OPTIMIZATION OF WORMHOLE ATTACK DETECTION PROTOCOL

Dissertation submitted to the Jawaharlal Nehru University
in partial fulfillment of the requirements
for the award of the degree of

MASTER OF TECHNOLOGY
IN
COMPUTER SCIENCE AND TECHNOLOGY

By

CHANCHAL KUMAR

Under the Supervision of

Dr. D. K. LOBIYAL

SCHOOL OF COMPUTER & SYSTEMS SCIENCES

JAWAHARLAL NEHRU UNIVERSITY

NEW DELHI-110067

INDIA

JULY, 2012

जवाहरलाल नेहरू विश्वविद्यालय

JAWAHARLAL NEHRU UNIVERSITY

School of Computer & Systems Sciences

NEW DELHI - 110067, INDIA

CERTIFICATE

This is to certify that the dissertation entitled "OPTIMIZATION OF WORMHOLE ATTACK DETECTION PROTOCOL", being submitted by **CHANCHAL KUMAR** to the School of Computer and Systems Sciences, **Jawaharlal Nehru University**, New Delhi, India, in partial fulfillment of the requirements for the award of the degree of **Master of Technology** in **Computer Science and Technology**, is a record of bonafide work carried out by him under the supervision of **Dr. D. K. Lobiyal.**

The matter embodied in this dissertation has not been submitted to any other University or Institution for the award of any other degree or diploma.

26/07/12

(Dr. D.K. Lobiyal)
Supervisor
School of Computer & Systems Sciences,
Jawaharlal Nehru University,
New Delhi-110067, India

(Prof. Karmeshu)
Dean
School of Computer & Systems Sciences,
Jawaharlal Nehru University,
New Delhi-110067, India

प्रोफेसर कर्मेशु/Professor Karmeshu
डीन / Dean
स्कूल ऑफ कम्प्यूटर और पद्धति विज्ञान संस्थान
School of Computer and Systems Sciences
जवाहरलाल नेहरू विश्वविद्यालय
Jawaharlal Nehru University
नई दिल्ली / New Delhi-110067

जवाहरलाल नेहरू विश्वविद्यालय

JAWAHARLAL NEHRU UNIVERSITY

School of Computer & Systems Sciences

NEW DELHI- 110067, INDIA

DECLARATION

This is to certify that the dissertation entitled **“OPTIMIZATION OF WORMHOLE ATTACK DETECTION PROTOCOL”**, which is being submitted to the School of Computer and Systems Sciences, **Jawaharlal Nehru University**, New Delhi, India, in partial fulfillment of the requirements for the award of the degree of **Master of Technology** in **Computer Science and Technology**, is a bonafide work carried out by me under the supervision of **Dr. D. K. Lobiyal.**

The matter embodied in this dissertation has not been submitted to any other University or Institution for the award of any other degree or diploma.

Chanchal Kumar
M.Tech,
School of Computer & Systems Sciences,
Jawaharlal Nehru University,
New Delhi - 110067, India

Dedicated
To
My mother, my father,
My Teachers & lastly to my brother
Who taught me to get up after a fall and start again

ACKNOWLEDGEMENT

I would like to express warm and sincere gratitude to my supervisor **Dr. D. K. Lobiyal**, for his precious guidance and unflinching encouragement throughout my dissertation. His way of teaching and numerous personal discussions led to create a strong foundation for my research work. This work would not have been possible without his constructive comments and kind co-operation during whole tenure. I feel privileged to have an opportunity to work under him. His truly scientist intuition inspired and enriched my growth as a student and as a researcher. I am indebted to him more than he knows.

I gratefully acknowledge to Mr. Sushil Kumar, Assistant Professor, SC&SS, J.N.U, New Delhi and Dr. Karan Singh, Assistant Professor, G.B.U, Greater Noida, for providing their valuable ideas and infrastructural facilities to accomplish my research.

I appreciatively thank to the Dean, faculties and administrative staff of SC&SS, for creating secular and healthy environment among the students.

Many thanks go to my seniors Shiv Prakash, Arun Kumar, Sanjoy Das, Buddha Singh, Sohan and my batch mates especially Shariq, Arun, Anuj, Mayank, Nitin, Vipin, Vinesh for helping in various ways not only during my dissertation work but also during the course. I expand my thanks to Dipesh my roommate, Afzal and Ravi for their cordial cooperation.

Where would I be without my family? My Parents, my elder brother Ved, sister Vedwati & sister in law Babita who raised me with care and gentle love deserve special mention for their unwavering support and blessing.

Words fail me to express my appreciation to Chetan Sharma, Rohit, Sunil, Anil my nephews Harsh, Abhishek and niece Khushboo, Anshul, whose persistent confidence, favour and support always encourages me during tough moments of my life.

Chanchal Kumar

CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS

ALOHA	Areal Location of Hazardous Atmospheres
AODV	Ad-hoc On Demand Distance Vector Routing
ARAN	Authenticated Routing for Ad-hoc Networks
CBR	Constant Bit Rate
CSMA	Carrier Sense Multiple Access
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
DELPHI	Delay Per Hop Indication
DREQ	DELPHI Request
DREP	DELPHI Reply
DoD	Department of Defence
DoS	Denial of Service
DPH	Delay Per Hop
DSR	Dynamic Source Routing
DSSS	Direct Sequence Spread Spectrum
EDWA	End to End Detection of Wormhole Attack
FHSS	Frequency Hopping Spread Spectrum
GLoMo	Globe Mobile Information
GPRS	General Packet Radio Service
GNSS	Global Navigation Satellite System
GPS	Global Positioning System
GSM	Global System for Mobile Communication
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
LITEWORP	Light Weight Counter Measure for Wormhole
MAC	Media Access Control
MANET	Mobile Ad-hoc Network
MD	Message Digest
NS	Network Simulator
NTDR	Near Term Digital Radio
NTTM	Novel Transmission Time Based Mechanism

PRNET	Packet Radio Network
PS	Packet Sent
RAP	Rushing Attack Prevention
RNG	Random Number Generator
RREP	Route Reply
RREP_DEC	Decision Route Reply Message
RREQ	Route Request
RTT	Round Trip Time
SAR	Security Aware Ad-hoc Routing
SETX	Secure Expected Transmission Count
SURAN	Survival Adoptive Radio Networks
TDMA	Time Division Multiple Access
TIK	TESLA with Instant Key
TTM	Transmission Time Based Mechanism
WARP	Wormhole Avoidance Routing Protocol

ABSTRACT

The cooperative nature and absence of infrastructure creates lot of research scopes in the area Mobile Ad-hoc Networks (MANETs). Due to dynamic nature, the most challenging task in MANETs is routing. In routing, main priority is given to the performance of routing protocol. Therefore, routing protocols provide a little defense against malicious activities.

In the context of MANETs, many attacks have been identified, but the most devastating attack is wormhole attack. The malicious node captures the control as well as data packets from the location near the source and directs to move it towards other colluding nodes placed at other locations in the network which in turn drop or replays back the packet into the network.

Novel Transmission Time based Mechanism (NTTM) to detect wormhole attack is proposed in this work. In NTTM model, the computation of RTT between a particular intermediate node and destination were carried out by its neighbor which is just previous node in the direction from source to destination. In NTTM, the computation of RRT for the node was shifted from itself to its neighbor. Therefore, every intermediate node is always under the surveillance of its neighbor which made the wormhole attack detection process more secure and accurate.

NTTM model is simulated using QualNet 5.0.2 Network Simulator (NS). Performance wise both TMM and NTTM models are almost equal. Finally, the PDR and throughput of the Dynamic Source Routing (DSR) protocol, DSR under wormhole attack and NTTM with wormhole attack are analyzed at different mobility and different node density. NTTM shows a significant improvement in PDR as well as throughput under wormhole attack. By changing the tunnel's length between colluding nodes, detection rate of NTTM is observed. The accuracy of wormhole attack detection in NTTM is also examined.

Chapter 1

Chapter 1

Introduction

Mobile Ad-hoc Networks (MANETs) is a category of distributed wireless networks that is self-organized and operates autonomously. It utilizes multi-hop radio relaying and capable of operating without the support of any fixed infrastructure. MANETs is a new paradigm of establishing a network especially where infrastructure setup is difficult. All activities like route finding, topology identification and packet delivery are done by the nodes. Therefore, to accomplish all these tasks nodes require more processing power and energy consumption.

1.1 Background

Era of MANETs starts from 1972 when Advanced Research Project Agency (ARPA) sponsored a project known as Packet Radio Network (PRNET) which was further evolved as Survival Adoptive Radio Networks (SURAN) in the early 1980s. Its primary objective was to provide packet switching networking to mobile elements in the battlefield, where infrastructure establishment was not possible [1].

MANETs development is categorized into three generations. The first generation starts in 1972 and known as PRNET. PRNET worked with Areal Location of Hazardous Atmospheres (ALOHA) and Carrier Sense Multiple Access (CSMA) for medium access and used static stations for routing. Bellman Ford type algorithm was used for routing in static stations. In 1980's, United State Department of Defence (DoD) funded two new projects, namely Globe Mobile Information System (GloMo) and Near Term Digital Radio

(NTDR). GloMo uses Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) and Time Division Multiple Access (TDMA) models and provides self-organizing network. The NDTR, which is only real non prototypical Ad-hoc network exploited today, used link state routing and clustering.

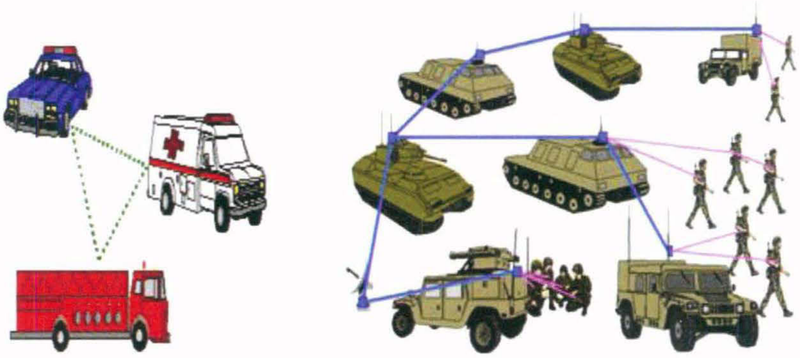

Fig. 1.1 Mobile Ad-hoc Networks [2]

With the accession of various wireless equipments, researchers proposed an idea to collect the nodes to form commercial Ad-hoc networks and Institute of Electrical and Electronics Engineers (IEEE) 802.11 subcommittee adopted the term "Ad-hoc network" for the same. Later in mid 1990's a new group by the name of 'Mobile Ad-hoc Networking Group' was brought up under Internet Engineering Task Force (IETF) to standardize the routing protocols. This group in turn availed the development of devices like palmtops, PDA's etc.[1,3].

1.2 Architecture of Mobile Ad-hoc Networks

- **Hierarchical Network Architecture:** Entire network is grouped into different levels of sub networks. A hierarchy is maintained which can be one tier or multi-tier. A node chosen dynamically acts as gateway to other sub networks [4].

