of node 1, replaces node 1's certificate with its own and forwards the packet to node 3, which sends the packet to destination node D. Upon receiving RDP message, destination node unicasts packet [REP, IPS, CertD , NS, t] K_D back to source node and this establishes route between node S and node D.

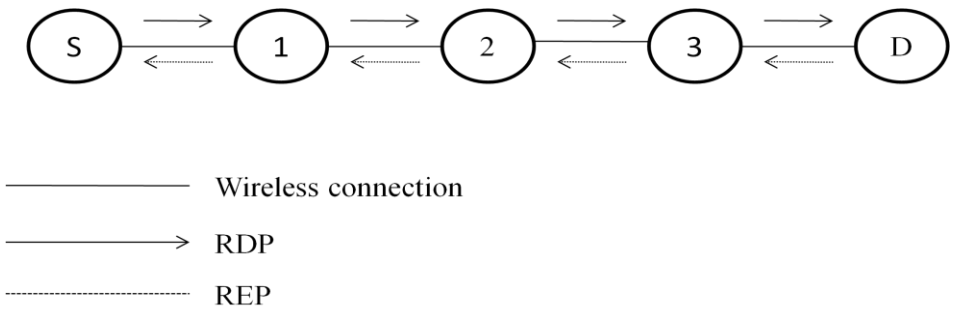

Figure 4.1: Route discovery using ARAN.

ARAN uses hop by hop authentication due to which a node cannot impersonate other's ID and it is impossible for a malicious node to form routing loop. Each RDP is signed and verified at each hop which restricts malicious node from using expired certificates. However this hop by hop authentication introduces large computational overhead at each hop. The other problem with hop by hop authentication is the cooperating malicious nodes. This protocol will fail to provide authenticity if there are cooperating malicious nodes in the network.

Kargl et al. [37] proposed secure dynamic routing protocol to protect network from different attacks including impersonation attack. The aim of this routing protocol is to secure the integrity of the route as well as freshness of the route. Integrity of the route is guaranteed by authenticating each node participating in the route discovery process. The protocol also exchanges session keys between source and destination and these keys are encrypted using Diffie-Hellmann protocol [38].

For route discovery, source node creates a RREQ) packet that includes source node ID, destination node ID, a route request ID which is unique per source, a public Diffie-Hellmann key, a random nonce N1 and an initial source route. This packet is digitally signed by source node and broadcasted to its neighbors. Intermediate nodes verify the signature and change nonce N1 to N2 and propagate the packet until it reaches destination. Upon reception of RREQ packet, destination node prepares a RREP and appends Diffie-Hellmann public key with it. This public key is used for hop by hop authentication and distributing the shared session keys among the nodes. After signing the packet, destination node sends this packet to source node. Source verifies the signature before sending data

packets through the route. The disadvantage of this routing protocol is the increased size of RREP packet. Since each node appends its key in RREP for the next hop to verify the RREP packet, thus resulting in huge RREP packet which severely increase traffic overhead as well as processing delay.

4.1.5 Defense against Modification Attack

Malicious node can tamper or modify the content of the packet before forwarding it. This type of attack can mislead source node to take different route from the legit route for data transmission. Hu et al. proposed Secure Efficient Ad hoc Distance vector routing protocol (SEAD) [39] to counter modification attack against network layer. The underlying routing for SEAD is Destination-Sequenced Distance-Vector routing protocol (DSDV). This protocol is similar to packet leash [30] which utilizes one way hash chain to authenticate nodes. SEAD protocol utilizes one way hash chain to secure contents in the packet to avoid modification from the malicious node. More specifically one way hash chain is used to prevent malicious node from increasing sequence number or decreasing hop count in route advertisements.

4.2 Defense against Sybil Attack

In sybil attack malicious node acquires multiple identities in the network and thus preventing sybil attack requires checking validity of each node's identity. The most cited method to prevent a node from acquiring multiple identities is through the use of certification from a trusted third party [40]. Certification Authority (CA) validates one to one correspondence between the node and its associated identity in the network, thus eliminating the need of building trust among the nodes for data transmission. However in MANETs there are implementation issues regarding CA.

Piro et al. [41] proposed two methods to efficiently detect Sybil nodes in the network. In first method, Passive Ad hoc Sybil Identity Detection (PASID), authors detected sybil nodes by overhearing traffic from all nodes. Each node overhears the traffic of other nodes and maintains the identities of the overheard nodes. Over time, each node builds a profile of every other node it overheard. Since physical device has only one radio channel to transmit

and receive data. Thus sybil nodes transmit data simultaneously and can be detected by looking into the identities of nodes that are overheard together. Each node suspects the multiple nodes that are overheard simultaneously as sybil nodes. This method can detect sybil nodes accurately if the network is dense and nodes are not far from each other. However false positive increases if nodes are distant from each other or the number of nodes increases in the network.

In second method, Passive Ad hoc Sybil Identity Detection with Group Detection (PASID-GD), false positives are reduced by monitoring collisions at MAC level. False positives are incurred when a group of nodes move or transmit together. Thus they are overheard simultaneously, and are falsely detected as sybil nodes. These false positives are reduced by monitoring collisions at MAC level. Since sybil nodes transmit data serially and thus collisions at MAC level will be fewer than group of nodes trying to send data simultaneously. Monitoring MAC level collisions improve efficiency of the scheme to detect sybil nodes.

The other method that can be used to detect sybil nodes in the network is resource testing. In this method resources associated with a node is checked. Since the resources for each node in a network is limited, sybil nodes increase the usage of resources and thus exceed the associated limit for each node. This resource testing is a commonly implemented solution to defeat sybil attack. Resources that can be checked to verify the limit of each node are computation, storage and communication resources. Radio resource testing proposed by Newsome et al. [42] is an extension for resource testing to detect sybil attack in MANETs. The key assumption of this approach is that any physical device has only one radio which cannot transmit and receive on more than one channel at the same time.

There exists a solution that is specifically designed to detect sybil nodes in MANETs. This solution is based on location or position of the nodes in MANETs. The location of sybil nodes remain at the same location when they are projected by a single physical device. The location of each sybil node can be verified using pre existing techniques such as triangulation [43]. Thus sybil attack from a single physical device appears to be at the same location and move together to a new location.

4.3 Defense against Selfishness

In general there are two type of misbehaving nodes. First type includes those nodes that are selfish and the second type includes malicious nodes. Selfishness is different from malicious activity. Selfish nodes do not participate in the network to save energy without damaging the network. On the other hand malicious nodes damage the network and degrade the performance by silently dropping the packets. Researchers have proposed various mechanisms to enforce cooperation among the nodes in the network. These mechanisms can be categorized as: token based, micro payment system and reputation system. Yang et al. [44] proposed a token based scheme while Buttyan et al. [45] proposed a mechanism based on micro payment or credit based system. Reputation based systems are CONFIDANT [46], CORE [47] and OCEN [15].

In token based schemes each node carries a token to participate in the network. The token is issued by its neighbors who collaboratively monitor the behavior of the node. The life of the token depends on the behavior of the node in the network. A well behaved node is exempted from frequently renewing the token from its neighbors. If the token is expired, the node is required to renew it from the neighbors. Any node with expired or invalid token is isolated from the network and all legitimate neighbors will not interact with this neighbor until it renews the token. To make token authentic, issuing node signs the token with its own private key. For token signing cryptographic primitives such as RSA is used in this approach.

Buttyan et al. [45] proposed a NUGLET scheme which is analogous to virtual currency. A node that utilizes the services of the network must pay the service providing node of the network. In watchdog and path rater schemes, any malicious node can still be a part of the network and it can receive and send the packet. However using NUGLET scheme neighbors lock out the malicious node.

CONFIDANT is based on reputation system in which each node maintains the reputation of other nodes by means of their trust values. CONFIDANT has four main components which help a node in enforcing cooperation among the nodes: a monitor, a reputation system, a trust manager, and a path manager.

The monitor component monitors the flow of traffic and analyzes the behavior of the node. The reputation system maintains reputation of each neighboring node. Trust manager increments or decrements trust values based on the behavior of the node. The network services are provided by considering the reputation of the node. Path manager is responsible for listing paths according to their trust values. Most trusted path will have nodes with highest trust values.

CONFIDANT enforces cooperation among the nodes and provides robustness by penalizing malicious node. In CONFIDANT nodes not only learn from their own experiences but also from the experiences of their neighbors in detecting malicious behavior.

4.4 Summary

This chapter presented countermeasures of the most common denial of service attacks. More specifically, in this chapter defending network layer against different attacks was focused. Countering attacks such as blackhole, grayhole, wormhole and impersonation attack is essential for proper operation of the network. Blackhole attack can be detected and mitigated through different schemes presented in the chapter. For example, one scheme that is commonly used to detect blackhole requires source node to wait for multiple route replies before selecting a particular route. The other common scheme relies on common neighbor acting as watchdog. However these techniques are limited only to the detection of blackhole attack in the network. Similarly techniques that detect wormhole link attack successfully, fail to detect the presence of blackhole or grayhole attack in the network. The most common technique that is limited to detection of wormhole link requires the use of GPS technology. Through the use of GPS, each node knows its position in the network and appends this information in the packet. The receiver then calculates the distance between itself and the sender based on the position information in the packet. This information about distances is used to detect the presence of tunnel in the network. If the travelled distance of the packet is less than calculated distance, then receiving nodes generates alarm about the possibility of a tunnel in the network.

