INTEGRATING WORMHOLE ATTACK DEFENSE MECHANISM WITH REACTIVE BASED ROUTING PROTOCOL

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

MASTER OF TECHNOLOGY
IN
COMPUTER SCIENCE AND TECHNOLOGY

By
Arun Kumar

Under supervision of
Dr. D.K. Lobiyal and Mr. Sushil Kumar

SCHOOL OF COMPUTER AND SYSTEMS SCIENCES
JAWAHARLAL NEHRU UNIVERSITY
NEW DELHI–110067
INDIA
JULY 2012

SCHOOL OF COMPUTER AND SYSTEMS SCIENCES

JAWAHARLAL NEHRU UNIVERSITY

NEW DELHI – 110067

INDIA

CERTIFICATE

This is to certify that the dissertation entitled "**Integrating Wormhole Attack Defense Mechanism with Reactive based Routing Protocol"** being submitted by **Mr. Arun Kumar** to the **School of Computer & Systems Sciences, Jawaharlal Nehru University, New Delhi** in partial fulfillment of 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 and Mr. Sushil kumar.

Dr. D. K. Lobiyal	Mr. Sushil kumar	Prof. Karmeshu
SC&SS, JNU	SC&SS, JNU	SC&SS, JNU
(Supervisor)	(Supervisor)	(Dean)

SCHOOL OF COMPUTER AND SYSTEMS SCIENCES

JAWAHARLAL NEHRU UNIVERSITY

NEW DELHI – 110067

INDIA

DECLARATION

This is to certify that the dissertation entitled ***"Integrating Wormhole Attack Defense Mechanism with Reactive based Routing Protocol"*** is being submitted to the ***school of Computer and Systems Sciences, Jawaharlal Nehru University, New Delhi,*** in partial fulfillment of the requirements for the award of the degree of ***Master of Technology*** in ***Computer Science & Technology***, is a record of bonafide work carried out by me under the supervision of Dr. D.K. Lobiyal and Mr. Sushil Kumar

The matter embodied in the dissertation has not been submitted in part or full to any University or institution for the award of any degree or diploma.

Arun Kumar

Dedicated to Late Prof. G.V. Singh

List of Figures

Abstract

Mobile Ad Hoc Networks (MANETs) can be rapidly deployed and it can tolerate the rapid changes in the network topology. Due to the infrastructureless, dynamic and broadcast nature of radio transmission, MANETs are susceptible to several types of security attacks. Thus, security emerges as a major concern for any MANETs as these attacks can affect the performance of different routing protocols.

This work focuses on collaborative routing attacks in which malicious nodes collaborate with partner nodes to send packets directly to each other and thus these nodes can adversly affect with the control and data packets sent through them. In this work, we mainly concentrate on wormhole attack in which, a malicious node captures packets from one location in the network and tunnels them to another malicious node at a distant point, which then relay those packet locally. Wormhole attacks can be launched easily and performed even when the network provides confidentiality and authenticity.

The algorithms proposed so far to detect wormhole in the path carries a high computational burden and follow a complicated session starting mechanism. Cell based open tunnel avoidance (COTA) detection scheme works basically on end-to-end detection algorithm but with some modifications to manage detection information comfortably. In this work, the impact and implications of wormhole attack on reactive routing protocol DSR has been carried out using open source network simulator GlomoSim.

Additionally, the analysis of the integration of COTA mechanism with reactive routing protocol DSR is made to detect wormhole nodes in the path. From the simulation results, it is observed that, Wormhole existence in the path results into smaller number of hop counts which reduces average end-to-end delay. In positive sense existence of wormhole is beneficial but, malicious behavior of wormhole nodes changes results into degradation of network performance. Our implementation of COTA mechanism gives us satisfactory results in respect of reactive routing protocol DSR.

Table of Contents

Chapter 3: COTA AND AlGORITHMS

Chapter 4: SIMULATION AND RESULTS

Chapter 5: CONCLUSION AND FUTURE SCOPE

Chapter 1

INTRODUCTION

1.1 Introduction

As the technology is progressing and hardware cost declining sharply e-gazettes are more common today. Statistics predict that the growth rate of e-gazettes sells will increase exponentially, due to these changes an environment of ubiquitous and pervasive computing emerges, which result into an interest of researchers towards mobile Ad hoc network (MANET). There is a significant historical perspective of network technological changes range from guided media network to wireless infrastructure and now wireless infrastructure less network.

Mobile Ad hoc network is an infrastructure less network of mobile nodes with a self-configuring capabilities and dynamic topology due to a high level of mobility. Mobile nodes in the Ad hoc network are less capable in terms of computing and battery power. Shared radio channels are used for communication, which uses the free license frequency zone, that is actually an additional advantage but on the other hand, small bandwidth is a constraint as well. In this type of network multi-hop relaying concept is used for packet forwarding. Bandwidth is a real constraint in Ad hoc network hence it must be used efficiently and effectively. Ad hoc network uses a complex medium access protocols for bandwidth reservation in real time transmission scenario. It is much contrary to cellular network, which is infrastructured and uses centralized routing for its operation. Here due to mobility and resource constraint distributed routing is used. Mobility leads to frequent path breaks, and then the network needs a complex makeup algorithm to refresh topology-effect in routing tables.

Nodes in this environment need more intelligence because here a node not only deals with its own management but also with network management. However both processing and battery power is weak here, hence every protocol on proper functioning of wireless Ad hoc network, and its design issue should be taken care of these technical, social and feasibility issues. Ad hoc network is a novice in its operation but has vast application area range from the military use in battle and rescue-search operation, an emergency situation like flood, earthquake and many others. Sensor network, Vehicular area network and students on a campus area network are some recent application areas which are very much popular in this information age.

1.2 Issues in Ad hoc Wireless Network

There are many issues concerning designing, operation, installation and maintenance of Ad hoc network. These are as follows[17]:-

1.2.1 Medium access protocol

MAC protocols in Ad hoc network are used to arbitrary distribute shared wireless channel among network nodes to transmit data packets. In this type of network where there is no central coordinator, medium access control should be distributed among the participating nodes. Scheme should be implemented in the way so that nodes in the network are well synchronized and take care of the hidden and exposed terminal problem. To maximize overall throughput, access delay should be minimized, and fairness should be high.

Protocol concerning MAC should support real-time traffic and for it, there should be a provision of resource reservation. There should be some measure for calculating resource availability, which helps in the survival situation to efficiently utilize battery power by regulating power used for transmission. Adaptive rate control canhandle congestion in the network. Directional antennas can very well overcome the situation of interference. So overall if we look, then MAC protocol in Ad hoc environment plays a decisive role in performance of the network.

1.2.2 Routing

The main responsibilities of routing protocol in Ad hoc network are exchanging route information, finding a feasible path to a destination based on criteria like minimum hop length, access delay, power required to transmit and network should reconfigure itself whenever the path breaks, utilizing minimum processing power and bandwidth.

Routing job in Ad hoc network faces a great level of challenges, which includes mobility that is on one part is an added advantage, but result into frequent topology changes and path breaks. To overcome and counterbalance, we require periodic routing updation. So concerning this, we require exchanging route information using control packets, which should be as minimal as possible due to bandwidth constraint. Protocol should take care of error-prone shared channel and location dependent contention. There is some resource constraint also in terms of processing, battery power and buffer storage space.

There are some major requirements from routing protocol. As routing process is a backbone of any Ad hoc network these requirements include minimum route acquisition delay, quick route reconfiguration and loop free routing. Scalability is also one of the requirements as QoS, which need to be addressed well. Above all routing should support time sensitive traffic and routing procedure should be well secure and resilient to any threats and vulnerabilities.

1.2.3 Multicasting

In Ad hoc environment multicasting plays an important role in applications like emergency search-rescue operation and military communication. Here, nodes form a group to carry out some useful task and this requires a point to multipoint and multipoint to multipoint communication links. The mobility, battery power and bandwidth constraint makes multicasting even more challenging. The approach here should be scalable, robust, secure, and efficient, and it should use minimum control overheads in order to utilize bandwidth efficiently. It should support quality of service issues and maintain group concerning activities like session management, nodes membership and connectivity among the group member.

1.2.4 Transport layer protocol

In wired and infrastructure wireless network TCP is used for end to end connectivity and reliable delivery of data packets, flow and congestion control. But directly these protocols can’t be used here because of some separate issues and the main reasons for performance degradation in reliable connection oriented transport layer protocol in Ad hoc wireless network is frequent path breaks, presence of stale routing information, high channel error rate and frequent network partition.

Here, when the path breaks result into reconfiguration, which may take more time than the retransmission time out leads to retransmission of packets and execution of congestion control, which shouldn’t be because it’s a path breaks situation not a congestion problem due to which congestion window size decrease hence results into low throughput. Many a time due to stale routing information a single data packet can be forwarded using multi-pathand this creates an out-of-order packet situation at destination node. Mobility of nodes creates a situation where a node isolates and network partition takes place, which may result into packet drop and again retransmission of TCP packets, which subsequently increase the retransmission timer time and due to these sorts of behavior node becomes inactive for a long period even when partition last for a short while.

