Chapter 5

A SECURE ACKNOWLEDGEMENT METHOD FOR MANETs

Introduction

Mobile Ad-hoc Network (MANETs) is decentralized, and nodes rely on each other to store and forward packets. Nodes can freely join and leave the network, without any centralized monitoring. The movements of nodes are independent of another, unlike others which use dedicated nodes to support functions like routing, packet forwarding and network management. The systems distribute these services to all available nodes. Due to these features, the nodes to be easily captured & compromised, it is essential to provide security measures [81]. Therefore, safety in MANET is a crucial consideration. The operations of packet forwarding and routing can also be easily jeopardized if countermeasures are not embedded into network functions.

MANETs are self-con igurable, infrastructure less networks and so, each node cooperates with others. To keep the overhead low, security measures are not implemented in the protocols i.e. nodes are not checked for maliciousness. Due to this, nodes are easy targets of attackers which inject non-cooperative nodes into the network. Hence, the security issues are an important consideration, so it is important to develop an ef icient intrusion detection system for protection against attacks.

In this chapter, we propose and simulate a secure Digitally Signed Secure Acknowledgement Method (DSSAM) with the use of digital signature. In the proposed system, we have used a cryptographic mechanism to make the network secure. Three parameters are considered viz. secure acknowledgement, node authentication and packet authentication. We have observed the performance of DSSAM and compared it with two standard methods namely Watchdog and TwoAck using DSR routing protocol. The rate of detection of malicious behavior is more for the proposed system. However, associated overheads are high. A tradeoff between performance and cost has been considered. Simulations are performed on Qualnet.

The rest of this paper is organized as follows. In next section, we present a literature survey on co-related work in this area followed by a discussion of security issues and their current solutions in the mobile ad hoc network; there are numerous security threats for mobile ad-hoc network. So we must have to consider useful vulnerabilities in

the mobile ad hoc networks, which make it much easier to suffer from attacks. Then we discuss the attack types with security criteria and current security solutions for the mobile ad hoc network. After that, in next section a discussion of standard intrusion detection techniques. Digital signature is discussed in next section followed by problems de inition and proposed method. Further, performance evaluation of proposed and existed way through simulation is explained followed by results and discussion. In the end, the chapter is concluded.

STATE of the ART

K. Liu et al. [82] proposed and evaluated a technique, termed 2-ACK, to detect and mitigate the effect of sel ish nodes in routing. 2-ACK is based on a simple 2-hop acknowledgment packet that is sent back by the receiver of the next-hop link. The 2-ACK scheme solves several problems including limited transmission powers, ambiguous collisions and receiver collisions. The 2ACK scheme can be used ef iciently in DSR in MANETs.

TARP as a new security routing scheme focusing on level of Trust was presented and evaluated by L. Abusa et al. [83]. TARP is a technique which enables the discovery of secure routes in mobile ad hoc networks. The authors determined the trust metric based on a given set of parameters and then used it in TARP. TARP was able to improve the security of an ad hoc network.

In article [84] authors explains two techniques watchdog and pathrater, which helps to improve throughput in an ad-hoc network. Watchdog detects misbehaving nodes and the pathrater technique helps routing protocols to avoid these nodes for packet movement.

Cluster based trust mechanism to mitigate the internal attacks was proposed by R. Murugan et al. [85]. Here network is divided in group of clusters. Each cluster has certi ied cluster head (CH). Each node calculates the trust value for its one hop neighbors and sends it to CH. In turn, CH issues the trust certi icate to its member nodes. This mechanism provides better PDR and resilience against internal attacks.

L. Zhou et al. [86] developed requirements and technology to secure MANETs by addressing network con iguration and security issues during the response and recovery phases. Here, authors analyzed the security threats and presented the security

objectives that need to be achieved and established a secure key management service in an ad hoc networking environment. Authors took advantage of the redundancies in ad-hoc network topology and use diversity coding on multiple routes to tolerate both benign and Byzantine failures. They used threshold cryptography to distribute trust among a set of servers.

An ef icient security & trust management based algorithm for MANET was given by A. Singh et al. [87]. The time based nonce is generated at different time interval which gives effectiveness to the proposed approach in the sense that it is not easy to detect the generated nonce. It has been compared with the already existing trust based approach and inds better detection performance of the security threat in MANET.

F. Daryabar et al. [88] have discussed the techniques such as repacking, reverse engineering and hex editing for bypassing host-based Anti Virus (AV) signatures, a comprehensive comparison study have been made of different methods when malware might reach the host from outside the networks are demonstrated, a new intrusion detection technique based on honey-net systems is discussed.

Wu & Anantvalee [89] has given a survey on IDSs in MANETs [90], they classify the architectures for intrusion detection system in mobile ad-hoc networks, each of which is suitable for different network infrastructures on node cooperation are reviewed and compared.

5.1 Vulnerabilities of the Mobile Ad Hoc Networks

Mobile ad hoc networks have more vulnerabilities than the traditional wired networks, due to its inherent nature and wireless medium. Various vulnerabilities exist in the mobile ad hoc networks.

5.1.1 Lack of Secure *Boundaries*

This vulnerability originates from the nature of the mobile ad hoc network: freedom to join, leave and move inside the network. Once the adversary is in the radio range of any other nodes in the mobile ad-hoc network, it can easily communicate with others in its radio range and thus join the network automatically. As a result, the mobile ad-hoc network does not provide a secure boundary to protect the network from potentially dangerous network accesses. Lack of safe boundaries makes the mobile ad hoc network susceptible to the attacks. The attacks mainly include passive eavesdropping, active

interfering, and leakage of secret information, data tampering, message replay, message contamination, and denial of service [98].

5.1.2 Threats from Compromised nodes Inside the Network

Some other attacks aim to gain the control over the nodes themselves by some unrighteous means and then use the compromised nodes to execute further malicious actions. This type of vulnerability depicts as the threats that come from the compromised nodes inside the network. Due to the mobility in the network, a compromised node can frequently change its attack target and perform a malicious behavior to different-different nodes in the network, this type of threats is more dangerous than the attacks from outside the network, and these attacks are much harder to detect. A good example of this kind of threats comes from the potential Byzantine failures encountered in the routing protocol for the mobile ad hoc network [98]. We call it a Byzantine failure when a set of nodes are compromised in such a way that the incorrect and malicious behavior cannot be directly detected because of the cooperation among these compromised nodes when they perform malicious behaviors.