The chapter also presented techniques that can be used to counter most common routing misbehaviors in MANETs. These techniques provide security layer over insecure routing protocols. The techniques such as ARAN, SECTOR and CONFIDANT were presented. ARAN provides security over insecure DSR routing protocol through the use of certification authority. ARAN requires that each node uses its assigned key to sign each packet, thus introduces routing overhead due to larger routing packets. SECTOR requires additional hardware to take control of the radio transceiver of a node from CPU. SECTOR like ARAN is also based on cryptographic primitives such as RSA and digital signature for authentication. The use of cryptographic primitives seems promising, but they are too expensive for resource constrained MANETs. However there are techniques that suit the resource constrained MANETs. These techniques are based on reputation systems. Each node builds and maintains reputation of all other nodes. The limitation of these techniques is that they lack blacklisting mechanism. Thus malicious node that is isolated from one place can join the network from another.

CHAPTER 5

Context Aware Monitoring Scheme

Chapter 3 presented attacks that kill the operation of MANETs by exploiting routing protocols. Most of the common attacks against MANETs are due to lack of security mechanism in routing protocols. These attacks include blackhole, grayhole and wormhole link attack. In presence of any of these attacks, network fails to operate and thus these attacks limit the applications of MANETs. In chapter 4 different existing schemes were presented to counter the attacks that target network layer. More specifically these techniques detect misbehaving node in MANETs and isolate it from the network. However these techniques have a common limitation. For example most common techniques that can detect blackhole attack successfully, fail to detect grayhole or wormhole link attack. The common techniques that can detect most routing misbehaviors are based on cryptographic primitives. For example ARAN requires the use of central authority to assign keys needed for authentication. The use of cryptographic primitives seems promising, but they are too expensive for resource constrained MANETs. However there are techniques that suit the resource constrained MANETs. These techniques are based on reputation systems. These techniques build and maintain reputation of each node in the network. But most reputation based schemes rely on strong nodes to observe other node's behavior and build reputation table. The other limitation of these techniques is that they do not have a mechanism to blacklist malicious node permanently. Thus malicious node that is isolated from one place can join the network from another place.

The focus of this chapter is to overcome the limitations of reputation based systems and devise a mechanism that is truly distributed. In this chapter, context aware monitoring scheme is presented. This scheme has two main components; monitoring and context awareness. The monitoring component is based on nodes acting as a watchdog. This means that all nodes monitor each other's behavior and maintain reputation (trust) table. The collaborative monitoring makes the scheme fault tolerant. This means that if a single neighbor of a node fails to monitor its behavior others would still be able to monitor it. The traffic sniffing is the basis of monitoring component which is used to detect the presence of malicious node in the network. After the misbehavior is detected by a node, local decision process is initiated to investigate the malicious node. Local decision process reduces false positives by considering trust values of each neighbor of the malicious node. Based on the accumulative trust value, local decision process takes decision regarding the isolation of malicious node from the network. Thus local decision process reduces the dependency on a single node to declare another node as malicious. The monitoring scheme enforces cooperation among the nodes and detects selfish nodes in the network. Selfish nodes are detected through the use of trust value. Selfish nodes will have lower trust values and thus network services are reduced accordingly.

The other component of the scheme is context awareness. This means that each node besides learning from its own experience also learns from the experience of other nodes. This property is necessary to restrict the entry of malicious node from other places. For example if a node has detected a malicious activity, then it shares the identity of the malicious node with every other node of the network through a flooded message. This flooding process makes sure that each node in the network knows the possible malicious ID and restricts its entry from anywhere in the network.

In the proposed context aware monitoring approach, promiscuous mode of a node is used to overhear the traffic of the neighboring node. The scheme assumes that wireless interface supports promiscuous mode. This means that any node can overhear the traffic of other nodes that lie in its communication range. In addition the scheme also assumes that each link between the nodes is bidirectional. This assumption is often valid since MAC layer protocol, including 802.11 requires bidirectional link between the communicating parties

for effective and reliable communication. The proposed scheme relies on first hop and second hop information of a node which it gathers through the exchange of control packets during network initialization. Thus overhearing traffic and maintaining first hop and second hop information are the key features of our scheme.

Currently, the scheme proposed in this chapter uses IDs based on Media Access Control (MAC) address, however, there are some concerns related to MAC address for example MAC spoofing. In order to guarantee the security and integrity of IDs, cryptographic processes should be used for their computations. This has been under consideration for future work.

5.1 Overhearing Traffic Mechanism

Figure 5.1 illustrates node 1 using promiscuous mode to overhear the traffic of node 2. Any node can overhear the traffic of other nodes that are in its radio range. In Figure 5.1, node 1 can overhear the traffic of node 2 but it cannot overhear the traffic of node 3 as node 3 lies outside its radio range. In other words all immediate neighbors or one hop away neighbors in MANETs can overhear the traffic of each other.

Node 2 and node 1 are immediate neighbors and thus both these nodes can communicate directly as well as overhear traffic of each other. Node 1 sends the packet to node 2, and monitors the behavior of node 2. If node 2 fails to forward the packet, node 1 decrements the trust value of node 2. However node 1 cannot decide whether node 2 has dropped the packet intentionally or the packet was dropped due to collision at link layer. To reduce the false positive introduced due to link layer collisions, node 1 suspects node 2 as malicious if packets dropped by node 2 falls below the threshold value.

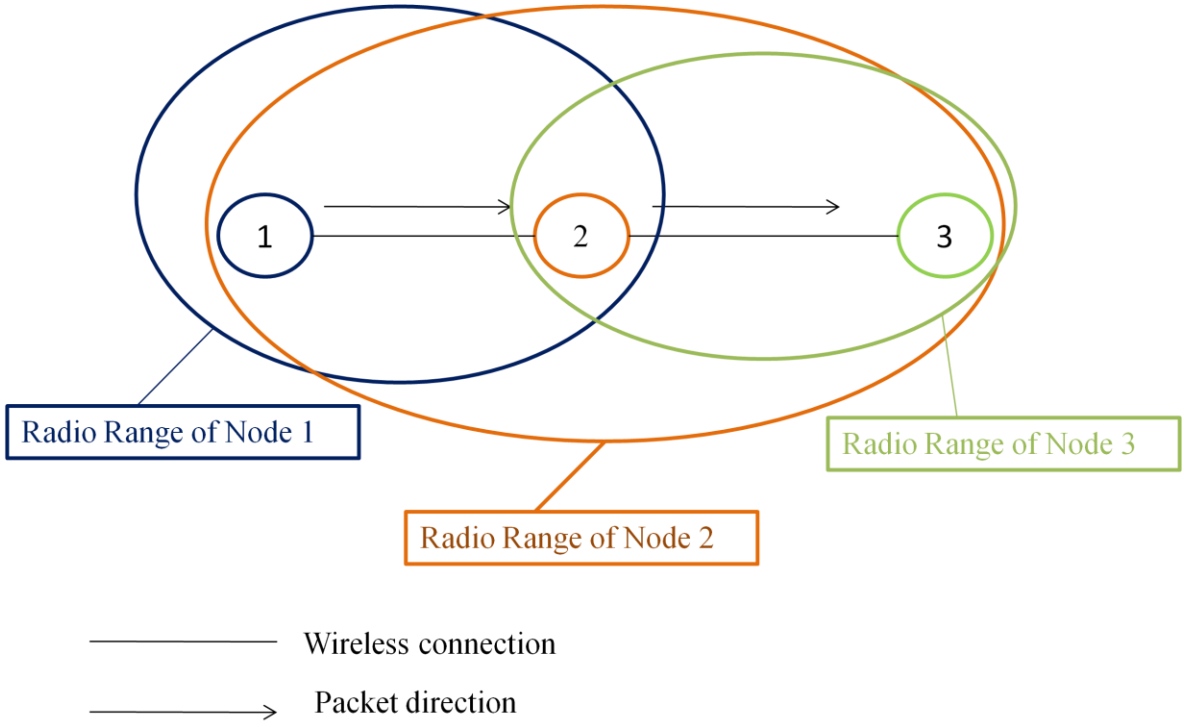

Figure 5.1: Packet overhearing mechanism

5.2 Network Initialization

Each node must broadcast its unique identity (ID) in order to join the network. The receiving node first checks the authenticity of that ID by comparing it with the IDs present in the malicious list. The concept of malicious list is explained in section 5.3. If the ID is found to be authentic, that is it does not match any of the IDs present in the malicious list, the receiving node sends back its own ID in response and thus only the authentic nodes can be a part of the network. Each node maintains a table containing first hop, second hop and trust information of its neighboring node. Figure 5.2 illustrates network initialization. Node 2 broadcasts its ID, since node 1 is the only neighbor of node 2, it sends back acknowledgement with its own ID only if the identity of the node 2 is found to be authentic. Both nodes acquire the desired first hop and node ID information. Similarly, when node 3 joins the network, it also broadcasts its ID and since node 2 is in the transmission range of node 1, thus node 1 can overhear the communication and adds node 3 as the second hop through node 2. To keep updated information in the table, nodes send keepalive message periodically. The keepalive message binds the corresponding node ID to ensure its

authenticity. For instance, when node 1 overhears keepalive message of node 3, it verifies the corresponding ID in keepalive message with the one already stored in its table. If there is no match, the keepalive message is considered as fake and thus the node ignores it. If node 1 does not overhear keepalive message from node 3 within a particular time interval, it will remove node 3 entry from its table. After the network is initialized each node maintains a table of its first and second hop neighbors. The table maintained by each node of Figure 5.2 is shown below.

