SECURITY ENHANCEMENT IN AODV PROTOCOL USING IDS AND HYBRID CRYPTOGRAPHY

Dissertation submitted to the Central University of Punjab

For the award of

Master of Technology

In

Computer Science and Technology

BY

Khushmeet Singh

Supervisor

Er Amanpreet Kaur

Centre for Computer Science and Technology

School of Engineering and Technology

Central University of Punjab, Bathinda

June 2014

DECLARATION

I declare that the dissertation entitled “SECURITY ENHANCEMENT IN AODV PROTOCOL USING IDS AND HYBRID CRYPTOGRAPHY” has been prepared by me under the guidance of Er. Amanpreet Kaur, Assistant Professor, Centre for Computer Science and Technology, School of Engineering and Technology, Central University of Punjab. No part of this dissertation has formed the basis for the award of any degree or fellowship previously.

Khushmeet Singh
Centre for Computer Science and Technology
School of Engineering and Technology
Central University of Punjab,
Bathinda - 151001.

Date:

CERTIFICATE

I certify that Khushmeet Singh has prepared this dissertation entitled "SECURITY ENHANCEMENT IN AODV PROTOCOL USING IDS AND HYBRID CRYPTOGRAPHY", for the award of M.Tech degree of the Central University of Punjab, under my guidance. He has carried out this work at the Centre for Computer Science and Technology, School of Engineering and Technology, Central University of Punjab.

Er Amanpreet Kaur
Assistant Professor
Centre for Computer Science and Technology
School of Engineering and Technology
Central University of Punjab,
Bathinda - 151001.

Date:

ABSTRACT

SECURITY ENHANCEMENT IN AODV PROTOCOL USING IDS AND HYBRID CRYPTOGRAPHY

Name of student:	Khushmeet Singh
Registration Number:	CUPB/MTECH/SET/CST/2012-13/03
Degree for which submitted:	Master of Technology
Name of Supervisor:	Er Amanpreet Kaur
Centre:	Computer Science and Technology
School of Studies:	School of Engineering and Technology

Key words:	MANET, IDS, AODV, NS, CBR, UDP

A mobile Ad hoc network (MANET) is a wireless decentralized self-configuring network in which nodes communicate with each other either directly or through intermediate nodes. These unique features (self-configuring, infrastructure-less, decentralized) make MANET suitable for use in emergency situations, military operations, education, entertainment, sensor networks etc. Besides the various advantages, the open medium, rapidly changing topology and lack of centralized monitoring make MANETs vulnerable to various attacks. This dissertation work focuses on network layer attacks. Network layer attacks in MANET are categorized into two basic types namely active and passive. In active attack, an attacker disrupts the regular operation of the network, change the data or harm the system. In passive attack, the attacker does not disturb the operation of network but attempts to seek some valuable information. So, it is vital to develop some security mechanism to protect MANETs from attacks. This dissertation work focuses on providing solution to prevent MANETs from two active attacks namely Blackhole and Malicious Packet Dropping and one passive attack namely Eavesdroping attack.

The existing AODV Protocol is modified to prevent these attacks. Solution is proposed and simulated to prevent Blackhole and Eavesdropping attack. Malicious packet dropping attack is prevented by using Watchdog Intrusion Detection System (IDS). Performance of AODV and Modified AODV protocol is analysed with respect to Packet Delivery Ratio, Average End-to-End Delay and Routing Overhead. To prevent Eavesdropping attack, a hybrid cryptography technique has been developed which combines best features of both symmetric key cryptography and asymmetric key cryptography i.e. speed and security. Simulation has been done in Network Simulator version 2.35.

Khushmeet Singh Er Amanpreet Kaur

DEDICATED TO GOD,
MY LOVING PARENTS AND MY FRIENDS

ACKNOWLEDGEMENTS

It is indeed a privilege as well as pleasant duty to express my gratitude to all those who have made it possible for me to complete this dissertation report.

I bow down to Almighty who showered his blessings to encourage me at every moment.

It is my proud privilege to acknowledge with respectful gratitude the invaluable guidance extended to me by my esteemed guide Er. Amanpreet Kaur, Assistant Professor, Centre for Computer Science & Technology, CUP, Bathinda. Her sincerity, thoroughness and perseverance has been a constant source of inspiration for me. It is only her cognizant efforts that my endeavors have seen light of the day.

I also take the opportunity to acknowledge the contribution of Prof. Dr. A.K.Jain, COC, Centre for Computer Science & Technology, Cup, Bathinda for providing a great academic environment.

I also do not like to miss the opportunity to acknowledge the contribution of all faculty members of the Centre for their kind assistance and cooperation during the dissertation work. Last but not the least, I am thankful to all my friends Mandeep Singh, Shifali Hans for their contribution in the successful completion of this dissertation report.

Khushmeet Singh

TABLE OF CONTENTS

LIST OF TABLES

LISTS OF FIGURES

LIST OF ABBREVIATIONS

Sr. No	Full Form	Abbreviation
1	Ad hoc On-Demand Distance Vector	AODV
2	Average End-to-End Delay	AED
3	Adaptive Acknowledgment	AACK
4	Constant Bit Rate	CBR
5	Current Hop Count	CHC
6	Digital Signature Algorithm	DSA
7	Destination Sequence Number	DSN
8	Enhanced Adaptive Acknowledgment	EAACK
9	File Transfer Protocol	FTP
10	Intrusion Detection System	IDS
11	Local Area Network	LAN
12	Mobile Adhoc Networks	MANET
13	Personal Digital Assistant	PDA
14	Packet Delivery Ratio	PDR
15	Principle of Flow Conservation	PFC
16	Routing Overhead	RO
17	Route Request	RREQ
18	Route Reply	RREP
19	Route Error	RERR
20	Ron Rivest, Adi Shamir, and Leonard Adleman	RSA
21	Secure Acknowledgement	S-ACK
22	Stored Hop Count	SHC
23	Source Sequence Number	SSN
24	Tool Command Language	TCL
25	Two Acknowledgements	TWO ACK
26	User Datagram Protocol	UDP

CHAPTER 1

INTRODUCTION

1.1 Introduction

Today wireless networks are at its zenith. Every user wants wireless connectivity to communicate and transfer data with each other irrespective of their geographic position. Two main characteristics of wireless networks that propelled their widespread usage are mobility and ease of deployment. Laying cables in wired network is very time consuming and maintenance is also very high. Wireless communication today surrounds us in many colors and flavors, each with its unique frequency band, coverage, and range of applications. Among all the wireless networks, MANET is of its unique importance.

A mobile Ad hoc network (MANET) is a wireless decentralized self-configuring network in which nodes communicate with each other either directly or through intermediate nodes. Each node transmits and receives data through bidirectional links. All nodes are mobile and configure themselves in network without help of any infrastructure. Due to mobility, network topology changes over time because nodes join or leave the network at any time. These unique features (self-configuring, infrastructure-less, decentralized) make MANET suited for use in Emergency situations such as military operations, education, entertainment, sensor networks etc. Nodes may consist of broad range of devices like laptops, PCs, PDAs, smart phones as shown in figure 1.1.

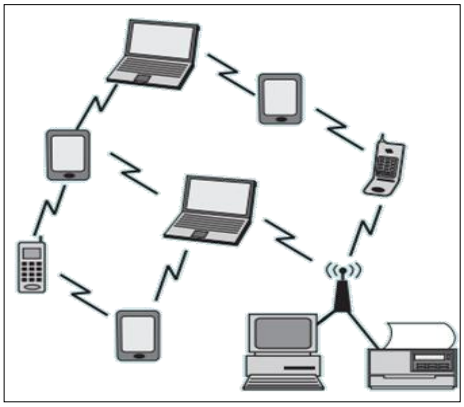

Figure 1.1 Mobile Adhoc Network (Kumar & Mishra, 2012)

Besides various advantages, the open medium, rapidly changing topology and lack of centralized monitoring make MANET vulnerable to various attacks that will be presented in later sections. In this case, it is vital to develop some security mechanism to protect MANET from attack. Security goals of MANET are same as compared to others networks i.e. Confidentiality, Integrity, Availability and Authenticity.

1.2 Security Goals in MANET

Main goal of security services is to protect the information and the resources from attacks and misbehavior. Various security goals in MANET are as follows (Djenouri, Khelladi & Badache, 2005):

- **Availability:** It ensures that inspite of attack network services are always available whenever they are requested.
- **Authenticity:** It ensures that communication between nodes is legitimate. A malicious node should not pretend to be a trusted node. Digital signature scheme provides message authentication.
- **Data Confidentiality:** It is main security goal of ad hoc networks. It ensures that message exchange between two nodes cannot be understood by anyone else. Data confidentiality may be achieved by applying various encryption techniques.
- **Integrity:** It ensures that a message sent from sender node to receiver node was not modified by any malicious node during transmission. Digital signature provides message integrity.
- **Non-Repudiation:** It ensures that the origin of the message is genuine. It guarantees that the sender of a message cannot deny that it has not sent the message. It also guarantees that the recipient cannot deny that it has not received the message. Digital signature schemes may be used to ensure non repudiation.

1.3 Characteristics affecting MANET Security

Various features of MANET which made it suitable for many real applications also make it more vulnerable to various types of attacks. These features are as follows (Djenouuri et al., 2005):

- **Infrastructureless:** No central access point is there. Nodes within range communicate directly with each other and nodes which are not in range communicate through intermediate nodes. Intermediate nodes may act as malicious nodes.
- **Wireless Links Use**: The use of wireless links make ad hoc network susceptible to attacks. Unlike wired networks where an intruder must gain physical access to the network wires or pass through several lines of defense at firewalls and gateways, attacks on a wireless ad-hoc network are easy to perform and any node may be targeted.
- **Multi-hop:** Because of no central routers and gateways, hosts themselves act as routers. Packets follow multi-hop routes before arriving to the destination. Because of the possibility of untrustworthiness of some nodes, this feature creates a serious vulnerability.
- **Node Movement:** Due to mobility of nodes any node can leave or join the network at any time. This means that tracking down a particular mobile node in a large scale ad hoc network cannot be done easily.
- **Power Limitation:** Due to small size of mobile nodes they are often supplied with small batteries, limited power resources, to ensure portability. This limitation causes vulnerability since a node powering-off can cause its breakdown. Attackers may targets some nodes batteries to disconnect them or to make network partition. This is called energy starvation attack or sleep deprivation attack.
- **Memory and Computation Power Limitation:** Ad hoc enabled mobile nodes are limited storage devices with weak computational capabilities. High complexity security solutions employed like cryptography should take these constraints into consideration.

1.4 Attacks in MANET

There are two basic types of network layer attacks in MANET i.e. passive and active attacks which are further classified into many types as shown in figure 1.2 (Schutte , 2006), (Nadeem & Howarth , 2013).

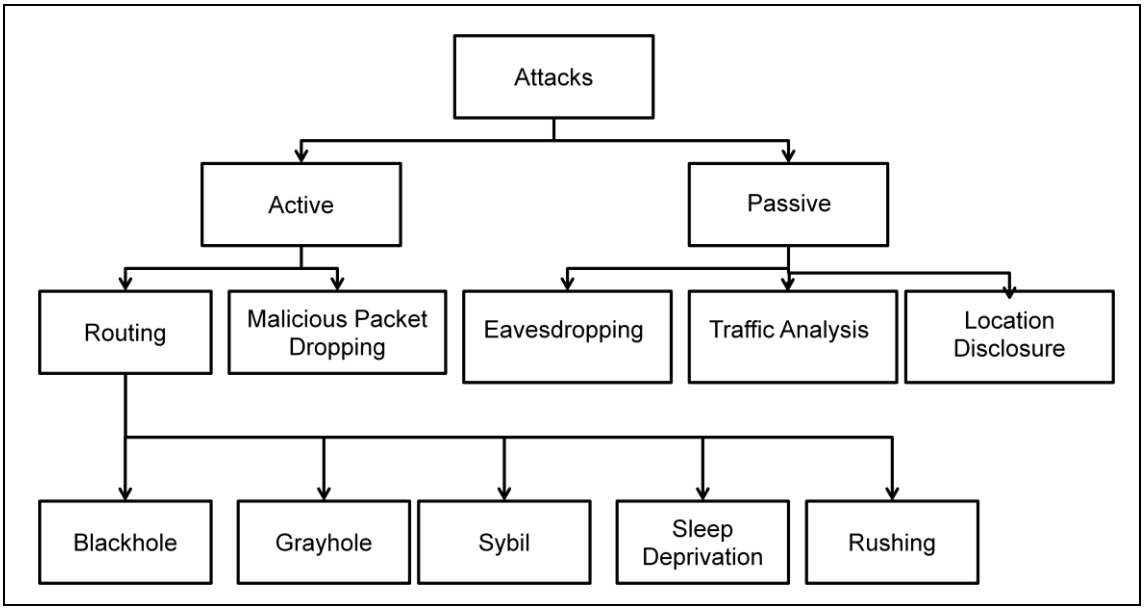

Figure 1.2: Attacks in Manet

1.4.1 Passive Attacks

In this attack, the attacker does not disturb the operation of the routing protocol but attempts to seek some valuable information through traffic analysis. Passive attacks are very difficult to identify because the network operation is regular. Attacker‘s goal is just to obtain information not to modify or harm the system. Encryption of data being transmitted may act as mechanism to prevent passive attack. Some examples of passive attacks are as follows:

- **Eavesdropping:** Message send by a node may travel through various intermediate nodes and if no encryption is used then the attacker can get useful information. The sender and receiver usually have no means of knowing that this attack has taken place. This attack is prevented by using encryption techniques. Basically there are two types of encryption techniques i) Symmetric encryption ii) Asymmetric Encryption. Symmetric encryption is very fast as compared to asymmetric encryption but at the same time, is less

secure than asymmetric. Difference between symmetric and asymmetric encryption is discussed in section 1.6.2.3 (table 5). The third type of encryption called Hybrid encryption. It incorporates a combination of asymmetric and symmetric encryption to benefit from the strengths of each form of encryption. These strengths are respectively defined as speed and security.

- **Traffic Analysis and Location Disclosure:** Attackers can listen to the traffic on wireless links to discover the location of target nodes by analyzing the communication pattern, the amount of data transmitted by nodes and the characteristics of the transmission. For example, in a battlefield scenario, a large amount of network traffic normally flows to and from the headquarters. Traffic pattern analysis therefore allows an intruder to discover the commanding nodes in the network.