The compromised nodes may seemingly behave well; however, they may make use of the laws and inconsistencies in the routing table with may advertise new routing information that contains a missing link, provide fake link state information, or even lood other nodes with routing traf ic. Because the compromised nodes cannot be easily recognized, their malicious behaviors are prone to be ignored by other nodes. Therefore, Byzantine failure is very harmful to the mobile ad hoc network. The inding of above statements is that we should be paid more attention to the threats like compromised nodes.

5.1.3 Lack of Centralized Management Facility

Mobile Ad-hoc networks do not have a centralized management facility like name server, which leads to some vulnerable problems. Due to the absence of centralized control service the detection of attacks a tough task because it is not easy to monitor the traf ic in a highly dynamic and large scale ad hoc network [99].

It is quite common in the mobile ad hoc network that benign failures, such as packet dropping, path breakages and transmission impairments, happen frequently. So that it

will be harder to detect, especially when adversaries change their attack pattern with periods of time.

There is the main problem of trust management as well, for the nodes in mobile ad hoc network, due to lack of centralized control facility [98]. Mobile ad hoc network, for better ef iciency, requires less complex and less load in protocols execution, this is the main reason of less security association on nodes.

Hence, the absence of centralized management facility will cause vulnerability. This vulnerability can in luence several aspects of operations in the mobile ad hoc network.

5.1.4 Restricted Power Supply

In the case of a wired network, do not need to consider power supply problem because they can get electric power supply from the outside but in the event of ad hoc network, the nodes in the mobile ad-hoc network need to consider the restricted battery power, which will cause several problems.

The irst issue that may be resulting from the limited power supply is denial-of-service attacks [98]. Since the adversary knows that the target node is battery-restricted, it can either continuously send additional packets to the destination, ask it to route those packages, or it can induce the target to be trapped in some time-consuming computations. In this way, the battery power of the destination node will be exhausted by these meaningless tasks, and thus, the target node will be out of service for all the good service requests since it has run out of power.

Furthermore, a node in the mobile ad hoc network may behave in a sel ish manner when it inds that there is only limited power supply, and the sel ishness can cause some problems.

When there is a need for this node to cooperate with other nodes to support some functions in the network. Just take the cluster-based intrusion detection technique as an example [100]. In this technique, there is no need that every node in the ad hoc network is the monitoring node all the time; instead, a cluster of neighboring MANET nodes can randomly and fairly elect a control node that will observe the abnormal behaviors in the network traf ic for the entire group. However, an essential precondition for the success of this technique is that every node in the cluster is willing to take their responsibility as a monitoring node and serve for all other nodes in a period. There may be some nodes

that behave sel ishly and do not want to cooperate in the control node election process, which will make the election fail if there are too many sel ish nodes. Moreover, we should not view all of the sel ish nodes as malicious nodes: some nodes may encounter restricted power supply problem and thus behave in a sel ish manner, which can be tolerated; however, there can be some other node who intentionally announces that it runs out of battery power and therefore do not want to cooperate with other nodes in some cooperative operation, but actually, this node still has enough battery power to support the collective action. In a word, sel ish behaviors should not be regarded as malicious behaviors, but we need to know if the sel ishness is caused by the limited battery power, or by the intentional non-cooperation.

5.1.5 Scalability

Finally, we need to address the scalability problem when we discuss the vulnerabilities in the mobile ad hoc network [98]. Unlike the traditional wired network in that its scale is generally prede ined when it is designed and will not change much during the use, the scale of the ad hoc network keeps changing all the time: because of the mobility of the nodes in the mobile ad hoc network, you can hardly predict how many nodes there will be in the network in the future. As a result, the protocols and services that are applied to the ad hoc network such as routing protocol and key management service should be compatible to the continuously changing scale of the ad hoc network, which may range from decades of nodes to hundreds of nodes, or even thousands of nodes. In other words, these protocols and services need to scale up and down ef iciently.

5.1.6 Vulnerabilities of the Mobile Ad Hoc Networks: Summary

From the discussions of this section, we can safely conclude that the mobile ad hoc network is insecure by its nature. There is no clear line of defense because of the freedom of the nodes to join, leave and move inside the network. Some of the nodes may be compromised by the adversary and thus, perform some malicious behaviors that are hard to detect. Lack of centralized machinery may cause some problems when there is a need to have such a centralized coordinator. The limited power supply can cause some sel ish problems. Continuously changing the scale of the network has set higher requirement to the scalability of the protocols and services in the mobile ad hoc network. As a result, compared with the wired network, the mobile ad hoc network will need more robust security scheme to ensure the safety of it. In the next section, we will

survey several security solutions that can provide some help to improve the safety environment in the ad hoc network.

5.2 Attacks in Mobile Ad-hoc Network: There are mainly two types of attacks as passive or active.

a) **Active Attacks:** These attacks cause unauthorized state changes in the network such as denial of service, modi ication of packets, and the like. These attacks are generally launched by users or nodes with authorization to operate within the network. We classify active attacks into four groups: dropping, modi ication, fabrication, and timing attacks. It should be noted that an attack can be classi ied into more than one group.

b) **Passive attacks:** In a passive attack an unauthorized node monitors and aims to ind out information about the network. The attackers do not otherwise need to communicate with the network. Hence they do not disrupt communications or cause any direct damage to the network. However, they can be used to get information for future harmful attacks. Examples of passive attacks are eavesdropping and traf ic analysis.

Attacks on different layer

The following table 5.1 explains the security attacks on each layer of the Internet model and table 5.2 express the appropriate security issues for MANET on each layer.

Layer	Attacks
Physical layer	Eavesdropping, jamming
Data link layer	Traf ic analysis, Monitoring
Network layer	Wormhole, Black hole
Transport layer	Syn. looding
Application layer	Repudiation, Data corruption
Multilayer Attacks	Impersonation, Replay

Table 5.1: Attacks on Different layers

Security issues for MANET

Layer	Security Issues
Physical layer	Preventing signal jamming and denial-of-service attacks
Data link layer	Protecting the wireless MAC protocol and providing link layer security support
Network layer	Protecting the ad hoc routing and forwarding protocols
Transport layer	Authentication and securing end-to-end or point-to-point communication through data encryption
Application layer	Detecting and preventing viruses, worms, malicious codes.