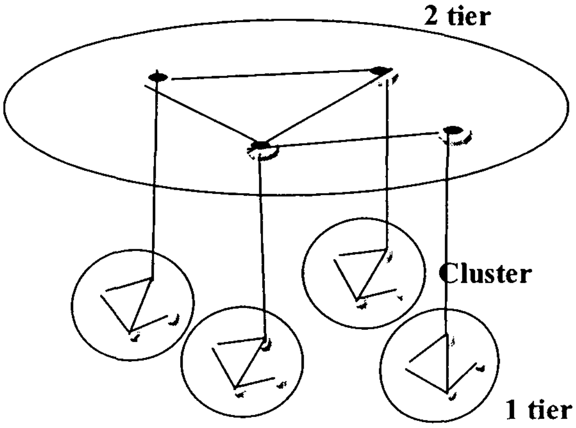

Fig. 1.2 Hierarchical Network Architecture [4]

- **Flat-Routed Architecture:** All nodes are identical in terms of responsibility i.e. every node is responsible to maintain connectivity at different levels.

□ Mobile Nodes ◌ Transmission Range ◂▸ Available connection

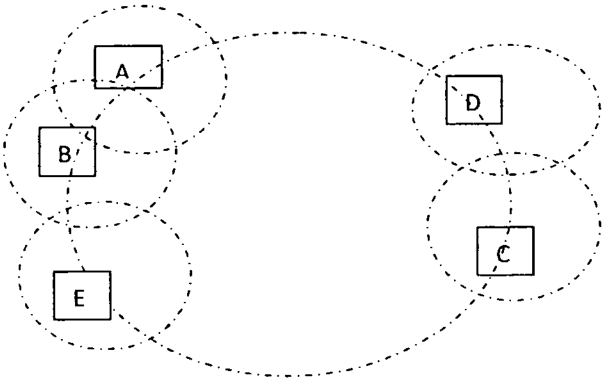

Fig. 1.3 Flat Routed Architecture [4]

1.3 Characteristics of Mobile Ad-hoc Networks

The characteristics of MANETs are different from normal network. Some unique characteristics are as the follows [5]:

- Quick and cost effective deployment
- Infrastructure less
- Shares radio channel and packet switch mechanism
- Self organizing and maintenance properties are in built
- Every node has routing capability
- Bandwidth reservation requires more complex medium access protocol
- Time synchronization is difficult and consumes extra bandwidth

1.4 Applications of Mobile Ad-hoc Networks

The application area of MANETs is very large. Quick, easy and cost effective establishment makes its application area very wide. Some of the application areas are as follows [5]:

- Military operations
- Collaborative and distributed computing
- Emergency operations
- Wireless mesh networks
- Disaster rescue operations

1.5 Network Security and Requirements

Due to high vulnerabilities toward the security attacks, it is necessary to build a reliable and secure protocol. Any such protocol should satisfy the following requirements listed below [5].

- **Confidentiality:** The data sent by the sender should be understandable to receiver for which it is being sent. If any intruder node captures the data that is being sent, it should not be able to understand the actual meaning of the data.
- **Availability:** Ensures that networks should be working all the times despite the Denial of Service (DoS) attacks. Whenever an authorized user wants to access the service it must be available. It should survive even under various attacks.
- **Integrity:** The data sent by the sender should be reached in its original form at the destination i.e. there should not be any tempering with the sent data.
- **Non-repudiation:** It guarantees that the sender and receiver of the data cannot deny later that he had not sent or received the data respectively.

1.6 Security Issues and Challenges

The networks can be damaged by active attacks as well as by passive attacks. We have to consider a lot of parameters like environment, radio transmission range, management security criticalities etc. having different impacts on the security of the network [5].

- **Operational Environment:** MANETs is used in very different environment as compared to a normal network. Some application areas are so critical that they require foolproof secure network. A silly mistake may result in a disaster. To capture secret information, enemies always attempt to damage or snoop the network. The operational environment like in the battlefield, the identification of actual nodes becomes very difficult because nodes are always moving in and out of the network.

- **Infrastructure:** MANETs is infrastructure-less i.e. there is no central authority that will monitor or direct the data flow over the network. Every node works as host as well as router. Every time a new node joins the network, it announces its presence and listens from the channel for acquiring the necessary information. Any adversary node can easily come in to the network.
- **Resource:** MANETs operates on low bandwidth channels and battery power is the only source of energy. Because of power constraints computational power of nodes is kept low. These constraints become big hurdles in the implementation of complex cryptography based security mechanism.
- **Topology:** Due to the mobility of nodes, topology of the network changes very frequently. Sometimes different Ad-hoc Networks mix together. Then it leads to IP address duplication.
- **Shared Broadcast Channel:** In MANETs, all the nodes in the transmission range of a node can hear the data broadcasted to each other. An adversary node can easily analyze the traffic and capture the relevant information [5, 6].

1.7 Classification of Attacks

Interrupting the normal working of the system, damaging the data sent over the network channel, monitor the traffic on the network which is not intended for them are considered as attacks. The attacks can be classified into several categories based on different criteria. The classification is not mutually exclusive i.e. some attacks can fall in more than one category.

1.7.1 Based on the Target

Either security mechanism protecting the network or basic vulnerabilities of the networks are kept in mind while an attack is launched into the network. In this context attacks are classified into two broad categories [7].

- **Basic Vulnerabilities of the Ad-hoc Networks:** The attackers attack on the basic vulnerabilities of the network that includes shared broadcast channels, cooperative routing and dynamic topology etc. These vulnerabilities are inherent in the basic structure of the MANETs therefore cannot be removed.
- **Security Mechanism and Key Management:** The security mechanism and key management are breached by the intruder. Such attacks can be precluded by using strong cryptographic algorithms. The attacks like public keys being replaced by adversary node, trusted server comes under the control of the attacker etc. fall under this category.

1.7.2 Based on Location of Attacker

Attacker may be the participant of the networks or may be an outsider. The attacks may classified into internal attacks and external attacks based on their location in the network [8].

- **Internal Attack**: In this attack, attackers are part of the same network. These attacks are done by compromised nodes of the network. Nodes damage the other nodes are known as compromised or malicious nodes. Involvement of authorized nodes in launching the attack makes them difficult to detect.
- **External Attack:** In this attack, attackers are not the part of the same network. They are easy to detect as compared to internal attacks.

These kinds of attacks can be prevented by using standard security mechanism and firewalls.

1.7.3 Based on Tempering with Data

- **Active Attacks:** An external or internal attack that alters or destroys the data being transferred over the channel is known as active attack. In these attack integrity requirement of security is violated. The wormhole attack, blackhole attack, byzantine attack, session hijacking, repudiation etc. fall under this category [9].
- **Passive Attacks:** These types of attacks are difficult to detect because the normal operation of the network is not disturbed. The eavesdropping and traffic analysis, adversary node snoops ongoing transmission collects secret information without disturbing the network. The confidentiality requirement of security may be violated, if adversary decrypts data completely and successfully capture actual information. To cope with such attacks a powerful encryption mechanism should be adopted [9].

1.8 Attacks and Countermeasures on Different Layers of the Network Protocol Stack

There are different types of attack exist for particular layer in the network protocol stack. However, some attacks can be launched at any layer known as multi-layer attacks.

1.8.1 Physical Layer Attacks

Some existing physical layer attacks i.e. jamming and eavesdropping are not confined to this layer, they may be launched at other layers.

- **Jamming:** These attacks are launched especially by military operation, and are less relevant to the commercial world. Adversary node sends a signal at the frequency that is same as the frequency at which the victim node is receiving the packets. First, trespasser snoops ongoing transmission in order to get correct operational frequency and then disrupts the communication. To obviate these attacks, Frequency Hopping Spread Spectrum (FHSS) and Direct Sequence Spread Spectrum (DSSS) techniques are used [5, 10].
- **Eavesdropping Attack:** The passive attack monitors the transmission of the data over the broadcast channel. Attacker captures the secret information without disturbing its normal operation. Strong encryption techniques must be used to prevent these attacks [5].

1.8.2 Data Link Layer Attacks

Attacks mounted at data link layer are generally passive in nature. Attacks launched at data link layer serve to mount active attacks at other layers. They are difficult to detect. Traffic analysis, monitoring and disruption are common attacks that are launched at data link layer. The information about the topology of the network, routing protocol and security mechanism defending the networks is collected by analyzing the traffic on this layer [5, 10].

1.8.3 Networks Layer Attacks

For routing, MANETs uses either on-demand or table driven protocols. In both the cases routing is the very tedious due to mobility. Each node has to perform the functionality of router as well as host. Nodes those are more than one hop away from each other use intermediate nodes to communicate between themselves. The routing process includes route establishment, route discovery, route updating and data forwarding phases. Attacks can be launched at any time in this process. Some of the attacks are described below [6].

- **Blackhole Attack (Sinkhole Attack):** Blackhole attacks are also known as sinkhole attacks. Depending on the intuition of attackers, blackhole attack can be used for variety of purposes. Some attackers divert whole traffic toward itself for eavesdropping, while others hinder the route discovery process to consume more power which may result in demolition of entire network. Blackhole attack has basically two properties. First, it exploits routing protocol by injecting false path information. Second it drops the packets without forwarding those [9]. This attack may be launched either in route discovery or in route updating phase. A compromised node registers optimal path through itself by showing shortest path or traffic free route whenever route request is received. Then all the data packets travelling through the network are diverted toward a node that discards them completely.

  In Fig. 1.4, routing table at A is modified by attacker and in place of path through B (Correct path) entire traffic is diverted toward E.

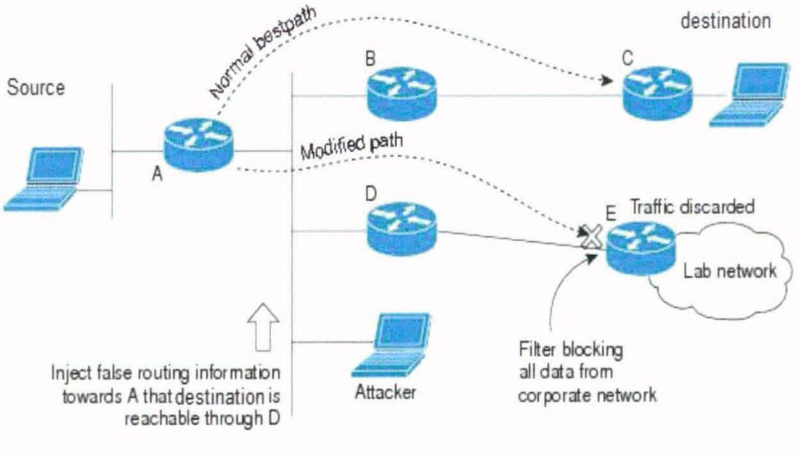
Normal bestpath
destination
Source
B
C
A
Modified path
D
E
Traffic discarded
Lab network
Inject false routing information towards A that destination is reachable through D
Attacker
Filter blocking all data from corporate network

Fig. 1.4 Blackhole Attack [11]

Blackhole attacks can be avoided by using secure on-demand routing protocols like Secure Expected Transmission Count (SETX), Security Aware Ad-hoc Routing (SAR) Protocol, one-way hash chains and merkle hash tree [7, 10, 11].

- **Byzantine Attack:** A malicious intermediate node or a set of intermediate nodes work in collusion with in the network and selectively drop the packets, form routing loops, and divert the data over non optimal path. They are very hard to detect [9].
- **Resource Consumption Attack**: Malicious node tries to waste scarce resources of network i.e. battery power, bandwidth. Adversary nodes unnecessarily generate route request packets. A node consuming battery power of other node is termed as sleep deprivation attack, and it falls under this category [5].
- **Wormhole Attack:** Most austere attacks in MANETs are launched during packet forwarding phase at the network layer. It involves pairs of attackers and a tunnel (wormhole). Both attackers in a pair first try get involved into the network and form a tunnel between themselves by means of wired link or single long range wireless link to pass the packet. Then one node receives the data from its neighbor and passes to other colluding node through the tunnel. This colluding node extracts information from the data packet and replays it in to the network near the destination. Presence of tunnel shows a short hop length because of which entire traffic is diverted through direct erroneous link. Besides being an attack, wormhole tunnel mechanism can be used as power saver by providing direct links for data flow from one end to other end, but it requires extra hardware.