1.4.2 Active attacks

An active attack may change the data or harm the system. In this type of operation, an attacker actively participates and disrupts the regular operation of the network services.

These attacks are normally easier to detect then to prevent because an attacker can launch them in variety of ways. Some examples of active attacks are as follows:

1.4.2.1 Routing Attacks

Routing protocols for MANETs are generally based on the assumption that all participating nodes are fully cooperative. However, due to the open structure and scarcely available battery-based energy, node misbehaviors may exist. Routing misbehavior can severely degrade the performance of MANET. Various routing attacks are as follows:

- **BlackHole Attack**: A black hole attack means that a malicious node utilizes the routing protocol to claim itself of being the shortest path to the destination node. When path is selected by the routing protocol, it starts dropping the routing packets and does not forward packets to its neighbors (Tseng,Chou & Chao, 2011).The way the intruder node initiates the Blackhole attack may vary in different routing protocols. In case of AODV Protocol, the destination

sequence number (DSN) and hop count is used to perform this attack. Destination sequence number is used to represent the freshness of the route. A high value of destination sequence number means a fresher route. To convince the target nodes, the attackers may reduce the hop count data or increase the destination sequence number .In addition, the attackers can also combine both techniques to increase severity of attacks. The severity of the attack depends on the number of routes in the network the intruder successfully becomes part of.

As shown in the figure 1.3, an attacker node M, listens to communication channel of node S. Node M sends a forged RREP to node S immediately after node S broadcasts RREQ. Using the forged RREP, node M claims that it has both valid routing path and shortest distance to the destination node D. Because node S has no knowledge about node D in previous, node S will consider the message from the attacker as legitimate route message. Complete mechanism of this process is shown in table 1 to table 4. Route Request (RREQ) and Route Reply (RREP) messages exchange in route discovery process are shown in table 1 and table 2. Node S will update its routing table as indicated in table 3. Due to this attack, node S also rejects the legitimate RREP from node B (Mandela , Abdullah , Ismail, Haron , Nagadi & Coulibaly,2013).

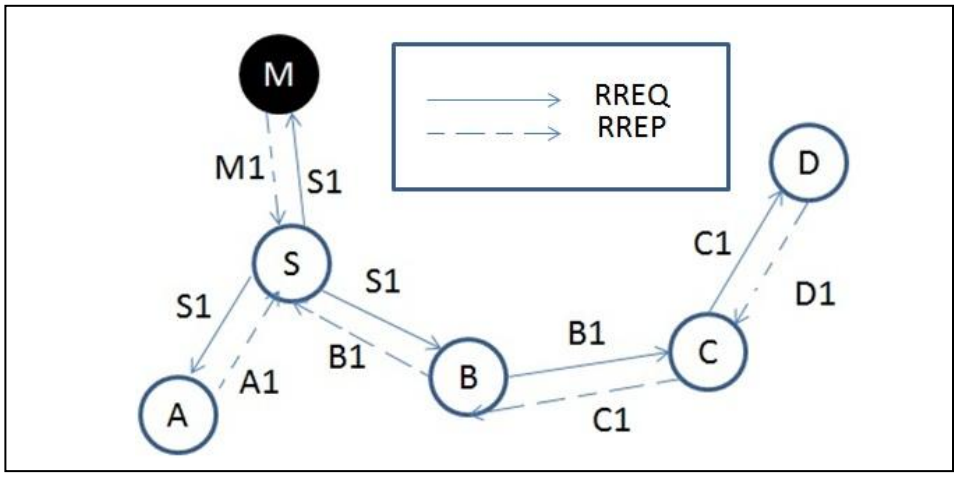

Figure 1.3 BlackHole Attack

Table 1 Route request messages

LastHop	**S**	**S**	**S**	**A**	**B**	**C**
Next Hop	M	A	B	S	C	D
RREQ	s1	s1	s1	--	B1	C1
HopCount	0	0	0	1	1	2
DSN	1	1	1	1	1	1
Origin	S	S	S	S	S	S
Dest	D	D	D	D	D	D

Table 2 Route reply messages

LastHop	**M**	**D**	**C**	**B**
Next Hop	S	C	B	S
RREP	M1	D1	C1	B1
HopCount	1	0	1	2
DSN	1	1	1	1
Origin	S	S	S	S
Dest	D	D	D	D

Table 3 Routing table under Blackhole attack

S ROUTING TABLE UNDER ATTACK			
Destination	**NextHop**	**DSN**	**HopCount**
S	0	0	0
D	M	1	2

Table 4: Routing table without Blackhole attack

S ROUTING TABLE WITHOUT ATTACK			
Destination	**NextHop**	**DSN**	**HopCount**
S	0	0	0
D	B	1	3

- **Grayhole Attack**: It is special case of black hole attack in which malicious node selectively drops the packets. Some nodes change their states from black hole to honest occasionally and vice versa. It is difficult to detect gray hole attack because nodes can drop packet due to congestion as well as malicious nature. Blackhole and Grayhole attacks comprise two tasks: the attacker first captures routes and then either drops all packets (Blackhole attack) or some packets (Grayhole attack).

- **Rushing Attack:** To limit the route discovery overhead, each node in network forwards only one RREQ originated from any route discovery. It is generally the one that arrives first. An attacker can exploit this property. It starts spreading RREQ packets rapidly all over the network to suppress any later genuine RREQ packets. As a result, the initiator will be unable to discover any usable routes (i.e. routes that do not include the attacker).
- **Sybil Attack:** Each node requires a unique address to participate in routing process. Nodes are identified by this unique address. But in MANET there is no central authority to verify these identities. In Sybil attack, a malicious node may generate fake identities of number of additional nodes. A Sybil node may fabricate a new identity for itself or it steals an identity of the legitimate node. It creates confusion in the network.
- **Sleep Deprivation Attack:** In this attack, a malicious node can attempt to consume battery life by requesting excessive route discovery, or by forwarding unnecessary packets to the victim. It is a type of DDOS attack in which a malicious node interacts with the genuine node in a manner that appears to be legitimate. But the purpose of the interaction is to keep the victim node out of its power conserving sleep mode.

1.4.2.2 Malicious Packet Dropping

Once the path is established between source and destination nodes, the source node starts sending the data packets to next nodes in the path and so on. All routing protocols in MANETs are generally based on the assumption that all the participating nodes are fully cooperative. But some nodes may participate in the route discovery and maintenance processes but refuse to forward data packets. Such nodes are called as selfish or misbehaving nodes. This is also known as a data packet dropping attack. Packet dropping attacks differ from black hole and grey hole attacks because there is no attempt to “capture” the routes in the network.

1.5 Intrusion Detection in MANET

MANETs are vulnerable to various types of attacks. Intruders can compromise the operation of the network by attacking at any of the physical, MAC or network layers. The network layer, especially the routing protocols, is vulnerable because of the use of cooperative routing algorithms, the limited computational ability of nodes, the exhaustible node batteries, a lack of clearly defined physical network boundary and the transient nature of services in the network. Standard information security measures such as encryption and authentication do not provide complete protection and therefore, intrusion detection and prevention (IDP) mechanisms are widely used to secure MANETs (Nadeem & Howarth, 2013).

An Intrusion Detection System (IDS) is a defense system that detects unusual activities in a network that compromise system security and then tries to prevent such activities. IDSs achieve detection by continuously monitoring the network for unusual activity. The prevention part may involve issuing alerts as well as taking direct preventive measures such as blocking a suspected connection. So intrusion detection is a process of identifying and responding to malicious activity targeted at computing and networking resources (Misra et al.,2004).

1.5.1 Intrusion Detection Schemes

Intrusion Detection Systems can be classified into three main categories:

(1) Anomaly-Based Intrusion Detection (ABID)

(2) Misuse Detection, also known as Knowledge-Based Intrusion Detection (KBID)

(3) Specification-Based Intrusion Detection (SBID)

1.5.1.1 Anomaly-Based Intrusion Detection (ABID)

Anomaly-based intrusion detection detects any action that significantly deviates from the normal behavior. Any activity that deviates from normal behavior is considered as malicious. The normal profiles of users are kept in the system. The system compares the captured data with these profiles, and then treats any activity that deviates from the baseline as a possible intrusion by informing system administrators or initializing a proper response (Xiao et al., 2006). Profiles can be developed for many behavioral attributes, such as the number of e-mails sent by

a user, the number of failed login attempts for a host, and the level of processor usage for a host in a given period of time. Figure 1.4 shows the basic ABID Process. It consists of two parts: training and testing. Training is the process of modeling the normal or expected behaviour of the network or of the users. The model also acts as a profile of user or network behavior. For any anomaly-based IDS to be effective, it must have a consistent and stable profile that characterizes this behaviour. A profile consists of information about the list of parameters which are specifically geared to the target being monitored. Constructing an effective profile involves gathering information on behaviour and activity that is considered acceptable for the network (Nadeem & Howarth , 2013).

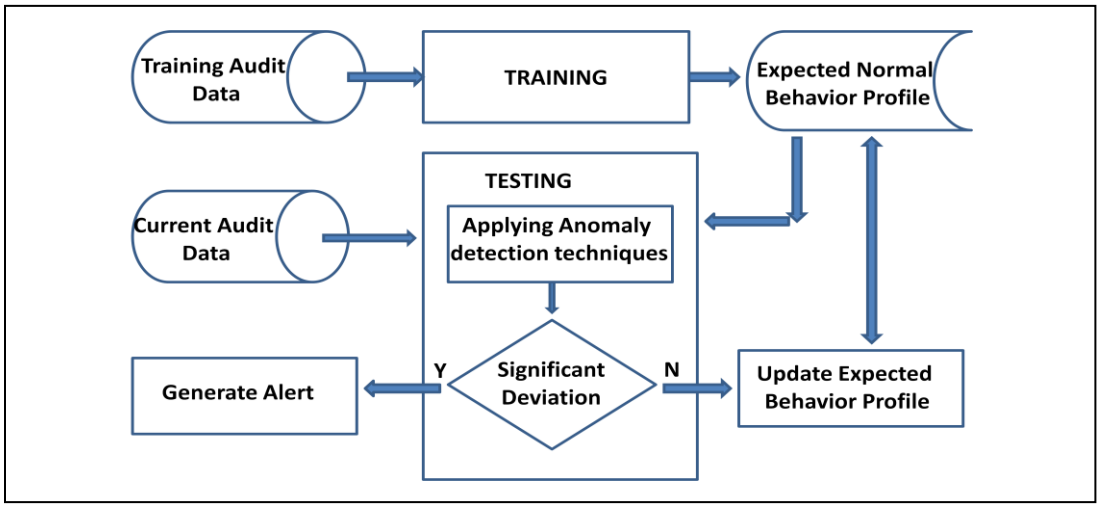

Figure 1.4: Anomaly-Based Intrusion Detection (Nadeem & Howarth, 2013)

1.5.1.2 Knowledge-Based Intrusion Detection (KBID)

This is very effective technique for detecting known threats. Unknown threats are difficult to track. The system keeps patterns of known attacks and uses them to compare with the captured data. Any matched pattern is treated as an intrusion e.g a virus detection cannot detect new kinds of attacks. A KBID system triggers an alarm when such an attempt is detected. A diagram illustrating the basic KBID process is shown in figure 1.5. KBID relies on knowledge about attacks so anything not explicitly recognized as an attack based on existing knowledge is declared as non-intrusive or acceptable (Nadeem & Howarth ,2013).

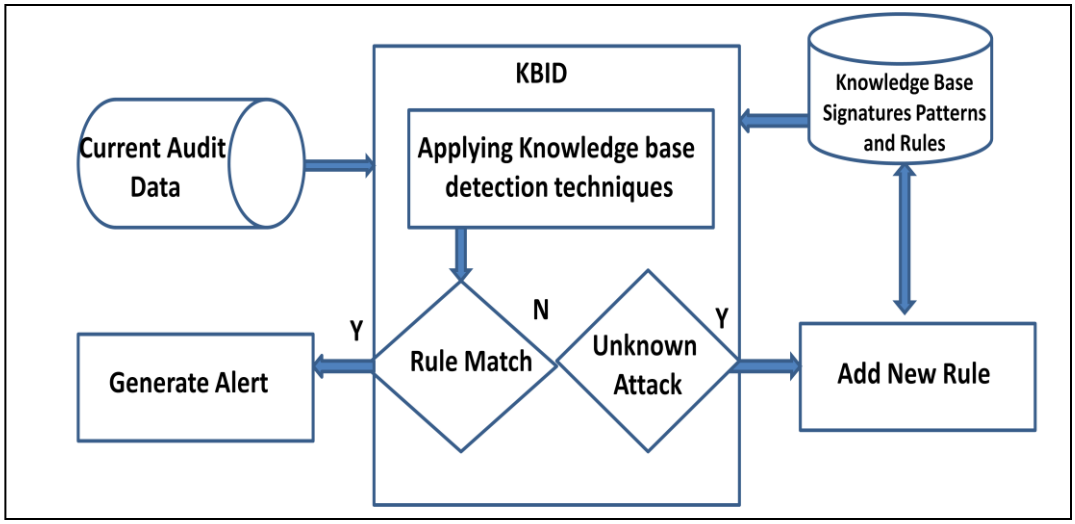

Figure 1.5: Knowledge-Based Intrusion Detection (Nadeem & Howarth, 2013)

1.5.1.3 Specification-Based Intrusion Detection (SBID)

The system defines a set of constraints that describe the correct operation of a program or protocol. Then it monitors the execution of the program with respect to the defined constraints. The basic process of SBID is shown in figure 1.6. The first step extracts the specifications, which define the correct operation of the network or the MAC layer protocol through a set of constraints. The system then monitors the execution of the protocol with respect to the given specification, deviations from the specification being treated as intrusion (Nadeem & Howarth, 2013).