Table 5.2: Security issues for MANET

Here we discussed few of important attack types that emerge mostly in the mobile ad hoc networks. [101,102]

5.2.1 Dropping packets attacks

There are many reasons for dropping packets in ad hoc networks. We can classify these reasons into two main types: unintentional and intentional mischievous activity. The chart of types of reasons for dropping is given in igure 5.1. The unintended playful activity could be caused by many reasons like network congestion or collision, node overloaded (due to lack of limited buffer space or CPU cycles). Because wireless channels are known to be unreliable, packet dropping may occur due to link errors such as interference or fading.

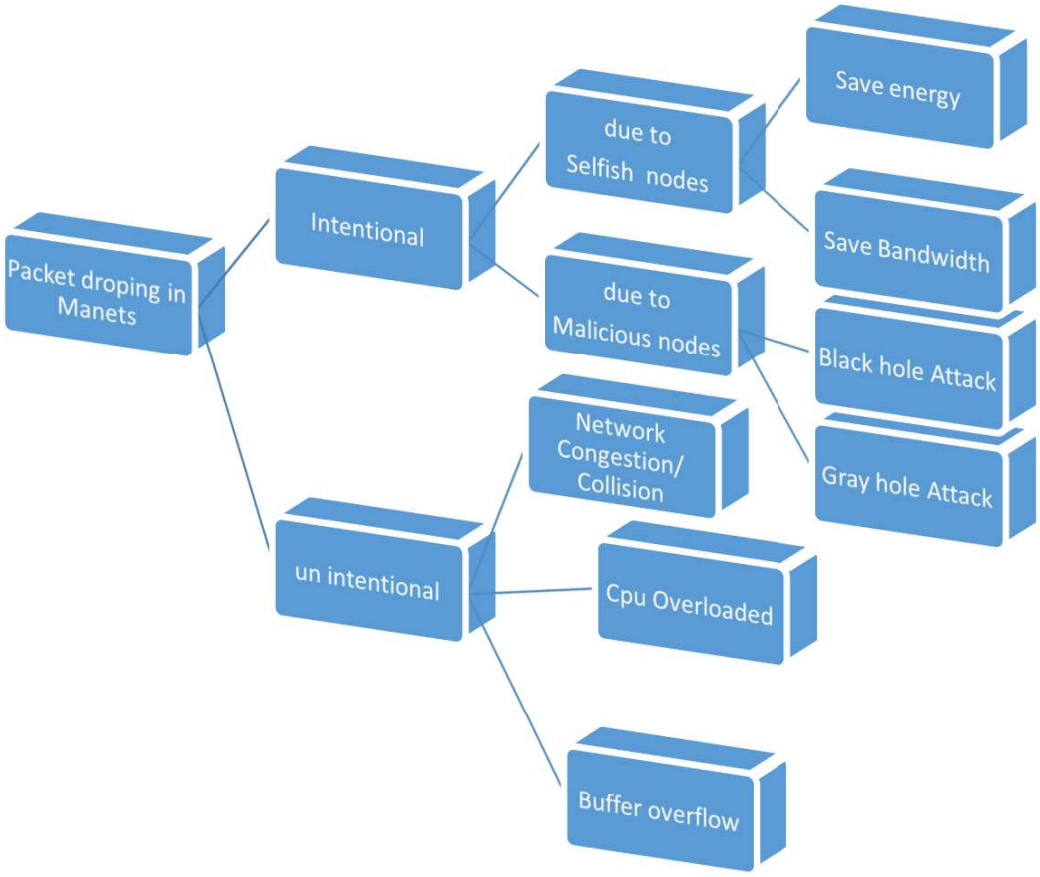

Figure 5.1: Chart of reasons for Packets dropping

5.2.2. Attacks on Routing

Among all network services; routing is unique web service. This service is much prone for attackers to conduct their malicious activity. In the mobile ad hoc networks, attacks on routing are classi ied into two categories attacks on packet forwarding/delivery and core routing protocols data low. Attacks on routing protocols data low aim to block the propagation of the routing information to the victim. Endeavor to disturb the package delivery along a prede ined path. The major effects on the network include network partition, routing loop, resource deprivation and route hijack [103].

5.2.3. Denial of Service

Denial of service; which aims to restrict or stop the availability of certain node or even the services of the entire ad hoc networks by various ways. In the wired network, this attack is carried out by looding some unwanted network traf ic to the target, so as to

exhaust the processing power of the target and make the services provided by the target become Unavailable. Nevertheless, it becomes not practical to perform the conventional Denial of service attack in the mobile ad hoc networks because of the distributed nature of the services.

In spite of the mobile ad hoc networks are more vulnerable than the wired networks because of the interference-prone radio channel and the limited battery power. Usually, such attackers use the radio jamming and exhaustion cell methods to conduct Denial of service attacks to the mobile ad hoc networks.

5.2.4. Impersonation

Impersonation attack is a severe threat to mobile ad-hoc network, if there is not such a proper authentication mechanism among the nodes, the adversary can capture some nodes in the network and make them look like benign nodes. In this way, the compromised nodes can join the network as the standard nodes and begin to conduct the malicious behaviors such as propagate fake routing information and gain inappropriate priority to access some con idential information.

5.2.5. Eavesdropping

Eavesdropping is another kind of attack that usually happens in the mobile ad hoc networks. The goal of eavesdropping is to obtain some con idential information that should be kept secret during the communication. The sensitive information may include the location, public key, private key or even passwords of the nodes. Because such data are critical to the security state of the nodes, they should be kept away from the unauthorized access.

Attack Types in Mobile Ad Hoc Networks: Summary

Here we mainly discuss the attack types in the mobile ad hoc networks. The attacks in MANET can be brie ly classi ied into two categories: external attacks and internal attacks, latter of which are far more dangerous to the mobile ad hoc network. Then we brie ly introduce the main attack types in the mobile ad hoc network, which are dropping packet attacks, attacks against routing, denial-of-service attacks, eavesdropping and impersonation attacks.