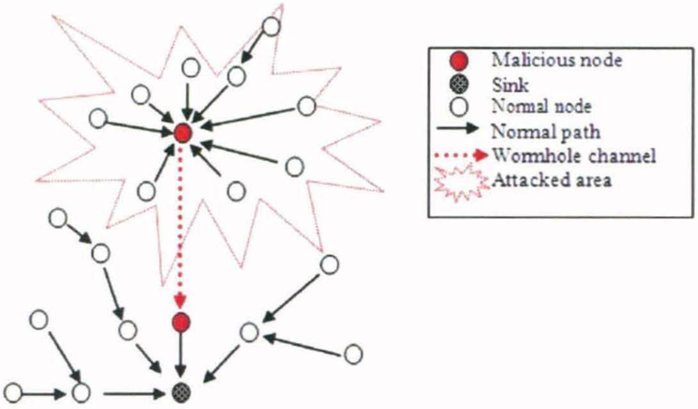

Fig. 1.5 Wormhole Attack [12]

There are many countermeasures like packet leash protocol, DELPHI protocol and directional antennas etc. has been proposed for the prevention of wormhole attacks in which some requires hardware support while other can without them [6, 7].

- **Routing Attacks:** Routing in MANETs is a complex process and more vulnerable. The motive of attacker is to disturb the routing by rushing attacks, routing table overflow, route cache poisoning etc.

  - **Rushing Attacks:** Rushing attacks are launched at the time of route discovery. Source node broadcasts route request packet in to network. Adversary node in the neighborhood of the source receives route request packet and again floods it quickly. This packet reaches the next *r* neighbor on the route before receiving the original packet. Actual packet is declared as duplicate at every neighboring node and discarded by them. Adversary node operates as an intermediate node in every route between source and destination. Detecting such attacks is extremely difficult [5].

- **Routing Table Overflow Attack:** Resources are limited in Ad-hoc networks. Malicious node tries to fill up the routing table of an authorized node by registering route to non-existence nodes. Whenever a legitimate node tries to register a new entry for route, this new entry is simply discarded because of overflow in routing table. Mostly these attacks are launched over on-demand routing protocols. Rushing Attack Prevention (RAP) is generic defense used to resist the rushing attack [13].
- **Route Cache Poisoning:** Attacker misuses the promiscuous mode reception of packet in the network. The promiscuous mode is usually operates in on-demand routing protocols. Whether a node belong to the route or not, it can hear packet transmitted over entire network. Malicious node modifies route information contained in its header route cache after overhearing route request. Adversary nodes use this technique to divert the data flow towards wrong direction [5].

1.8.4 Transport Layer Attacks

In MANETs, main task of the transport layer is to set up end-to-end connection, congestion control and reliable end-to-end delivery of packets etc. The entire session can be hijacked due to the vulnerabilities of this layer. Such attacks are known as Session Hijacking attack.

- **Session Hijacking:** The authentication of a node is verified only at the start of the session. Once the session has been established, no further authentication takes place. Attacker takes benefit of this vulnerability and tries to hijack the session. After the establishment of the session, adversary node snoops IP address of a legitimate node. Attacker impersonates the victim node and hijacks the session [9].

1.8.5 Application Layer Attacks

Non-repudiation is an essential requirement of the security protocols. Repudiation attacks are specific to application layer of network protocol suite.

- **Repudiation Attack:** Repudiation attacks are the denial of participation by node in any kind of communication. Once a node has sent the data it cannot deny this. Spoofing is used to carry out repudiation attacks. Adversary node copies the IP address of the node and then takes part in the communication by masking its IP [9].

1.9 Multi-layer Attacks

Some attacks are not specific only to a particular layer. They can be launched at any layer of the network protocol stack. Denial of service (DoS) and impersonation are common multi-layer attacks.

1.9.1 Denial of Service (DoS) Attacks

Blocking authorized users to use the services of the system for which they have right to access is called DoS attack. In MANETs, there is no central monitoring authority i.e. every node has similar access rights and processing power. This unique characteristic of MANETs makes it more vulnerable for attack like jamming attacks, sys flooding etc. If a large number of adversary nodes are distributed throughout the network and are blocking legitimate nodes from accessing the services then DoS attacks are termed as Distributed DoS attacks [5].

- **SYS flooding:** SYS packets are used to establish end-to-end connection at transport layer. Adversary node floods large number of SYS packets. Then victim node replies by sending ACK packet to respond these SYS packets. Afterwards adversary node spoofs the return address of SYS packet and then victim nodes wait for ACK from adversary. The legitimate node registers this half open connection in its routing table. Routing table gets overflowed by large number of such half connections. Although there is expiry limit for such pending connections after which these entries are flushed out. But new entries are registered so fast that they overflow the routing table. Victim node rejects new connection request even if it is from legitimate node [9].

1.9.2 Impersonation Attacks

Adversary node targets vulnerabilities of authentication mechanism for impersonation attacks. Adversary node steals the identity of the authorized users and it uses the services and resources of victim which are not meant for them. Adversary node can apply different mechanisms to obtain the identity of authorized nodes. Many of the impersonation attacks like man in middle attack, trust attacks, Sybil attacks etc. can be launched at any layer [13].

1.9.3 Device Tempering

Node can be damaged or stolen by the enemies. Such attacks come under the category of device tempering attacks [5].

1.10 Motivation

Ad-hoc Networks emerged as vibrant area in networking field. Easy deployment and self organizing without any infrastructure continues to attract the attention from industrial and academic research projects. Host as well as routing decision functionality by a node in Ad-hoc network makes uncertainty about the next hop in the communication which makes system very complex and distributive in nature. The basic feature like dynamic topology, wireless links, and operational environment makes MANETs vulnerable for attacks. The application areas like battle field, rescue operations and police services require security up to full extent and operate always in untrusted environment. The power, security and routing, the major key issues in Ad-hoc network, require additional care to make network robust. Many researchers have worked and are still working in area of energy and routing over past few decades, but not much work has been done to secure the network.

Although existing vulnerabilities draw the attention of researcher toward this area yet the research is mainly focused around routing i.e. how to find efficient path to route the packets. Still security is an unexplored area in Ad-hoc networks where large scopes of potential research exist. Among various attacks, wormhole is a particularly severe attack which is launched at the time of routing and it is difficult to detect. The goal of the research on wormhole attack is to detect it before it harms the network. In this context, this study focuses on the aspects of prevention of wormhole attack.

1.11 Problem Statement

In the detection of wormhole attack based on transmission time, the detection process is completely depends on the correctness of the Round Trip Time (RTT). The source computes RTT of the packets i.e. Route Request (RREQ) and Route Reply (RREP) between in the neighbors while the RTT of every node is calculated by the node itself. The intermediate nodes send back RTT to the source node. There are high chances of inserting false RTT information in RREP by the malicious nodes which in turn results in incorrect computation of RRT between the neighbors. Therefore, malicious nodes are able to hide themselves during detection process. Therefore, a more secure and efficient mechanism is required to preclude the malicious nodes so that they are not able to insert false information in RREP.

1.12 Objectives

- To modify the format of RREP packet and cache of neighbor node appropriately to store the information required for detection of wormhole attack.
- Apply the proposed scheme on the Dynamic Source Routing (DSR) Protocol with wormhole attack
- Simulate the behavior of the protocol using realistic scenario

1.13 Organization of Dissertation

The dissertation is organized in five chapters. Chapter 1 provides an overview of MANETs, network security issues and requirements. The description of Layer wise attacks is also given. The chapter also includes motivation, problem statement and objectives.

Chapter 2 gives brief overview of various wormhole attack detection models and their weaknesses.

Chapter 3 includes proposed model. First the existing transmission time based wormhole attack detection protocol is discussed in detail then the modifications are cited as suggested in the objectives.

Chapter 4 presents the experiments conducted and the results obtained.

Chapter 5 concludes the work carried out in the thesis along with discussions on possible future extensions.

Chapter 2

Chapter 2

Literature Review

A lot of threats and their countermeasures have been identified till now. In all possible threats in MANETs, wormhole attack is most critical and it is lunched at the time of route discovery phase. In this attack two malicious nodes located at different positions and form a secret tunnel. Through this tunnel one node bypasses routing packets towards other colluding nodes. This creates an illusion effect that there exists a shortest path for the destination. By using link, malicious node launches variety of attacks against the data flow such as selective dropping, reply attack, eavesdropping etc.

2.1 Classification of Wormhole Attacks

Wormhole attacks can be classified broadly into hidden and exposed attacks. In hidden attacks legitimate nodes are unware of malicious nodes but in exposed attacks they are aware of the fact that malicious nodes are forwarding packets. But they actually do not know that they are malicious nodes. Here, attackers neither modify packet header nor the content of the packet. The nodes forwards the packets only add its own MAC address in the header of the packet. So that the receiver will know the exact information about the sender of packets. In the Fig. 2.1, *S* want to establish a route to *D* using Ad-hoc On Demand Distance Vector (AODV) protocol. Then RREQ packet is broadcasted by the sender. If RREQ packet is received for first time, then receiving node updates the hop count information and puts its identity in the packet header.

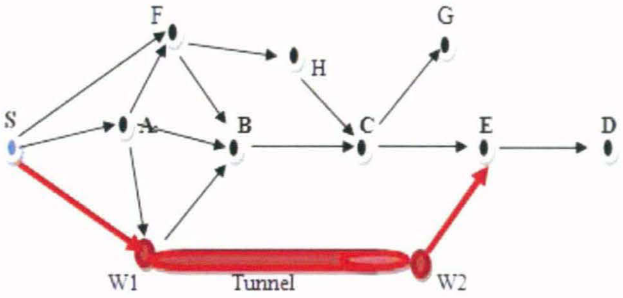

Fig. 2.1 Wormhole Attack [14]

Actual Path: S-A-B-C-E-D

In the hidden wormhole attack, malicious nodes don't upadate hop count field in packet header i.e. only legitimate nodes change the hop length during route establishment. As shown in Fig. 2.1, the actual hop count is 4 but it is shown as 2.

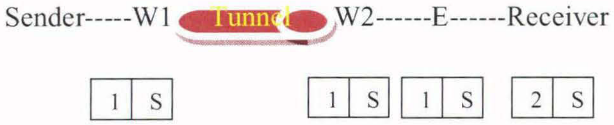

Fig 2.2 Hidden Wormhole Attack [15]

Path shown = S---E----R

In exposed wormhole attack, attacker updates the hop count field in packet header. In the Fig. 2.3, both W1 and W2 node updates the hop count by one and forward the packet. In this scenerio, legitimate nodes aware about existence of the wormhole, but they do not know they are malicius nodes [15, 16].

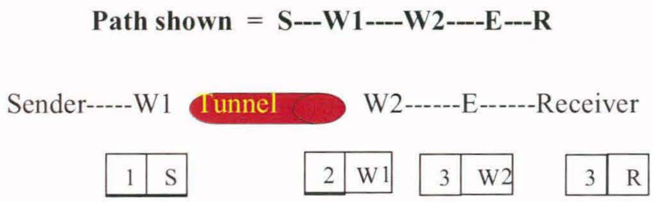

Fig. 2.3 Expose Attack [15]

2.2 Tunnel Model

Wormhole or tunnel can be formed either by packet encapsulated channel or out-of-band channel. The packet encapsulated channel is also known as In-band-channel. In this channel, malicious node captures the route message and puts it in data packet payload. This packet is transmitted using legitimate nodes towards other malicious node. The malicious node draws the routing message from packet payload and further braodcast it. Hop count is reduced between sender and receiver because of tunnel. The Secure AODVprotocol protects the routing messages and Authenticated Routing for Ad-hoc Networks (ARAN) authenticate each neighbour [17, 18].