1.2.5 Pricing scheme

Ad hoc network is based on multi-hop relaying concept where a relay node’s willingness to relay another node’s data packets is a major concern. It may be possible that a node ‘*X*’ is in the optimal path from ‘*A*’ to ‘*B*’ but while relaying ‘*X*’ is down in power than any other non optimal route would be used so pricing scheme should be flexible enough and the relay nodes which use their computing and battery power while routing, and packet forwarding should be compensated appropriately.

1.2.6 Self organization

Independent natures of participating nodes in an Ad hoc environment raise the need for self-configurability and organization. The major activities that an Ad hoc wireless network requires to perform self-organization are neighbor discovery, topology organization and new node adoption in Ad hoc network.

1.2.7 Addressing and service discovery

Due to the absence of a central coordinator both addressing and service discovery needs to be addressed. An address of a node should be in a way that it is logically universally unique and auto-reconfiguration of address as well require to allocate non duplicate addresses to mobile nodes in a highly dynamic environment where partitioning and merging of network takes place frequently.

In this type of network, nodes should be able to locate services provided by other network nodes. Hence, efficient service advertisement mechanism is necessary. Topology change may lead to change in location of a service provider so that it may be possible to merge routing with service discovery though it violates routing design issues, but a viable option.

1.2.8 Energy management

It is a process of managing source and consumers of both computational and battery energy in a way so that the overall lifetime of network increases. It may include finding route with minimum total energy consumption in the network. Use distributed scheme to do various jobs so that all batteries are fairly utilized and handle the processor and interface device to minimize power consumption. The use of variable power in MAC protocols can save energy at nodes, bandwidth reuse and reduction in interference.

1.3 Routing

The main responsibilities of routing protocol in Ad hoc network are exchanging route information, finding a feasible path to a destination based on criteria like minimum hop length, access delay, power required to transmit and network reconfiguration whenever the path breaks, utilizing minimum processing power and bandwidth.

Routing job in Ad hoc network faces a great level of challenges, which includes mobility that is on one part is an added advantage, but result into frequent topology changes and path breaks. To overcome and counterbalance, we require periodic routing updation. So concerning this, we require exchanging route information using control packets, which should be as minimal as possible due to bandwidth constraint. Protocol should take care of error-prone shared channel and location dependent contention. There is some resource constraint also in terms of processing, battery power and buffer storage space.

There are some major requirements from routing protocols. These requirements include minimum route acquisition delay, quick route reconfiguration and loop free routing. Scalability is also one of the requirements as QoS, which need to be addressed well. Above all routing should support time sensitive traffic and routing procedure should be well secure and resilient to any threats and vulnerabilities.

1.3.1 Classification of routing protocols

The routing protocols for ad hoc wireless networks can be broadly classified into four categories based on [1]:

The routing information updates mechanism

Here, the classification is in three major categories first one is proactive in which every node maintains the network topology information in the form of routing tables by periodically exchanging routing information. Second one is the reactive protocol here; it doesn’t maintain the network topology information. They obtain the necessary path when it is required and the last one is the hybrid protocol which combines the best feature of the both. Here routing within a particular zone proactive is used and outside this zone reactive is used.

The use of temporal information for routing

Here, the classification is in two categories first one is routing protocols that use past temporal information and the second one is the one which uses future expected temporal information.

The routing topology

Here, the first one is flat topology routing protocols which makes use of a flat addressing scheme which assumes the presence of a globally unique addressing mechanism. The second one is hierarchical topology routing protocols which makes uses of a logical addressing.

The utilization of specific resources

Here, the power aware routing which aims at minimizing the consumption of a very important resource in the ad hoc wireless networks: the battery power. **The geographical information** assisted routing protocols belonging to this category improves the performance of routing and reduce the control overhead by effectively utilizing the geographical information available.

1.4 Dynamic Source Routing

The Dynamic Source Routing Protocols is a simple and efficient routing protocol used in MANET. It allows the network to be completely self-organized and self-configuring able. In mobile networks, network nodes co-operate to route packets from one-hop to another. As nodes in ad hoc network move out or join the network results into topological changes which are automatically determined and maintained by the DSR.

This protocol allows nodes to dynamically discover a source route across multiple hops. Each data packet contains in its header a complete ordered list of nodes from source to destination. This allow the packet routing to be trivially loop free and avoiding updation in routing information for intermediate nodes.

1.4.1 DSR Protocol description

DSR composed of two mechanisms, one is Route Discovery and another one is route maintenance[5].

Route Discovery

It is a mechanism in which when a source *S* want to send packet to Destination node *D*. Sender node obtains a source route to D. Route discovery is used only when source *S* does not have path up to destination.

Route Maintenance

It is a mechanism which is used while sending message to destination *D*, but source*S* came to know that the existing source route does not lasts. In this situation this mechanism operates in which, any other path from *S*to *D* if available can be used or again route discovery can be called.

Route Discovery and Route Maintenance operate entirely on demand. DSR does not use any periodic routing advertisement, link status, or neighbor detection packets. Hence due to this number of packetsoverhead caused by DSR scale to level zero. In DSR, the routing packet overhead automatically scales to only that level which is needed to backup the routes currently in use. A node in the network may learn and cache multiple routes to any destination which may help the network in route maintenance phase. The operation of Route discovery and maintenance in DSR allows unidirectional and asymmetric routes to be easily supported.

1.4.2 Basic DSR route discovery

In transmitting originating packets destined to some node *D* from source node*S*, the source node *S*places the destination and source node addresses in the header of the packets. A source node, which directs the packet up toits destination *D*. Normally *S* obtains its route from its route cache memory if routeexists there.Otherwise, route discovery mechanism is initiated. Fig.1 shows an example of route discovery, in which node *A* is attempting to discover a route to node *E*. To initiate the Route discovery, *A* transmits a route request message, which is received by all nodes in transmission range of *A*. Each request message identifies the initiate of the request and this message also contains the intermediate nodes ids. The destination nodes on receiving it piggyback the route from *A* to *E* in route reply packet and send it back to source node. When another node receive a route request and its cache contains the path towards destination node then further request is not propagated and route reply packets initiate from that intermediate node.

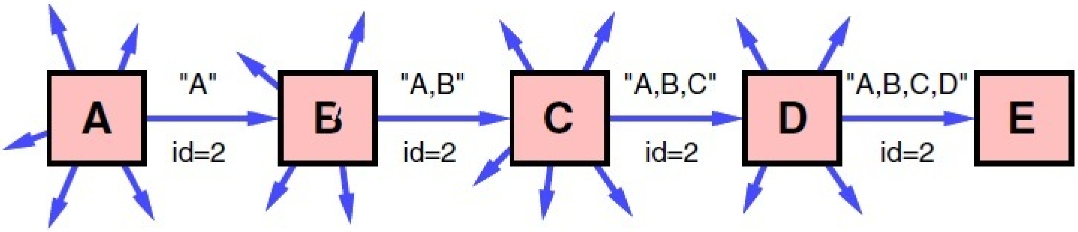

Fig. 1 Route discovery [5]

1.4.3 Basic DSR route maintenance

Figure 2 is route maintenance example in whichNode *C* is unable to forward a packet from *A* to *E* over its link up to next hop *D*.When forwarding a packet using a source route, each node transmitting the packet is responsible for conforming that the packet has been received by the next hop along the source route. The packet is retransmitted up to maximum number of attempts. Here in figure 2 Node *C* is responsible for receipt at node *D*.

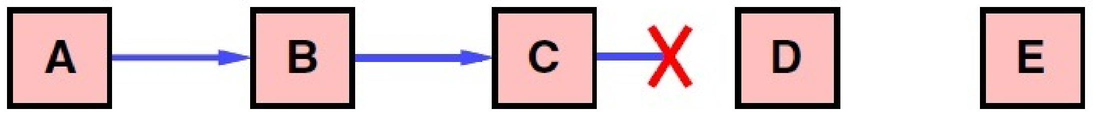

Fig. 2 Route maintenance [5]

If the packet is retransmitted by some hop the maximum number of time and no receipt conformation is received. Then node return route error message to the original sender of packet. For example node *C* is unable to deliver, then *C* return route error to *A*, stating that link from *C* to *D* is currently broken, then node *A* remove this path from its cache and again either another path to *E* is chosen if exists or route discovery mechanism is initiated.

There are some additional route discovery features using them efficiency of DSR can be improved. Among those is one in which overhead routing information can be cached by intermediate nodes and then these cached information can be used in route reply, which in turns leads to shorten the route establishment time and there should also be limits on route request hop counts.

Likewise, some additional route maintenance feature may be used in which packet salvaging is done in which a node may attempt to salvage the data packet rather than discarding it. When source node contains any obsolete item then it should be discarded and increased the spreading of route error message.