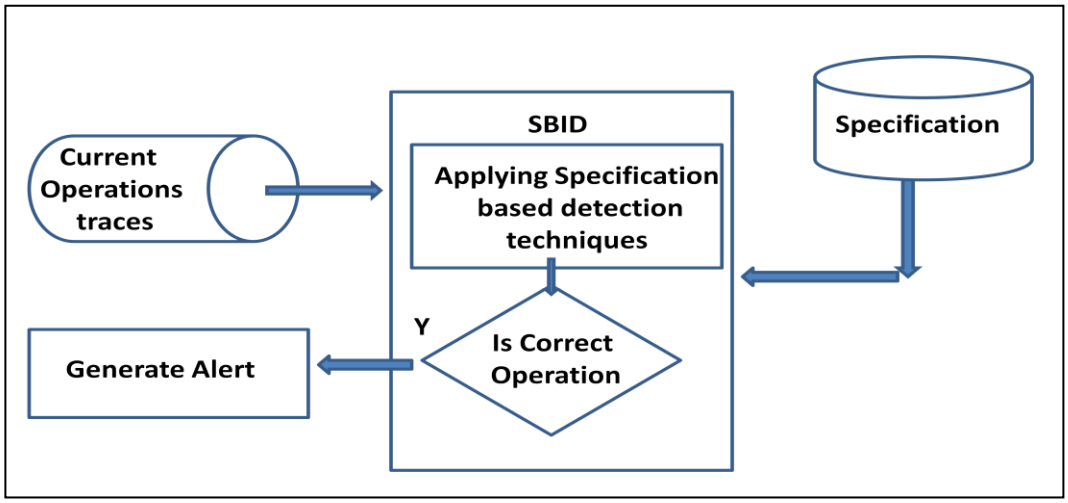

Figure 1.6: Specification-Based Intrusion Detection (Nadeem & Howarth, 2013)

1.6 Cryptography

Cryptography is the science of using mathematical functions to encrypt and decrypt data. Using cryptography we can store data or transmit it across insecure network in a form which cannot be understood by anyone else except the intended recipient. It is the art of secret writing.

1.6.1 Components of cryptography

- **Plain Text:** The original message written by sender, before being transformed, is called as plaintext.
- **Encryption Algorithm:** An Encryption algorithm transforms plaintext into ciphertext.
- **Cipertext:** This is the output of plaintext after encryption by encryption algorithm.
- **Key:** Key is any number(s) or character(s) that is used as an input to encryption or decryption algorithm. Key may be same or different for encryption and decryption process.
- **Decryption Algorithm:** Decryption algorithm transforms ciphertext into plaintext. It is basically reverse of decryption algorithm.

1.6.2 Cryptographic Algorithms

Cryptographic algorithms can be divided into two categories

1) Symmetric Key Cryptography
2) Asymmetric Key Cryptography

But one more new emerging cryptographic technique is there i.e **Hybrid Cryptography**. It is combination of best features of both Symmetric key cryptography and Asymmetric key cryptography.

1.6.2.1 Symmetric key Cryptography

In this type of cryptography same key is used for encryption and decryption process as shown in figure 1.7.

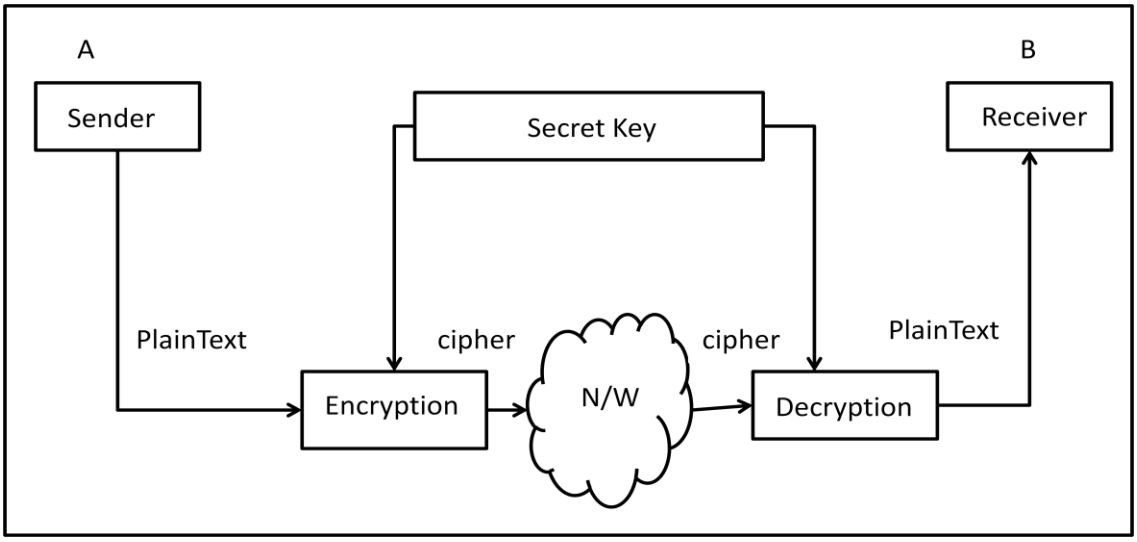

Figure 1.7: Mechanism of Symmetric Key Cryptography

Advantages:

- Easy to Implement.
- Takes Less time to Encrypt and Decrypt messages.
- Good for long messages.

Disadvantages:

- Key agreement is a big problem.
- Security is less. If anyone knows encryption key, he (she) can decrypt message easily.
- Number of keys increase with increase in number of participants.

Examples:

Below is the list of some symmetric key algorithms:

1) Substitution Ciphers
   - Caesar Cipher
2) Monoalphabetic Ciphers
3) Playfair Cipher
4) Polyalphabetic Ciphers
   - Vigenere Cipher
   - Autokey Cipher

5) Transposition cipher

- RailFence
- Columner

6) Data Encryption Standard (DES)

7) Advanced Encryption Standard (AES)

1.6.2.2 Asymmetric Key Cryptography

In asymmetric key cryptography or public key cryptography, different keys are used for encryption and decryption. There are two keys: a public key and a private key. The public key is announced to the public and private key is kept by the receiver. Sender encrypts the message using public key of receiver and receiver decrypt the message using its private key as shown in figure 1.8.

Advantages:

- More secure
- Key distribution is not a problem

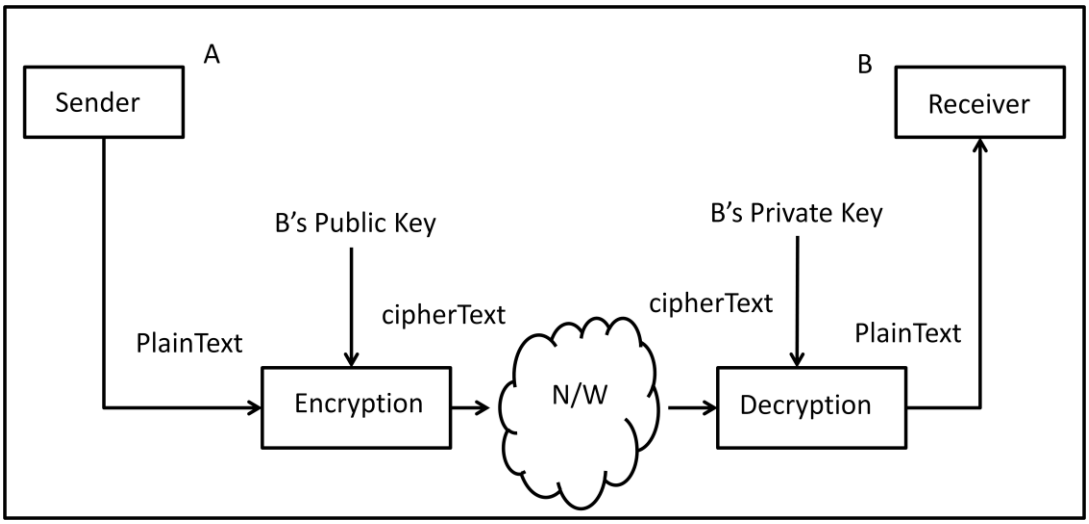

Figure 1.8: Mechanism of Asymmetric key Cryptography

Disadvantages:

- Algorithms are more complex.
- Use only for short messages.

Examples:

1) RSA
2) ElGamal
3) Diffie–Hellman key exchange protocol

1.6.2.3 Hybrid Cryptography

A hybrid encryption scheme uses public-key encryption to encrypt a random symmetric key. This symmetric key is used to encrypt the message. The receiver decrypts the symmetric key using the public-key encryption scheme and then uses the recovered symmetric key to decrypt the message.

Definition-A hybrid cryptosystem is one which combines the convenience of a public-key cryptosystem with the efficiency of a symmetric-key cryptosystem.

Hybrid cryptography is a type of cryptographic technique that merges two or more cryptographic techniques. It is a combination of asymmetric and symmetric key cryptography. It takes benefit from the strengths of each form of cryptography. These strengths are respectively defined as speed and security. Table 5 shows difference between symmetric and asymmetric key cryptography (Frozan & Mukhopadhyay, 2012)

Table 5 Symmetric vs Asmmetric Key Cryptography

Characteristics	Symmetric Key Cryptography	Asymmetric Key Cryptography
Key used for Encryption/Decryption	Same key used for both	One key used for encryption and another, different key is used for decryption.
Speed	Fast	Slow
Size of resulting encrypted text	Same or less	More than original plain text
Security	Less secure	More secure
Key agreement	Big problem	No Problem at all

No. of keys required as compared to the number of participants in the message exchange	Square of the number of participants	Same as number of participants

Hybrid cryptosystems remove drawbacks of both cryptosystems. Public-key encryption is used only to encrypt the key which is relatively a small amount of data. One party then sends the encrypted symmetric key to the other party who then decrypts the key. Both parties now have the same symmetric key. Secure and quick communication can be ensured using hybrid cryptography. Mechanism of Hybrid cryptography is shown in figure 1.9 (Kryptotel, 2010).Hybrid cryptography consists of best features of both worlds:

- The solution is more secure.
- Encryption and Decryption process doesn't take long time.
- The generated cipher text is compact in size
- Key distribution problem is solved

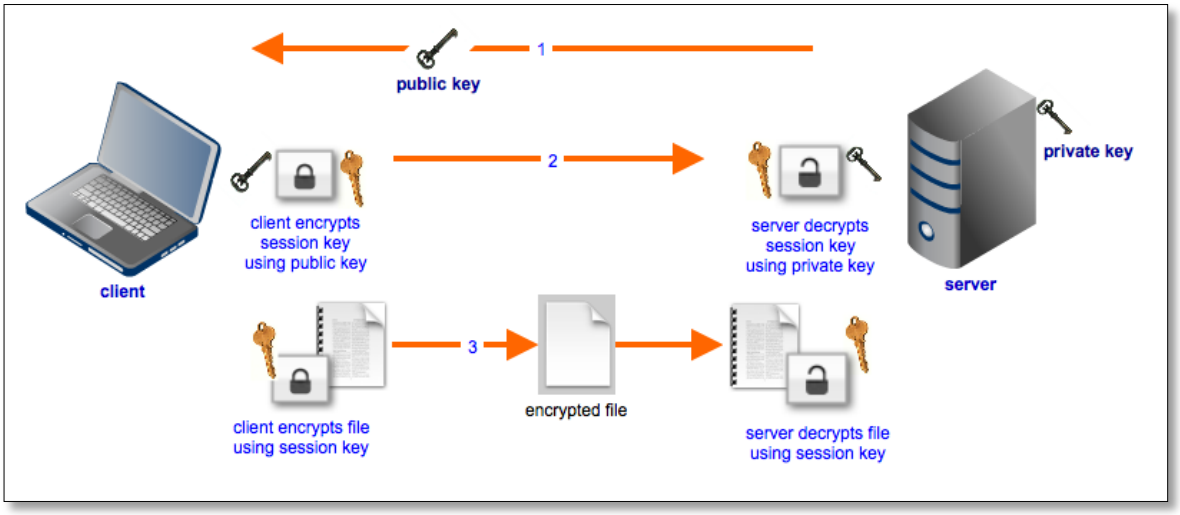

Figure 1.9: Mechanism of Hybrid cryptography

1.7 AODV PROTOCOL

Ad hoc On-Demand Distance Vector (AODV) Routing is a routing protocol for mobile ad hoc networks (MANETs). It is jointly developed in Nokia Research Center, University of California, Santa Barbara and University of Cincinnati by C. Perkins, E. Belding-Royer and S. Das. It is a reactive routing protocol. It establishes a route to a destination only on demand means it discovers route only when necessary (Kumar, 2009).

Nodes that are not actively used don't maintain routes to destinations. AODV Protocol does not play a role as long as the endpoints of a communication connection have valid routes to each other. The protocol uses different messages to discover and maintain links: Route Requests (RREQs), Route Replies (RREPs) and Route Errors (RERRs).

AODV uses a DSN (destination sequence number) for each route entry. Every node maintains its monotonically increasing sequence number which increases every time the node notices any change in the neighborhood topology. Destination creates destination sequence numbers for any information it sends to request nodes. Use of destination sequence numbers ensures loop freedom. It also helps to know that which of several routes is more fresh. If there are two routes to a destination, a requesting node always selects the one with the greatest sequence number.

When a node wants to send message to another node, it broadcasts a RREQ packet in the entire network until the destination is reached or another node with a fresh route to the destination is found. Then a RREQ is sent back to the source node and the discovered route is made available.

Nodes which are part of an active route offer connectivity information by broadcasting periodical local Hello messages. These are special RREQ messages which active nodes in path send to its immediate neighbors. The connection is assumed to be lost if Hello messages stop arriving from a neighbor beyond some given time threshold. (Usop, Abdullah, & Abidin, 2009).

Node removes the routing entry from table if it detects that a route to a neighboring node in network is not valid. It then sends a RERR message to neighbors that are active and using the route. This is possible by maintaining active neighbor

lists. This process is repeated for nodes that receive RERR messages. A source that receives an RERR can reinitiate a RREQ message.

1.8 Problem Statement

All routing protocol in MANET are based on assumptions that all nodes are co-operative and transmitting the data. But due to rapidly changing topology and decentralized approach MANET is vulnerable to various attacks. A malicious node interrupts the transmission of data. This research work focuses on providing solutions to prevent Blackhole Attack, Malicious Packet Dropping and Eavesdropping Attack. The existing AODV is modified to prevent these attacks using the various security techniques.