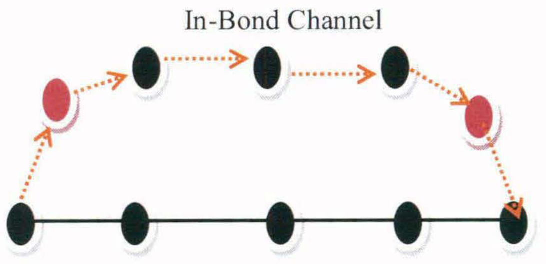

Fig. 2.4 In-Bond Channel Tunnel Model [17]

These are not sufficient to defend against attacks from an encapsulated channel.

While in Out-of-Bond channel, a special channel may be a direct wired link or a long range wireless link that exists between malicious nodes [17, 18].

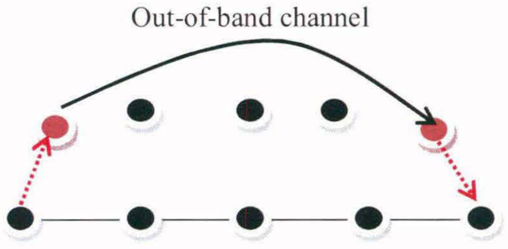

Fig. 2.5 Out-of-Band Channel Tunnel Model [17]

● Malicious node ● legitimate node

2.3 Related Work

All the previous proposed models either avoid or detect wormhole attacks by modifying the AODV protocol during route request phase. Otherwise, they require extra hardware and monitoring devices. Some of the models are described below.

2.3.1 Packet Leashes Model

A general mechanism to defend against wormhole attack is packet leashes. Leash is small amount of information that is added into a packet, which is designed to restrict a packet's maximum allowed transmission distance. The main purpose behind packet leash is to limit the transmission range to one hop. Here, node can be authenticated either by precise timestamp or location information combined with loose timestamp. A receiver can determine whether a packet has travelled an unrealistic distance. Leash can be geographical or temporal [15, 19].

In geographical leash, whenever any node wants to send the data packet then it inserts their location and sending time into the packet. To form geographical leash, every node should know their positions. Let the sender node location be denoted by l_s and sending time by t_s. . Both l_s and t_s are inserted in the packet to be sent. The receiver node compares these parameters with its location l_r and t_r (the receiving time). The maximum speed with which the packet can travel is the speed of light. In Ad-hoc environment nodes are moving with speed V and the clock is loosely synchronized, so let e be the error factor. Then the maximum distance that a packet can travel is

$$D_{ST} < \| l_s - l_r \| + 2\, V * | t_r - t_s + e | + \lambda \quad \text{....................} \quad (2.1)$$

After receiving packet, receiver will calculate the maximum distance between sender and itself. It also records its receiving time. If the distance exceeds the maximum limit then node discards the packet [19].

While in the temporal leash, a special off-the-shelf hardware based on LORAN-C [20], WWVB [21], is used in place of loose clock synchronization to provide tight time synchronization. Temporal leash talks about upper bound of its lifetime. When the source sends the packet then it inserts its sending time in it. The receiver receives the packet and records its time of receiving. Sending time and receiving time both are compared. On the basis of comparison, receiver observes the maximum distance travelled by the packet. Temporal leash are implemented through TESLA with Instant Key (TIK) disclosure protocol. TIK is an extension of TESLA broadcast authentication protocol. It requires accurate time synchronization. TIK is based on the symmetric key cryptography. Main drawback of packet leash mechanism is that it requires extremely tight time synchronization and Global Positioning System (GPS). It can neither identify the malicious nodes nor the exposed attacks [15, 19, 22].

2.3.2 Delay Per Hop Indication (DELPHI) Model

An approach based on delay analysis called DELPHI is used to detect wormhole attack. DELPHI model is capable to detect both kinds of wormhole attacks. It does not require clock synchronization, position information and any other special hardware equipment. Therefore, it consumes less power. It consists of two phases; in the first phase source node collects the information about hop count and delay of disjoint paths. Afterward, in the second phase the collected information is processed at source end and compute delay per hop. It is based on the principle that the packet travelled through wormhole experience more delay as compare to normal path. The DELPHI Request (DREQ) and DELPHI Reply (DREP) packet are used to find the disjoint path between source and destination. The source node broadcasts DREQ into network which is further forwarded by intermediate nodes same like AODV. Only the destination node is authorized to reply to DREQ packets. The time stamp field in DREQ is protected by signing message authentication code to maintain its integrity. On receiving DREP at source, delay per hop of every route is calculated. Delay Per Hop (DPH) is very large in case path contains tunnel as compared to normal path. Difference between delay per hop under normal condition and under wormhole attacks helps to detect the existence of wormhole. To improve the reliability, the process is repeated 3 times in order to collect better information. To identify the wormhole all collected DPH values are arranged in descending order. If the difference between DPH_j is greater than DPH_k by threshold value where I and K shows different path, then it shows the existence of wormhole. DELPHI approach does not work, in case all path results same delay per hop i.e. all route are tunneled. This mechanism is only capable of determining the existence of wormhole. The location of wormhole on the path cannot be identified through this approach [15, 23, 24].

2.3.3 WARP: Wormhole Avoidance Routing Protocol

Another recent work related to wormhole attack is WARP based on AODV. WARP uses the concept of multi-path routing algorithms. Therefore, WARP keeps multiple link disjoint paths into consideration during route discovery phase and eventually use only one path for data transmission. The malicious nodes have great tendency to get involved in the path discovery process. Thus malicious nodes try to get involved in every disjoint path between source and destination. WRAP uses this characteristic of malicious nodes to detect the wormholes attack. Four major modifications are done in basic AODV protocol to implement WRAP. First, a new "First Hop" field is added in RREQ frame format of AODV for obtaining disjoint paths. Second, the functions of HELLO packet are changed. In AODV protocol, HELLO packets are used to keep the record of neighbors of a node during all the time. Every node continuously receives HELLO packets from its neighbors after a regular interval of time. If node does not receive HELLO packet from any particular node for a long time then the entry for that node is flushed out from its routing table. While in WRAP protocol if a node receives HELLO packet from any node it will record the entry of that node in its routing table and accordingly modifies routing table. Third, in order to collect the information of intermediate nodes, a new concept of Decision Route Reply Message (RREP_DEC) is applied, which is sent through the established route. Fourth, the format of routing table is modified to accommodate these changes. The anomaly value of every node, that is part of any disjoint path, is calculated on the basis of the information collected through RREP_DEC.

The probability of involvement of a node among the multi joint path is known as its anomaly value. It is defined as

$$(\text{Anomaly value})_x = (\text{Number of RREP\_DEC })_x \,/\, ((\text{Number of RREP})_x + 1))..\ (2.2)$$

Each node records anomaly value of its neighboring node. If the anomaly value of a particular node exceeds the threshold value, then its neighbor declares it as a malicious node and discards all the requests coming from that node to form a route. A legitimate node at the key position in the network has to participate in many paths. This results in high anomaly value of that node. Therefore, there are high chances that such legitimate nodes may be considered as malicious and isolated by their neighbors. But the topology of the network is always dynamic in nature therefore after some time its anomaly value decreases and will be considered a legitimate node again [17, 25, 26].

2.3.4 LITEWORP: Light Weight Counter Measure for Wormhole Attack

One of the popular protocols is LITEWORP in Wireless Networks which uses the concept of guard node. Many local nodes are used for local monitoring and they are called guard nodes. Guard node is a common node on the link between two nodes to monitor their behavior. If one of its neighbors behaves abnormally then guard node declares it as malicious node. LITEWORP uses secure two-hop neighbor discovery and local monitoring of control traffic to detect nodes involved in the wormhole attack. It provides a countermeasure technique that isolates the malicious nodes from the network. Therefore, guard nodes block their ability to cause damage in the future [18, 23].

2.3.5 WHOP: Wormhole Attack Detection Protocol using Hound Packet

WHOP is a new mechanism to detect the wormhole without using any hardware support such as directional antenna and précised synchronized clock. It can detect the wormhole attack as well as the malicious nodes forming wormhole in the network. It is based on AODV protocol. Like other protocols, WHOP does not use the nodes that are part of the route. On the other hand, WHOP takes help of remaining nodes that are involved in route discovery process. The route from source to destination is established using AODV protocol. Source node broadcasts AODV RREQ packet to its neighbors. If the neighbors have a route to destination then they prepare RREP packet, otherwise they broadcast RREQ packet again after registering the entry in their table. The RREP packet is unicasted back to the source either by any intermediate node having route to destination or by destination itself.

Type	Flag	Reserved	Total Hop Count
Destination IP Addr			
Destination Sequence Number			
Source IP Addr			
Source Sequence Number			
Addr[n-1]	Processing Bit	Count to reach Next Hop	
Addr[n-2]	Processing Bit	Count to reach Next Hop	
Addr[2]	Processing Bit	Count to reach Next Hop	
Last Hop			

Fig. 2.6 Format of Hound Packet in WHOP

The format of the RREP packet is modified by adding new field to store the identity of all nodes on the route. WHOP modifies the function of HELLO packet from what it used to be in AODV. HELLO packet is used to share the public key of a node among its one hop neighbors. If a node receives a

HELLO packet and does not find corresponding entry in its routing table then node registers an entry in its routing table as its neighbor. Thus any new node introduced in network gets the information of all its neighbors through HELLO Packet. Once the route has been established then source node prepares hound packet which contains entries of all nodes that are members of the route. Source node computes Message Digest (MD) of hound packet and signs MD with its own private key. Hound packet is broadcasted into the network. Each node checks its IP address in the hound packet. If node finds its IP address in hound packet then it simply forwards the hound packet, otherwise it will process the hound packet. Malicious nodes have the tendency to get involved in every packet forwarding process. Therefore, they will try to involve in forwarding process again. The hound packet arrives at the destination node and that node will processes this hound packet. After the processing of hound packet, the destination node announces whether route is safe or under the wormhole attack [17, 19, 23].

2.3.7 End-to-End Detection of Wormhole Attack (EDWA)

A location based end to end wormhole detection mechanism calculates "minimum hop count" from every node to the destination. EDWA mechanism is so strong that it can detect the presence of wormhole attack on the path as well as the end points of the wormhole. After the identification of the wormhole end points, information is broadcasted to inform other nodes regarding these malicious nodes. The EDWA can work with both AODV and DSR routing protocols with a constraint that only destination node can reply to the RREQ packet. It assumes that each node is capable of identifying the geographical location either through GPS or Global Navigation Satellite System (GNSS) [27, 28].

The routing protocol is modified to detect the wormhole. The RREQ packet is broadcasted into network through same mechanism as used in any existing protocol such as AODV or DSR. RREQ packet travels to establish route to destination. Eventually, RREQ packet reaches to the destination and destination responds to it by sending RREP packet. Some additional fields are attached in the frame format of RREP packet to get the necessary information for the detection of wormhole. The position coordinates of destination node are inserted into RREP packet. Based on the position of source and the destination, source node calculates the shortest path in terms of hop length. Let the source node estimate hop count value to be h_e. The sender retrieves value of hop count h_r inserted by destination into RREP packet during route discovery. Both these values are compared. If $h_e > h_r$ then it is assumed that there is wormhole somewhere on the path [27, 28].