1.5 Problem Statement

In MANETs environment colloborating nodes can compromise and then these nodes can falsely project themselves as a optimal intermediate nodes for a path from source to destination this, resulting into a false scenario. This fake path will then attract the data traffic, that is, the packets will be routed through a wormhole path being either compromised or dropped. Wang. proposes the COTA mechanism to identify wormholes in the path which is based on End-to-End detection mechanism with some modificications to store and manage detection information.

In our dissertation, we propose to implement the COTA mechanism over the reactive based routing protocol Dynamic Source Routing (DSR). We further, provide a detailed analysis of wormhole attack on DSR in both static and dynamic ad hoc network and measure the performance of COTA through simulations carried out using the GlomoSim simulator.

1.6 Objectives

The complete work is divided into three scenarios first one is the normal DSR routing, the second one is DSR routing with wormhole in static environment and the third scenario is DSR routing with wormhole in mobile ad hoc network. The objectives are:

- To study the impact of wormhole in a path from source to destination through the measurement and comparison of various network parameters.
- To study the performance of COTA on DSR in terms of number of times this mechanism fails to alarm right about wormhole in the path.

1.7 Organization of Dissertation

The complete dissertation consists of five chapters. First chapter provides an introduction about ad hoc network and the various challenges associated with ad hoc network. In this chapter we mainly focus on ad hoc network routing in DSR and defines our problem statement and objective for the dissertation. Chapter second includes literature survey associated with security and wormhole attack. Chapter third defines the cell based open tunnel avoidance (COTA) scheme to defend wormhole attack and include COTA Algorithms. Chapter four, Simulation and Results includes the performance measure graphs and the result discussion. Chapter five concluded the whole dissertation work and provides the insight into future scope.

Chapter 2

SECURITY AND LITERATURE SURVEY

Mobile Ad hoc network is more vulnerable than traditional wired network. Security is very difficult to maintain in this environment due to unreliability of a wireless link between nodes. Vulnerabilities of mobile ad hoc network facilitate a healthy environment for the attacker nodes to disrupt the normal functioning of the system. Mostly attacker nodes play with a routing mechanism to disrupt data transmission.

2.1 Vulnerabilities of the mobile Ad hoc network

Vulnerabilities are the open doors in a network which can be exploited by intruders to attack network operation in a way or another. It is a weakness that makes targets susceptible to an attack. There are various vulnerabilities in MANET, which makes it more susceptible to security attack. These are[19]:

2.1.1 Lack of secure boundaries

Here, in MANET, there is no clear line of defense as in the wired network where adversaries have to pass through firewall and gateway to get access the physical medium. However in Ad hoc network, there is no requirement for physical access to visit the network, once any node is in the radio range of another one can join and communicate with it. This sort of vulnerability mainly originates from the nature of MANET: Freedom to join, leave and move inside the network.

2.1.2 Threats from compromised node inside the Network

It is a type of attack where adversary node’s aim is to gain control over the network nodes through unrighteous means and then these compromised nodes are used further to execute malicious action.

Attack of this type is very difficult to figure out because based on malicious behavior only we can’t figure out the adversary nodes as there exists no centralized trust authority and these adversary nodes are so clever that they can change their attack pattern and location of attack. Byzantine failure and wormhole attack encountered in the routing protocol for MANET is an example of this type.

2.1.3 Lack of Centralized Management Facility

Absence of centralized management machinery will cause vulnerabilities that can influence several aspects in the MANET.

Firstly, due to the lack of this, it’s very difficult to detect and monitor attack in a highly dynamic and large scale Ad hoc network.

Secondly, lacks of centralized management machinery impede the trust management in Ad hoc network to perform prior classification of network nodes in trusted and non-trusted ones.

Thirdly, many algorithms where cooperation is required in Ad hoc network like election algorithm for monitoring purpose there due to lack of centralized management authority compromised node can break the co-operative algorithm.

2.1.4 Restricted Power Supply

Nodes in a mobile Ad hoc network rely on battery power that is limited and thus causes several problems. Due to restricted power supply, adversaries can exploit the situation by targeting the node's processing capabilities and battery power unnecessarily, and this may even further result in denial-of-service attack.

Furthermore, adversary node may behave in a selfish manner too in an environment where the network needs co-operation. There these malicious nodes may falsely project themselves in running out of power.

2.1.5 Scalability

Unlike the traditional wired network where at any time, scale is predefined. However in case of MANET, it is not known in advance that how many nodes will be going to leave and join the network in the next go. So protocol and services like routing and key management should be compatible enough with the continuous changing scale.

Due to all these vulnerabilities, the mobile Ad hoc network will need a more robust and tight security scheme in comparison with the wired network.

2.2 Security Criteria

When the matter is of security concern then the solution's design to solve security issues must be validated against security criteria. There are some widely used criteria to evaluate security aspects. Network nodes should be available to provide all the designated services assigned to it regardless of security attacks. Solution should make it sure that the identity of a message remains same throughout the transmission. Identity of the message can be compromised through malicious and accidental altering.

One has to make sure the confidentiality of the message through which information is only accessible to those for whom it is intended. Message should be authentic enough, which assures that participants in communication are genuine but not impersonators. Solution should ensure that the sender and receiver of a message cannot deny that they have never sent or receive a message. Security's criteria should include the specification of authority, privileges and credential assigned to network nodes. Security's criteria also include privacy preserving in which entity node is protected by not disclosing its privacy to any other node [19].

2.3 Attack Type in Mobile Ad hoc Network

Attack includes any action that intentionally aims to cause damage to the network. It is an action taken against a target with the intention of doing harm.

Classification of attack is based in following criteria[18]:

2.3.1 Origin based classification

Here, classification is in two types of attacks that are in External and Internal attack**.** External attack is an attack launched by a node that does not belong to the network or is not allowed to access it. Internal attack includes attacks done by the internal compromised node, and it is much more severe than external attack.

2.3.2 Nature of attack classification

Here also classification is in two attacks types that are in Active attack and Passive attack**.** Passive attack is an attack in which a malicious node keeps an eye on traffic pattern, and collects information that might be further used to launch an active attack. Information confidentiality is a security attribute that must be provided to defy against passive attack. Active attack includes all the attacks launched through actively interacting with victims. These include, sleep deprivation torture which targets the battery, hijacking in which attacker takes control of a communication link between two entities and then masquerades as one and Jamming, which causes the channel unavailability due to overuse of it.

2.3.3 Misbehavior

Misbehavior threat is an unauthorized behavior of an internal node that may result in unintentional damage to other nodes of the network. It is something where a node does not want to launch an attack, but want to gain undue advantage over other nodes. The nodes may execute MAC protocol improperly to have a higher bandwidth, or it may be also possible that it refuses to forward packet intentionally for saving its own resources.

2.3.4 Attack against routing

Routing is an important service for any Ad hoc network. Hence, most of the attackers want to disturb the routing services in order to disturb normal functioning of the network.

Attacks against routing are classified into two categories[18]:

Attack on routing protocol

Here, an aim is to block the routing information from other nodes to reach the victim node even when there exists a route from victim to destination.

Attack on packet forwarding

It is an attack on packet forwarding, which try to disturb the packet delivery while transmission.

2.3.5 Routing attack

Routing attack results in network partition, routing loop, resource deprivation and route hijack. There are some more attacks against routing [18]:-

- Impersonating another node to spoof route message.
- Advertising a false route metric to misrepresent the topology.
- Sending a route message with a wrong sequence number.
- Flooding route discover excessively as DOS attack.
- Suppressing route error to mislead others.

Due to the mobility and constantly changing topology in the mobile Ad hoc network it is very difficult to validate all the route messages. There are some more complex routing attack such as rushing attack, black-hole attack, jellyfish attack and wormhole attack.

Considering space as a constraint, we restrict ourselves only up to the analysis of wormhole attack, which disturbs the routing in Ad hoc network. As the concept of pervasive and ubiquitous computing expands, so the concern for security enhancement issues in the Ad hoc network also need to be address well and as Ad hoc network is dependent on multi-hop routing so if any attack which can directly affect the routing operation should be tackled strictly.

2.4 Wormhole Attack

In wormhole attack, an attacker can receive a packet at one location in the network and then tunnels them to another location and replay them there. Wormhole attack can be divided into a two phase process. Firstly, the malicious node lures the legitimate node to send a packet via them and secondly thereafter these nodes compromised with data packets[13].

Here, the tunnel get establish between malicious nodes through different ways like, encapsulation, out-of-band-channel, high power transmission and packet relay. All the ways through which an attacker can create a tunnel may lead to affect routing badly. Hence, studying these attacks from attacker point of view can help in designing the counters.

2.4.1 Classification

The classification of these attacks facilitates in designing counters well. Literature classifies the wormhole attack based on[11]:-

How many nodes are compromised?

- **Hidden Wormhole:** In this wormhole adversary, node may record and retransmit packets. Here, attacker need not to compromise with another host to attack in the network. The only attacker needs hardware to perform an attack. This type of attack is more challenging to defend against as there exist no centralized trust management authority and even cryptographic technique doesn't solve our purpose because malicious node need to just replay the packets, and they can also change their attack pattern and location of attack to defend against trace out.