1.9 Objectives

- To study and simulate Blackhole and Malicious Packet Dropping attack in AODV Protocol.
- To propose and simulate solution to prevent Blackhole Attack in AODV Protocol.
- To simulate watchdog IDS in AODV Protocol to prevent malicious packet Dropping Attack.
- To analyze the performance of AODV and Modified AODV protocol under Blackhole and Malicious Packet Dropping Attack with respect to Packet Delivery Ratio, Average End to End Delay and Routing Overhead.
- To analyze the performance of AODV and Modified AODV Protocol under Dual attack i.e. Blackhole and Malicious Packet Dropping simultaneously.
- To compare the results of both protocols i.e. AODV and Modified AODV to analyze which protocol is more vulnerable to attacks.
- To Propose Hybrid Cryptography Technique for securing AODV from Eavesdropping attack and compare processing time of symmetric, asymmetric and hybrid cryptography technique.

CHAPTER 2

REVIEW OF LITERATURE

The various solutions available to alleviate the effects of malicious nodes are discussed in this chapter.

2.1 Study of Literature

Papers related to Intrusion Detection System and Hybrid Cryptography

Martiet et al., 2000 provided a scheme named Watchdog. The main aim of this scheme is to improve the throughput of network in presence of malicious nodes (i.e. nodes which agree to forward packets but fail to do so). Authors discuss two techniques namely Watchdog and Pathrater. Watchdogs identify misbehaving nodes and a pathrater helps routing protocols avoid these nodes. When any node forwards a packet, watchdog verifies that whether the next node in the path also forwards the packet or not. Next node is misbehaving if it does not forward the packet. The watchdog detects misbehaving nodes and increments the failure counter. If the counter exceeds a certain threshold then this node is avoided by pathrater which runs on each node in the network. Watchdog's weaknesses are that it might not detect a misbehaving node in the presence of Receiver Collisions, Ambiguous Collisions, False Misbehavior, Limited Transmission Power, Collusion, and Partial Dropping.

Djenouuri et al., 2005 surveyed on security problems in ad hoc networks and the various proposed solutions. They studied the different MANET's security issues, and have shown that the features of this new environment make it more vulnerable to threats and that the solutions developed for standard networks are often unsuitable in this environment. They have divided threats into two categories; attacks and misbehavior, and then they have presented how these threats affect the MANET's security in different layers, especially in the network and the Medium Access Control (MAC) layers.

Hasswa et al., 2005 provided a new intrusion detection and response system called Routeguard. It is run by each node in the network. Each node stores a rating for all the nodes it knows. Routeguard is an improvement to Pathrater. Rating is assigned

by Routeguard to each node and a path metric is calculated in a refined way. Routeguard provides a more detail classification system. Each node in the network is rated into one of the five classes: Fresh, Member, Unstable, Suspect or Malicious. Each node is treated differently depending on its status and rating. Depending on the rating the Pathrater always categorizes nodes as either neutral or malicious.

Xiao et al., 2006 classified the architectures for IDS in MANETs, each of which is suitable for different network infrastructures. Current intrusion detection systems corresponding to those architectures are reviewed and compared. Authors also provide some directions for future research.

Nasser & Chen, 2007 provided an enhanced intrusion detection system called Exwatchdog for discovering malicious nodes in MANETs. ExWatchdog extends the Watchdog proposed by Marti et al. The main characteristic of Exwatchdog is its capability to discover malicious nodes which can partition the network by falsely reporting other nodes as malicious. A table is maintained by Exwatchdog on each node. It stores the number of packets sent by node, forwards or receives respectively. When the source node receives a report about the misbehaving node, it will find another path to destination. Main aim here is to ask the destination node about the number of received packets. If it is equal to the packets sent by source node, then the actual malicious node is the node that reports other nodes as misbehaving. Otherwise, nodes being reported malicious do misbehave.

Liu et al., 2007 provided a scheme called 2ACK. The main idea of the 2ACK scheme is to send two-hop acknowledgment packets. These packets are send in the opposite direction of the routing path. Only a small part of the received data packets are acknowledged in this scheme because acknowledging all packets leads to routing overhead. The basic idea of the scheme is that when a node forwards a data packet successfully over the next hop, the destination node of the next-hop link will send back a special two-hop acknowledgment called 2ACK. It indicates the successful reception of data packet. Such a 2ACK transmission takes place for only a fraction of data packets, but not all. Such a “selective” acknowledgment is intended to reduce the additional routing overhead caused by the 2ACK scheme. Node behavior is judged after observing its behavior for a certain period of time.

Sunita & Shandilya, 2010 briefly explored the various intrusion detection methods. They analyzed some challenges and problems of intrusion detection in MANET. They conclude that there is an utmost need of a general foundation for all intrusion detection and supporting activities that can able to adapt dynamic network conditions. These activities include detecting all types of attack on MANET; collecting, and correlating intrusion events; responding to intrusions; and managing intrusion detection and all related functions to cater for a secure communication.

Sheltamiet et al., 2010 proposed a new scheme named Adaptive Acknowledgement (Aack). Authors proposed this scheme for solving two major problems: the limited transmission power and receiver collision. This scheme is an enhancement to the previous TWOACK scheme. In this scheme detection overhead is reduced while the detection efficiency is increased. The AACK is a network layer acknowledgment-based scheme that may be considered as a combination system of an Enhanced-TWOACK (E-TWOACK) scheme called TACK and an end-to-end acknowledgment scheme. The concept of adopting a hybrid scheme in AACK greatly reduces the network overhead. But both schemes i.e. TWOACK and AACK still suffer from some problems. They fail to detect malicious nodes in presence of forged acknowledgment packets and false misbehavior report.

Narasimha & Samreen, 2012 present a mechanism that enables the detection of nodes exhibiting packet forwarding misbehavior. The approach is based on the usage of two techniques. These two techniques will be used in parallel in such a way that the results generated by first technique are further processed by the other to finally generate the list of misbehaving nodes. The first part detects the misbehaving links using the 2ACK technique and this information is fed into the second part which uses the principle of conservation of flow (PFC) technique to detect the misbehaving node. The problem with the 2ACK algorithm is that it can detect the misbehaving link but cannot decide upon which one of the nodes associated with that link are misbehaving. Hence the principle of conservation of flow is used for the second part which detects the misbehaving nodes associated with that of the misbehaving link.

Shakshuki et al., 2013 proposed a scheme named Enhanced Adaptive Acknowledgement (EAACK). This scheme is designed to solve three out of six

weaknesses of Watchdog scheme. These weaknesses are false misbehavior, receiver collision and limited transmission power. EAACK is consisted of three major parts, namely, ACK, secure ACK (S-ACK), and misbehavior report authentication (MRA). To increase the merits of their research work, Authors plan to investigate possibilities of adopting hybrid cryptography techniques to further reduce the network overhead caused by digital signature.

Papers Related to Attacks in MANET

Ullah and Rehman, 2010 study blackhole attack on MANETs using different MANET routing protocols. Main aim of their work is to analyse the effects of Black hole attack in MANET using both Proactive routing protocol i.e. Optimized Link State Routing (OLSR) and Reactive routing protocol Ad-Hoc On Demand Distance Vector (AODV). Comparative analysis of Black Hole attack is taken into account for both protocols. The impact of Black Hole attack on the performance of MANET is evaluated. Study shows which protocol is more vulnerable to the attack, impact of the attack on both protocols. The Performance parameters evaluated are throughput, end-to-end delay and network load.

Tseng et al., 2011 discuss different types of black hole attacks. Black hole attack is divided into two categories i) Ordinary Blackhole Attack ii) Collaborative Blackhole Attack. Authors also discuss and compare various detection schemes. Performance metrics measured are packet delivery ratio (PDR), packet routing overhead (RO), Average end-to-end delay (AED) by varying the node density and mobility with total number of errors.

Kanthe et al., 2012 shows the effects of black hole attack, packet drop attack and gray hole attack on AODV protocol under different performance metrics such as throughput, packet drop rate and end-to-end delay. The simulation is done in Network Simulator (NS2).

Nadeem & Howarth, 2013 present a survey of the main types of attack at the network layer and detail review of intrusion detection and protection mechanisms. Authors classify these mechanisms as either point detection algorithms that deal with a single type of attack or as intrusion detection systems (IDSs) that can deal with a range of attacks.

Sahu et al. 2013 presents a simulation analysis of reactive routing protocol AODV in the presence of malicious attack under different loads. Authors present the simulations results based on packet delivery fraction, throughput, normalized routing load, and packet loss. Result shows that throughput and packet delivery ratio of normal AODV is much better than AODV with malicious attack.

CHAPTER 3

SIMULATION SETUP AND METHODOLOGY USED

This chapter discusses about software used for simulation, simulation parameters, research methodology (working of proposed algorithms) and performance metrics.

3.1 SOFTWARE USED: NS 2.35

NS2 is a free and open-source event-driven simulator. It is designed specifically for research in computer communication networks. NS is a discrete event simulator where the advance of time depends on the timing of events which are maintained by a scheduler. NS2 has continuously gained fabulous interest from industry, academia, and government since its inception in 1989. NS2 now contains modules for numerous network components such as routing, transport layer protocol, application, etc. NS2 works under Linux, Mac, and Windows. It is also possible to add your own protocol and contribute to the code. Researchers can simply use an easy-to-use scripting language to configure a network and observe results generated by NS2. Undoubtedly, NS2 has become the most widely used open source network simulator (Issariyakul & Hossain, 2012).

It covers a large part of applications (Web, FTP, CBR), protocols (transport and routing protocols), network types (Satellite links, wired and wireless LAN), network elements (mobile nodes, wireless channel models, link and queue models) and traffic models (exponential, uniform). NS-2 is based on an object oriented simulator written in C++ and a OTcl interpreter (an object oriented extension of Tool Command Language TCL) (Neglia & Ibrahim, 2013).

As shown in figure 3.1, an OTcl script written by a user is interpreted by Network Simulator. Tcl is a free script language that has a simple syntax, easy to be integrated with other languages and platform independent. While OTcl script is being interpreted, NS creates two main analysis reports simultaneously. One is NAM (Network Animator) object that shows the visual animation of the simulation.

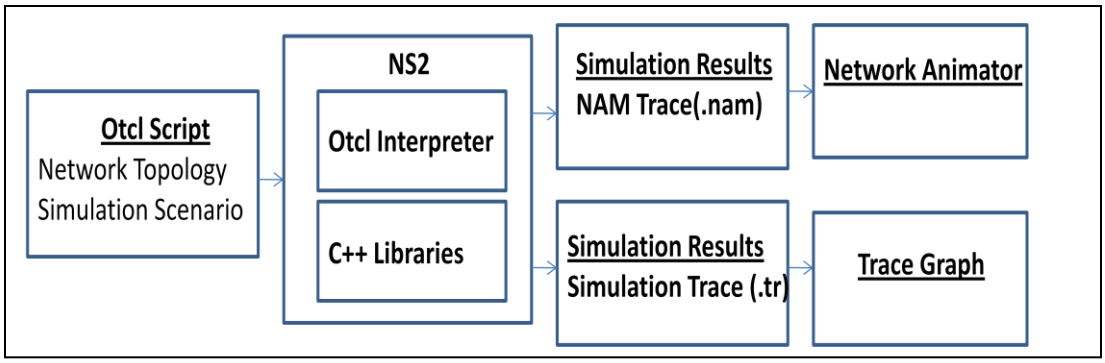

Figure 3.1: Structure of NS2

The other is the trace object that consists of the behavior of all objects in the simulation. Trace file contains following fields:

Event	Time	From Node	To Node	Pkt Type	Pkt Size	Flags	Fid	Src Addr	Dest Addr	Seq No	Pkt Id

Both of them are created as a file by NS. Former is .nam file used by NAM software. Another is a ".tr" file that includes all simulation traces in the text format. Awk Scripts are used for processing the data from the trace files. NS project is normally distributed along with various packages (ns, nam, tcl, otcl etc.) named as "all-in-one package", but they can also be found and downloaded separately. In this dissertation work the version 2.35 of ns all-in-onepackage is used and installed the package in the ubuntu operating system version 12.10.

3.2 RESEARCH METHODOLOGY

3.2.1 Work Flow

The work flow of this dissertation is divided into various phases.

Phase 1: To study the working of AODV protocol

In this phase, working of Ad hoc On Demand Distance Vector (AODV) Routing Protocol has been studied (i.e. its Route discovery, Flooding, Route Maintenance, Local Connectivity Management process). Simulation of AODV in Network Simulator is also done. Various TCL scripts have been made to understand working of AODV in NS2.

Phase 2: To study and simulate Blackhole and Malicious Packet Dropping attack

In this phase working of Blackhole and Malicious packet dropping (i.e. selfish nodes) attacks have been studied and implemented in AODV protocol. Blackhole and Malicious packet dropping attacks are discussed in chapter 1.

Phase 3: To analyze performance of AODV protocol in presence of malicious nodes

This phase further consists of two stages:

Stage 1: In this stage performance of AODV protocol is analyzed in presence of Blackhole attack.

Stage 2: In this stage performance of AODV protocol is analyzed in presence of Malicious Packet Dropping attack.

The parameters taken in simulation and performance metrics are listed in section 3.3 and section 3.4.

Phase 4: To simulate proposed solution and measure performance metrics

This phase further consists of two stages:

Stage 1: In this stage AODV protocol is modified with proposed solution to prevent Blackhole attack.

Stage 2: In this stage AODV protocol is modified with watchdog intrusion detection system to prevent Selfish node attack.

Performance metrics of standard AODV protocol is compared with Modified AODV. Graphical results are shown and discussed in Chapter 4.

Phase 5: To perform dual attack on AODV protocol

In this phase two attacks namely Blackhole and Malicious Packet Dropping are simultaneously performed on AODV protocol and performance metrics are recorded.

Phase 6: To combine proposed solution to prevent Blackhole Attack with watchdog IDS

In this phase proposed solution is combined with watchdog IDS and implemented in AODV Protocol. Main aim of this simulation is to make AODV capable of detecting both attacks. Standard AODV i.e. without any prevention scheme is compared with Modified AODV. Graphical results are shown and discussed in Chapter 4.

Phase 7: To Develop a Hybrid Cryptographic Technique

There are two types of cryptography techniques i.e. symmetric and asymmetric. Both techniques have their own advantages and disadvantages as discussed in Chapter 1. Main focus here is to develop a hybrid cryptography technique which combines the advantages of both.

Phase 8: Compare processing time of symmetric, asymmetric and hybrid cryptographic technique

Processing time of Symmetric Algorithm, Asymmetric Algorithm and Proposed Hybrid Algorithm is calculated and compared with respect to Number of Bytes sent. Processing time means time taken by processor to encrypt and decrypt the message.