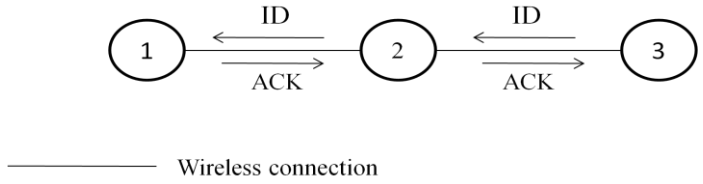

Figure 5.2: Network initialization

Table 5.1: Node 1 Entries

1st hop (ID)	2nd Hop (ID)	Trust Value
2	3	100

Table 5.2: Node 2 Entries

1st hop (ID)	2nd Hop (ID)	Trust Value
1 3		100 100

Table 5.3: Node 3 Entries

1st hop (ID)	2nd Hop (ID)	Trust Value
2	1	100

5.3 Detecting Blackhole Attack

In the proposed scheme, first and second hop information is used to detect any malicious activity in the network. Each node maintains the trust values of its neighbors based on their behavior in the network and therefore, blackhole attack can be detected locally. Consider

the MANET depicted in Figure 5.3 where node M is the malicious node. The neighboring nodes that are, node 1, node 2 and node 3 monitor the behavior of M and thus can detect malicious activity by M. When node M receives RREQ for node D. On the one hand, node 1 having the information of node 2 and node 3 as the neighbors of node M, expects M to forward RREQ. On the other hand, node 2 and node 3 can overhear RREQ sent to node M and thus expects to receive RREQ from node M. Any deviation from this behavior is considered malicious and therefore, node 1, node 2 and node 3 decrease the trust value of the malicious node M accordingly. When the trust value of node M declines beyond a specific threshold value (Ω) for any of its neighbors (in this case node 1, node 2 and node 3), they after deciding locally, flood alarm message about this malicious ID to warn all the nodes in the network. In this way, all nodes store the corresponding ID in their malicious list and therefore, the malicious node cannot re-join the network once gets isolated.

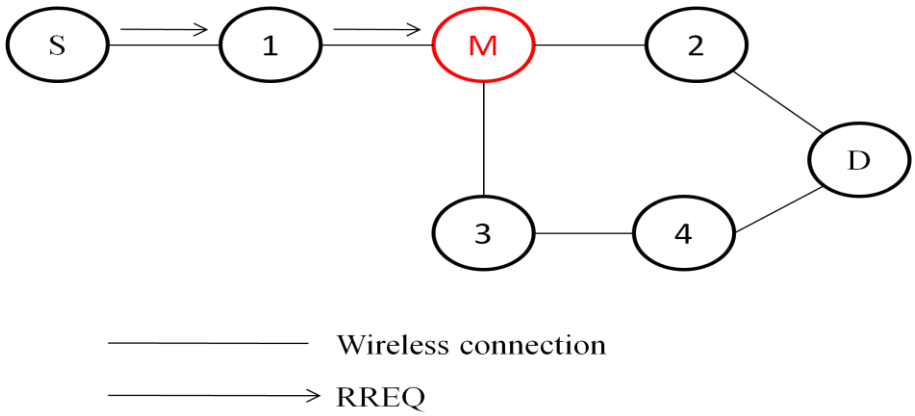

Figure 5.3: Malicious node detection

The proposed scheme can detect the cooperation among malicious nodes. Let us assume node 3 and node M are cooperating for a routing misbehavior. When node 3 receives RREQ packet it needs to propagate RREQ but rather it sends back a false RREP packet claiming it has an optimal route to node D. The monitoring nodes of node 3 are node M and node 4. Since node M is taking part in the malicious activity and thus does not generate alarm message about the malicious activity for its neighbors that are node 1 and node 4. However node 4 can still be able to detect the malicious activity and can generate alarm message to inform all the nodes in the network. Thus upon receiving alarm message

generated by node 4, neighbors of M suspects it for cooperation in the attack since they did not receive alarm message from node M.

5.3.1 Isolating Malicious Node

The scheme implements local decision process to ensure that the malicious activity of a node is detected and malicious node is penalized. Local decision means that if trust value for a malicious node in the table of any one of its neighboring nodes decreases below Ω, that particular neighbor then exchanges the corresponding trust value with other neighbors of the malicious node.

Figure 5.4 illustrates the local decision process for isolating malicious node M. The local nodes of M are node 1, node 2 and node 3, which have observed the behavior of node M. A node can initiate local decision process if the trust value of any other node falls below the threshold value Ω. For instance node 1 can initiate local decision if trust value of node M falls below Ω. Node 1 exchanges the trust value of malicious node with node 2 and node 3 which in turn send their trust values to node 1. After calculating the average of trust values, node 1 declares node M as malicious if the average trust value is below mentioned threshold value.

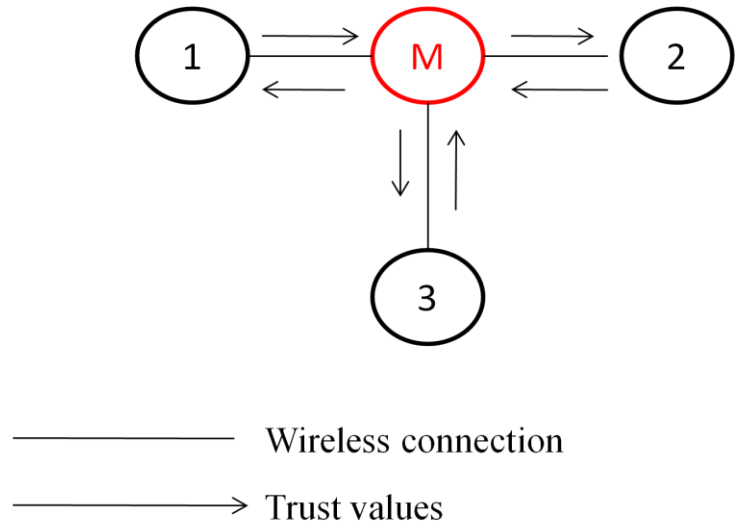

Figure 5.4: Local decision process

If the average trust value of malicious node falls below Ω, alarm message is flooded across the network. This flooding is to ensure that each node of the network stores the malicious ID in its malicious list. In this way, each node gets the information about malicious node, and therefore, any packet from malicious node will simply be dumped by all the nodes. Consequently, the malicious node gets isolated from the network and cannot rejoin the network.

The local decision is introduced in the scheme to reduce the probability of false positives, as the decision is dependent on each neighbor's trust assessment and not only on one specific neighboring node. Although CAMS has little overhead of flooding but this in turns gives the immense advantage of blocking a malicious node from rejoining the network.

5.4 Detecting Wormhole Link Attack

As mentioned in section 3.4 that wormhole link is a kind of tunneling attack in which two colluding nodes (worms) tunnels the packet through their private high speed channel. The purpose of this attack is to deny the services to legitimate nodes by dropping their packets. The two possible scenarios of wormhole link attack are considered. Figure 5.5 illustrates the tunnel formed by nodes A1 and A2, when both worms have only one neighbor. The other possible scenario is depicted in Figure 5.6 when both worms are located within the range of two legitimate nodes. In both of these scenarios node D is the target that is both worms launch the attack to deny node D from getting network services. The proposed scheme that is Context Aware Monitoring Scheme (CAMS) can prevent the wormhole link attack. The scheme is presented for both the scenarios illustrated in Figure 5.4 and Figure 5.5.

In Figure 5.5, node 5 and node 1 maintain the table containing A1 and A2 as their respective immediate neighbors. Source node broadcasts RREQ packet to node 1 which further propagates to node A1 and node 3. On the one hand, node 1 maintains second hop information through A1 and in this case there is no legitimate neighbor of A1. However node 1 cannot overhear the traffic sent and received by node A1 on wired channel. Thus it is not able to overhear the RREQ packet sent through tunnel, but it has the information that A1 does not have a legit neighbor.

On the other hand node 5 maintains its first hop and second hop neighbors and thus concludes that there is no second hop neighbor through node A2. When node 5 receives the RREQ packet from node A2, it suspects it as malicious since there is no neighbor of node A2 which could have sent RREQ to node A2. Thus node 5 silently drops the RREQ packet received from node A2 and propagates the RREQ received from node 4. In the mean while node 5 floods the alarm message about the malicious activity of node A2. When the node 1 receives the alarm message, it also suspects A1 as malicious.