- **Exposed wormhole attack:** In this wormhole attack, two end points are the two compromised nodes and both adversaries built a virtual tunnel between the two compromised nodes, which used to lure data packets for routing and thereafter, forwarding of data packets can be compromised.

Attacker's visibility

- **Closed wormhole attack:** In it, both the malicious nodes are invisible from a path starting from source to destination. Hence, invisibility of malicious nodes makes this attacks mode even more challenging to defend against. As making other host node to compromise with malicious node is not so easy hence closed wormhole attack is difficult to perform.

- **Half open wormhole:** In this wormhole attack one out of the two malicious nodes is visible in a path from source to destination. Here, malicious node need not to compromise with other host nodes hence an attack is easy to perform and even cryptographic solutions cannot restrict the attacker from attacking.

- **Open wormhole:** In this, both the malicious nodes are visible in a path from source to destination.

2.4.2 Impact of wormhole on routing

If we look and analyze the wormhole attack in broader sense and looks at its positive perspective, then it is not a problem because the path chosen by malicious nodes may be the best one between source and destination provided that no node in this path is compromised. However the irony is that, this situation puts the malicious nodes on such a powerful position that it could be exploited.

Wormhole attack can mislead routing packets in a reactive protocol and thus result into false route setup. Where compromised node can selectively discard some data packets or can completely choke the transmission result in denial-of-service attack. Malicious nodes can modify the content of certain data packets and even in replay attack these compromised node need not to know cryptographic keys for authentication purpose hence these sorts of attacks are difficult to counter.

In proactive routing protocol, it can affect the periodic neighbor discovery mechanism which results into maintaining the wrong topological records in routing table. Due to this wormhole impact, distant nodes may be treated as a neighbor. The wormhole lure data traffic towards these malicious nodes and then this position can be exploited to do eavesdrop and man in the middle attack.

2.4.3 Detection and Prevention of Wormhole Attack

Today, this is an open area in which research is going on, and various solutions are proposed regarding this. Some out of these are[11]:

Hardware solutions

In earlier stage of this problem, some effort was put on hardware design and signal processing techniques considering that only neighbor nodes can understand the specially modulated signal. This method is resistant to closed wormhole, but can be compromised if any malicious node can accurately capture the signal pattern.

Use the directional antenna[4] to specify the neighborhood relation. In it, nodes examine the directions of the received signal from each other. When the direction of both the pair matches then the neighborhood relation gets confirmed. These hardware constraints makes the solution costly and as well as error prone.

Some other approaches

There are some ways through which the position of mobile nodes in an indoor environment can be located and then the conflicting positions of a same node can be traced out by comparing the original packet and the resent one's source position thereafter either any central co-coordinator or good node broadcast this as an anomaly.

There is another approach to detect closed wormhole in which each node in the network is equipped with special hardware, which responds to a one-bit challenge without delay. Then, the challenger measures the round trip time with an accurate clock to measure the distance between the nodes[11]. As the number of challenger increases, probability of an attacker to guess all bits correctly decrease exponentially.

There is also another approach of a packet leash in which extra information is added with packet defining its transmission distance and time. The two ways of doing so are:-

- **Geographical packet leash [9]:** In this approach, each node maintains its own location, and the nodes must be loosely synchronized. Here, when the packet reaches the destination, it compares the distance metric with an upper bound of distance between source and receiver if it comes below the desired, then the packet is discarded.

- **Temporal packet leash [9]:** Here, the nodes are tightly synchronized and the information regarding lifetime of the packet is added with it. Which is compared with the destination's clock and thereafter accordingly packet is accepted or discarded.

In both the approaches, we require an authentication technique so that malicious nodes in the middle can't overwrite the leash information for that either a hash-function or a digital signature[7] is used. The geographical leash technique can practically be integrated with authentication technique as there exist no time bar and clocks are loosely synchronized. Whereas with temporal leash, it is impractical to integrate as calculating hash-function and digital signature need an extra time which may affect the real time communication.

2.5 Related work

As ad hoc networks are merging into the pervasive computing environment, security becomes a central requirement. Wormhole attack may affect the routing mechanism. Since the mobile devices use a radio channel to send information, the malicious nodes can drop, spy packets, tunnel them to another location in the network, and retransmit them. This generates a false scenario that the original sender is in the neighborhood of the remote location. This may lead to choice of a non-existent route. **Zero-interaction Authentication (ZIA) [16]** is designed to protect the data from illegal access.

In wormhole attack packets are re-sent in the exactly same way, encryption or authentication alone cannot prevent the attacks. The safety and effectiveness of some security enhancements for ad hoc network would be improved if wormhole can be defended. Attack can negatively impact distributed monitoring of node misbehaviors. The Classification of such attacks will facilitate the design of detection methods. According to whether the attackers are visible on the route, we classify the *wormhole into three types: closed, half open, and open.* The previous research focuses on the prevention of closed wormhole. The mechanisms that only examine direct neighbors cannot guarantee the detection of other two types. Therefore, an end-to-end mechanism[14] must be designed to defend against the half open and open wormholes.

Wormhole detection needs to be conducted when a neighbor relation or a route is first established. Besides, it must be conducted repeatedly during the lifetime of the neighbor relation or the route due to mobility issue and wormhole can be formed dynamically. The detection frequency impacts the overhead and the detection accuracy

Wormhole attacks on mobile ad hoc networks were independently discovered by Dahill et al, Hass et al, and Hu et al. To defend against them, some efforts have been put on hardware design and signal processing techniques. Both mechanisms will be compromised if the malicious nodes can accurately capture the signal pattern. Neither of them can prevent half open or open wormhole.

The adoption of directional antenna[4] by mobile devices can raise the security levels. A solution that uses such equipment to defend against closed wormholes has been presented. The nodes examine the directions of the received signals from each other. Only when the direction of both pairs match, the neighbor relation is confirmed. Detection scheme can be integrated into Intrusion Detection Systems (IDS).

Some mechanisms proposed to locate the position of a mobile node in an indoor environment can be applied to prevent wormholes. One approach to detect closed wormholes without clock synchronization is proposed by Capkun et al. Every node is assumed to be equipped with a special hardware that can respond to a one-bit challenge without any delay. The challenger measures the round trip time of the signal with an accurate clock to calculate the distance between the nodes. The probability that an attacker can guess all bits correctly decreases exponentially as the number of challenges increases.

Another approach to detect closed wormholes is packet leash[9], which was proposed by Hu, Perrig and Johnson. The leash is the information added into a packet to restrict its transmission distance. In the geographical leashes, the location information and loosely synchronized clocks together verify the neighbor relation. In temporal leashes, the packet transmission distance is calculated as the product of signal propagation time and the speed of light. Both mechanism use lightweight hash chains to authenticate the nodes. The end-to-end mechanism assumes the knowledge of location information and loosely synchronized clocks. It can be deployed in the environment where geographical leash can be used to detect closed, half open, and open wormholes.

A lot of research in ad hoc networks has been conducted based on the position awareness assumption. They cover routing, energy consumption, to lactation based services. Some work has been conducted based on loose synchronization assumption, such as geographical leashes, Secure Tracking of Node Encounters (SECTOR), Ariadne. A lot of efforts have been put on clock synchronization in ad hoc and sensor networks. There have been solutions based on LORANC[6], WWVB; Reference Broadcast, TINY/MINI-SYNC, and GPS.

Chapter 3

COTA & ALGORITHMS

3.1 Cell based Open Tunnel Avoidance Scheme (COTA)

Wormhole detection is a way in which the odd nature of wormhole nodes is detected and news about these nodes is broadcasted in the network. So that, Routing mechanism avoids these malicious nodes while searching for route in the ad hoc network.

As the research progresess towards finding mechanism to detect wormhole, There came an End-to-End detection mechanism in which packet leash approach is used. The packet contains (Time, Position) for detection purpose. In it detection packets are sent from source to destination with both nodes trust each other and the detection packet is encrypted. So that, only detection nodes can open it and do the useful for finding the wormhole. In End-to-End detection mechanism, detection node has not only to store each and every packet encountered to it but also has to process each and every combination possible of (time, position) pairs stored in a packet encoutered with the already data stored in it[11].

But, in case of COTA only the limited number of packets being entertain for detection purpose out of all packetsencoutered by detection node. This flexibility limited the communication and processing overhead as compare to End-to-End detection mechanism.COTA divides the whole area into same-sized cells (hexagon), and divides time into same length slots. COTA only store the first received (time, position) pair of every node that falls into same slot. Through adjusting the cell size and slot length we can control the computation and space compexity of detction algorithm [11].

3.1.1 End-to-End mechanism VS COTA

- In End-to End detection mechanism, time and space is not been discrete while, in COTA both time and space become discrete.

- In COTA whole space is divide into equal space Hexagon and the whole simulation time is divided into equal size slots with length *T* and number of slots=[Simulation time/*T*].