3.2.2 Proposed Algorithm to prevent Blackhole Attack

A black hole attack means that one malicious node utilizes the routing protocol to claim itself of having the shortest path to the destination node, but drops the routing packets and does not forward packets to its neighbors. To convince the target nodes, the attackers may reduce the hop count data or increase the destination sequence number (DSN). In addition, the attackers can also combine both techniques to increase severity of attacks. Proposed Algorithm to prevent Blackhole Attack is as follows:

AODV::recvReply(Packet *p)

/* When a node receives a packet of type REPLY, it calls this function*/

1. If(SSN < DSN) or
2. (SSN = DSN) and
3. (SHC>CHC)

4. {
5. if (SSN < DSN) and (CHC!=1)
6. {
7. Call procedure Update Route Table entry
8. }
9. if (SSN < DSN) and (CHC==1)
10. {
11. if (Source=Destination)
12. {
13. Call procedure Update Route Table entry
14. }
15. }
16. }

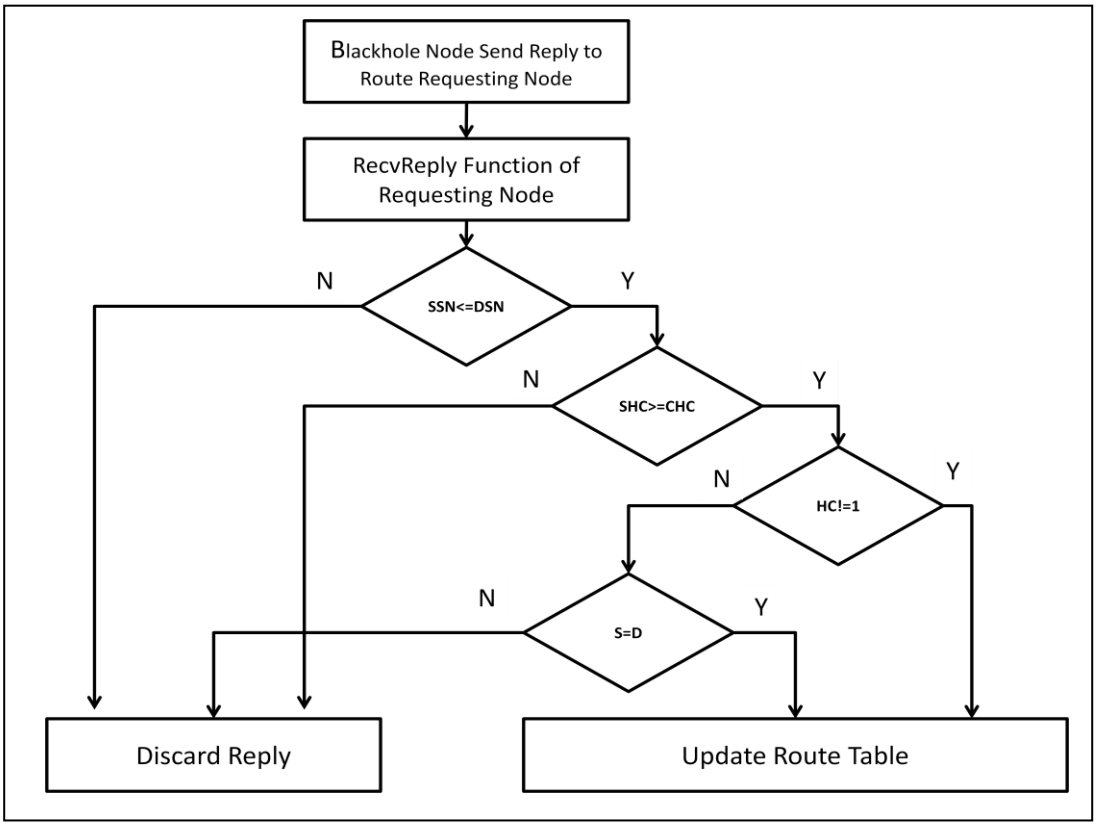

Figure 3.2 Flowchart for proposed algorithm to prevent Blackhole Attack

Where

SSN=Source Sequence Number

DSN=Destination Sequence Number

SHC=Stored Hop Count

CHC=Current Hop Count

Now if Blackhole Node send Route Reply with Hop count=1, Packet is rejected and no updation is done in routing table. But in case, if genuine nodes send reply with hop count=1, Routing table is updated. If(source=destination) in line 11 of algorithm means if destination IP address send by source in Route Request Packet is equal to Destination IP address send by destination node in Route Reply Packet. It means that there is no intermediate node between source and destination. So Route Reply by any node with hop count equal to one is always rejected except if destination IP address by source in RREQ is equal to destination IP address by destination node in RREP (Singh & Kaur, 2014). Flowchart for this process is shown in figure 3.2.

3.2.3 Watchdog Procedure to Prevent Malicious Packet Dropping Attack

The watchdog method maintains a buffer that contains recently sent packets. This helps in detecting misbehaving nodes. When any node forwards a packet, it is ensured by node's watchdog that the next node in the path also forwards the packet. This is done by node's watchdog by listening all nodes promiscuously. If the next node does not forward the packet then it is termed as misbehaving. In this scheme, every packet overheard by the watchdog is compared with the packet in the buffer. A match confirms that the packet has been successfully delivered and it is removed from the buffer. If a packet remained in the buffer beyond the timeout period, then a failure counter for the node responsible for forwarding the packet is incremented. If this counter exceeds a predetermined threshold then the node is termed as malicious. Network is informed accordingly by a message sent by the node that detects the problem (Hortelano, 2010). Flowchart for this process is shown in figure 3.3.

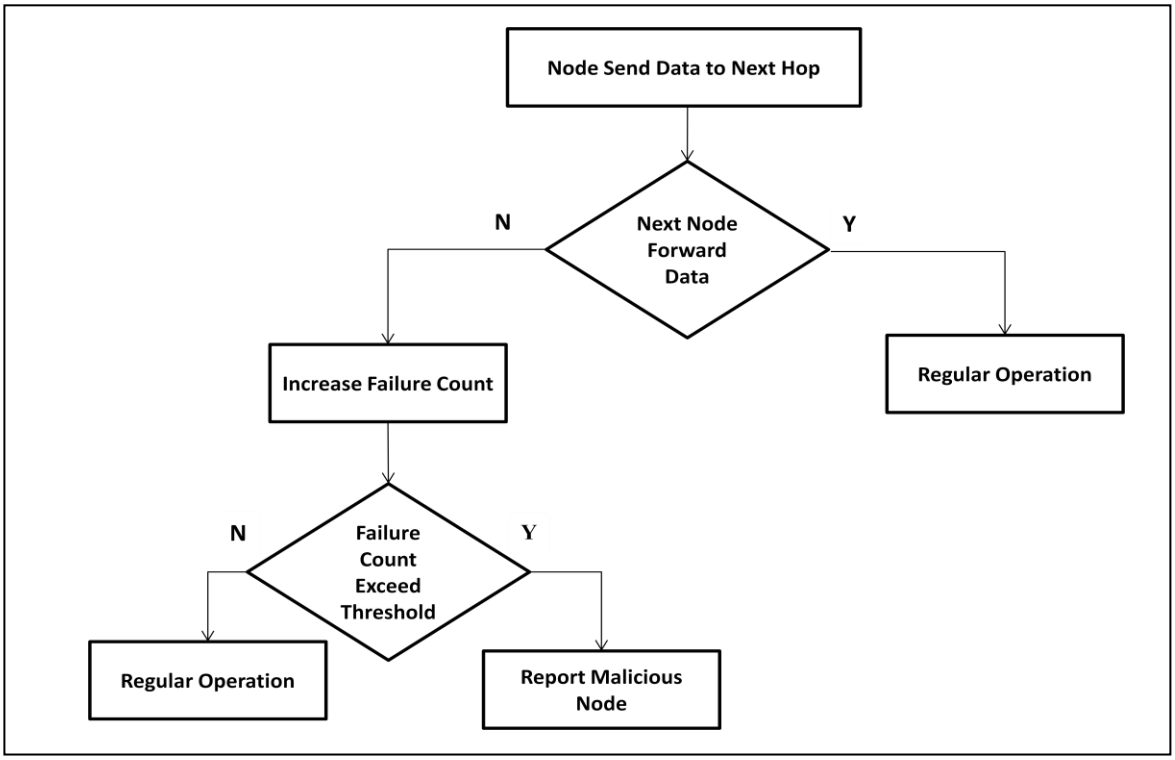

Figure 3.3 Flowchart for Watchdog Intrusion Detection System

3.2.4 Proposed Hybrid Algorithm

Hybrid algorithm is developed by combining Symmetric key Algorithm and Asymmetric Key Algorithm.

Symmetric key Algorithm used: Vigenere Cipher

Asymmetric Key Algorithm used: RSA

3.2.4.1 Working of Symmetric Algorithm (Vigenere Cipher)

Substitution ciphers are more prone to frequency analysis. They can be easily broken by mapping the frequency of its letters to the known frequencies. Polyalphabetic ciphers is encryption technique which is immune to frequency analysis. In polyalphabetic cipher one alphabet is replaced by more alphabets means a single letter can be encrypted to several different letters instead of just one (Pachghare, 2008). The working of vigenere cipher is based upon table 6.

Each row consists of 26 English alphabets. In first row each alphabet is shifted by zero, in second row each shifted by one; and the last is a shift of twenty five. The Vigenere cipher uses this table together with a keyword to encrypt a message. For example, suppose we want to encipher the plaintext message:

Table 6 Vigenere Square

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

using the keyword COMPUTER. We begin by writing the keyword and repeated it as many times as length of the plaintext message. To derive the ciphertext we have to find the intersection of the row given by the corresponding keyword letter and the column given by the plaintext letter from the table for each letter in the plaintext to pick out the ciphertext letter.

Keyword: COMPUTE RCOMPUTERC OM PUTERC OMPUTERC

Plain Text: CENTRAL UNIVERSITY OF PUNJAB BATHINDA

Cipher Text: ESZILTP LPWHTLLMKA CR EOGNRD PMIBBRUC

Decipherment of an encrypted message is equally straightforward. One writes the keyword repeatedly above the message:

Keyword: COMPUTE RCOMPUTERC OM PUTERC OMPUTERC

Cipher Text: ESZILTP LPWHTLLMKA CR EOGND PMIBBRUC

Plain Text: CENTRAL UNIVERSITY OF PUNJAB BATHINDA

Note that there are 4 A's in plaintext. First A is replaced by 'T' second by 'R' third by 'M' and fourth by 'C'. So frequency analysis is difficult in vigenere cipher.

3.2.4.2 Working of Asymmetric Key Algorithm (RSA)

RSA is named after its inventors, Ron Rivest, Adi Shamir, and Leonard Adleman. It is very popular public key encryption algorithm.

The RSA algorithm is discussed here :

1) Choose two large prime numbers P and Q.
2) Calculate n=P*Q
3) Calculate m=(P-1)(Q-1)
4) Select an integer e, 1<e<m, Such that gcd(e,m)=1
5) Compute secret component d ,1<d<m such that
   d*eMod(P-1)(Q-1)=1
6) Public key is (e,n)
7) Private key is (d,n)

The value of P, Q and M should be kept secret.

N: Modulus

e: Encryption Component

d: Decryption Component

Encryption of Data

- Sender obtains the public key (e,n) of recipient.
- Represent plaintext as a positive integer M.
- Compute ciphertext $C=M^e \bmod n$.
- Send the ciphertext C to recipient.

Decryption of Data

- Receiver use his private key (d,n) to compute $M=C^d \bmod n$.
- Extract the plaintext from the integer representation 'M'.

Example:

- Choose p = 17 and q = 7
- Compute n = p * q = 17 * 7 = 119
- Compute m = (p - 1) * (q - 1) = 16*6 = 96
- Choose e such that 1 < e < m and e and n are coprime. Let e = 5
- Compute a value for d such that (d * e) % m= 1. One solution is d = 77

  [(77 * 5) % 96= 1]
- Public key is (e, n) => (5, 119)
- Private key is (d, n) => (77, 119)
- The encryption of *m = 6* is $c = 6^5 \% 119 = 41$
- The decryption of *c = 41* is $m = 41^{77} \% 117 = 6$

3.2.4.3 Working of HYBRID Algorithm

Working of hybrid algorithm is shown in figure 3.4. Let

Secret Key	COMPUTER
Plain Text	CENTRAL UNIVERSITY OF PUNJAB BATHINDA
Prime Numbers	P=17 Q=7

At Sender Side

a) Vigenere Cipher generates Symmetric key equals to the length of message (i.e. repeats it until it matches the length of the plaintext).

   Secret key: COMPUTERCOMPUTERCOM PUTERCOMPUTERC

b) Vigenere cipher encrypts plaintext using this cipher key.