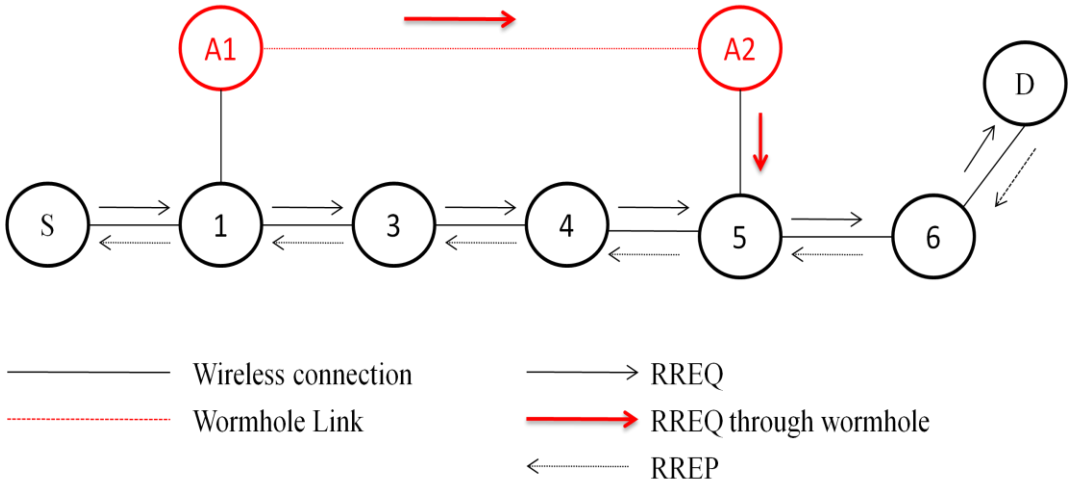

Figure 5.5: Worms are in range of exactly one legit neighbor

Figure 5.6 shows network scenario when both worms are in the range of two other legitimate nodes. Each node maintains a table during network initialization which was explained in section 5.2. For Figure 5.6, table maintained by node 1 and node 7 are shown below before detecting wormhole link attack is described.

Table 5.4: Node 1 Entries of Figure 5.5

1st hop (ID)	2nd Hop (ID)	Trust Value
S	4	100
A1	A2	100
7		100

Table 5.5: Node 7 Entries of Figure 5.5

1st hop (ID)	2nd Hop (ID)	Trust Value
1	S	100
A2	8	100

Let us assume node S needs to discover a route for node D. Node S broadcasts a RREQ packet to node 1 which further propagates it to node A1 and node 7, and observes the behavior of both nodes. Node A1 behaves normally and forwards the packet to node 4 but also sends the same RREQ to A2 through the tunnel. Node 1 cannot overhear the traffic sent and received on wired channel thus node 1 concludes the behavior of node A1 as normal. Node A2 receives two RREQ packets (one from node 7 and one from node A1), and RREQ through tunnel is received ahead of RREQ from node 7. Thus when A2 sends RREQ received through tunnel to node 8, node 7 being the monitoring node of A2, detects the malicious activity of node A2. One worm is detected and to detect the second worm that is node A1, RREP packets are used since RREP through tunnel will be received ahead of all RREP thus node 4 can detect this fake RREP and this way both nodes A1 and A2 are concluded as malicious.

CAMS propose another possibility to detect wormhole link when timing of the packets cannot be used to detect malicious nodes. For example node A2 could wait for RREQ from node 7 and before forwarding RREQ packet to node 5. To detect the possible wormhole link attack when timing of the packets can no longer be used to detect it, CAMS introduces previous hop address field in the RREQ. Each node appends node ID from where it has received RREQ packet. This means when node 1 receives RREQ from node S, it appends ID of node S, before forwarding the packet. Thus when malicious node A2 needs to forward RREQ packet, it has two possible choices for previous hop, it can append node A1 ID or node 7 ID. Since node 5 knows the second hop through node A2, thus A1 ID cannot be appended with RREQ; otherwise the packet will simply be discarded by node 5. If A2

appends the node 7 ID, node 5 considers it legitimate but node 7 can generate the alarm message since it has not forwarded the RREQ to node A2. To detect the other worm RREP packet with the additional previous hop address is used. Node A1 can receive RREP from node A2 and node 4. Since node 1 has the information of second hop so node A1 cannot append node A2 ID with the RREP packet thus A1 can only add ID of node 4. Adding node 4 ID causes alarm message flooded across the network.

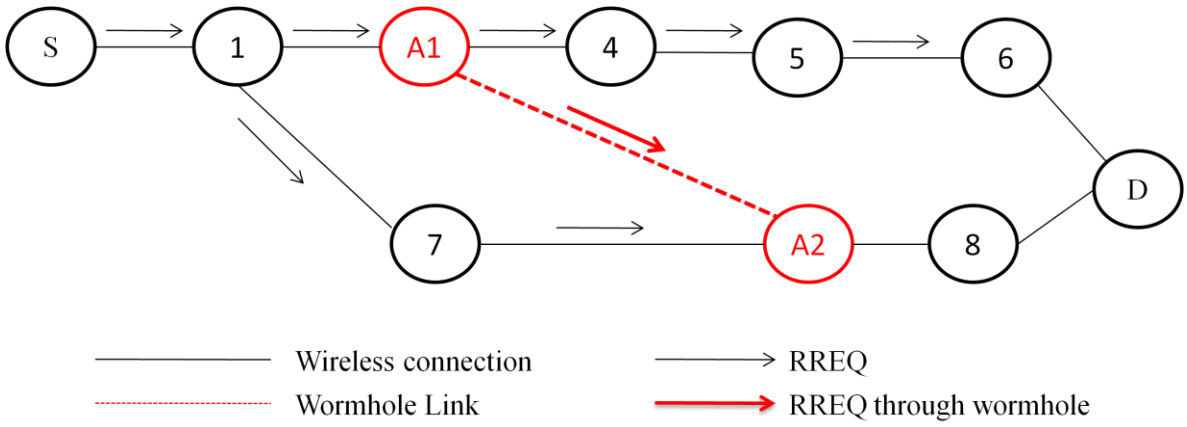

Figure 5.6: Worms are in range of more than one legit neighbor

5.4.1 Isolating Malicious Node

We use the same concept of node isolation as described in section 5.3.1. Since there are two malicious nodes located at different positions in the network, thus two separate local decision processes are initiated.

To detect worm A2, node 7 and node 8 exchange trust values and calculate average of their trust values. This average trust is compared against threshold trust value. Alarm message is generated if average trust value falls below threshold value. Alarm message contains malicious node ID. When node 4 receives the alarm message, it declares node A1 as the other worm after it overhears the fake RREP sent to node 1 by node A1. Thus both these nodes are discarded from the network and their IDs are stored in the malicious list maintained by each node to restrict their entry into the network.

5.5 Detecting Multiple Identities

CAMS can also be used to detect multiple identities across the network. Through the use of multiple identities, a node can utilize more network resources and it can also control traffic by affecting routing protocols. Let us assume the network scenario depicted in Figure 5.7. The new node 4 impersonated the id of already authenticated node and tries to join the network from a different location. New node 4 is in radio range of node 6 and thus sends its ID to node 6. Since both nodes 2 and 7 are also in the communication range of node 6 thus node 6 also knows second hops through both of these nodes.

Before authenticating new node, authenticated node is required to sends new node's ID to its second hop neighbors for verification. Each node matches new node's ID with already existing IDs from the trust table. If the match is found, fake ID message is generated and sent back to the source node. In Figure 5.7, node 6 sends new nodes ID to node 3 and node 8 which compare the new ID with its first hop and second hop IDs. In this case node 3 has a match thus it generates a fake ID message and sends it to node 6 through node 2. Node 2 can also verify since it has the information of second hop through node 3 in its table. The new node is thus restricted from joining the network with already existing ID.