- In End-to-End mechanism, the destination node stores all detection packets (Time, Position) pair. While, in case of COTA only the first received (time, position) pair of every node that falls into the same slot time.

3.1.2 Advantages of COTA

As we know that COTA divides the whole area into same sized cells and slot length. So, we have the following advantages of COTA:-

- COTA restricts the number of time slots that COTA needs to store for every intermediate node. Let the slot length is *T* the destination wants to store at most $(T_{life}+\Delta)/T+1$ records for every intermediate node.

- COTA restrict the longest moving distance of a node during the delivery of a single packet.

- COTA prevents the attackers in open wormhole or half open wormhole from buffering the packets for a long time and declaring that the packet moves to the new position and forward the packet.

3.2 COTA Mechanism

The main operation in implementing COTA mechanism for an ad hoc network is to maintain database in real time situation for an each destination node running this mechanism to check wormhole in a path on receivingdetection packet.

Mainly the COTA mechanism operations are divided into three major parts:-

- Data structure creation for storing the (Time, Position) pair of intermediate nodes for future comparision.
- Maintaining this data structure throughout the life time of path existence.
- Running the detection algorithm on receiving detection packet destined to destination *D*.

3.2.1 Data structure to detect Wormhole

It is created and maintained by the destination node to store the (time, position) pair, which are used in COTA detection algorithm to check the wormhole in the route. Here, each packet in the network has it's life time due to which obselete information stored in it does not impact on datastructure. Destination node while creating data structure, looks for active nodes in the path and then create active nodes link listed. In each node it also store the expiration time of the latest (time, position) pair of every node. Then each node point to the cell linked structure which store the cells that have active records. Each cell remembers the expiration time of the latest record pair stored in it.

3.2.2 Data structure maintenance

COTA only stores the first received (time, position) pairs of the same cell and the same slot. Through adjusting the cell size and slot length, a node can control the effort that it wants to put on wormhole detection. The destination nodes maintain data structure once in every slot to keep itself up to date in maintaining real time situation constraint.

3.2.3 Detection algorithm

When a new (time, position) pair of a node arrives, the destination first locate the cell list of that node. Then for each cell of that node, it uses a linear search to locate the records that has the shortest time difference from the new time stamp. Then compare the velocity through the detection formula to check whether the node is lying or not.

In Real world scenario, many routing paths may exists, hence simultaneously many detection algorithm needs to operate on different path which in terms leads to high computation cost. Space recovery can also be done while searching for the latest pair in cell arrays. During this, as we know the expiration time of new records as well as the stored recorded in the cell, obsolete records of that cell and node can be deleted and in this way memory space can be recovered. Detection packet can also be send while network is ideal once in two time slot or in N time slots as per our needs.

3.3 Mathamatical Aspect of COTA

COTA divides the whole area into same-sized cells (hexagon), and divides the total time into same length slots. COTA only store the first received (time, position) pair of every node that falls into same cell and the same slot. Through adjusting the cell size and slot length one can control the overhead associated with detection scheme.

T_{life} is the lifetime of a packet which is a few seconds for a packet in a network. In our case, clocks are loosely synchronized and COTA can estimate the packet traveling time. The packet arrives at destination *D* within its lifetime, the sending time at *S* and the receiving time at *D*.Then, it must satisfy this equation$\mathbf{(T_{Drecv} - T_{Ssend}) \leq T_{life}} + \Delta$, where Δ= Estimated clock error [11].

3.3.1 Wormhole detection

In order to detect wormhole, we have to calculate the average moving speed of the node. Let $\mathbf{P_{new}}$ and $\mathbf{P_{select}}$ be the position of the nodes at $\mathbf{T_{new}}$ and $\mathbf{T_{select}}$ time respectively and $\boldsymbol{\delta}$ is the maximum error distance and Δ is the clock error [11].

Then by using Eq.3.1 we have $\boldsymbol{V_{calc}}$:-

$$\boldsymbol{V_{calc}}=\max((0,\|P_{new}-P_{select}\|)-\delta)/(\|T_{new}-T_{select}\|+\Delta) \qquad 3.1$$

Let **V** be the average moving speed in the network. Then If $\boldsymbol{V_{calc}} > \mathbf{V}$, it means the selected node sent the false information so there may be a wormhole on the concern route [11].

3.3.2 Detection capability of COTA

COTA avoids to store and compares all the (time, position) pairs. Due to which COTA can misses the detection of some anomalies in the network.To remove these anomalies, COTA define an offset **(2r+vT)** where **r**=radius of cells, **v**=highest speed of the nodes, **T**=length of the time slot and this offset is added in Eq.1 to modifies it to Eq.3.2 which is as below [11]:-

$$V=\max((0,\|P_{new}-P_{select}\|)-\delta+2r+vT)/(\|T_{new}-T_{select}\|+\Delta) \qquad 3.\ 2$$

Using the above equation COTA's detection capability touches the detection capability of End-to-end mechanism. But even now, COTA introduce false positive alarm for some special cases.

3.4 Parameters in COTA

The required parameters used to implement the COTA mechanism are Packet life$\mathbf{(T_{life})}$, Cell size**(r)** and Slot length**(T)**. These parameters are chosen in a manner so that, COTA gives best result. The choice of packet life is directly related to the end to end delay in ad hoc networks. The value of packet life taken is in few seconds.

3.4.1 Storage space in COTA

Due to limited processing power of ad hoc nodes which is used to linearly search the data space for detection purpose, we need minimum storage complexity. In COTA mechanism the storage complexity is as such [11].

Now let the position of a node be with in a circle with diameter, $\mathbf{2r = v(T_{life} + \Delta)}$

$$\text{so } r= v(T_{life} + \Delta)/2 \qquad 3.\,3$$

If there is no wormhole then the number of cells that have active records for the node is atmost [11]:-

$$\text{Area of circle/area of cell} = \mathbf{(\Pi(v(T_{life} +\Delta)/2)^2)/1.5\sqrt{3}r^2} \qquad \mathbf{3.4}$$

We already known that in each cell at most $\mathbf{[(T_{life}+\Delta)/T]+1}$ records are stored. The total number of records stored by destination for one node is at most:-

$$\mathbf{(\pi v^2(T_{life}+\Delta)^3)/6\sqrt{3}T*r^2} \qquad \mathbf{3.\,5}$$

Now, if the path length is **H** then the destination node store at most $\mathbf{H* (\pi v^2(T_{life}+\Delta)^3)/6\sqrt{3}T*r^2}$ records for one route.

3.4.2 Number of operations in COTA

Let there are ***Z*** COTA packets for one route and the path length is ***H*** then the total number of operations required by COTA is Eq.3.5 .Now if number of packets>number of records stored i.e [11].

$$Z > \mathbf{(Pv^2(T_{life}+\Delta) ^3)/6\sqrt{3}T*r^2}$$

In this way, COTA will save space and computation both[11].

3.4.3 Sensitivity of COTA

For detection of wormhole in Eq.3.2, we add an offset **2r+vT** where **r, v, T** has its usual meaning. The offset **2r+vT** is called sensitivity of COTA [11]. Practically it is the maximum distance a mobile node can move in unit distance time period.

3.4.4 Effect of sensitivity of COTA

If the sensitivity of COTA **2r+vT** is predetermined then we can choose suitable values of **r** and **T** to minimize the required storage and computational overhead. Let **2r+vT=X** where **X** is constant.Eq.5 is minimized when Eq. 3.6:-

$$\frac{\partial}{\partial r}\left(r^{2}(X-2r)^{-1}=0 \tag{3. 6}$$

This results into optimal value of**r=X/2.**

3.5 Algorithms

3.5.1 Algorithm to Implement COTA

This algorithm helps us to divide the whole job for a detection node in major three parts as already discussed .

```
ALGO COTA:
Start {
Step1: Create Data Structure for checker node.
Step 2: Maintain this Data Structure with respect of time.
Step 3: Use the above Data Structure to detect wormhole in path.
} End.
```

In implementing COTA we need to divide both space and time in discrete values. To divide space in discrete values whole area is divided into hexagon. To divide time, a whole time is divided into equal length time slots.

ALGO Create_ Hexagon:

Input: simulation area co-ordinates as $\mathbf{X_{bottam},Y_{bottam,}X_{top},Y_{bottam}}$, **r** is the radious of hexagon.

Output: Number of hexagon with center points in array.

```
Start {
For(i=0 to i<$Y_{top}$ with increment 1)
{
For(j=0 to j<$X_{top}$ with increment 1)
{
If(i/2==0)
Cord[0]=X+j*(1.732*r)
Else
Cord[0]=X+(0.8666*a)+j*(1.732*r)
Cord[1]=Y+i*(1.5*r)
Cord[2]=0
Id=i*($X_{top}$/1.732*r)+j
Struct cord[0],cord[1],cord[2] in file for further use.
}End.
```

This result into the division of whole area into hexagons and simulation time is also divided into equal slot time **T**.

3.5.2 Algorithm to Create Data structure

AlGO Create_Data _Structure:

Input: A node for which structure to make.