5.3 Safety solutions to the Mobile Ad Hoc Networks

We have discussed several vulnerabilities that potentially make the mobile ad hoc networks Insecure in the previous section. However, it is far from our ultimate goal to secure the mobile ad hoc network if we merely know the existing vulnerabilities in it. As a result, we need to ind some security solutions to the mobile ad hoc network. In this section, we survey some protection schemes that can be useful to protect the mobile ad hoc network from malicious behaviors.

Security Criteria

Before we survey the solutions that can help secure the mobile ad hoc network, we think it necessary to ind out how we can judge if a mobile ad hoc network is secure or not. In other words, what should be covered in the security criteria for the mobile ad hoc network when we want to inspect the safety state of the mobile ad hoc network. In the following, we brie ly introduce the widely-used criteria to evaluate if the mobile ad hoc network is secure.

Availability

The term *Availability* means that a node should maintain its ability to provide all the designed services regardless of the security state of it [98]. This security criterion is challenged mainly during the denial-of-service attacks, in which all the nodes in the network can be the attack target and thus some sel ish nodes make some of the network services unavailable, such as the routing protocol or the key management service.

Integrity

Integrity guarantees the identity of the messages when they are transmitted. Integrity can be compromised primarily in two ways:

a. Malicious activity
b. Accidental

A message can be removed, replayed or revised by an adversary with malicious goal, which is regarded as malicious altering; on the contrary, if the message is lost or its content is changed due to some benign failures, which may be transmission errors in communication or hardware errors such as hard disk failure, then it is categorized as accidental altering.

Con identiality

Con identiality means that certain information is only accessible to those who have been authorized to access it. In other words, in order to maintain the con identiality of some con idential information, we need to keep them secret from all entities that do not have the privilege to access them.

Authenticity

Authenticity is essentially assurance that participants in communication are genuine and not impersonators [98]. It is necessary for the communication participants to prove their identities as what they have claimed using some techniques so as to ensure the authenticity. If there is not such an authentication mechanism, the adversary could impersonate a benign node and thus get access to con idential resources, or even propagate some fake messages to disturb the normal network operations.

Non-repudiation

Non-repudiation ensures that the sender and the receiver of a message cannot deny that they have ever sent or received such a message. This is useful especially when we need to discriminate if a node with some abnormal behavior is compromised or not: if a node recognizes that the message it has received is erroneous, it can then use the incorrect message as an evidence to notify other nodes that the node sending out the improper message should have been compromised.

Authorization

Authorization is a process in which an entity is issued a credential, which speci ies the privileges and permissions it has and cannot be falsi ied, by the certi icate authority. Authorization is generally used to assign different access rights to different level of users. For instance, we need to ensure that network management function is only accessible by the network administrator. Therefore there should be an authorization process before the network administrator accesses the network management functions.

Anonymity

Anonymity means that all the information that can be used to identify the owner or the current user of the node should default be kept private and not be distributed by the node itself or the system software. This criterion is closely related to privacy preserving, in which we should try to protect the privacy of the nodes from arbitrary disclosure to any other entities.

Security Criteria: Summary

We have discussed several main requirements that need to be achieved to ensure the security of the mobile ad hoc network. Moreover, there are some other security criteria that are more specialized and application-oriented, which include location privacy, self-stabilization and Byzantine Robustness, all of which are related to the routing protocol in the mobile ad hoc network. Having dealt with the main security criteria, we then move to the discussion on the main threats that violate the security criteria, which are generally called as attacks.

5.3.1 Intrusion Detection Techniques in MANETs

In MANETs, every node presumes that other nodes cooperate with each other to transmit and receive data. This paves opportunity for the attackers to react and perform the malicious activity on the network, with few compromised nodes. To address this problem, we should consider three important functions viz. prevention, detection and recovery [90]. These features provide three-layered security to MANETs. In this section, we are discussing the intrusion detection system -usually the second security layer. Two classical detection approaches exists namely:

a. Watchdog & Path-rater [84]

b. TWOACK

5.3.1.1 Watchdog & Path-rater

Watchdog and Path-rater are two main components of a system that tries to improve the performance of ad hoc networks by detecting disruptive activity nodes in the presence of disturbing nodes, the particular working principles of which are discussed below [84,104]. Watchdog determines misbehavior by copying packets to be forwarded

to a buffer and monitoring the behavior of the adjacent node to these packages. Watchdog promiscuously snoops to decide if the adjacent node sends the packets without modi ications or not. If the packages that are snooped match with the observing node's buffer, then they are discarded; whereas packets that stay in the buffer beyond a timeout period without any successful match are lagged as having been dropped or modi ied. The node responsible for forwarding the packet is then noted as being suspicious. If the number of violations becomes greater than a certain predetermined threshold, the violating node is marked as being malicious. Information about malicious nodes is passed to the Path-rater component for inclusion in path rating evaluation.

The logical process is explained in igure 5.2; it detects the misbehaving nodes. Suppose there is a path from node S to D through A, B and C. Now, A can't transmit to C, but can listen to B. So, A can tell if B sends the packet. If encryption is not performed on each link (which itself is a costly affair), then A can also determine if B has tampered with either payload or header.

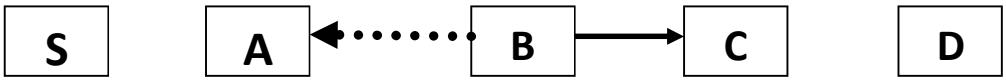

Figure 5.2 Watchdog technique

DSR routing protocol can detect misbehavior at the forwarding level. The weakness of watchdog lies in the fact that it may not be able to detect a misbehaving node in the presence of:

1. Ambiguous collisions
2. Receiver collisions
3. Limited transmission power
4. False misbehavior
5. Collision and Partial dropping

5.3.1.2 TwoAck

To overcome the weakness of watchdog Liu et al. [82] proposed TWOACK method. It aims to resolve the receiver collision and limited transmission power problems of Watchdog. It acknowledges every data packet transmitted over two hops distance and

every three consecutive nodes along the path from source to destination. In this way, it detects misbehaving links. Figure 5.3 shows the working of TWOACK method. I sends packet 1 to J, and J sends the same to K. Upon receiving the packet, K generates a TWOACK packet containing the reverse route from K to I and sends it back to I. This message when received by I, shows successful transmission of packet from I to K. Otherwise, if this TWOACK packet is not received within a prede ined period, both nodes J and K are reported malicious. The same process applies to every three consecutive nodes along the rest of the route. The acknowledgement process required in every packet transmission process added a signi icant amount of unwanted network overhead. Due to the limited battery power nature of MANETs, such redundant communication process can quickly degrade the lifespan of the entire system. However, many research studies are working in energy harvesting to deal with this problem [91, 92].