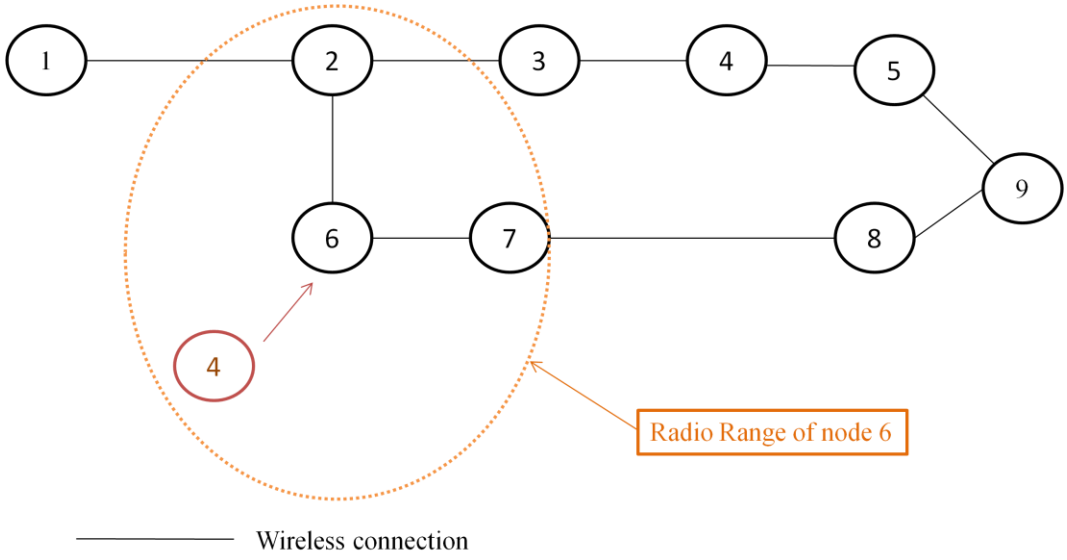

Figure 5.7: New node joining through node 6

5.6 Detecting Packet Modification

In packet modification attack, malicious node attempts to change the contents of packet. The motivation behind changing content varies according to the goal of the attacker. If attacker successfully changes content of RREQ packet then it controls traffic flow by affecting routing protocols.

Through the use of CAMS, it can be detected whether destination has received same packet content as sent by source. To detect modification each node saves packet in its buffer, after forwarding it to immediate neighbors and observe their behavior. Since every node can overhear traffic of its immediate neighbors thus it overhears packet sent by them and matches forwarded packet with the packet in its buffer. If there is mismatch in the contents of two packets it means immediate neighbor has changed contents of packet. Thus monitoring node can generate alarm message indicating to destination and source about a possible packet modification.

5.7 Summary

In this chapter technical detail of CAMS was presented. CAMS is a distributed, context aware monitoring scheme that detects and mitigates routing misbehaviors successfully. The key features that distinguish CAMS from other techniques are protocol independence and blacklisting mechanism. Local decision process was introduced which significantly reduced the probability of false positives. The chapter presented detection of blackhole, wormhole link attack through CAMS. These attacks are killer attacks for MANETs, thus countering these attacks is essential for proper operation of MANETs. The chapter also introduced detection of sybil and packet modification attack through CAMS. Packet modification attack could mislead source node to take different route than the legitimate route to send packets.

CHAPTER 6

Performance Analysis of CAMS

A simulation was performed in QualNet 5.0 in order to evaluate the performance of the proposed CAMS scheme. CAMS successfully detected blackhole attack and wormhole link attack and isolated malicious nodes from the network.

6.1 CAMS performance Under Blackhole Attack

The proposed scheme is compared with AODV to analyze packet delivery ratio and throughput under blackhole attack. The network model used for simulation is shown in Figure 6.1. The network model consisted of 20 nodes, out of which 2 were malicious nodes. A source node and a destination node were chosen randomly. Constant Bit Rate (CBR) traffic was used and source node generated 1 packet per second, 1000 in total, each carrying 512 bytes of data. Ω was taken as 10. Simulation was observed for 1000s with random mobility of nodes. Moreover, the mobility of nodes was varied between 0 to 50m/s to evaluate its impact on the performance of both CAMS and AODV. The complete set of simulation parameters is shown in Table I.

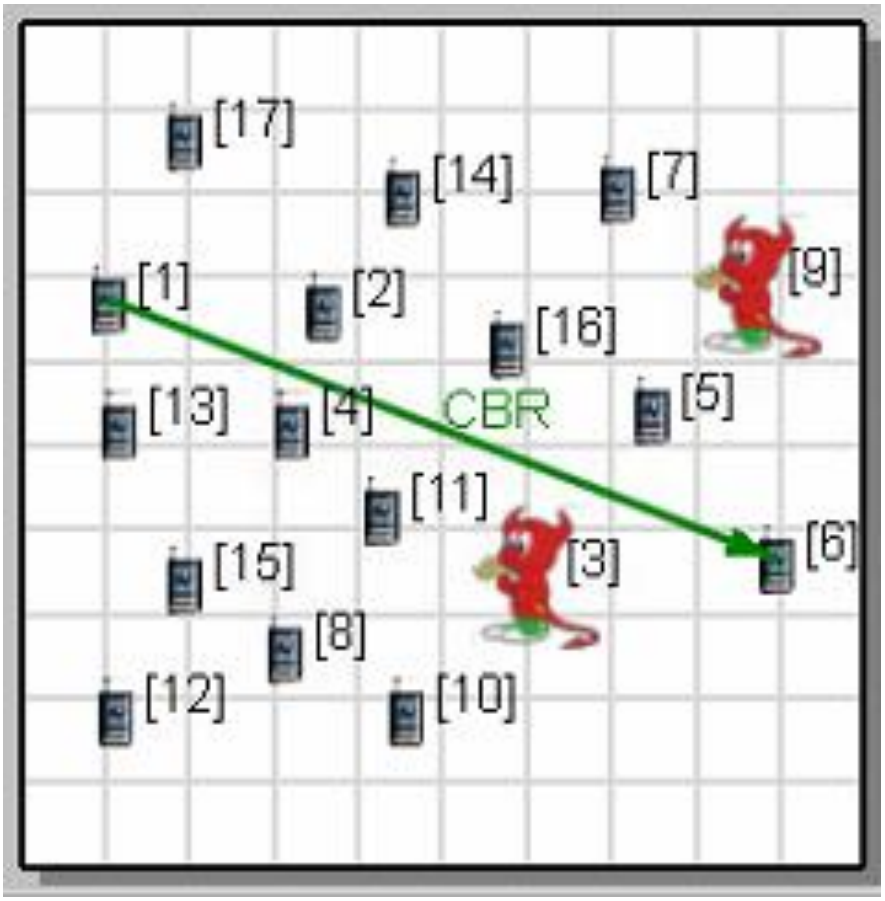

Figure 6.1: Network model for Blackhole attack detection using CAMS

Table 6.1: Simulation Parameters

Simulation parameters	**Values**
Topology dimensions	1000 m x 1000 m
Traffic type	CBR
Number of packets	1000
Packet size	512 bytes
Packet generation rate	512 bytes/s
Number of nodes	40
Simulation time	1000s
Mobility model	Random Waypoint
MAC/ PHY	802.11
Number of malicious	2

Figure 6.2 shows the operation of blackhole attack in the network model. Malicious node successfully convinced node 1 that it has optimal path for node 6. Once the route is established through malicious node, it discards packet causing denial of service to node 6.

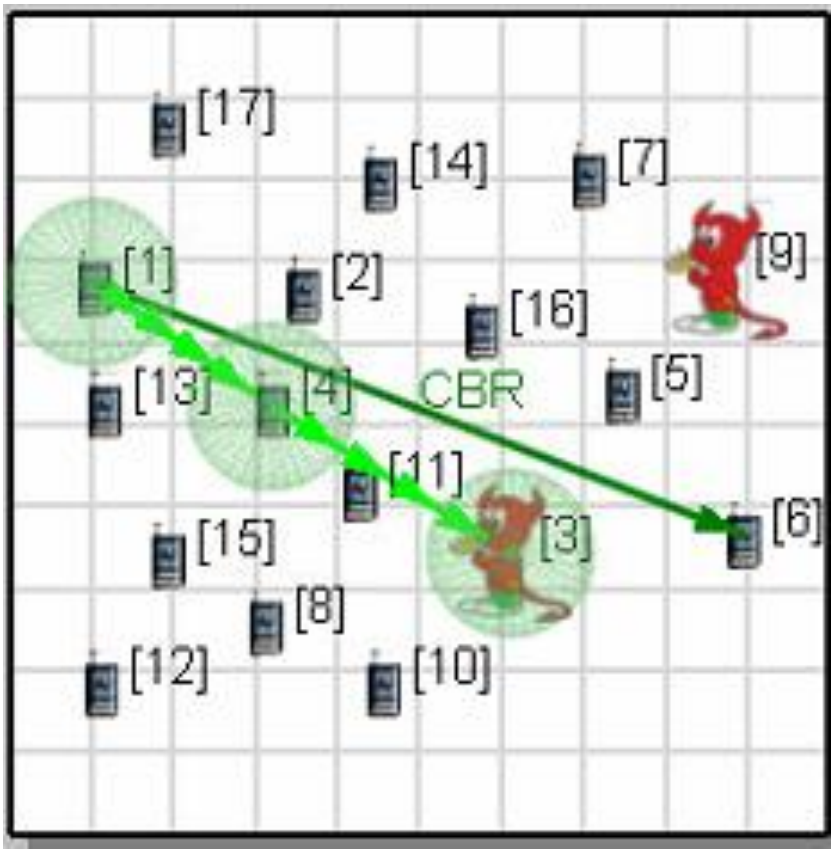

Figure 6.2: Spurious route through malicious node 3

Malicious behavior is observed by node 11 and node 16 thus they are responsible for generating alarm message indicating malicious behavior of node 3.