Output: A node pointer pointing to head node.

```
Start{
Step 1: Find the active nodes i.e the intermediate nodes of path upto destination.
Step 2: Make link list for these active nodes structure and store latest pair for this node.Step 3: Then for each active node update the cell linked structure i.e the cells through which this node moves in meantime of running this algo.
Step 4: In each cell structuremake space for the cell array of size $(T_{life}+\Delta)/(T+1)$,which store (time,position) pairs.
Step 5: Return head pointer to first active node.
}End.
```

3.5.3 Algorithm to Maintain Data Structure

ALGO Maintain_ Data_ structure:

Input1: A node which maintains it.

Input2: A data or detection packet receive.

Output:A node pointer to head node.

```
Start {
Step 1: Access head pointer.
Step 2: for(each node in active link list)
    {
    If (Node is in data, detection packet)
        {
        Update(Time,Position) pair in cell linked structure.
        }
    }
Step 3: Return
} End.
```

3.5.3 Algorithm for wormhole detection

```
ALGO Wormhole_ Detection:
Input: Packet p, Node N.
Output: BOOL: YES or NO.
Start {
Step1: Access Head Pointer
Step 2: step up to node N in active node link list.
Step 3: take (time , position) pair from each cell array concern with that node, where time difference between these two pairs is minimum.
Step 4: Then apply equation a for each two pairs selected and calculate $v$.
Step 5: if $v$>v then raises alarm for wormhole
Else
No wormhole
} End.
```

Chapter 4

SIMULATION & RESULTS

4.1 Simulation Setup

This chapter provides a simulation and its results for a wormhole attack and its defense mechanism COTA in Reactive routing protocol environment. The protocol used to study wormhole attack and defense mechanism COTA is DSR (Dynamic Source Routing). The tool used to simulate our work is open source simulator GlomoSim.

Simulation parameter set for our study is as below:-

Parameter	**Value**
Simulation duration	10 minute
Simulation area	1000*1000 meter
Number of mobile nodes	100
Transmission power	15 db.
Mobility model	Random waypoint
Traffic type	CBR
Data payload	512 bytes
Mobile speed	(0-20) m/s

Table 1: Simulation parameter

Here, we use the Cell based Open Tunnel Avoidance Scheme to detect wormhole in the path from source to destination. We also analytically analyze the behavior of COTA with DSR.

4.2 Discussion Parameters

We compare our results considering the following scenarios:-

- DSR without wormhole (Both static and mobile ad hoc network).
- DSR with wormhole in static ad hoc network.
- DSR with wormhole in Mobile ad hoc network.

These above scenarios are compared in terms of packet delivery ratio, End-to-End delay and throughput against the number of packets sent. Then, these scenarios are also compared with each other which provide us valuable insight about wormhole existence in the path. We also compare the number of times destination node raise a false alarm even when there exists no wormhole in the path. Number of false positive alarms is compared against the sensitivity which is the maximum mobility in unit distance time. Thereafter, we also check the improvement in number of false positive alarm with respect to added offset in concern with detection equation Eq.3.2.

4.3 Assumptions

Two or more nodes in our network can collaborate with each other and then these nodes can behave in malicious manner also. Collaborating nodes have high transmission power and their malicious behavior is very intelligent in which sometimes they drop the packet or another time forward it normally. In this way it is tough to identify malicious nodes in normal traffic operation.

4.3 Simulation Results

4.4.1 Scenario 1: DSR without Wormhole

This scenario depicts the normal DSR working without any wormhole nodes in the network. These results will act as a base result in calculating the damage done by wormhole path in the network.

Here, we compare this scenario for both static and mobile ad hoc environment on our analysis parameters and then these results help us further in analyzing wormhole efficiently.

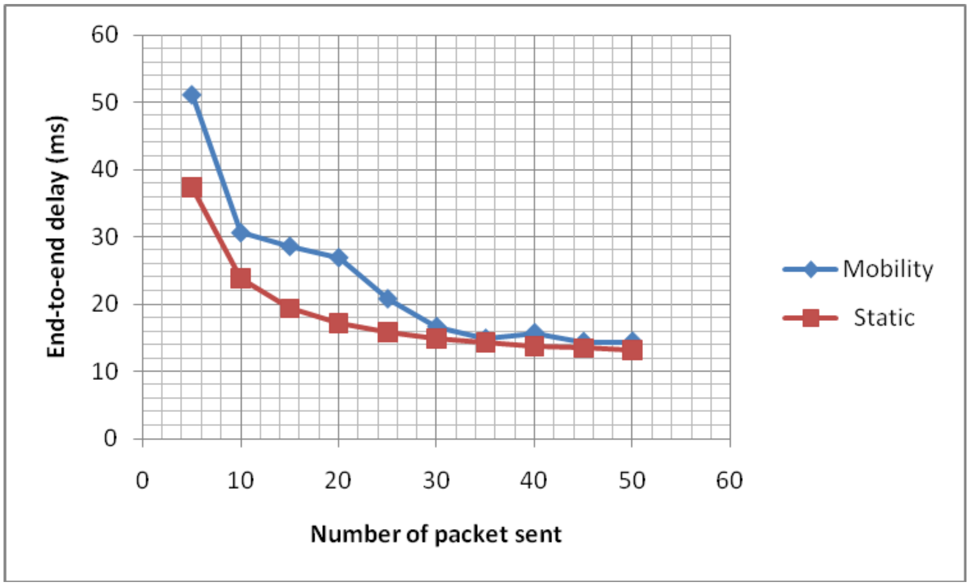

Fig. 4.1: End-to-End delay

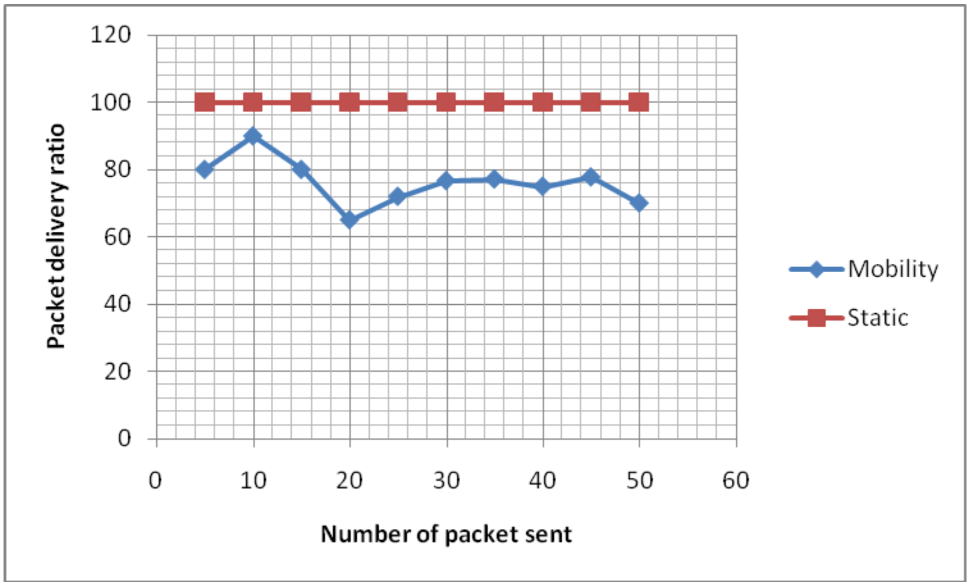

Fig. 4.2: Packet Delivery Ratio

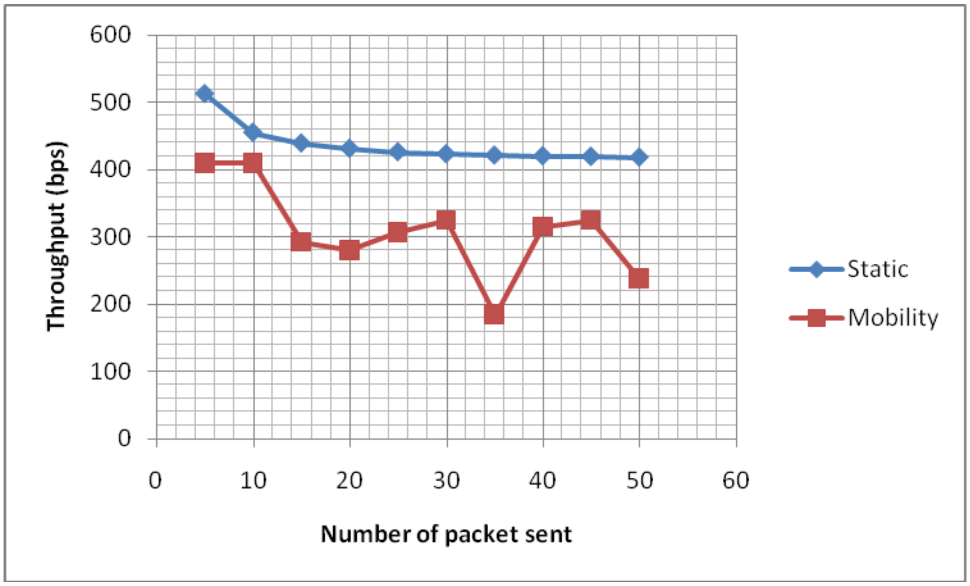

Fig. 4.3 Throughput

Discussion

Normally DSR works comfortably with an approximately 15 ms average End-to-end delay. As the number of packets sent increases and go beyond the 40 packets average End-to-End delay decreases. if we compare the average end to end delay for static and mobile ad hoc network in DSR then we figure out that, in case of mobility it is slightly more than the delay in static environment. PDR is 100% for static ad hoc network but on introduction of mobility PDR varies from 70% to 96% depend upon mobility scenario. Mobility also decreases the throughput which is between 200 bps to 424 bps as compare to throughput which is much higher in static environment around 470bps.