   Secret Key: COMPUTE RCOMPUTERC OM PUTERC OMPUTERC

   Plain Text: CENTRAL UNIVERSITY OF PUNJAB BATHINDA

   Cipher Text: ESZILTP LPWHTLLMKA CR EOGNRD PMIBBRUC

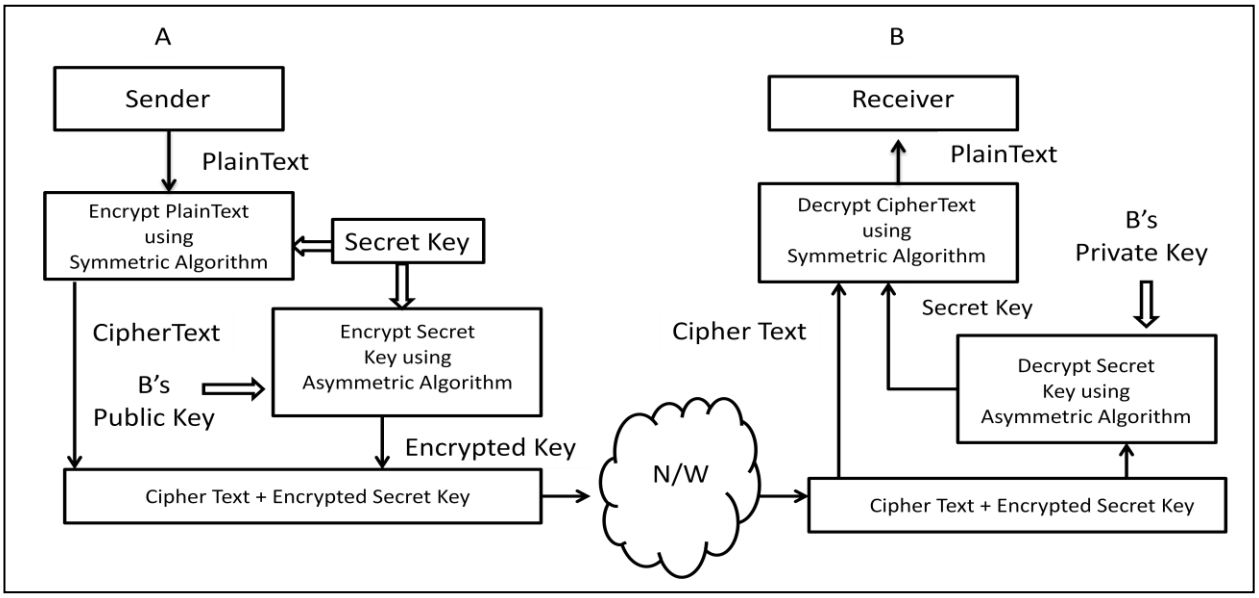

Figure 3.4 Mechanism of Proposed Hybrid Algorithm

c) RSA Algorithm Encrypts Secret Key using Public key of Receiver Node,

Public Key (e, n): (5,119)

Secret key: COMPUTER

While (i<= Length(SymmetricKey))

{

Set A=Ascii(Symmetrickey[i])

$C=A^{e}Modn$

EncryptedKey[i]=C

}

Encrypted Key= 29767991871143388

d) Generate cipher Text is of format :

Key Length	Encrypted Key	Encrypted Message
8	29767991871143388	ESZILTP LPWHTLLMKA CR EOGNRD PMIBBRUC

This generated Cipher Text is now send to Node B.

AT Receiver Side

a) Receiver reads length of key from key Length field of Cipher Text.

b) Receiver fetch Encrypted key from cipher Text.

c) Receiver Decrypt symmetric key using its private key.

Private Key (d, n): (77,119)

Encrypted key: 29767991871143388

While (i<= KeyLength)

{

P=EncryptedKey[i]^{d}Modn

DecryptedKey[i]=P

}

Decrypted Key= COMPUTER

d) Receiver fetch message from cipher Text.

e) Using Vigenere Algorithm and symmetric key, Receiver decrypts the message.

Keyword: COMPUTE RCOMPUTERC OM PUTERC OMPUTERC

Cipher Text: ESZILTP LPWHTLLMKA CR EOGNRD PMIBBRUC

Plain Text: CENTRAL UNIVERSITY OF PUNJAB BATHINDA

3.3 SIMULATION PARAMETERS

The simulation is conducted within the Network Simulator (NS) 2.35 environment on a Ubuntu 12.10 operating system. The system is running on a laptop with Core i3 CPU and 4-GB RAM. For each case, the network scenario is run five times and calculated the average performance. Simulation parameters are shown in table 7.

Table 7 Simulation Parameters

Channel type	Wireless channel
Number of nodes	100
Traffic type	CBR
Data Payload	512 bytes/packet
MAC Types	802_11
Node Placement	Random
Mobility	Random way point
Speed	1-10 m/s
Area of simulation	1000m X 1000m
Number of Maliciuos attacks	1-10
Time of simulation	150 sec
Protocol	AODV

3.4 Performance Metrics

The various parameters analyzed and measured are as follows:

- **Average end-to-end delay (AED):** The average end-to-end delay is calculated for each data packet by subtracting the sending time of the packet from the received time at final destination.

$$AED = \frac{\sum_1^N (T_R - T_S)}{N}$$

Where

N =Number of successfully received packets

T_R=Packet Received Time

T_S=Packet Sent Time

- **Packet Delivery Ratio(PDR):** It is the ratio of the number of packets received by the destination node to the number of packets sent by the source node

$$PDR = \frac{\sum \text{Received packets at destinations}}{\sum \text{Sent packets by sources}}$$

- **Routing Overhead (RO):** RO defines the ratio of the amount of routing-related transmissions (Route REQuest (RREQ), Route REPly (RREP), Route ERRor (RERR)). This metric gives an idea of the extra bandwidth consumed by overhead to deliver data packet.

$$RO = \frac{\sum \text{Routing transmissions}}{\sum \text{Data transmissions} + \sum \text{Routing transmissions}}$$

CHAPTER 4
RESULTS AND DISCUSSION

In this chapter, outputs of the experiments performed are given in graphical form along with discussion of results.

4.1 Modified AODV to prevent Blackhole Attack

In this, Proposed Solution to Prevent Blackhole Attack and AODV protocol are simulated. The Modified AODV is compared with standard AODV protocol in two different scenarios.

First Scenario (Low Mobility State):

100 nodes are randomly moving in 1000m *1000m area with speed of 1m/s.

Second Scenario (High Mobility State):

100 nodes are randomly moving in 1000m *1000m area with speed of 10m/s.

In both scenarios, nodes randomly send CBR data to each other. Numbers of blackhole nodes are chosen randomly between 1 and 5. Performance metrics calculated under these scenarios are as follows:

4.1.1 Packet Delivery Ratio

Packet delivery ratio of AODV and Modified AODV is compared in low and high mobility state as shown in figure 4.1 to figure 4.6. In standard AODV protocol, Packet Delivery Ratio decreases as number of blackhole nodes increases. But decrease is less in case of Modified AODV protocol. Standard AODV protocol drops more packets under blackhole attack as compared to Modified AODV.

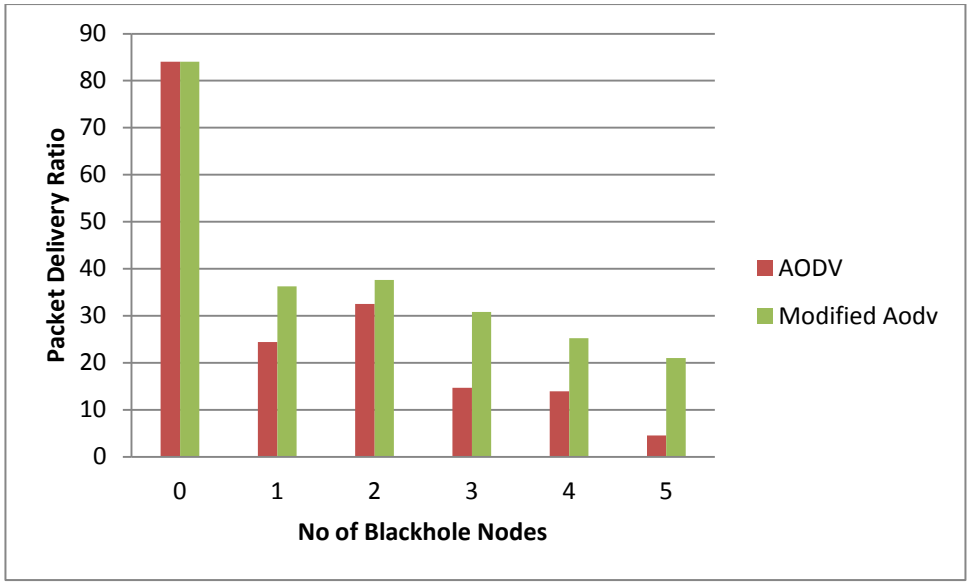

Figure 4.1: Packet delivery ratio in Low mobility state

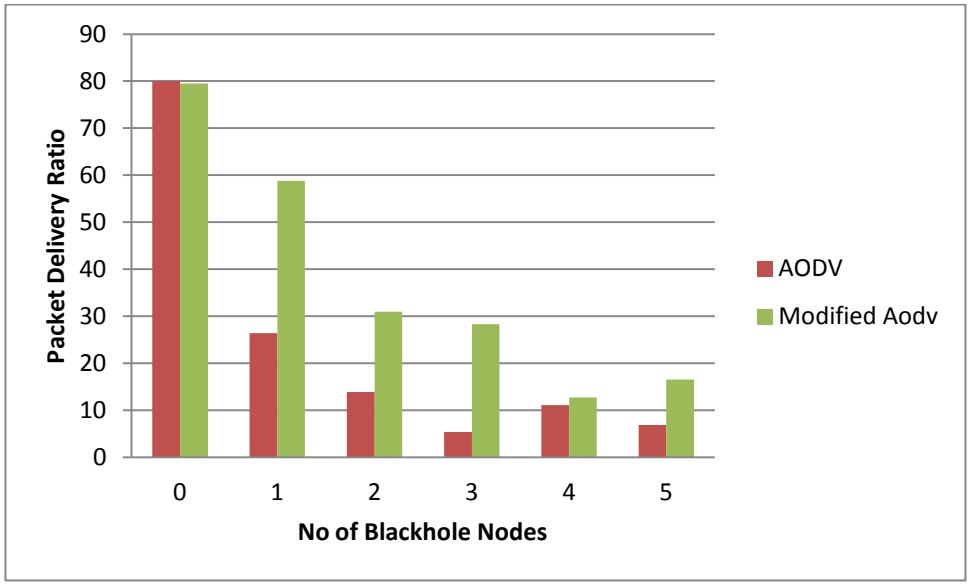

Figure 4.2: Packet delivery ratio in High mobility state

4.1.2 Routing Overhead

Routing overhead increases as no. of blackhole nodes increases as shown in figure 4.3 and 4.4. But increase is very less in case of Modified AODV protocol. Sometimes Routing Overhead in standard AODV increase to such a great extent as result of which PDR falls to zero. But in Modified AODV, Routing overhead never increase to such a great extent.

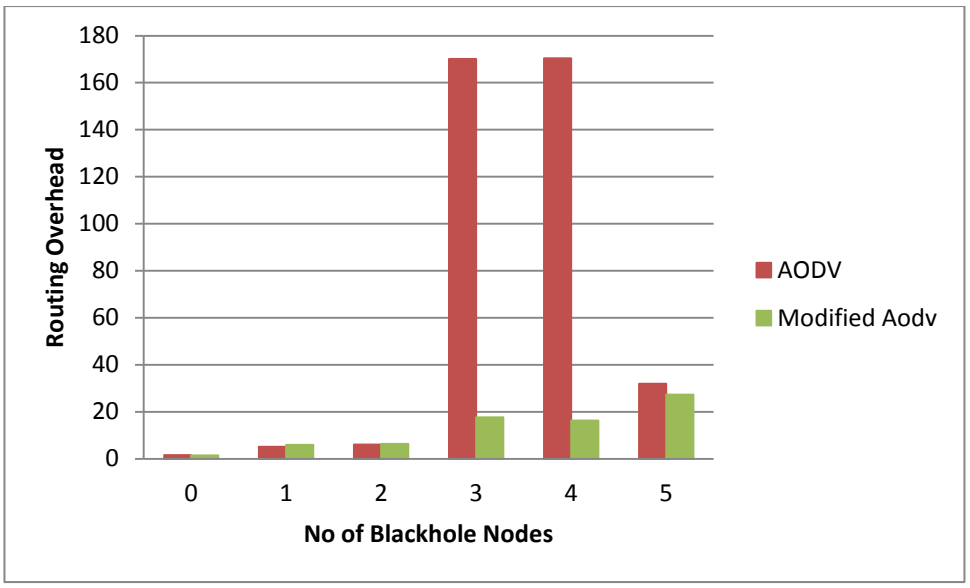

Figure 4.3: Routing overhead in Low mobility state

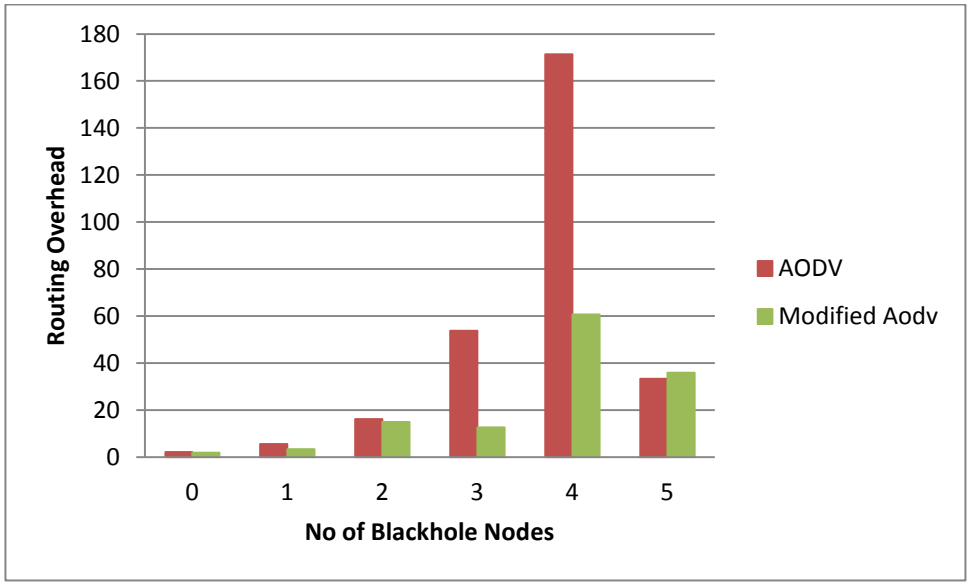

Figure 4.4: Routing overhead in High mobility state

4.1.3 Average End-to-End Delay

Average end to end delay is more in case of Modified AODV as shown in figure 4.5 and 4.6. Reason behind this is that, packet delivery ratio is more in Modified AODV. Average end-to-end delay increase with increase in no. of packets transmitted between source and destination node. To support this fact a small simulation is done in NS2 as shown in figure 4.7. Fifty CBR packets of size 512 byte are being

transmitted from source Node 0 to destination Node 1 and Average end-to-end delay is calculated. It comes out to be 100ms. But when packets are increased to 100, Average end-to-end delay comes out to be 145ms.