Figure 6.3 shows trust values of each node. Initially all nodes are trustworthy and assigned trust value is 100. This value is decreased whenever node's misbehavior is observed by its neighboring nodes. Since node 3 and node 9 did malicious activity by not forwarding the packets destined for node 6, thus their trust value is decreased by their monitoring nodes. When trust value falls below threshold value, both malicious nodes are isolated from the network.

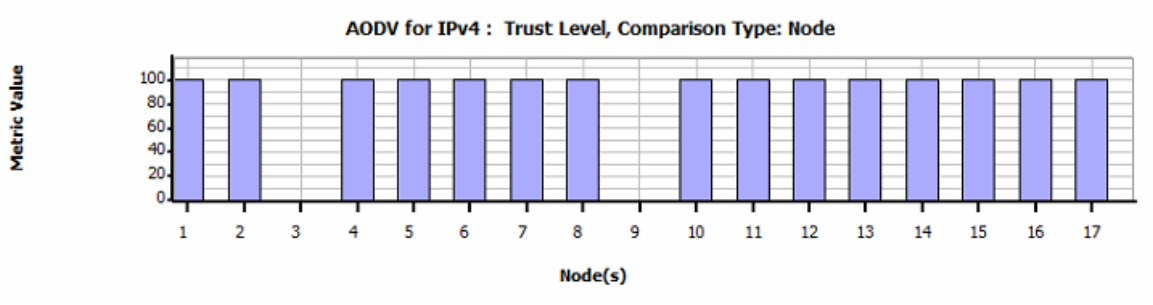

Figure 6.3: Decreased trust values of malicious nodes

Figure 6.4 presents the comparison of packet delivery ratio for AODV and CAMS. Initially the behavior of CAMS and AODV with static nodes (0 m/s) was analyzed. The malicious nodes were placed in such positions so that they could not disrupt the normal operation of the network. This is just to certify that CAMS does not cause any degradation in performance under normal circumstances. As the mobility of nodes is increased to 10 m/s, malicious nodes attempt to establish route through them by sending false RREP. The packet delivery ratio for AODV severely degrades and drops below 15% when the node mobility is 10 m/s, however, performance increases with the node mobility. This is due to link breakages in the communication as link breakages allow source node to discover new routes and thus it may find routes with no malicious node. Consequently, packet delivery ratio increases. In contrast to AODV, the packet delivery ratio for the proposed scheme CAMS is greater than or equal to 95% for each case. This result reveals that CAMS has consistent behavior and node mobility has very little impact on its performance.

Figure 6.5 compares throughput for CAMS and AODV. This result also strengthens the argument that CAMS does not cause any degradation in performance under normal conditions. Moreover, CAMS maintains very high throughput as compared to AODV. Thus, CAMS is a very effective and efficient scheme to detect and mitigate blackhole attack.

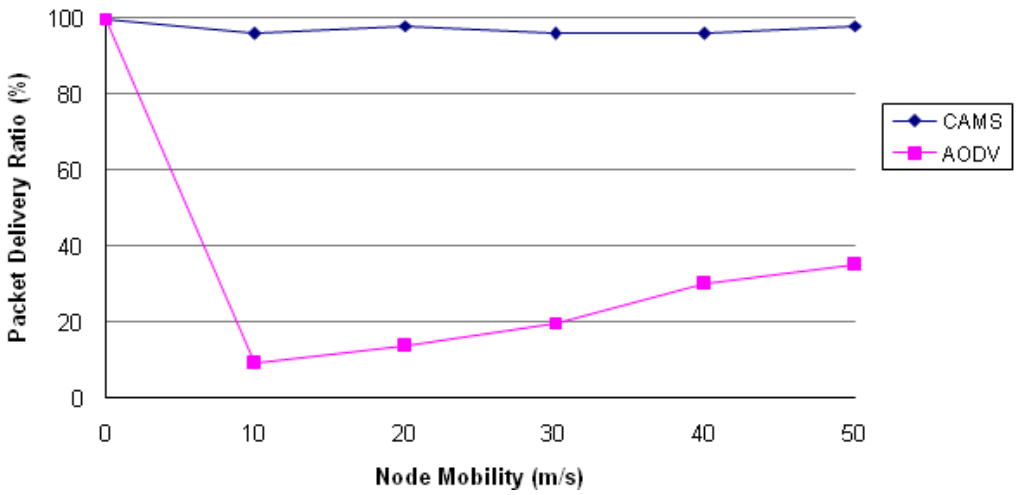

Figure 6.4: Comparison of packet delivery ratio between AODV and CAMS

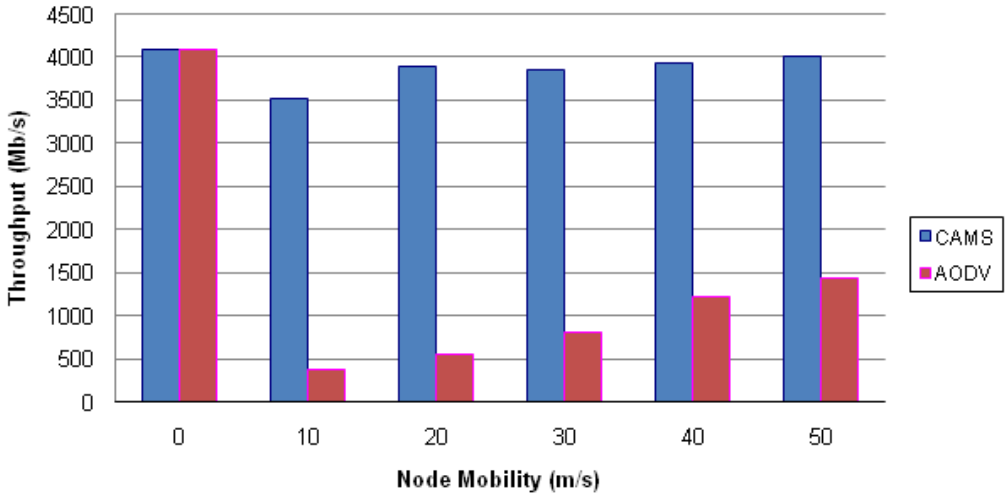

Figure 6.5: Comparison of throughput between AODV and CAMS

6.2 CAMS performance Under Wormhole Link Attack

To observe CAMS performance under wormhole link attack, two tunnels were created in the network model as shown in Figure 6.6. One tunnel is created between node 3 and node 12 while node 9 and node 7 forms second tunnel in the network.

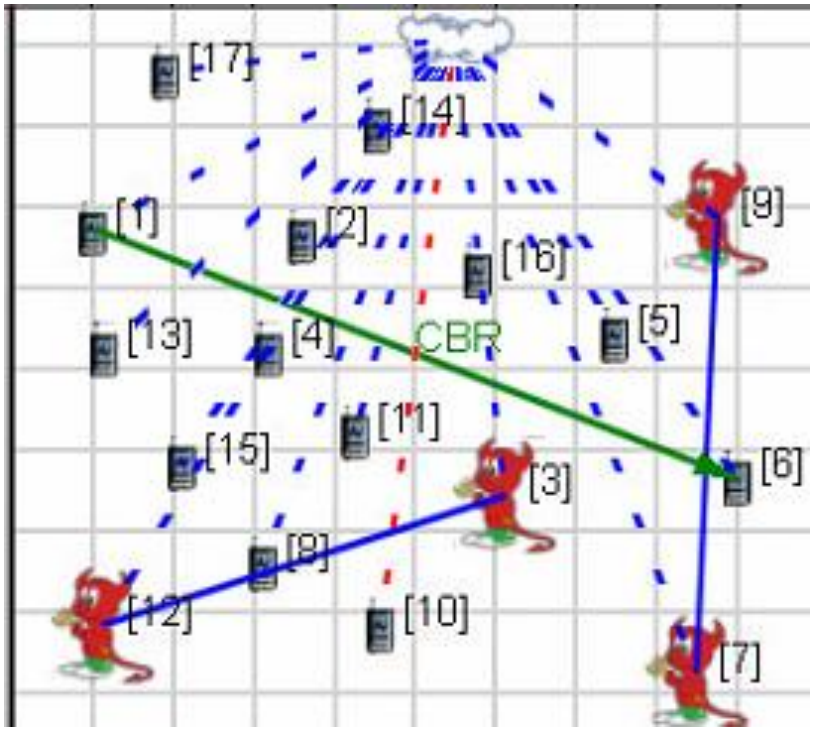

Figure 6.6: Tunnel between node 3 and node 12

Figure 6.7 presents the comparison of packet delivery ratio for AODV and CAMS. The initial behavior is similar to blackhole attack. Thus to certify that CAMS does not degrade performance under normal situations, worms were not allowed to tunnel the packets initially.

Since node 1 is trying to establish connection with node 6 and one of the worm lies between node 1 and node 6 which tunnels packet to second worm. Initially packets (RREQ and RREP) are not dropped since worm's goal is to establish route through it so that it can replay packets to other worm. Thus packet delivery ratio for AODV severely degrades and drops below 20% after route is established through one of the worm. There is a rise in packet delivery when mobility speed is increased. This is due to breakages in the communication as link breakages allow source node to discover new routes and thus it may find routes with no malicious node. Consequently, packet delivery ratio increases. In contrast to AODV, the packet delivery ratio for the proposed scheme CAMS is greater than or equal to 80% for each case. This result reveals that CAMS has consistent behavior and node mobility has very little impact on its performance.