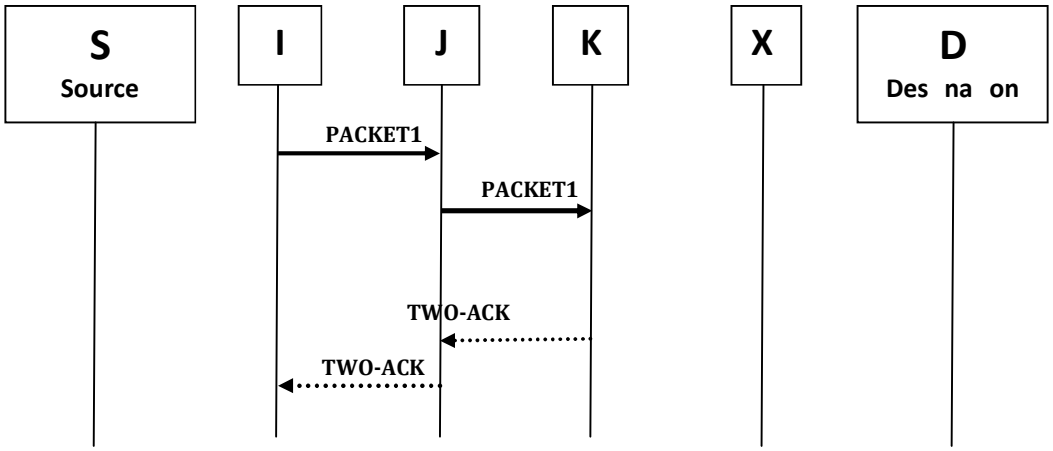

Figure 5.3: TWOACK Method

DIGITAL SIGNATURE:

Digital signatures are often used to implement electronic signatures, a broader term that refers to any electronic data that carries the intent of a signature, but not all electronic signatures use digital signatures. In some countries, including the United States, India, Brazil, Saudi Arabia, the European Union and Switzerland, electronic signatures have legal signi icance.

Digital signatures employ asymmetric cryptography. In many instances they provide a layer of validation and security to messages sent through a non-secure channel: Properly implemented, a digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signature schemes, in the sense used here, are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid. Digitally signed messages may be anything representable as a bit string: examples include electronic mail, contracts, or a message sent via some other cryptographic protocol.

A digital signature scheme typically consists of three algorithms;

- A *key generation* algorithm that selects a *private key* uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding *public key*.
- A *signing* algorithm that, given a message and a private key, produces a signature.
- A *signature verifying* algorithm that, given the message, public key and signature, either accepts or rejects the message's claim to authenticity.

Two main properties are required. First, the authenticity of a signature generated from a ixed message and ixed private key can be veri ied by using the corresponding public key. Secondly, it should be computationally infeasible to generate a valid signature for a party without knowing that party's private key. A digital signature is an authentication mechanism that enables the creator of the message to attach a code that acts as a signature.

It is used for identi ication and authentication of entities as the source of the electronic message and indicates who (entity or person) are approved to use the information contained in message packets. It provides

A. Authentication of the signer’s identity and

B. Authentication of the contents of the signed message.

RSA algorithm [93]: It is one of the irst practical public-key cryptosystems and is widely used for secure data transmission. It deals with a digital signature with message recovery scheme. It does not require any other information besides the signature itself in the veri ication process.

Key generation in the RSA digital signature scheme is the same as a key generation in the RSA. RSA involves a public key and a private key. The public key can be known by everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key.

5.4 PROBLEM DEFINITION:

The proposed method is designed to overcome three weaknesses of Watchdog scheme namely:

A. Receiver collision,

B. Limited transmission power and

C. False identity problem.

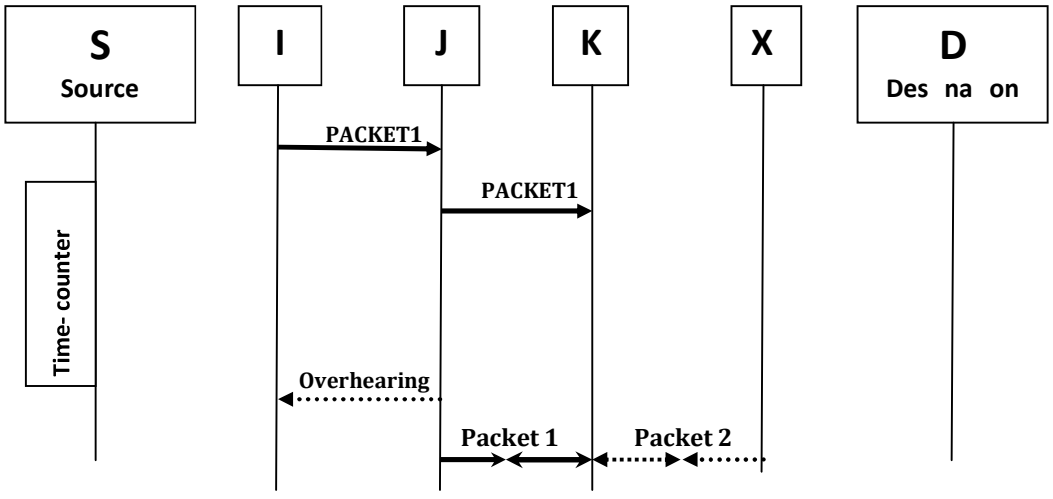

Figure 5.4: Receiver collisions

In the case of receiver collisions (igure 5.4), after I sends Packet 1 to J, it tries to overhear if J forwarded this packet to K; meanwhile, X is forwarding Packet 2 to K. In such case, I overhears that J has successfully forwarded Packet 1 to K but failed to detect that K did not receive this packet due to a collision between Packet 1 and Packet 2 at K.