4.4.2 Scenario 2: DSR with Wormhole in static ad hoc networks

In this scenario, we analyze the impact of wormhole in an ad hoc network when there is no mobility. The statistics collected here enable us to analyze the positive aspect of wormhole in the network. Then we compare these statistics in the same situation but, this time collaborative nodes are malicious. This comparison depicts the wormhole attack's damage to static ad-hoc network.

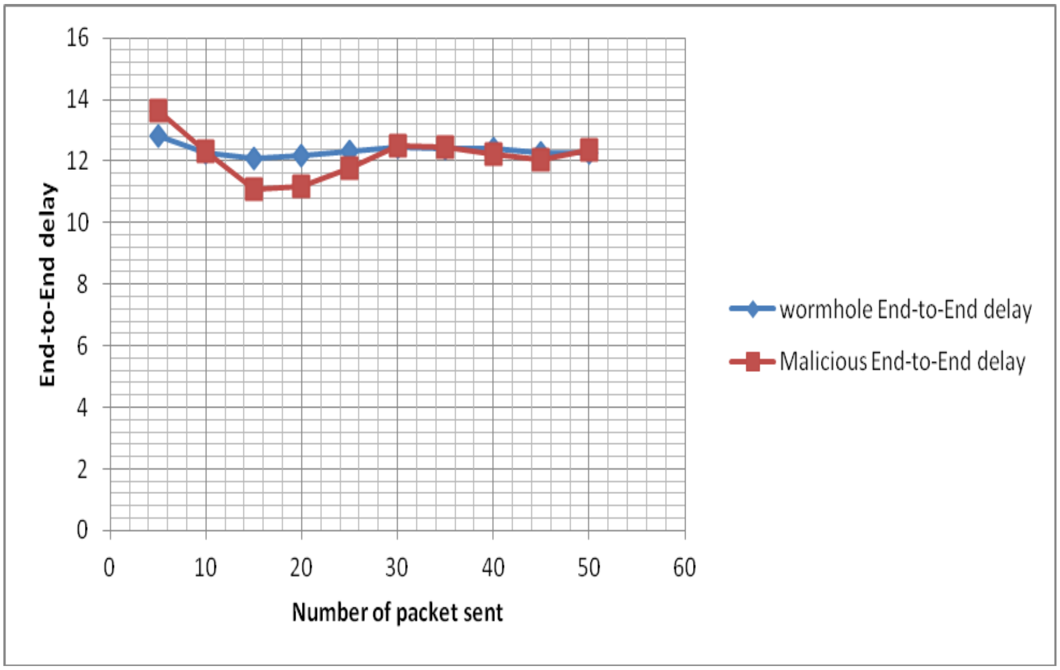

Fig. 4.4 End to End delay (Static)

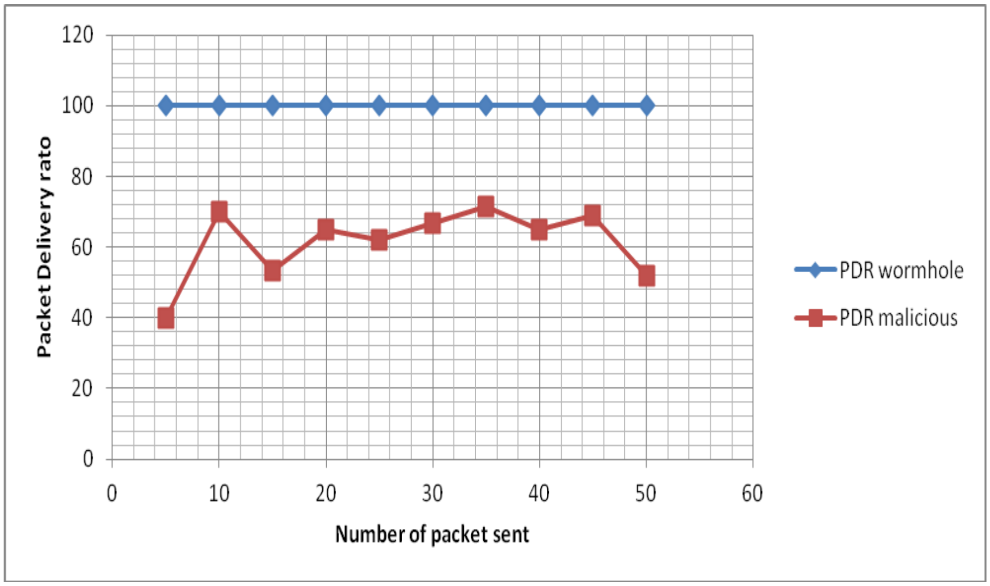

Fig. 4.5 PDR (Static)

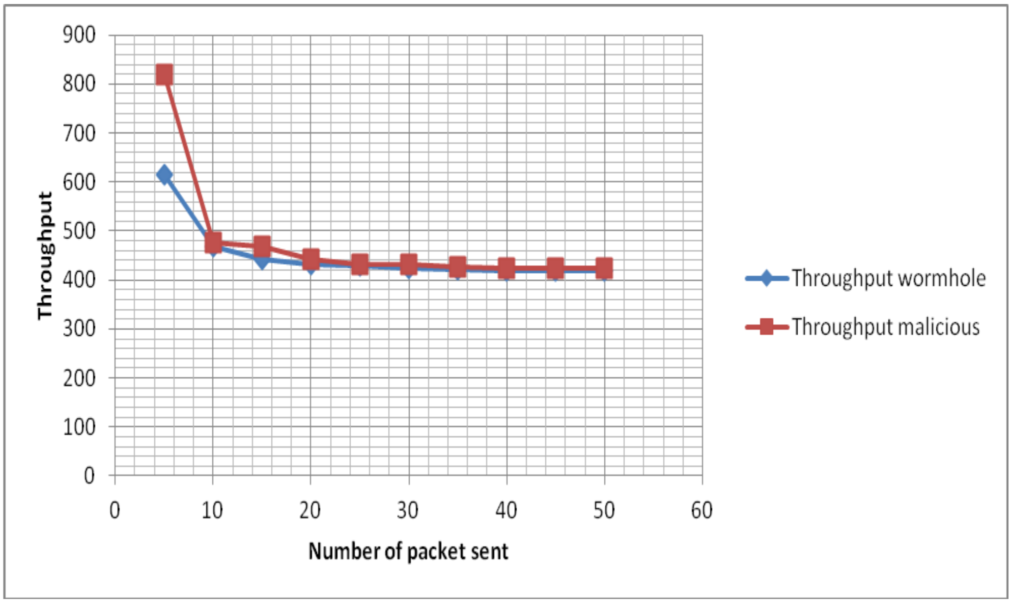

Fig. 4.6 Throughput (Static)

Discussion

The results collected in this static environment indicate that, when wormhole comes in the path results into less average End-to-End delay. The reason for this decrement is decrement in hop length which leads to less processing and queuing time. Here, End-to-End delay is 12ms as compared to 15 ms in previous scenario.

Here, due to malicious activity end to end delay is not much impacted but the main impact of malicious activity is shown in PDR. Due to maliciousness the packet delivery ratio goes down remarkably and the randomness in PDR in malicious activity graph is due to random behavior of attacking nodes. PDR in wormhole without maliciousness is 100% but as we introduce maliciousness, it varies between (40%) to (70%). Throughput increases for the static wormhole without maliciousness as compare to normal DSR without wormhole.

4.4.3 Scenario 3: DSR with Wormhole and Malicious Activity in Mobile Ad hoc Network

In this scenario we compared the situation of wormhole attack with or without maliciousness for mobile ad hoc network. These results help us to analyze the both positive and negative aspects of wormhole in an mobile ad hoc networks.