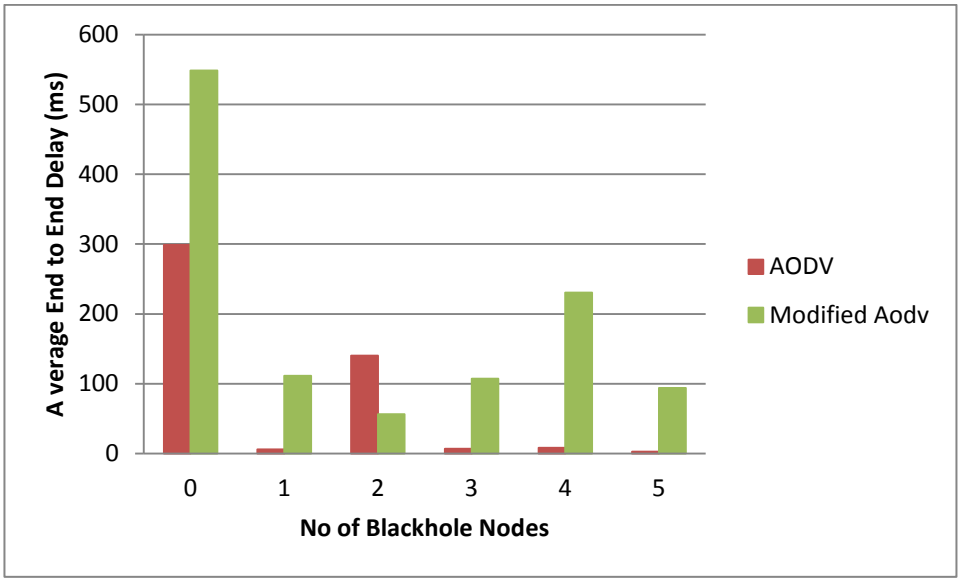

Figure 4.5: Average end-to-end delay in low mobility state

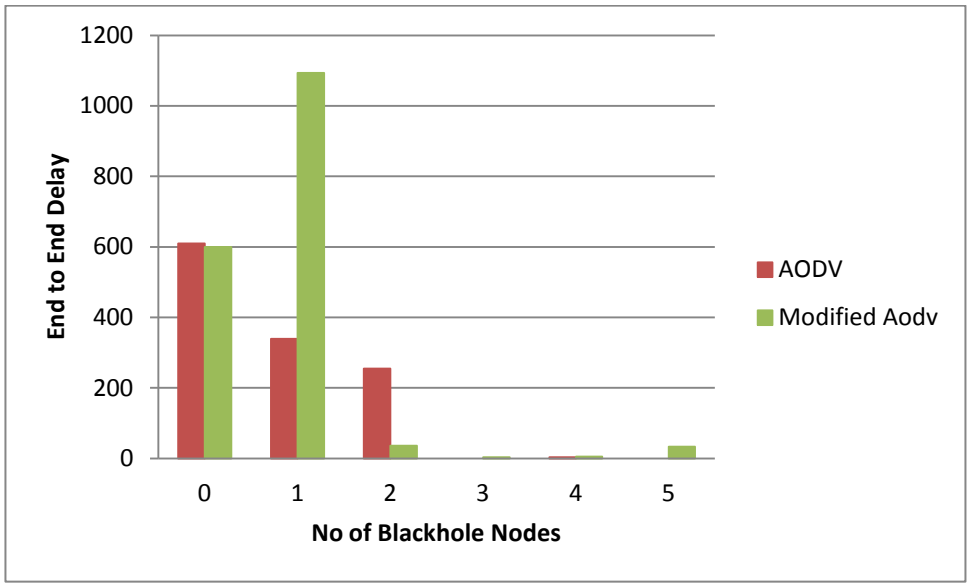

Figure 4.6: Average end-to-end delay in High mobility state

Figure 4.7: Source sending CBR data to destination

4.2 Modified AODV to prevent Malicious Packet Dropping Attack

In this, Watchdog IDS to Prevent Malicious Packet Dropping Attack is added in AODV protocol. The Modified AODV is compared with standard AODV protocol in scenario having 100 mobile nodes moving in 1000m *1000m area with speed of 10m/s. Performance metrics calculated under this scenario are as follows:

4.2.1 Packet Delivery Ratio

Packet delivery ratio generally decreases in presence of selfish nodes. As shown in figure 4.8, PDR decrease with increase of selfish nodes in standard AODV protocol. Modified AODV shows some fluctuating behavior but its PDR always greater than standard AODV.

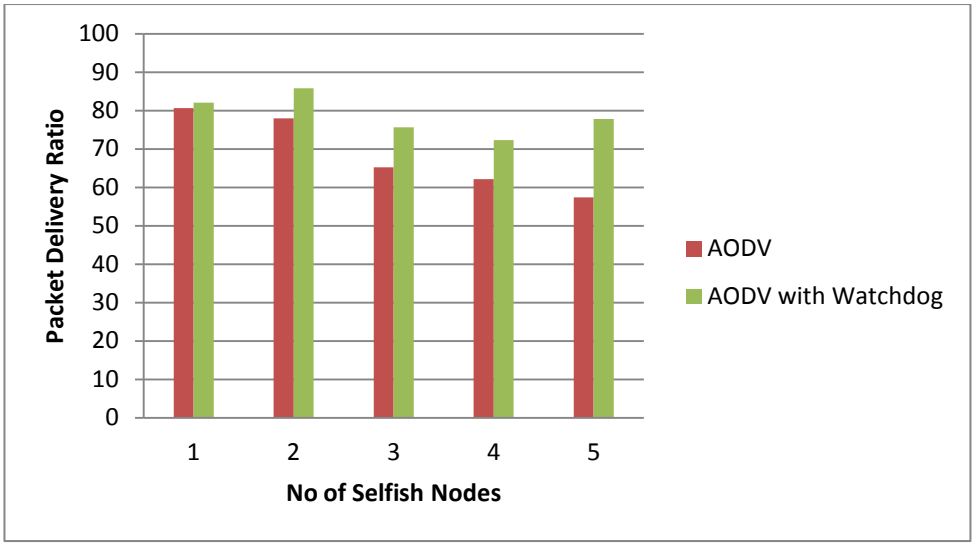

Figure 4.8: Packet Delivery Ratio in presence of selfish nodes

4.2.2 Routing Overhead

Generally, routing overhead increases in presence of selfish nodes. As shown in figure 4.9, RO increase with increase in number of selfish nodes in case of standard AODV protocol. But increase is very less in modified AODV as compared to standard AODV protocol.

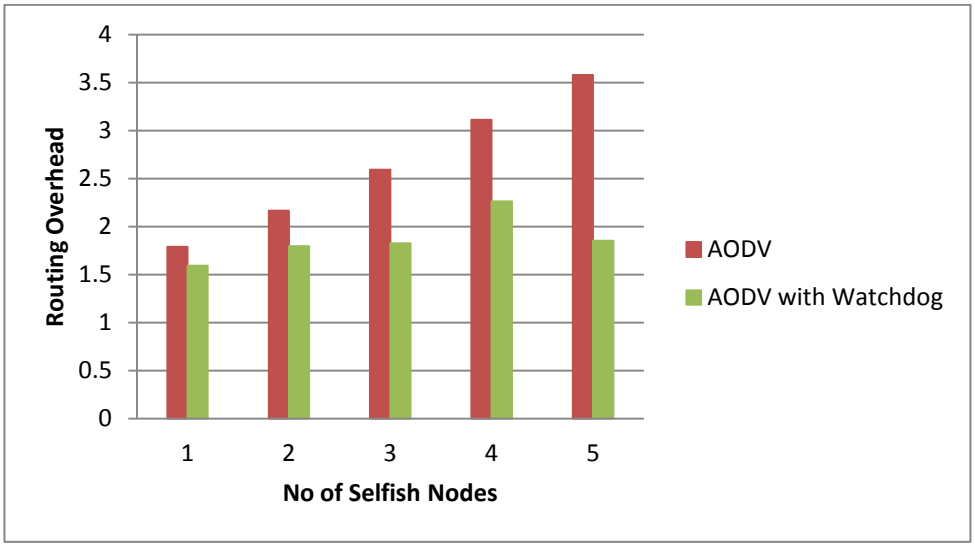

Figure 4.9: Routing overhead in presence of selfish nodes

4.2.3 Average End-to-End delay

Average End-to-End delay shows fluctuating behavior in both cases as shown in figure 4.10. Reason behind this behavior is that, nodes are randomly moving in 1000 m*1000m area. Sometimes sender and receiver nodes are close to each other and sometimes they are far apart from each other. Besides this reason, selfish nodes are also randomly selected; therefore number of selfish nodes in path may increase or decrease.

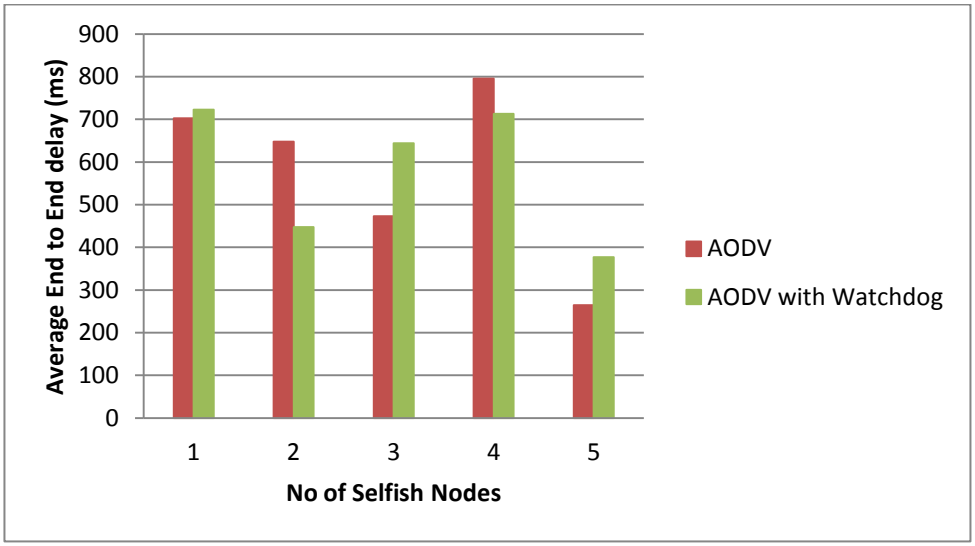

Figure 4.10: Average End-To End Delay in presence of selfish nodes

4.3 Modified AODV to Prevent Blackhole and Malicious Packet Dropping Attack

In this, proposed solution to prevent blackhole attack is combined with watchdog intrusion detection system to prevent both attacks. Main aim of this simulation is:

- To Analyse performance of AODV protocol in presence of dual attack (i.e. Blackhole and Malicious Packet Dropping) without any prevention scheme.
- To Analyse performance of AODV protocol in presence of dual attack with prevention scheme.

AODV is compared with modified AODV in scenario having 100 mobile nodes moving in 1000m *1000m area with speed of 10m/s. No. of malicious nodes taken as 2, 4, 6, 8 and 10. Performance metrics calculated under this scenario are as follows:

4.3.1 Packet Delivery Ratio

Packet delivery ratio generally decreases in presence of Selfish and Blackhole nodes. As shown in figure 4.11, PDR decreases with the increase of malicious nodes in standard AODV protocol. But decrease is less in case of Modified AODV protocol. It means that both solutions are compatible with each other and performing their respective jobs to prevent Blackhole and Malicious packet dropping attack.

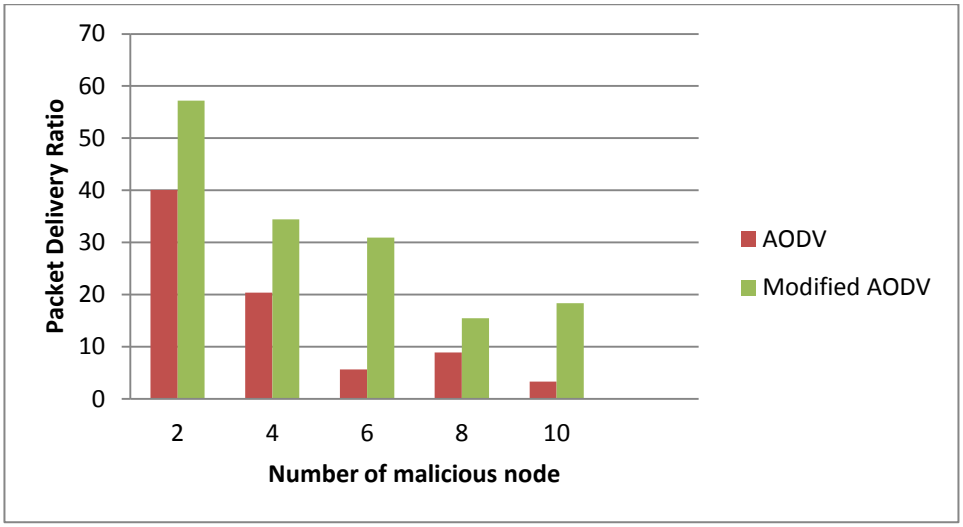

Figure 4.11: Packet Delivery Ratio in presence of malicious node

4.3.2 Routing Overhead

As shown in figure 4.12, Routing Overhead increase with increase in number of

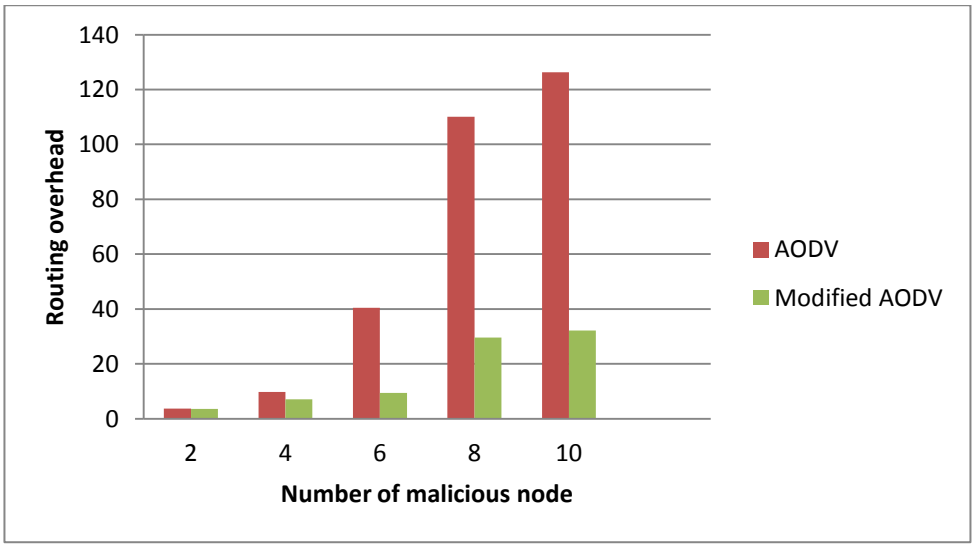

Figure 4.12: Routing overhead in presence of malicious nodes

malicious nodes in case of standard AODV protocol. But increase is very less in modified AODV as compared to standard AODV protocol.