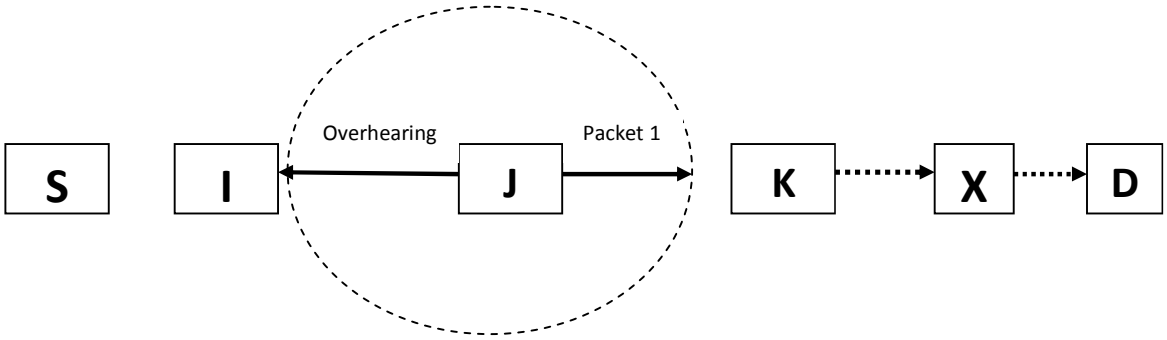

Figure 5.5: Limited transmission power

In the case of limited transmission power (igure 5.5), in order to preserve its own battery power, J intentionally limits its transmission power so that it is strong enough to be overheard by I but not strong enough to be received by K.

In the case of false misbehavior acknowledge (igure 5.6), although I successfully overheard that J forwarded Packet 1 to K, node I still reports J as misbehaving. Due to the open medium and remote distribution of MANETs, attackers can easily capture and compromise nodes to achieve this false misbehavior report attack.

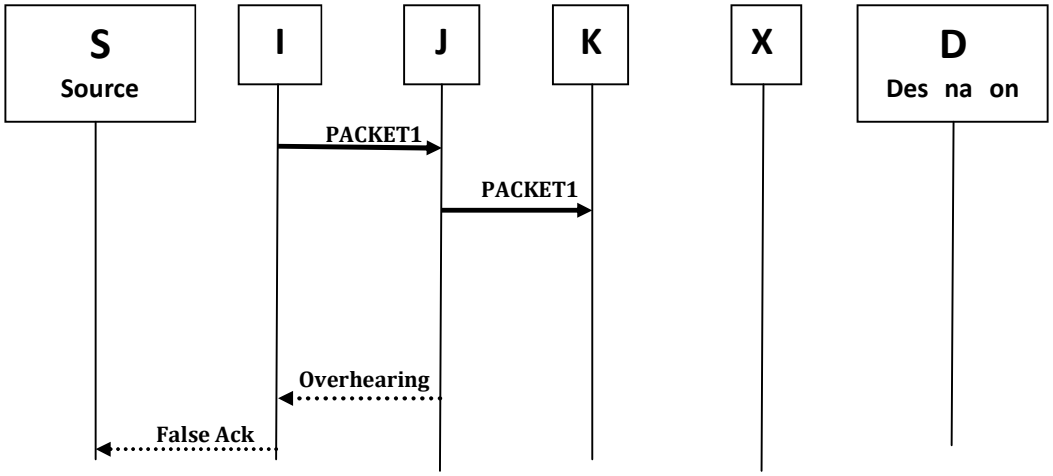

Figure 5.6: False Misbehavior acknowledge

5.5 PROPOSED METHOD: DSSAM

DSSAM stands for Digitally Signed Secure Acknowledgement Method. We use digital signature technique to prevent the attacker for falsifying packets. DSSAM consists of three major parts namely,

a. Secure ACK,

b. Node authentication and

c. Packet authentication.

We ensure security at two layers. In the irst tier, extra reserved bits are used to maintain sequence number, keeping transmission time ixed to de ine packets sequence in the proper interval for that particular time. This is done for both packet and acknowledgement transmission. Next layer is set by double safeguarding the forwarded packets, by putting digital signature. According to the draft of DSR [94, 95], 8 bits are reserved in the DSR header. We are using these bits to maintain sequence number. We assume bi-directional communication links with source and destination not being malicious. All data packets and acknowledgement packets are required to be digitally signed by source. They are also validated by destination. We use RSA in our proposed method to encrypt the packet.

5.5.1 PERFORMANCE EVALUATION:

Simulation Approach

CASE 1: In this case, we simulated a basic packet-dropping & delay attack [96]. Malicious nodes simply drop all the packets that they receive. The purpose of this scenario is to test the performance of intrusion detection systems against two weaknesses of watchdog, namely, receiver collision and limited transmission power, when transmission power is speci ied with ixed range.

CASE 2: This case is designed to test Intrusion detection systems performances against false acknowledgement. In this case, malicious nodes always drop the packets that they receive and send back a false acknowledge whenever it is possible.

Simulation Setup

We have done simulation in Qualnet Simulator on a desktop with i3 CPU and 3-GB RAM. Both the physical layer and the 802.11b MAC layer are taken in consideration. For each scheme, we run every network scenario 5 times and calculated the average. The parameters for simulation are given below in table 5.3.

Parameters	
Packet Size	512 Bytes
Packet Rate	4 packets/sec
Data traf ic	CBR
Dimensions	1000m x 1000m
No. of nodes	50
Min. speed	1m/s
Max. speed	10m/s
Max. hops	5
Radio transmission range	200m
Simulation time	1500s
Antenna Model	Omni-direction
Propagation model	Two ray
Mobility Model	Random Waypoint

Table 5.3: Parameters for simulation

We have observed the performance of DSSAM and compared with watchdog and TwoAck. For this we have considered packet delivery fraction (PDF) and routing overhead, as the performance metrics.

1) Packet delivery fraction (PDF): It is the ratio of the number of packets originated by the application layer sources and the number of packets received by the destinations. It describes the loss rate that will be seen by the transport protocol.

Packet delivery fraction = (data packets received)/ (data packets sent)

2) Routing overhead (RO): It refers to network routing information sent by an application, which uses a portion of the available bandwidth. This extra data is referred to as overhead.