After the detection of the wormhole existence on the path, mechanism to identify the end points is triggered by the source node.

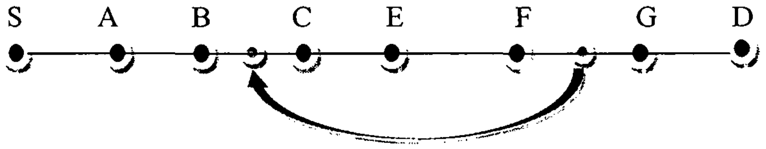

Fig. 2.7 Wormhole Tracing in EDWA

The source node prepares a TRASH packet and sends it along the path established during path discovery. Every intermediate node receiving TRASH packet will respond to source node by sending their current position and forwarding the TRASH packet to the next node along the path. After obtaining the position coordinates through TRASH RESPONSE packet, sender starts calculating the hop count between source and each intermediate node.

S	A	B	G	D
Received route length (Hop Count)	1	2	3	4
Estimated route length (Hop Count)	1	2	6	7

Table 2.1 Comparison of Received and Estimated Hop Count in EDWA

As the TRASH packet approaches towards destination node through intermediate nodes the hop count is increases. If the large increment (more than one) is observed in hop count between any pair of neighbors, then it shows that this pair of nodes comprises the end points of the wormhole. As shown in Fig. 2.7, there exists a wormhole between B and G. Therefore, Table 2.1, based on the end to end mechanism, shows an extreme increment in the hop count between B and G. The EDWA mechanism performs better when the source and destination are not far away.

Chapter 3

Chapter 3

Novel Transmission Time based Mechanism

The Transmission Time based Mechanism (TTM) to detect the wormhole attack proposed in [20] is evaluated with Ad-hoc on demand distance vector routing protocol (AODV). It relies on the round trip time (RTT) experienced by packet. The RTT is calculated on the basis of RREQ packet broadcast time and RREP packet receiving time by the node itself. In Novel Transmission Time based Mechanism (NTTM), TTM is optimized using Dynamic source routing (DSR) protocol with some modifications.

3.1 Transmission Time Based Mechanism to detect the Wormhole Attack

An efficient wormhole attack detection model based on time stamps is known as Transmission Time Based Mechanism (TTM) use Round Trip Time (RTT) of packets between each neighbor. It detects wormhole attack launched on AODV routing protocol. It is based on the concept that the RTT between malicious nodes forming wormhole is comparatively high than the legitimate nodes. The RTT value between each pair of legitimate node is almost same. Although there is minor difference between RTT values of the neighbors when one or both are at key position in the network but this difference is much smaller as compare to threshold value. TTM is tested over the AODV protocol with some modification. The format of RREQ packet is same as used in AODV protocol. The route discovery process is initiated when a node wants to send some data. The source node broadcasts a RREQ packet in to the network. If RREQ packet is received for the first time then each intermediate node inserts its node identity in RREQ packet as shown in Fig. 3.1 otherwise discards the packet.

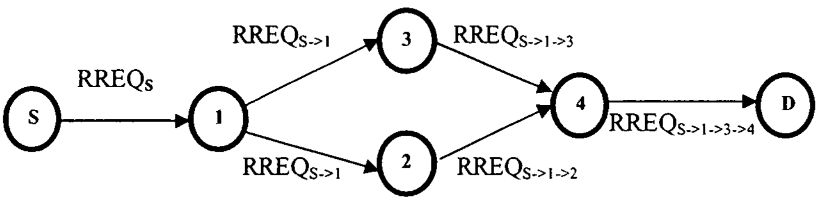

Fig. 3.1 Route Request in DSR

The intermediate nodes are further broadcast RREQ packets and keep the record of RREQ sending time in their route cache until RREP packet received [24, 26].

3.1.1 Route Reply by the Destination

When RREQ packet reached at destination, the destination node triggers the route reply mechanism. The destination node capture the information about the number of hops RREQ travelled. The destination node modified the RREP packet format of normal AODV by adding an extensional part. The size of extensional part is according to hop count field in RREQ packet. When RREP packet is received at intermediate nodes, they calculate RRT between destination and itself. The RTT is inserted in extensional part which must be sufficient to store the all RTT values calculated by each node on the path [24, 29].

3.1.2 Computation of RTT

Each node keeps recorded the time of sending RREQ packet. While receiving RREP packets every node records its receiving time before further processing. The value of RTT between node and destination is computed according to the equation-3.1 [24].

$$(RTT)_{x,d} = abs((RREQ\ Time)_x - (RREP\ time)_x) \ldots\ldots\ldots\ (3.1)$$

The value of RTT between each neighbor nodes on the path is computed according to equation 3.2.

$$(RTTneighbors)_{x\,y} = abs((RTT)_{x,d} - (RRT)_{y,d}) \ldots\ldots\ldots\ldots\ (3.2)$$

Where

$(RTTneighbors)_{x\,y}$	Time between any two neighbors **x** and **y** on the same route
$(RREP\ Time)_x$	Time of receiving RREP packet at any node **x**
$(RREQ\ Time)_x$	Time of sending RREQ packet from any node **x**
$(RTT)_{x,d}$	Round trip time at any node x and destination
Abs(x - y)	Absolute difference between **x** and **y**

Let us consider a path established during route discovery in any network.

S---1---2---W_1---W_2---D

The table 3.1 shows the timing record of broadcasting RREQ packet as well as receiving RREP packets. The computation of RTT for each node is also shown in table 3.1

Nodes	RREQ sending Time ($T_{(RREQ)}$)	RREP receiving Time ($T_{(RREP)}$)	RRT time of node = ($T_{(RREP)}$) - ($T_{(RREQ)}$)
S	0	33	33
1	2.5	30.5	28
2	4	28	24
W_1	7	25	18
W_2	14	18	4

Table 3.1 RREQ and RREP Record in TTM

The timing diagram shows the travelling of the RREQ and RREP packet between source and destination node.

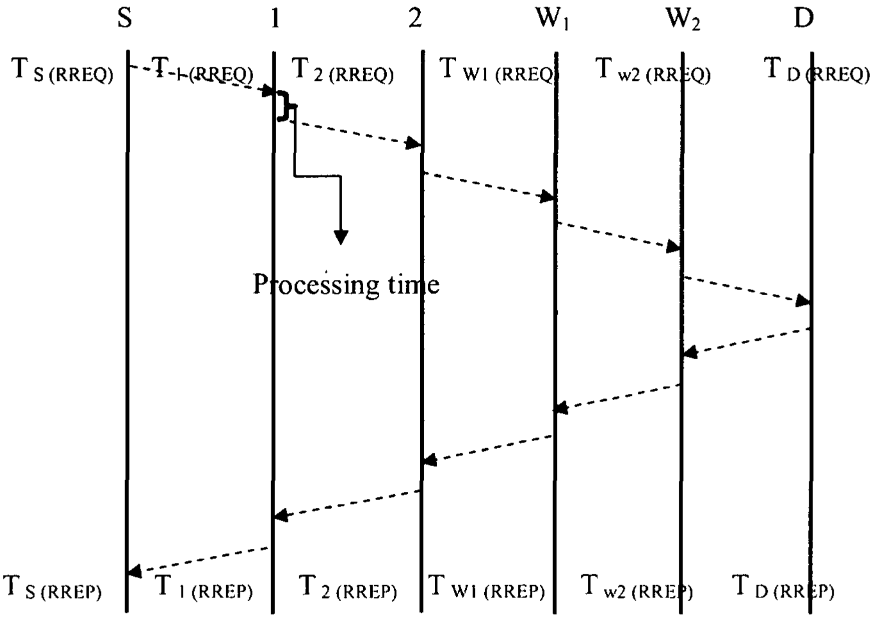

Fig. 3.2 Route Discovery Timing Diagram [16]

Each node inserts RTT values in the extensional part of RREP packet and sends to the source. Thus source get the information regarding the RTT time of each node. Now the source node starts wormhole attack detection process and calculates RTT time between each neighbor on the path using equation 3.2 [16, 29].

$(RTT)_{x\,d}$	$(RTT)_{y,\,d}$	$(RTTneighbors)_{x\,y}$
33	28	5 (RTT_{S1})
28	24	4 (RTT_{12})
24	18	6 (RTT_{2W1})
18	4	14 (RTT_{W1W2})

Table 3.2 RTTneighbors Computation in TTM at Source Node

3.1.3 Detection of Wormhole Attack

The value of RTT between the "fake neighbors" is much higher than the value between real neighbors. The nodes which are not real neighbor i.e. not in the transmission range of each other but presence of wormhole makes them feel that they are neighbors, are considered as "fake neighbor". In table 3.2, an average RTT between each pair of node is 5 but it is 14 between W_1 and $W_{2,}$ which shows the aberrant behavior between these nodes. We consider this aberrant behavior as Wormhole attack. Therefore, if RTT value between any pair of neighbor's nodes exceeds the threshold time limit then it shows the existence of the wormhole on the route. The threshold time value is considered on the basis of simulation environment and parameters. The performance of above mechanism depends upon the fact that how much accurately the calculation of RTT is done by individual nodes. Therefore, for improved results experiments are repeated many times although it increases the overhead. Thus there is always trade of between accuracy and overhead. As the calculation of RTT time is done by individual node itself and inserted in RREP packet. Therefore, the chances of inserting false information in RREP packet by malicious nodes are extremely high. In such situation this scheme will not be capable to detect wormhole and consequently overall performance of the network degrades [16, 24, 29].

3.2 NTTM Model

The TTM mechanism showed good performance with respect to bandwidth utilization and can detect the wormhole before it makes any harm to the network. But there is scope to improve RTT mechanism for the better accuracy and results. The proposed a model known as (full form) Novel Transmission Time based Mechanism (NTTM) model. The DSR protocol works well even under high mobility of node even though it requires extra memory as compare to other protocols like AODV. Therefore, NTTM model is tested with DSR. Even though some additional features are included in DSR protocol yet fundamental concepts of route discovery and route reply remains intact.

3.2.1 NTTM Algorithm

1. *If a node wants to send a data then node initiates route discovery process.*
2. *The Source node will generate RREQ and put its own IP address into Record Route List (RRL) option in RREQ packet as an originator.*
3. *Source node broadcasts RREQ packet and store T_{RREQ} (time of broadcasting RREQ packet).*
4. *Each node in the transmission range of sender node receives RREQ packet.*
5. *If a node receives a packet with same source ID, broadcast ID and hop length greater or equal than already received packet, then drop the packet.*
6. *Otherwise node receiving RREQ matches destination (target) IP address*
7. *If target IP address matched with receiver IP address then go to step 15.*
8. *Otherwise each neighbor node starts checking RRL.*
9. *If IP address at (N-1) th position in RRL matched with receiver IP address.*

   // where N is the number of addresses stored in RRL in RREQ packet at any time T.

10. *If receiver node satisfies condition in step 9, then stores T_{RREQ} and drop the packet.*

    // neighbor node hear RREQ broadcasting of other nodes.

11. *Otherwise node continuously further searches RRL.*

12. *If node receiving RREQ packet, IP address matched at other position in RRL, then drop RREQ packet.*

13. *Otherwise receiver node appends its address at tail of RRL in RREQ packet and broadcast it further.*

14. *Repeat the step 4 to 13 for each intermediate node till destination.*

15. *When the RREQ packet arrived at destination.*

16. *Destination generate RREP packet to respond RREQ packet.*

17. *The RRL is reversed and copied into RRL of RREP packet.*

18. *An extensional part is added into basic DSR RREP packet by destination.*

    // To store RTT calculated for each node on the route by its neighbor.