4.3.3 Average End-to-End Delay

Average End-to-End delay shows fluctuating behavior in both cases as shown in figure 4.13. Reason behind this behavior has been already discussed in previous sections.

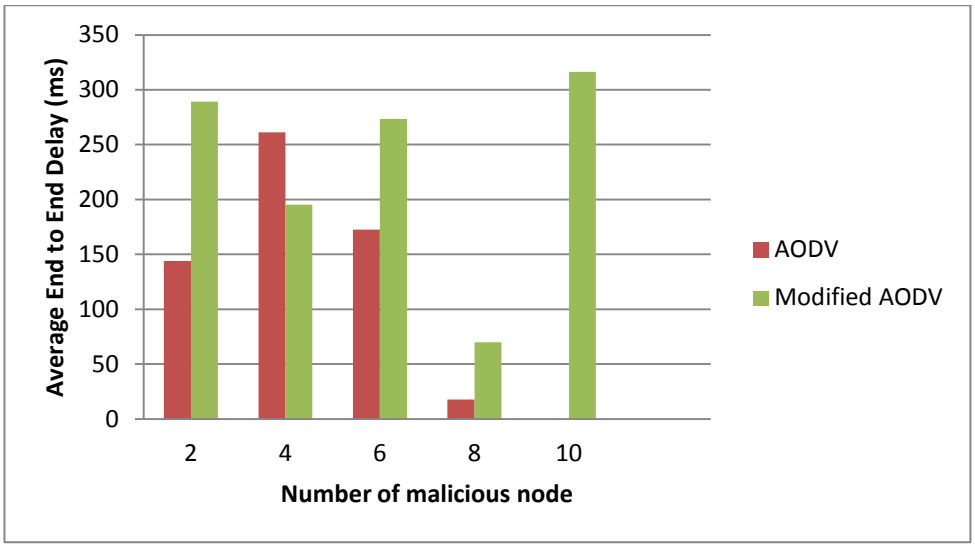

Figure 4.13: Average End-To End Delay in presence of malicious nodes

4.4 Hybrid Cryptography to Prevent Eavesdropping Attack

Processing time of Symmetric Algorithm, Asymmetric Algorithm and Proposed Hybrid Algorithm is calculated and compared with respect to Number of Bytes sent as shown in figure 4.14. Processing time means time taken by processor to encrypt and decrypt the message.

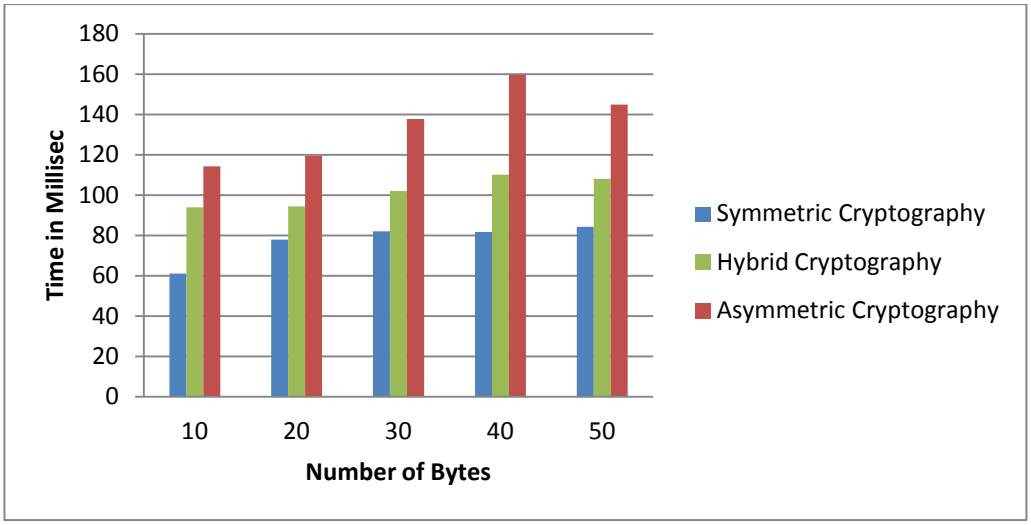

Figure 4.14: Processing Time v/s No. of Bytes

As shown in figure 4.14, asymmetric key cryptography i.e. RSA takes more time to encrypt and decrypt messages as compared to symmetric key cryptography i.e. Vigenere Cipher. As discussed in chapter 1 that asymmetric cryptography is slower but more secure as compared to symmetric cryptography. Hybrid cryptography which is combination of both shows better results. It is more secure as compared to symmetric key cryptography and faster as compared to Asymmetric key cryptography. Average end-to-end delay is sum of transmission delay, processing delay and queuing delay. Increase in processing time to encrypt and decrypt messages by a node results into increase in Average end-to-end delay. So, average end-to-end delay is less if hybrid cryptography is used to encrypt messages as compared to asymmetric cryptography.

CHAPTER 5
CONCLUSION AND FUTURE SCOPE

5.1 Conclusion

The work presented here is primarily concerned with security issues in Mobile Adhoc Networks(MANETs). The open medium, rapidly changing topology and lack of centralized monitoring make MANET vulnerable to various attacks. The performance of AODV protocol is analysed in presence of Blackhole and Malicious Packet Dropping attack.

Packet Delivery Ratio decreases and Routing Overhead increases in presence of these attacks. Solution is proposed to prevent Blackhole attack. Proposed solution increases performance of AODV protocol i.e. increase PDR and decrease RO. Malicious packet dropping attack is prevented by using Watchdog Intrusion Detection System which also increases the performance of AODV protocol.

Performance of AODV protocol is also analysed in presence of both attacks. Some nodes are programmed as blackhole nodes and some as selfish. It severely degrade performance of AODV protocol. Then proposed solution to prevent blackhole attack is combined with watchdog intrusion detection system in order to prevent both the attacks. New solution increases the performance of AODV protocol in presence of dual attack.

In case of eavesdropping attack message send by a node may travel through various intermediate nodes and if no encryption is used, then the attacker can get secret information. To prevent this attack, a hybrid cryptography technique has been developed which combines best features of both symmetric key cryptography and asymmetric key cryptography. Results show that Average End-to-End delay is less in case of Hybrid Cryptography as compared to Asymmetric key cryptography.

5.2 Future Work

In this dissertation, the research work is done on AODV protocol. AODV is modified to prevent Blackhole, Malicious Packet Dropping, and Eavesdropping attack. In future, the work may be extended on AODV or different routing protocols under multiple

attacks i.e. active or passive simultaneously. This research can also be extended further to analyse the effect of Hybrid cryptography on transmission of routing packets.

REFERENCES

Al-Roubaiey, A., Sheltami, T. Mahmoud, A., Shakshuki, E., Mouftah, H. (2010).AACK: Adaptive Acknowledgment Intrusion Detection for MANET with Node Detection. In Proceedings of Paper presented at 24th IEEE International Conference on Advanced Information Networking and Applications. Pp. 634-640. doi:10.1109/AINA.2010.136.

Djenouri, D., Khelladi, L., & Badache, N. (2005). A survey of security issues in mobile ad hoc networks. *IEEE communications surveys*, ***7(4)***.Pp. 1-27. Retrived from: http://www.lsi-usthb.dz/Rapports_pdf/2004/ LSIIR-TR0504.pdf.

Forouzan., B.A. and Mukhopadhyay D, Cryptography and Network security. Tata McGraw Hill, New York.

Hasswa, A., Zulkernine, M., & Hassanein, H. (2005). Routeguard: an intrusion detection and response system for mobile ad hoc networks. IEEE-Wireless and Mobile Computing, Networking and Communications.***3***. Pp. 336-343. doi:10.1109/WIMOB.2005 .1512922.

Hortelano, j. (2010). SafeWireless. Homepage <http://sourceforge.net/projects/ safewi reless/files/ >Accessed 2013 Oct,15.

Issariyakul, T., & Hossain, E. (2009). An introduction to network simulator NS2. Springer.New York, USA.

Jonathan, K.. (2004) .Advance Topics in Cryptograpy. Retrieved from: http:/ /www.cs.umd.edu/~jkatz/ gradcrypto2 /NOTES /lecture4.pdf.

Kanthe, A. M., Simunic, D., & Prasad, R. (2012). Effects of malicious attacks in mobile ad-hoc networks. In Proceeding of 2012 IEEE International Conference on Computational Intelligence and Computing, Coimbatore. doi:10.1109/ICCIC.20 12.6510172.

Kahate, A. (2012).Cryptography and Network security. Tata McGraw Hill, New York.

Kryptotel.(2010),Homepage< http://en.kryptotel.net /encryption.html> Accessed 2014 July,2.

Kumar, V. (2009). Simulation and Comparison of AODV and DSR routing protocols in MANET. M.Tech Thesis,Thapar University, Patiala. Retrieved from http://dspace.thapar.edu:8080/dspace/ bitstream/10266/845/3/.

Kumar, M., & Mishra, R. (2012). An Overview of MANET: History, Challenges and Applications. *Indian Journal of Computer Science and Engineering (IJCSE)*, ***3(1).***Pp. 121-125.

Liu,K., Deng.J, Varshney,P.K, Balakrishnan,K. (2007). An Acknowledgment Based Approach for the Detection of Routing Misbehavior in MANETs.*IEEE TRANSACTIONS ON MOBILE COMPUTING*.***6(5)***.Pp.536-550. doi:10.1109 /TMC.2007.1036.

Mandala,S., Abdullah,A.H., Ismail,A.S., Haron,.H., Ngadi,A.H., Coulibaly, Y.(2013). A Review of Blackhole Attack in Mobile Adhoc Network. In Proceedings of 3rd International Conference on Instrumentation, Communications, Information Technology, and Biomedical Engineering (ICICI-BME)Bandung. Pp. 339-344. doi:10.1109/ICICI-BME.2013.6698520.

Marti, S., Giuli, T. J., Lai, K., & Baker, M. (2000, August). Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th annual international conference on Mobile computing and networking .***6(11)***. Pp 255-265. Retrieved from: http://www.hpl.hp.com/personal/Mary_Baker/publications/mitigating.pdf.

Mishra,A., Nadkarni,K., Patcha A. (2004). Intrusion Detection in Wireless Adhoc Networks. IEEE Wireless Communications.Pp 48-60.

Nadeem,A., Howarth,M.P. (2013).A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks. *IEEE COMMUNICATIONS SURVEYS & TUTORIALS*.***15(4)***.Pp**.** 2027-2045. doi:10.1109/SURV.2013. 030713.00201.

Nasser, N., & Chen, Y. (2007). Enhanced intrusion detection system for discovering malicious nodes in mobile ad hoc networks. In Proceedings of Paper presented at IEEE International Conference,Glasgo. Pp. 1154-1159. doi:10.1109/ICC.2007.196.

Neglia,G., Ibrahim,M. (2013).Introduction To Ns2. Retrieved From : www-Sop.Inria.Fr /Maestro/Personnel/Giovanni.Neglia/Ns Course/Ns Course.Html.

Pachghare, V. K. (2008). Cryptography and information security. PHI Learning Pvt. Ltd.,NewDelhi,India.

Sahu, P., Bisoy, S. K., Sahoo, S. (2013). Detecting and Isolating Malicious Node in AODV Routing Algorithm. *International Journal of Computer Applications*, ***66(16)****.*

Sharma,.S., Gupta R. (2009). Simulation Study Of Blackhole Attack In The Mobile Ad Hoc Networks. *Journal Of Engineering Science And Technology* ***4(2)****.*Pp. 243 – 250.

Samreen, S., Narasimha, G. (2013). An efficient approach for the detection of node misbehaviour in a MANET based on link misbehaviour. In Proceedings of 3rd International Conference In Advance Computing Conference (IACC) IEEE. Pp. 588-592. doi:10.1109/IAdCC.2013.6514293.

Schutte, M. (2006). Detecting Selfish and Malicious Nodes in MANETs. SEMINAR: SICHERHEIT IN SELBSTORGANISIERENDEN NETZEN, HPI/UNIVERSITÄT POTSDAM, SOMMERSEMESTER, 2006. Retrieved from: http://mschuette.name/ files/uni/soN-text.pdf.

Shakshuki, E.S.,Kang N., Sheltami,T.R. (2013).EAACK-A Secure Intrusion-Detection System for MANETs. *IEEE Transactions on Industrial Electronics.* ***60 (3)****. Pp.* 1089-1098. doi:10.1109/TIE.2012.2196010.

Singh, K., Kaur. A. (2014).Security Enhancement in AODV protocol against Blackhole Attack. In Proceedings of NCISC (National Conference on Information Security Challenges),Babasaheb Bhimrao Ambedkar University.Lucknow, ***1(1)****. Pp.* 59-64.

Sunita.,S, Shandilya,S.K. (2010).A Comprehensive Survey On Intrusion Detection In Manet.*International Journal of Information Technology and Knowledge Management.****2(2)***.Pp.305-310. Retrieved from http://csjournals.com/IJITKM/ PDF%203-1/26.pdf.

Tseng, F. H., Chou, L. D., & Chao, H. C. (2011). A survey of black hole attacks in wireless mobile ad hoc networks. *Human-centric Computing and Information Sciences*, ***1(1).*** Pp. 1-16. Retrived from: http://link.springer.com/article/10.1186/ 2192-1962-1-4

Ullah, I., & Rehman, S. U. (2010). Analysis of Black Hole attack on MANETs Using different MANET routing protocols. Master Thesis, School of Computing Blekinge Institute of Technology, Sweden. Retrived from: http://www.bth.se/ fou/ cuppsats. nsf/all/448194ba63f382fdc1257751006226b8/$file/Final_Thesis_Report_irua08_resa08%20Analysis%20of%20Blackhole%20Attack.pdf.

Xiao,Y., Shen,X., Z.D.(2006). A Survey on Intrusion Detection in Mobile Ad Hoc Networks. *Springer-Wireless/Mobile Network Security*. Pp. 170 - 196.Retrived from-ucis.temple.edu/~jiewu/research/publications/Publication.../intrusion06.pdfp