During the simulation, the source route broadcasts an RREQ message to all the neighbors within its communication range. Upon receiving this RREQ message, each neighbor appends their addresses to the message and broadcasts this new message to their neighbors. If any node receives the same RREQ message more than once, it ignores it. If a failed node is detected, which generally indicates a broken link in lat routing protocols like DSR, a RERR message is sent to the source node. When the RREQ message arrives to its inal destination node, the destination node initiates an RREP message and sends this message back to the source node by reversing the route in the RREQ message.

Concerning the digital signature scheme, we have taken an open source library named Botan [97]. For RSA schemes, we have taken a 512-b RSA key for every node in the network. We assumed that a public key and a private key are generated for each node and they were all distributed in advance. The sizes of public-key and private-key iles for 512-b RSA are 256 and 512 B, respectively. The signature ile size for RSA is 120 B.

5.5.2 Results and discussion:

Case 1: Here, malicious nodes drop all the packets. Figure 5.7 table 5.4 shows the simulation results that are based on packet delivery fraction. Our proposed method DSSAM outperforms Watchdog's performance by average of 20% when there are 20% of malicious nodes in the network.

From the results, we observe that acknowledgment-based schemes, including TWOACK and DSSAM, are able to detect misbehaviors with the presence of receiver collision and

limited transmission power. However, when the number of malicious nodes reaches above 40%, our proposed scheme DSSAM's performance is better than others.

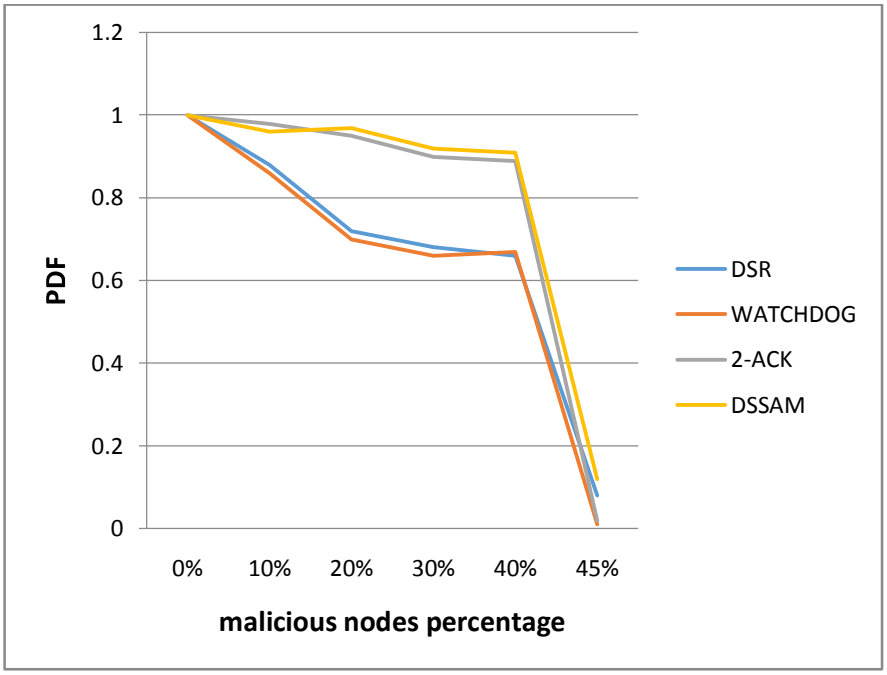

Figure 5.7: Case 1-Packet delivery fraction

CASE 1-PDF	DSR	WATCHDOG	2-ACK	DSSAM
0%	1	1	1	1
10%	0.88	0.86	0.98	0.96
20%	0.72	0.70	0.95	0.97
30%	0.68	0.66	0.90	0.92
40%	0.66	0.67	0.89	0.02
45%	0.04	0.011	0.02	0.18

Table 5.4: Case 1-Packet delivery fraction

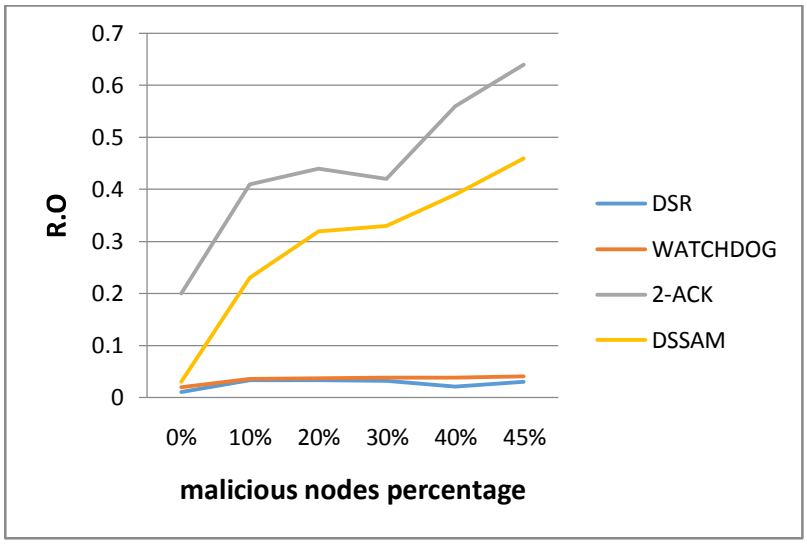

Figure 5.8: Case 1-Routing overhead

CASE 1-R.O	DSR	WATCHDOG	2-ACK	DSSAM
0%	0.01	0.02	0.2	0.03
10%	0.033	0.035	0.41	0.23
20%	0.033	0.037	0.44	0.32
30%	0.032	0.038	0.42	0.33
40%	0.02	0.038	0.56	0.39
45%	0.03	0.04	0.64	0.46

Table 5.5: Case 1-Routing overhead

The obtained routing overhead in case 1 is shown in igure 5.8, table 5.5. We observe that dynamic source routing and watchdog scheme attains better result, because they don't require acknowledgment method to detect mischief-nodes. TWOACK and DSSAM have effective overhead. Even though DSSAM requires digital signature in all packet and acknowledgement packets are also considered, hence overhead is increased. But DSSAM still performs well compared to other techniques. This is because of the hybrid scheme used here.