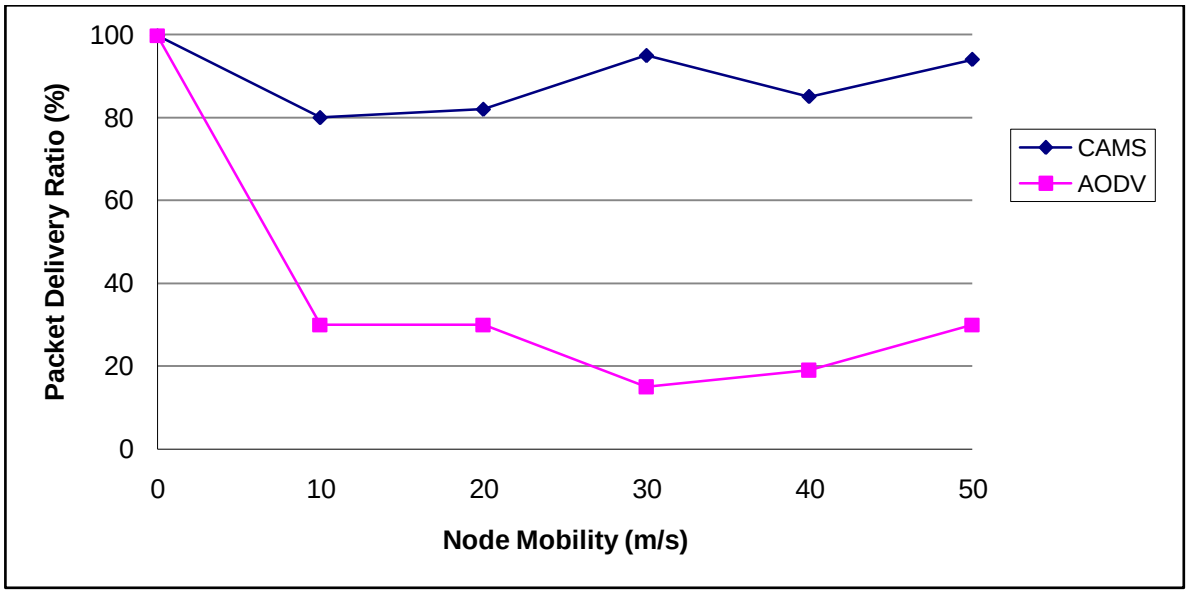

Figure 6.7: Comparison of packet delivery ratio between AODV and CAMS

Figure 6.8 compares the throughput for CAMS and AODV. This result also strengthens the argument that CAMS does not cause any degradation in performance under normal conditions. Moreover, CAMS maintains very high throughput as compared to AODV. Thus, CAMS is a very effective and efficient scheme to detect and mitigate wormhole attack.

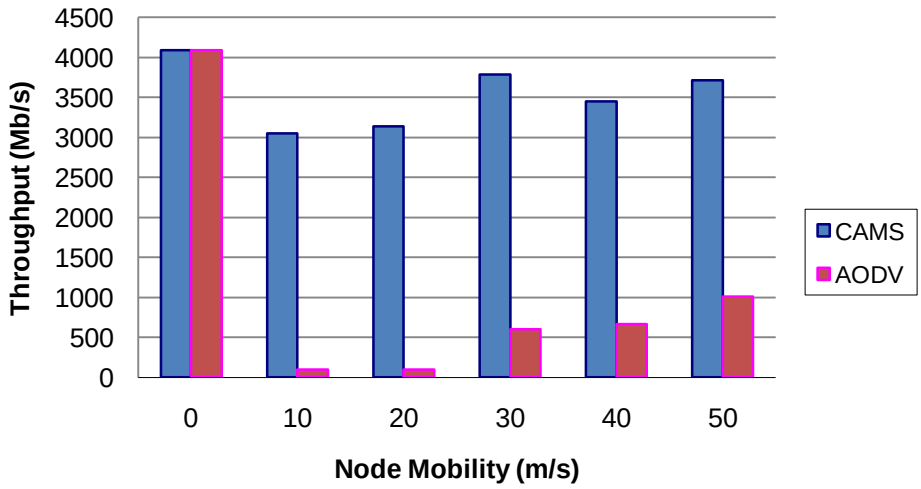

Figure 6.8: Comparison of throughput between AODV and CAMS

CHAPTER 7

Conclusion

A MANET is an emerging wireless technology that does not require predefined infrastructure. Thus these networks are suitable for mission critical applications such as disaster management and military operations. The distinguishing features of MANETS like lack of central administration and wireless medium make them vulnerable to various attacks including active and passive attacks. Passive attacks do not disrupt the flow of traffic while active attacks disrupt proper operation of the network. Due to lack of central authority, routing in MANETs relies on cooperation among the nodes. Routing protocols and its categories are thoroughly explained in chapter 2. Reactive routing protocols discover routes when requested by the sender whereas proactive routing protocols exchange control messages periodically. Both reactive and proactive routing protocols for MANETs lack security mechanisms and thus cannot detect and mitigate routing misbehaviors from a node.

Chapter 3 presented security attacks against each layer of TCP/IP reference model. The primary focus of chapter 3 is the attacks against network layer. The attacks that exploit routing protocols include blackhole, grayhole and wormhole link attack. In blackhole attack, malicious node falsely claims to have an optimal path to a destination. When data is transmitted through the advertised path, malicious node simply dumps the packets. Grayhole attack is a variation of blackhole in which behavior of the malicious node is unpredictable. In wormhole Link attack, two malicious nodes form their private tunnel in

the network and exchange messages through the tunnel. In presence of any of these attacks, network fails to operate properly and thus these attacks are killer attacks for the network.

Chapter 4 briefly reviewed existing countermeasures against routing misbehaviors. In this chapter pros and cons of each technique that detects and mitigates routing misbehaviors, were described. Most common techniques that detect blackhole attack successfully, fail to detect wormhole link or grayhole attack. The techniques that are based on cryptographic primitives such as RSA and digital signatures are too expensive for resource constrained MANETs. However there are techniques that suit the resource constrained MANETs. These techniques are based on reputation systems. Each node builds and maintains reputation of all other nodes. The limitation of these techniques is that they do not have a blacklisting mechanism. Thus malicious node that is isolated from one place can join the network from another place.

In chapter 5 an efficient, robust and distributed context aware monitoring scheme was proposed. This scheme has two main components; monitoring and context awareness. The monitoring component is based on nodes acting as a watchdog. This means that all nodes monitor each other's behavior and maintain reputation/trust table. The collaborative monitoring makes the scheme fault tolerant. The second component of the scheme is context awareness. This means that each node besides learning from its own experience also learns from the experience of other nodes. This property is necessary to restrict entry of the malicious node from any other place in the network. For example if a node has detected a malicious activity, then it shares the identity of the malicious node with each node of the network through a flooded message. This flooding process makes sure that each node in the network knows the possible malicious ID and restricts its entry from every place in the network. CAMS also detects selfish nodes in the network, thus enforces cooperation among nodes. Trust value is maintained by each node and network services are provided according to node's trust value.

The proposed scheme is implemented and tested in Qualnet 5.0. In chapter 6 performance of proposed scheme is discussed. As a benchmark the network model with default AODV and AODV with CAMS were used. Packet delivery ratio and throughput was compared with AODV protocol. The results were remarkable as the packet delivery ratio for CAMS is

more than or equal to 95%. Moreover, CAMS maintains high throughput and the node mobility has very little impact on its behavior.

References

[1] S. Ci, M. Guizani, H. Chen, and H. Sharif, "Self-Regulating Network Utilization in Mobile Ad Hoc Wireless Networks," IEEE Transactions on Vehicular Technology, vol. 55, no. 4, pp. 1302-1310, 2006.

[2] C. Perkins, E. Belding-Royer, and S. Das, "Ad hoc On-Demand Distance Vector (AODV) Routing," IETF RFC 3561 (Experimental), 2003.

[3] D. Johnson, Y. Hu, and D. Maltz, "The Dynamic Source Routing Protocol (DSR) for Mobile Ad Hoc Networks for IPv4," IETF RFC 4728 (Experimental), 2007.

[4] V. Park, and S. Corson, "Temporally-Ordered Routing Algorithm (TORA) Version 1 Functional Specification," IETF Internet Draft, draft-ietf-manet-tora-spec-04.txt, 2001.

[5] I. Chakeres, and C. Perkins, "Dynamic Manet On-demand (DYMO) Routing," IETF Internet Draft, draft-ietf-manet-dymo-09.txt, 2007.

[6] C. Perkins, and P. Bhagwat, "Highly Dynamic Destination-Sequenced Distance-Vector Routing (DSDV) for Mobile Computers," in proceedings of ACM SIGCOMM Conference on Communications Architectures, Protocols and Applications, pp. 234-244, London, UK, 1994.