19. *Destination unicasts RREP packet along reversed RRL.*

20. *Next node in RRL will receive RREP packet.*

21. *If receiver node IP address is at 2nd position in reversed RRL (RREP RRL) or second last on RRL of RREQ, then store $(T_{RREP})_x$ (Time of receiving RREP at any node X) at appropriate position in extensional part of RREP and forward the packet further.*

    // Receiver node is just before the destination node.

22. *Otherwise if node addressed at k^{th} position on reveres RRL, receives RREP packet, then receiver extracts T_{RREP} from extensional part.*

23. *Then receiver calculate RTT of neighbor at (k-1)th position on reverse RRL or at (k+1)th position on RRL of RREQ using T_{RREQ} stored in step 10 and T_{RREP} extracted by receiver from extensional part i.e. equation 3.1.*
24. *Stores RRT of corresponding neighbor at position from where T_{RREP} extracted.*
25. *Repeat steps 20 - 24 till RREP reached at source.*
26. *When RREQ packet arrived at source then source repeat step 23, 24 one time and calculate RTT value of its neighbors node on the route.*
27. *Now source will extract RTT value of each node from extensional part and calculate RTT between each neighbor node on the route using equation 3.2.*
28. *If RTT value between neighbors is more than threshold value then source declares the existence of wormhole on the route.*

3.2.2 Route Discovery

In Fig. 3.3, node *S* wants to send the data to node *D*. The sending node *S* triggers route discovery and broadcasts a RREQ packet into network. The source node stores T_{RREQ}. Each RREQ packet contains address of sender, receiver as well as broadcast ID. The broadcast ID in RREQ packet is used to discard the duplicate packets received at a node.

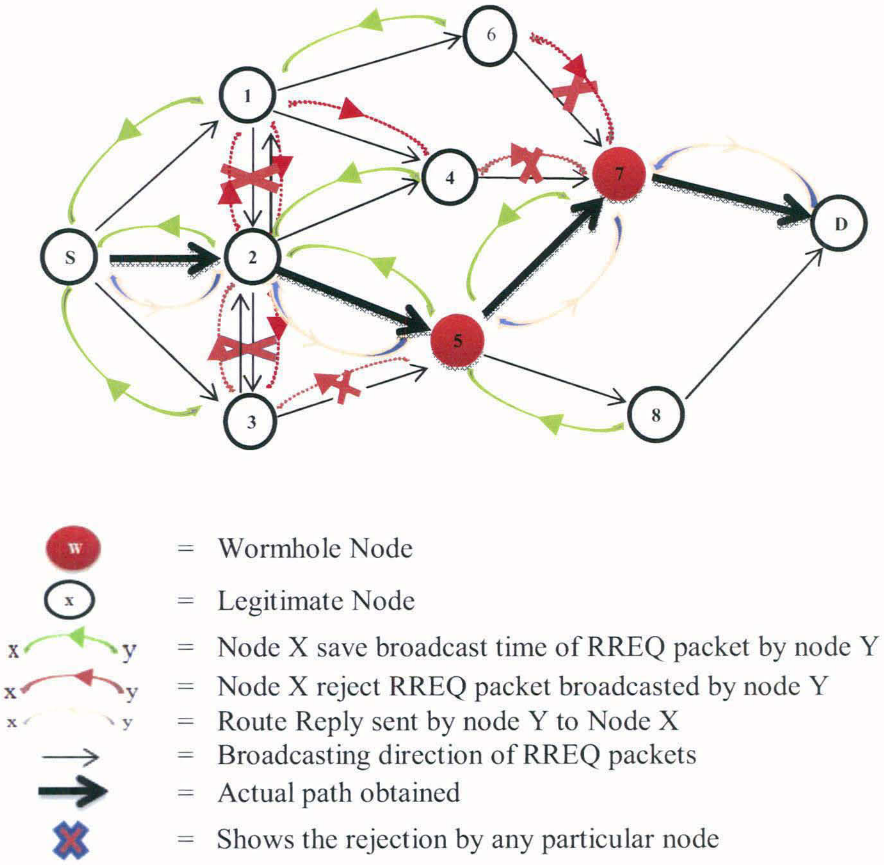
6
1
4
7
S
2
D
5
3
8
W
= Wormhole Node
x
= Legitimate Node
x y
= Node X save broadcast time of RREQ packet by node Y
x y
= Node X reject RREQ packet broadcasted by node Y
x y
= Route Reply sent by node Y to Node X
= Broadcasting direction of RREQ packets
= Actual path obtained
= Shows the rejection by any particular node

Fig. 3.3 Route Discovery in NTTM

Node 1, 2 and 3 receive RREQ packet broadcasted by node S. Each Node match destination address recorded in RREQ with its IP address according to step 6. None of them (1, 2, and 3) is destination, so they will process the

RREQ packet and put their IP address in RRL. They rebroadcast the RREQ packet in to network. The node *S* hears the RREQ packet again as shown in Fig. 3.3 and find its address at (n-1)th position in RRL according to step-9 . Therefore, store T_{RREQ} of each node and drop the packet step10.

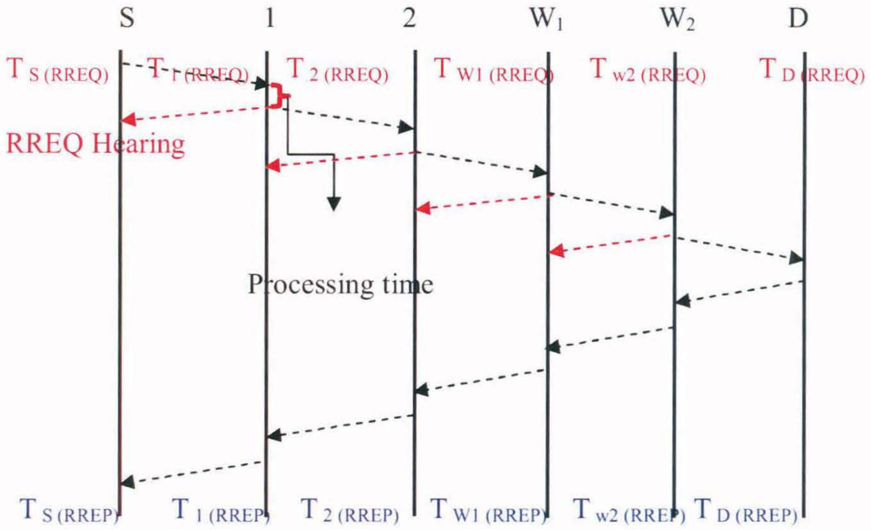

Fig. 3.4 Timing Diagram of Hearing of RREQ in NTTM

At node 4 two RREQ is received through node 1 and node 2. Suppose RREQ broadcasted by 2 reaches first at node 4, then node 4 will discard RREQ packet (step 5) broadcasted by node 1 because of duplication (broadcast ID, originator ID). Similarly, node 5 receives RREQ packet from node 3 and node 2 and RREQ through 2 received first. Both of the nodes execute step 6. They are neither destination nor the RREQ packet has their address in RRL. So they will append their address in RRL tail and broadcast again. Now node 2 satisfies the condition of step 9 for both node 4 and 5. Hence, node will store T_{RREQ} of the both nodes. A node stores T_{RREQ} by neighbor of a particular node till T_{RREP} received at that particular node. In this way RREQ packet will reach at destination node D after moving through the intermediate nodes (2, 5, and 7). Thus the route established is

S ----- 2 ----- 5 ----- 7 ----- D

Now destination node responds RREQ by generating RREP. Node D copies the RRL in RREP packet and attaches an extensional space to record the RRT between each neighbor on the route. When RREP packet is unicasted back then node 7 will receive it. Node 7 satisfies the condition mentioned in step 21 and simply put the time of receiving of RREP T_{RREP} at the corresponding space in RREP packet without any computation. When the RREP packet proceeds further according to RRL, it will be received by node 5. Node 5 could not meet step 21, so it will extract $(T_{RREP})_7$ *i.e.* Time of receiving RREP at any node *7* from extensional part in RREP. The RTT of its neighbor 7 calculated using equation3.1 by node 5 (through step 22 to 24 of algorithm) and put it back at the place from where $(T_{RREP})_7$ was extracted. Similarly each intermediate node repeats steps from 20 to 24 till RREP packet reached back at source.

3.2.3 Computation of RTT in NTTM

The NTTM enforced to change normal TTM by shifting the calculation of RTT for a particular node from itself to its neighbor. Each node extracts T_{RREP} of its neighbor from extensional part and after the calculating RTT inserts back RTT in place of $T_{RREP.}$ Here, we have assumed that the time at which RREQ sent by a particular node is same as time of hearing the broadcast of RREQ by its neighbor.

Nodes	Node Hearing RREQ Broadcast	RREQ Hearing Time ($TH_{(RREQ)}$)	RREP receiving Time ($T_{(RREP)}$)
S	S	-	30
2	S	2.5	27
5	2	5.5	23
7	5	13	15.5
D		-	-

Table 3.3 RREQ and RREP Time Record in NTTM

Nodes	Node Calculating RTT	RREQ sending Time ($T_{(RREQ)}$)	RREP receiving Time($T_{(RREP)}$)	RRT of node = ($T_{(RREP)}$) - ($T_{(RREQ)}$)
S	S	0	29	29
2	S	2.5	26	23.5
5	2	5.5	23	17.5
7	5	13	16	3

Table 3.4 Computation of RRT of Each Node in NTTM

Now the RTT between each neighbors is calculated same as calculated in TTM (by using equation 2)

$(RTT)_{x\,d}$	$(RTT)_{y,\,d}$	$(RTTneighbors)_{x\,y}$
30	24.5	5.5 ($RTT_{S\,2}$)
23.5	17.5	6 ($RTT_{2\,5}$)
17.5	3	13.5 ($RTT_{5\,7}$)

Table 3.5 RTTneighbors Computation in NTTM at Source Node

The transmission time between node 5 and node 7 is comparatively very high. Therefore, wormhole attack is considered between node 5 and node 7

Chapter 4

Chapter 4

Simulation and Experimental Evaluation

In this chapter the performance of proposed NTTM model in real world environment is evaluated through simulation. The simulation is the process to create an illusion that model is operational in real world environment.

4.1 Simulation Environment

- **QualNet 5.0.2**

  QualNet is a comprehensive suite of tools for simulating large networks whether it wired and wireless. It helps to improve the performance of network by creating an illusion of real world scenario. It supports real-time speed to enable software-in-the-loop, network emulation, and hardware-in-the-loop modeling [29].

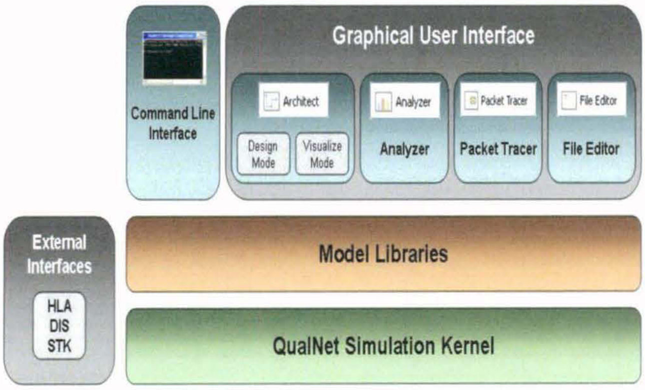

Fig. 4.1 QualNet Architecture [29]

It supports parallel computing and can run on cluster, multi-core, and multi-processor systems to model large networks with high fidelity. QualNet 5.0.2 and its library of models can run on a various platforms, including Windows XP, Mac OS X, and Linux operating systems. It supports both 32- and 64-bit computing platforms. It provides the facility of Graphical user interface as well as command line interface [29].