Case 2: Here, we seeded malicious nodes which send fake acknowledgement to the source node. This case is designed to check the intrusion detection systems

performance under fake acknowledgement. Figure 5.9 and table 5.6 shows the results for packet delivery fraction. When the percentage seeding of malicious nodes is 10%, the performance of DSSAM is about 3% better than TWOACK. When the malicious nodes are at 20% and 30%, DSSAM outperforms all other schemes.

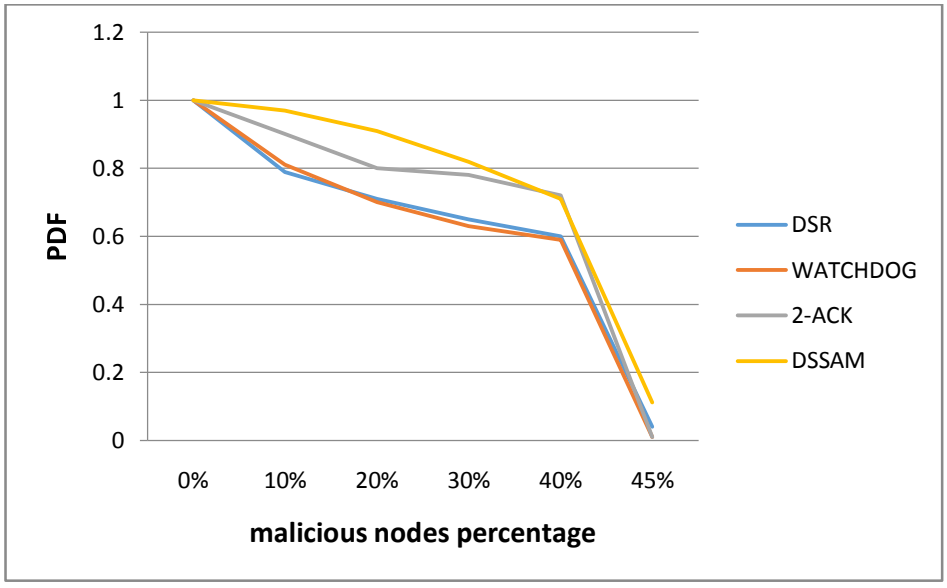

Figure 5.9: Case 2-Packet delivery fraction

CASE 2-PDF	DSR	WATCHDOG	2-ACK	DSSAM
0%	1	1	1	1
10%	0.79	0.81	0.90	0.97
20%	0.71	0.69	0.80	0.91
30%	0.65	0.63	0.78	0.82
40%	0.60	0.59	0.72	0.71
45%	0.04	0.01	0.01	0.11

Table 5.6: Case 2- Packet delivery fraction

The simulation results of Routing Overhead in case 2 are shown in igure 5.10 and table 5.7. DSSAM maintains a lower network overhead compared to TWOACK and watchdog schemes in most cases. However, routing overhead rises rapidly with the increase in

malicious nodes. The reason being more malicious nodes require more acknowledgment packets and digital signatures. The routing overhead for DSSAM is more compared to other techniques, this is due to the hybrid nature and extra processing for digital signature but it is compensated by high packet delivery fraction better achieved security level in the packet communication.

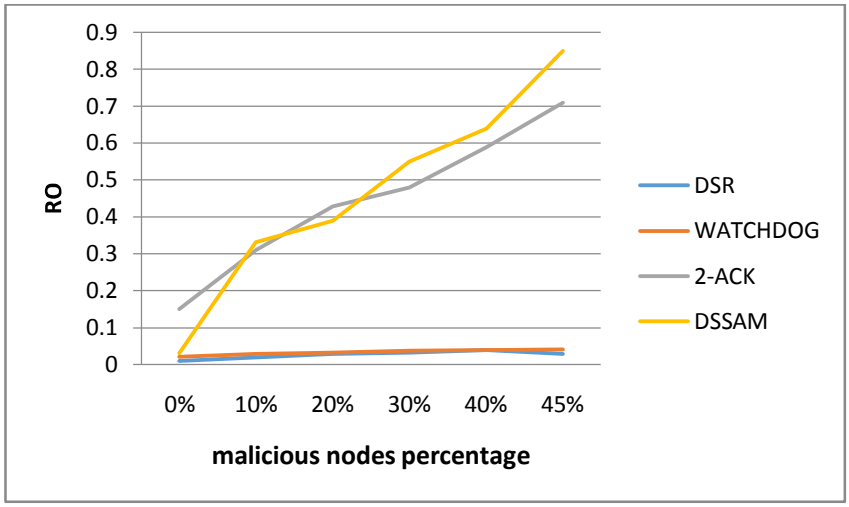

Figure 5.10: Case 2-Routing overhead

CASE 2-R.O	DSR	WATCHDOG	2-ACK	DSSAM
0%	0.01	0.02	0.15	0.03
10%	0.020	0.029	0.31	0.33
20%	0.029	0.032	0.43	0.39
30%	0.0321	0.037	0.48	0.55
40%	0.039	0.037	0.59	0.64
45%	0.03	0.04	0.71	0.85

Table 5.7: Case 2-Routing overhead

5.6 Conclusion

There are many possible reasons for packet drop in MANETs, which falls broadly under two types namely, intentional and unintentional misbehavior. The unintentional misbehavior could be caused by:

- Overloaded node (due to lack of CPU cycles or limited buffer space)
- Network congestion
- Collision.

Packet drop may occur due to link errors because of interference or fading. Packet-dropping attack has always been a signi icant threat to the security in MANETs. Here we have described and simulated the method DSSAM in a standard environment and compared it with existing methods under different scenarios.

The obtained simulation outcome provides enhanced performance against watchdog and TwoAck in the cases of receiver collision, limited transmission power, and false misbehavior acknowledgement. We incorporated digital signature in the method. Even though it generates more routing overhead in few cases but there was a performance improvement in packet delivery fraction. We used RSA algorithm for digital signature.

In future work, we will try to understand and estimate the performance when partially misbehaving nodes intentionally degrade performance owing to their greediness for saving their battery power. We will try to determine the battery consumption with varying percentage of greedy nodes in the same environment. There is not much work done in this area. Therefore, it is an interesting topic for future research.