[7] C. Adjih, T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, and L. Viennot, "Optimized Link State Routing Protocol, " IETF RFC 3626, 2003.

[8] A. Qayyum, L. Viennot, and A. Laouiti, "Multipoint Relaying for Flooding Broadcast Messages in Mobile Wireless Networks," in proceedings of the 35th Annual Hawaii International Conference on System Sciences, pp. 3866-3875, Hawaii, USA, 2002.

[9] Z. Haas, M. Pearlman, and P. Samar, "The Intrazone Routing Protocol (IARP) for Ad Hoc Networks," IETF Internet Draft, draft-ietf-manet-zone-iarp-02.txt, 2002.

[10] Z. Haas, M. Pearlman, and P. Samar, "The Interzone Routing Protocol (IERP) for Ad Hoc Networks," IETF Internet Draft, draft-ietf-manet-zone-ierp-02.txt, 2002.

[11] Z. Haas, M. Pearlman, and P. Samar, "The Bordercast Resolution Protocol (BRP) for Ad Hoc Networks," IETF Internet Draft, draft-ietf-manet-zone-brp-02.txt, 2002.

[12] H. Nguyen, and U. Nguyen, "Study of Different Types of Attacks on Multicast in Mobile Ad Hoc Networks," in proceedings of International Conference on Mobile Communications and Learning Technologies, pp. 149-154, Tahiti – Moorea, French Polynesia, 2006.

[13] R. Jhaveri, A. Patel, J. Parmar, and B. Shah, "MANET Routing Protocols and Wormhole Attack against AODV," International Journal of Computer Science and Network Security, vol. 10, no. 4, pp. 12-18, 2010.

[14] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," in proceedings of International Conference on Mobile Computing and networking (MobiCom), pp. 255-265, Boston, Massachusetts, USA, 2000.

[15] S. Bansal and M. Baker, "Observation-based cooperation enforcement in ad hoc networks," Technical Report, Computer Science Department, Stanford University, USA, 2003.

[16] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in Mobile Ad Hoc Networks: Challenges and Solutions," IEEE Wireless Communications, vol. 11, no. 1, pp. 38-47, 2004.

[17] Y. Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 370-380, 2006.

[18] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks," in proceedings of IEEE International Conference on Network Protocols (ICNP), pp. 78-87, Paris, France, 2002.

[19] M. Al-Shurman, S. Yoo, and S. Park, "Black Hole Attack in Mobile Ad Hoc Networks," in proceedings of ACM Southeast Regional Conference, pp. 96-97, Huntsville, Alabama, USA, 2004.

[20] G. Peng, and Z. Chuanyun, "Routing Attacks and Solutions in Mobile Ad hoc Networks," in proceedings of International Conference on Communication Technology, pp. 1-4, Guilin, China, 2006.

[21] S. Lee, B. Han, and M. Shin, "Robust Routing in Wireless Ad Hoc Networks," in proceedings of International Conference on Parallel Processing Workshops, pp. 73-78, Vancouver, B.C., Canada, 2002.

[22] S. Kurosawa, H. Nakayama, N. Kato, A. Jamalipour, and Y. Nemoto, "Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method," International Journal of Network Security, vol. 5, no. 3, pp. 338–346, 2007.

[23] L. Tamilselvan, and V. Sankaranarayanan, "Prevention of Blackhole Attack in MANET," in proceedings of International Conference on Wireless Broadband and Ultra Wideband Communications, pp. 21-26, Sydney, New South Wales, Australia, 2007.

[24] A. Fatima, A. Nassima, and B. Rachid, "Defending AODV Routing Protocol Against the Black Hole Attack," International Journal of Computer Science and Information Security, vol. 8, no. 2, pp. 112-117, 2010.

[25] P. Raj, and P. Swadas, "DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV Based MANET," International Journal of Computer Science Issues, vol. 2, no. 3, pp. 54-59, 2010.

[26] G. Xiaopeng, and C. Wei, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad-Hoc Networks," in proceedings of International Conference on Network and Parallel Computing Workshops, pp. 209-214, Dalian, China, 2007.

[27] P. Agrawal, R. Ghosh, and S. Das, "Cooperative Black and Gray Hole Attacks in Mobile Ad Hoc Networks," in proceedings of 2nd International Conference on Ubiquitous Information Management and Communication, pp. 310-314, Suwon, Korea, 2008.

[28] S. Banerjee, "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks," in proceedings of World Congress on Engineering and Computer Science, pp. 337-342, San Francisco, USA, 2008.

[29] O. Gonzalez, G. Ansa, M. Howarth, and G. Pavlou, "Detection and Accusation of Packet Forwarding Misbehavior in Mobile Ad-Hoc Networks," Journal of Internet Engineering, vol. 2, no. 1, pp. 181-192, 2008.

[30] Y. Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Networks," IEEE Journal on Selected Areas in Communications, vol. 24, no. 2, pp. 370-380, 2006.

[31] D. Raffo, C. Adjih, T. Clausen, and P. Miihlethaler, "Securing OLSR Using Node Locations," in proceedings of Next Generation Wireless and Mobile Communications and Services Conference, pp. 1-7, Nicosia, Cyprus, 2005.

[32] L. Qian, N. Song, and X. Li, "Detecting and Locating Wormhole Attacks in Wireless Ad Hoc Networks through Statistical Analysis of Multi-path," in proceedings of IEEE Wireless Communications and Networking Conference, pp. 2106-2111, New Orleans, LA, USA, 2005.

[33] L. Hu, and D. Evans, "Using Directional Antennas to Prevent Wormhole Attacks," in proceedings of Network and Distributed System Security Symposium, pp.131-141, San Diego, California, USA, 2004.

[34] L. Lazos, and R. Poovendran, "SeRLoc: Secure Range-Independent Localization for Wireless Sensor Networks," in proceedings of ACM Workshop on Wireless Security, pp. 21-30, Philadelphia, PA, USA, 2004.

[35] S. Capkun, L. Buttyan, and J. Hubaux, "SECTOR: Secure Tracking of Node Encounters in Multi-hop Wireless Networks," in proceedings of ACM Workshop on Security of Ad Hoc and Sensor Networks, pp. 21-32, Fairfax, Virginia, USA, 2003.

[36] K. Sanzgiri, B. Dahill, B. Levine, C. Shields, and E. Belding-Royer, "A Secure Routing Protocol for Ad Hoc Networks," in proceedings of IEEE International Conference on Network Protocols (ICNP), pp. 78-87, Paris, France, 2002.

[37] F. Kargl, A. Geiß, S. Schlott, and M. Weber, "Secure Dynamic Source Routing," in proceedings of Hawaiian International Conference on System Sciences, pp. 320-329, Hawaii, USA, 2005.

[38] W. Diffie, and M. Hellmann, "New Directions in Cryptography," IEEE Transactions on Information Theory, vol. 22, no. 6, pp. 644–654, 1976.

[39] Y. Hu, D. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," in proceedings of IEEE Workshop on Mobile Computing Systems and Applications, pp. 3-13, Callicoon, New York, USA, 2002.

[40] B. Levine, C. Shields, and N. Margolin, "A survey of solutions to the Sybil attack," Technical Report, University of Massachusetts Amherst, Amherst, MA, USA, 2006.

[41] C. Piro, C. Shields, B. Levine, "Detecting the Sybil Attack in Mobile Ad hoc Networks," in proceedings of International Conference on Security and Privacy in Communication Networks, pp. 1–11, Baltimore, MD, USA, 2006.

[42] J. Newsome, E. Shi, D. Song, and A. Perrig, "The Sybil Attack in Sensor Networks: Analysis & Defenses," in proceedings of International Symposium on Information Processing in Sensor Networks, pp. 259–268, Berkeley, California, USA, 2004.

[43] A. Tangpong, "Managing Sybil Identities in Distributed Systems," Ph.D. Dissertation in Computer Science and Engineering, The Pennsylvania State University, 2010.

[44] H. Yang, J. Shu, X. Meng, and S. Lu, "SCAN: Self-Organized Network-Layer Security in Mobile Ad Hoc Networks," in proceedings of ACM Workshop on Wireless Security, pp. 11-20, Atlanta, GA, USA, 2002.

[45] L. Buttyan, and J. Hubaux, "Nuglets: A Virtual Currency to Simulate Cooperation in Self organized Ad Hoc Networks," Technical Report, Swiss Federal Institute of Technology - Lausanne, Switzerland, 2001.

[46] S. Buchegger, and J. Boudec, "Nodes Bearing Grudges: Towards Routing Security, Fairness, and Robustness in Mobile Ad Hoc Networks," in proceedings of Workshop on Parallel, Distributed and Network-based Processing, pp. 403-410, Canary Islands, Spain, 2002.

[47] P. Michiardi, and R. Molva, "CORE: A Collaborative Reputation Mechanism to Enforce Node Cooperation in Mobile Ad Hoc Networks," in proceedings of Communication and Multimedia Security Conference, Portoroz, Slovenia, 2002.