- **Network Simulator Parameters**

The wormhole "All Pass" model in QualNet 5.0.2 Network Simulator (NS) was used to launch wormhole attack. During the simulation, many parameters were kept constant to observe better accuracy of results. The simulation parameters considered are listed in Table. 4.1

Parameters	***Value***
Simulation Time	*1000sec*
Simulation Repetition	*100*
Routing protocol	*DSR*
MAC Layer	*802.11*
Packet Size	*512 bytes*
MAC Protocol	*802.11*
Data Rate	*2Mbps*
MAC propagation delay	*1 μs*
Terrain Size	*1500 x 1500*
Network layer protocol	*IPv4*
Mobility Model	*Random waypoint*
Data Traffic Type	*CBR*
Maximum buffer size for packets	*50 packets*
Antenna Model	*Omnidirectional*
Antenna Height	*1.5metres*
Noise Factor (SNR)	*10.0*
Transmission Power	*15dBm*
Transmission range	*367metres*

Table 4.1 Network Simulator Parameters

- **Assumptions**

It is assumed that the time of receiving RREQ packet at node (who will calculate RTT) is same as the time of broadcasting RREQ packet by its neighboring node for which RTT is calculated. All nodes are working in promiscuous mode. The network diameter of the network is small.

4.2 Simulation Results

The simulation was carried out for duration 1000s and repeated for 100 times for each parametric value. The simulation results were recorded in text file and graphs were generated using Microsoft Office Excel 2007. From the statistics file we have computed average value Packet Delivery Ratio (PDR) and throughput for different scenarios.

S. No	Node Density	Node Mobility	Tunnel Length	Malicious Nodes
Scenario 1	50	5,15,25,35,45, 55,65	2-8	2
Scenario 2	10,20,30,40,50	0-10	2-8	2
Scenario 3	50	0-10	2,3,4,5, 6,7,8	2
Scenario 4	50	0-10	0-8	2

Table 4.2 Parameters Changed during Simulation

Scenario 1: The scenario was created using the parameters shown in Table 4.1. The scenario is tested within same environment by changing parameters in Table 4.2.

The trend is observed through the line graph between node's speed verses PDR. The DSR, DSR under the wormhole attack and NTTM under wormhole attack were compared in term of PDR and throughput by varying node mobility.

Under the wormhole attack, PDR value decreased consistently as compared with DSR protocol. The NTTM model improved the results as shown in Fig. 4.1. It showed maximum growth in PDR of 11% at the mobility rate 35m/s while the worst performance was observed at mobility rate 25m/s where the growth in PDR was only approximately 6%.

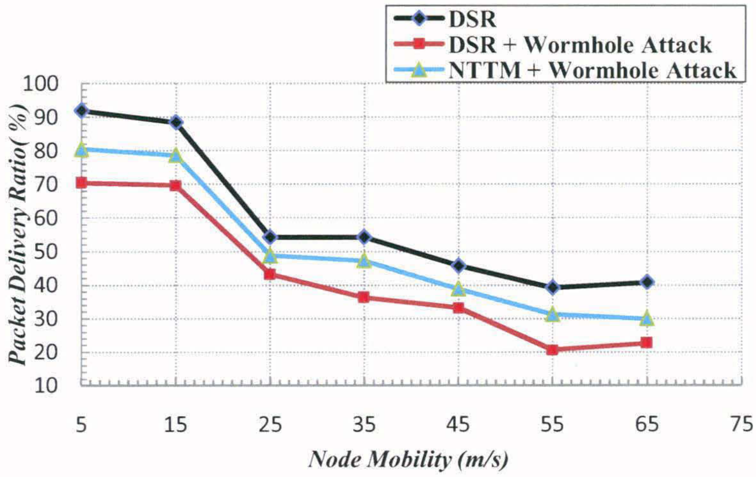

Fig. 4.1 Packet Deliver Ratio verses Node Mobility

The same pattern was observed for throughput when NTTM is applied. As shown in Fig. 4.2 NTTM showed maximum growth in throughput is at speed of 35m/s.

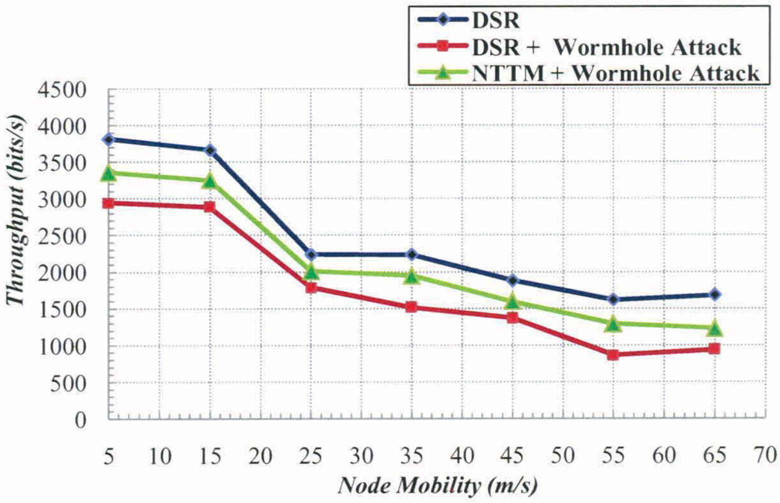

Fig. 4.2 Throughput verses Node Mobility

It is approximately 20% while minimum growth was at speed of 25m/s which is only 10%.

On increasing the speed of the nodes, the topology changes very rapidly. Due to this, it is difficult to build new routes and also the frequency of route breakage increased. Therefore, the PDR as well as throughput decreases with increase in the speed of nodes. The PDR and throughput both initially fell rapidly. But with the further increment in speed, route breakage was going to be saturate. Thus both metric values fell relatively low. From the results, it is evident that the NTTM model performed better in the same environment. It showed a significant growth in PDR and throughput value. On average, NTTM achieved increment of 9% in PDR and 15% in throughput as compared to DSR protocol under the wormhole attack.

Scenario 2: The scenario was created using parameters in Table 4.1.The Table 4.2 showed the parameters those were changed.

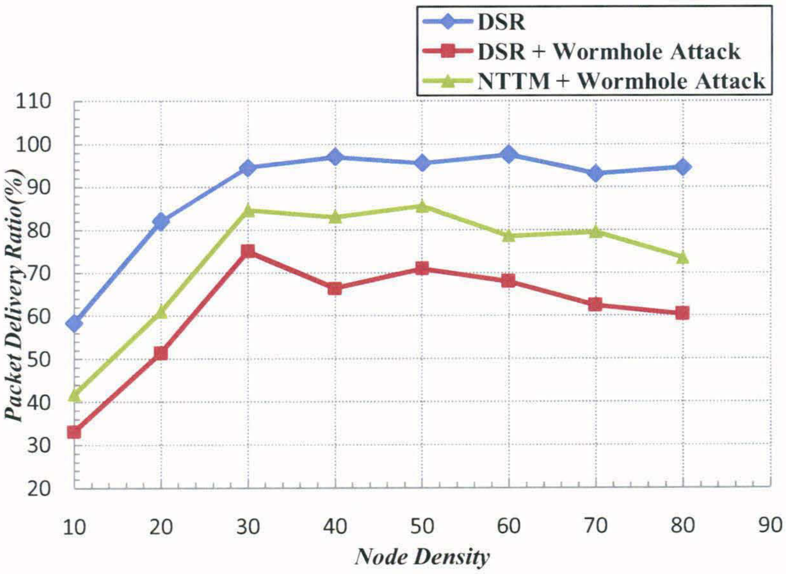

Fig. 4.3 Packet Deliver Ratio verses Node Density

Under wormhole attack with different node density, the PDR value as well as throughput decreased as expected theoretically by 29% and 32% (on average) respectively. When NTTM model applied and wormhole attack was launched then NTTM achieved its best performance at node density 40where NTTM model increased PDR value by 16% as compared to DSR under wormhole attack as shown in Fig. 4.3. At node density 10, NTTM showed its poorest performance where it increased PDR value only by 8% approximately.

The Fig. 4.4 showed NTTM performance in term of throughput. The similar pattern matched with PDR as it showed best and worst performance on node density 40 and 10 respectively. The maximum growth in throughput is 17% while the minimum is 13%. On average, NTTM achieved 13% increment in PDR while 14% in throughput as compared to DSR under wormhole.

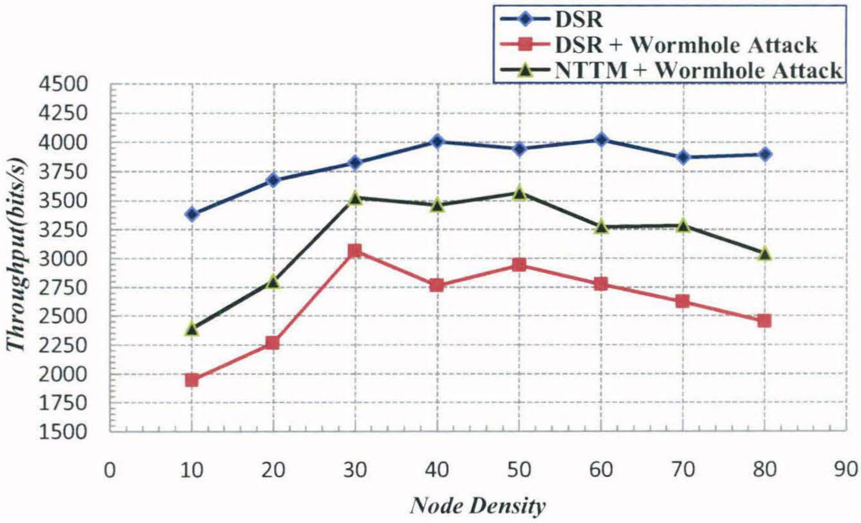

Fig. 4.4 Throughput verses Node Density

Due to low nodes density i.e. 10, there was connectivity problem because nodes were spread in large area. Therefore, nodes were not within the transmission range of each other. As the node density rose up then it leads to better connectivity between the nodes. Therefore, the PDR as well as throughput increased. If the node density is further increased, although connectivity between nodes improved but more route breakage occurs due to large number of collisions. It also makes it difficult to establish new route due to collision. Thus the PDR and throughput showed a little up and down after node density 40.

Scenario 3: Two malicious nodes were chosen to launch wormhole attack with different tunnel length. The NTTM model was applied to measure its detection rate. The detection rate increased exponentially with respect to tunnel length up to 5 hops. NTTM showed 100% detection as the tunnel length exceeds 6 hops. With increment in the tunnel length, the RTT between malicious nodes also increase. In the scenario without wormhole attack, the average RTT value between neighbours was 14ms under NTTM model.

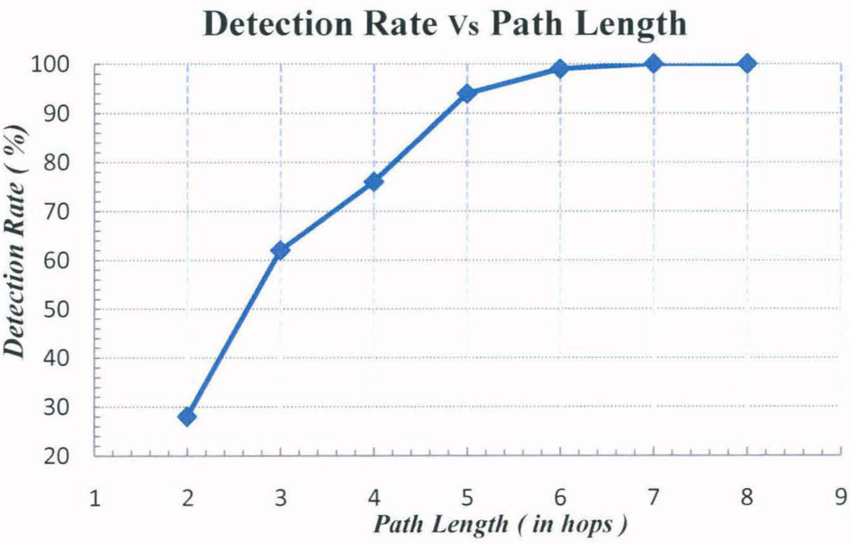

Fig. 4.5 Detection Rate in NTTM

The RTT between fake neighbours increased with increment in the hop length between them. Thus RRT value between fake neighbours exceeded the threshold value. More the tunnel length more will be RTT value. Therefore, wormhole attack detection rate improved with increment in the tunnel length.

Scenario 4: Threshold value played an important role in NTTM model. To determine threshold value, the threshold value picked up with respect the RTT between real neighbours and then incremented further. If the nodes were at critical in the network, then nodes experienced large delay could be considered as malicious nodes. Thus, low threshold value result in high false positive. While at high threshold value the wormhole attack launched with small tunnel length were undetected and slowly damage the network, therefore false negative increases. The detection accuracy graph showed an extreme increment after 25s and achieved best detection accuracy at 35s as shown in Fig. 4.6. At 35ms, both false positive and false negative were low, therefore, 35ms were chosen as threshold limit value..

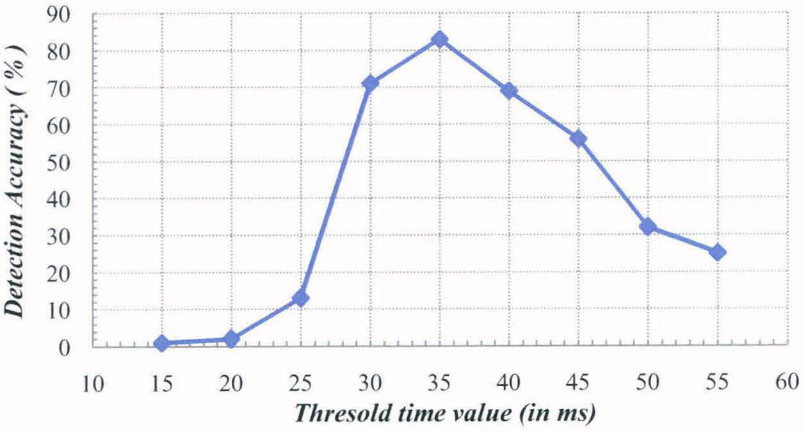

Fig. 4.6 Detection Accuracy of NTTM

4.3 Comparison of Assumptions and Accomplishments with other Protocols

Name	Based on	Extra Hardware	Clock synchronization	Monitoring by neighbour	Detection of Wormhole node
Packet Leashes	AODV	No	Yes	No	No
EDWA	AODV	Yes	Yes	No	Yes
WARP	AODV	No	No	Yes	Yes
WHOP	AODV	No	No	No	Yes
LITEWORP	DSR	Yes	Yes	Yes	Yes
DelPHI	AODV	No	No	No	No
NTTM	DSR	No	No	Yes	Yes

Table 4.3 Comparison with other Protocols

Chapter 5

Chapter 5

Conclusion and Future Work

5.1 Conclusion

The study regarding the wormhole attack leads us to draw the conclusion that Wormhole attack is most dangerous attack in MANETs. It can be launched easily even in the network with confidentiality and integrity. By identifying the wormhole attack during route discovery, NTTM avoids the chances of damages in the network due to attack.

A comparative study of scenarios with varying node's speed, node density, tunnel length and threshold time value were taken into consideration. When DSR protocol compared with DSR under wormhole attack by varying speed of nodes, it was observed that PDR and throughput on average falls by 17% and 28%. Further, NTTM was applied which results in growth of PDR and throughput on average by 9% and 15% respectively. With respect to varying node density, NTTM increased the PDR by 12% and throughput by 14% (on average) as compared to DSR under wormhole attack. With the increment in tunnel length, the detection rate too grew exponentially. When tunnel length exceeds 5, detection rate approached to approximately 100%. The maximum detection accuracy of NTTM was observed at 35ms, therefore it was taken as optimal threshold time value.

5.2 Future Work

It is very difficult to develop a foolproof model to defend against the malicious activities. Due to time factor, the model was developed with some assumptions. In future, the difference between the sending time of RREQ packet and receiving time of RREQ packet at its neighbor can be taken into consideration which was assumed negligible in NTTM. NTTM can be implemented over other routing protocols like TORA, DSDV etc.

References

References

[1]. Humayun Bakht, "Wireless Infrastructure: The History of Mobile Ad-hoc Networks",http://www.computingunplugged.com/issues/issue200508/0000 1598001.html, October, 2011

[2]. Wireless Ad-hoc Technology, http://www.atacwireless.com/adhoc.html, October, 2011.

[3]. R. Ramanathan and J. Redi, *A brief overview of Ad-hoc networks: challenges and directions,* IEEE Communications Magazine **50th** Anniversary Commemorative, Vol.40, No 5, pp. 30-32, May, 2002.

[4]. J. Freeberyser and B. Leiner, A DoD Perspective on mobile Ad-hoc Networks, Addision-Wesely Longman Publishing Co., Inc. Boston, MA, USA, pp. 29-51, 2001.

[5]. C. Siva Ram Murthy and B.S. Manoj, *Ad-hoc Wireless Networks: Architectures and Protocols*, 2^{nd} Edition, Pearson Education, India, 2005.

[6]. Praveen Joshi, "Security issue in routing protocols in MANETs at network layer", Int. J. of Procedia Computer Science, Elsevier, Vol. 3, pp. 954-960, February, 2011.

[7]. P. S. Bhadoria and M. Narwariya, "A survey on security issues in Mobile Ad-hoc Networks", Int. J. of Computing science and Communication Technologies, Technia, Elsevier, Vol. 2, No.1, pp. 229-232, July, 2009.

[8]. N. Komninos, D. Vergados and C. Douligeris, "Layered Security design for Mobile Ad-hoc Networks", Int. J. of Computer and Security, Elsevier, Vol.25, pp.121-130, 2006.

[9]. B. Wu, J. Chen, J. Wu and M. Cardei, *A Survey on Attacks and Countermeasures in Mobile Ad-hoc Networks*, Wireless/Mobile Network Security, Springer, pp 103-135, 2007.

[10]. K. Osathanunkul and N. Zhang, "A Countermeasure to Black Hole Attacks in Mobile Ad-hoc Networks". In Proc. IEEE on Networking, Sensing and Control Delft, Netherlands, pp. 508-513, 11-13 April, 2011.

[11]. "Cisco IOS XR Security Guide, Release 3.3", http://www.Cisco.com/en/ US/docs/ios_xr_sw/iosxr_r3.3/security/design/guide/sg33ddos.html.

[12]. M. Majid, O. Suat and G. Inan, "A survey of Wormhole-based Attacks and their Countermeasures in Wireless Sensor Networks", Int. J. of IETE TECHNICAL REVIEW, Vol. 28, No. 2, pp. 89-102, March-April, 2011.

[13]. R. Mishra, S. Sharma and R. Agrawal, "Vulnerabilities and security for Ad-hoc networks". In Proc. IEEE on Networking and Information Technology, pp. 192-196, June 11-12, 2010.

[14]. M. Taheri, M. Naderi and M.B. Barekatain, "New Approach for detection and defending the Wormhole Attacks in Wireless Ad Hoc Networks". In Proc. ICEE, pp. 331-335, May 11-13, 2010.

[15]. H.S. Chiu and K.S. Lui, "DELPHI: wormhole detection mechanism for ad hoc wireless networks". In Proc. of IEEE 1st Symposium on Wireless Pervasive Computing, pp. 6-11, January, 2006.

[16]. Van Phuong Tran et al, "Transmission Time-based Mechanism to Detect Wormhole Attacks" In Proc. of IEEE 2nd Asia-Pacific Services Computing Conference, pp. 172-178, 2007.

[17]. M. Y. Su, "WARP: A wormhole-avoidance routing protocol by anomaly detection in mobile Ad-hoc networks", Int. J. of *Computer and Security*, Elsevier, Vol.29, pp. 208-224, March 2010.

[18]. I. Khalil, S. Bagchi and N.B. Shroff, "LITEWORP: a lightweight countermeasure for the wormhole attack in multi-hop wireless networks", In Proc. IEEE on Dependable Systems and Networks, pp. 612-621, 2005.

[19]. Y.C. Hu, A. Perrig and D. B. Johnson, "PACKET LEASHES: A defense against wormhole attacks in wireless ad hoc networks". In Proc. IEEE INFOCOM 2003, Vol. 3 pp. 1976-1986, 2003.

[20]. D. L. Mills, "A Computer-Controlled LORAN-C Receiver for Precision Timekeeping", Department of Electrical and Computer Engineering, University of Delaware, New York, Technical Report 92-3-1, March 1992.

[21]. D. L. Mills, "A Precision Radio Clock for WWV Transmissions", Department of Electrical and Computer Engineering, University of Delaware, New York, Technical Report 97-8-1, August 1997.

[22]. M.A. Azer et al, "Intrusion detection for wormhole attacks in Ad-hoc networks a survey and a proposed decentralized scheme". In Proc. IEEE on Availability, Reliability and Security, pp. 636–641, 2008.

[23]. S. Gupta, S. Kar and S Dharmaraja, "WHOP: Wormhole attack Detection Protocol using Hound Packet". In Proc. IEEE on Innovations in Information Technology, pp. 226-231, 2011.

[24]. P. V. Tran et al, " TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks", In Proc. IEEE ,Wireless Sensor Network Track at Consumer Communications and Networking Conference(CCNC), Las Vegas, USA, pp.593-598, January 11-13, 2007.

[25]. Mahesh K. Marina and Samir R. Das, "Ad-hoc on-demand multipath distance vector routing", Int. J. Wirel. Commun. Mob. Comput., Wiley InterScience, Vol.6, pp. 969-988, 2006.

[26]. C. E. Perkins, E.M. Royer and S.R. Das, *Ad hoc on-demand distance vector (AODV) routing,* IETF Internet draft. MANET Working Group, January, 2004.

[27]. H. Wu, C. Wang and N.F. Tzeng, "Novel self-configurable positioning technique for multi-hop wireless networks", Int. J. of IEEE Transactions on Networking, Vol.13, No.3, pp. 609-621, June 2005.

[28]. X. Wang and J. Wong, "An end-to-end detection of wormhole attack in wireless Ad-hoc networks", In Proc. 31st computer software and applications, IEEE Computer Society Washington, DC, USA, Vol. 1, pp. 39-48, 2007.

[29]. *QualNet 5.0.2 User's Guide*, Scalable Network Technologies Inc., Los Angeles, 2010, pp. 1-3.