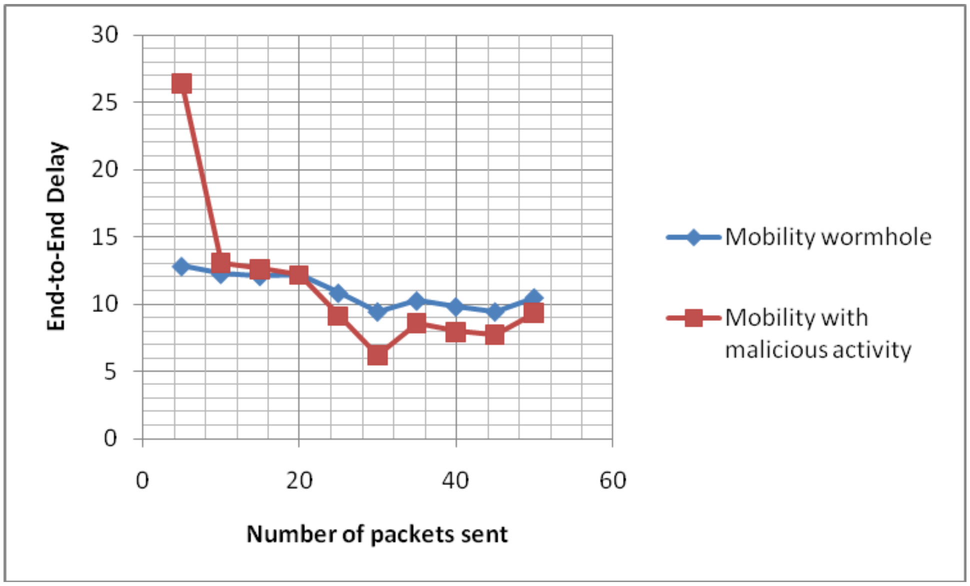

Fig. 4.7 End-to-end delay (Mobile)

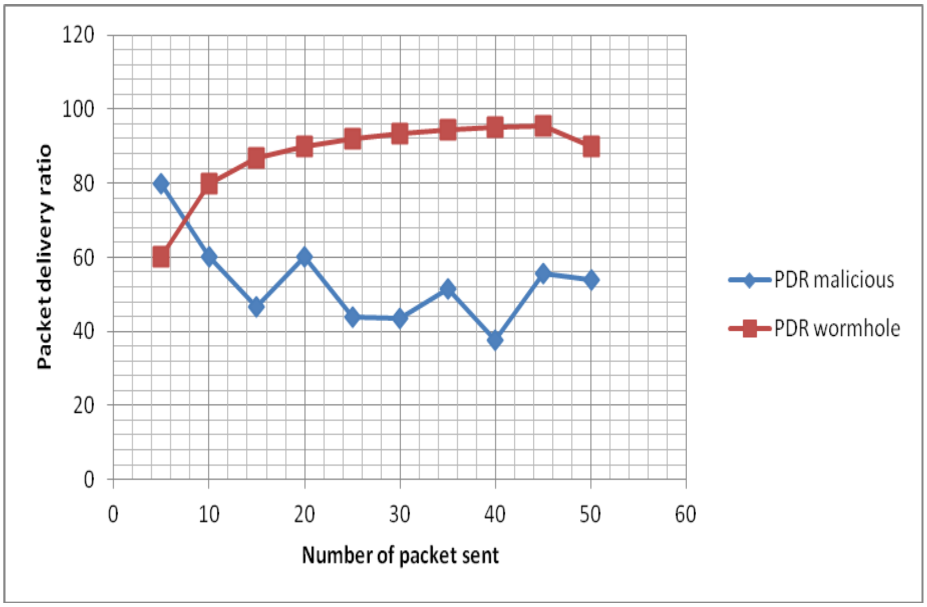

Fig. 4.8 PDR (Mobile)

Discussion

The results obtained show the effect of wormhole in mobility scenario. As compare to scenario1's mobility case here, average End-to-End delay decreases from 17 ms to 10 ms due to wormhole existence in the path. The impact of maliciousness is not on average End-to-End delay as our malicious nodes only drops data packets but control packets are relayed normally.

Here for both, wormhole with malicious activity and without malicious activity more or less average end to end delay is same. Second parameter is PDR and the impact of malicious activity is completely shown in figure 4.8. PDR goes down remarkably as compared to PDR with wormhole in mobile ad hoc network which is between (60%) to (95%). There is less impact of wormhole on throughput in this scenario.

4.4 COTA Analysis

To analyze the impact of COTA scheme for defending wormhole is calculated in terms of number of false positive alarm i.e. the number of times COTA raise alarm of having wormhole even when there exist no wormhole. This parameter is judged with respect of sensitivity per unit distance. Sensitivity is related to node mobility, Which is the maximum distance a node can move in per unit distance time. Here, we analytically analyze COTA defense mechanism analytically using the results finds in scenario 3.

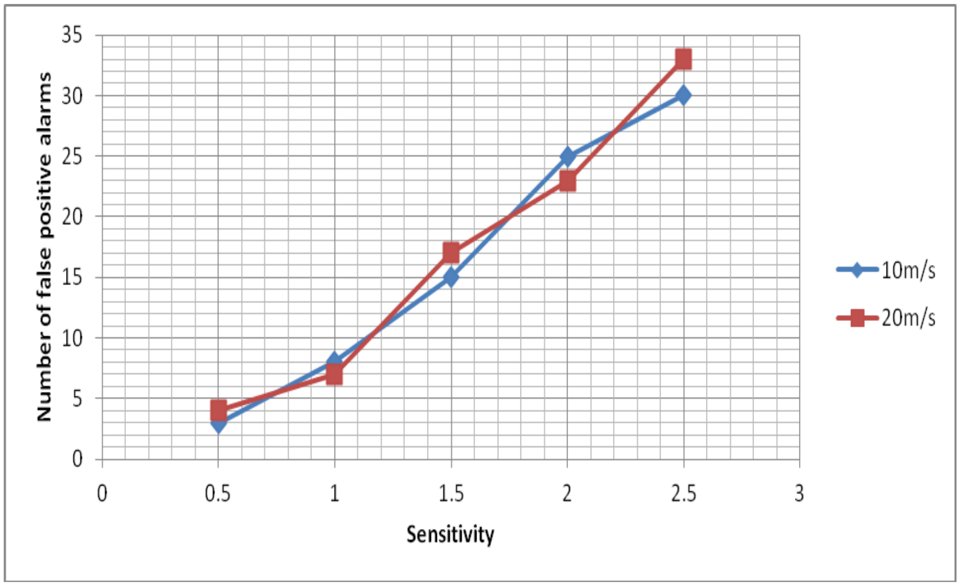

Fig. 4.10 False positive alarm (Mobile)

The number of false positive alarm increases for both10 ms and 20 ms velocity with respect of increment in sensitivity. Number of false positive alarm is approximately same for both velocities in this situation. So, we can conclude that velocity does not impact much on number of false positive alarm when compared with respect of sensitivity per unit distance.

Number of false positive alarm leads to high communication overhead as once the destination broadcast negatively for existing path. Then once again route is formed which results into undue uses of network resource. Hence, number of false positive alarms should be minimized. To lower the number of such mistakes, the following equation needs to be updated by adding offset.

$$\boldsymbol{V=\max\left(\left(0,\|P_{new}-P_{select}\|\right)-\delta+\text{offset}\right)/\left(\|T_{new}-T_{select}\|+\Delta\right)} \qquad \mathbf{4.1}$$

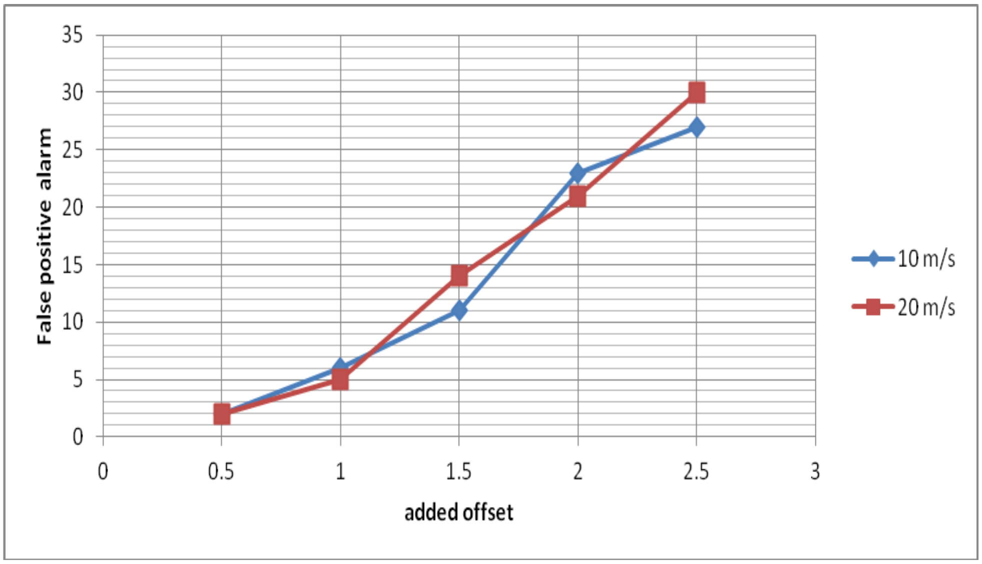

Fig.4.11 Added offset (Mobile)

Added offset lower the number of false positive alarm only up to (1.2) sensitivity. Thereafter its impact is not good as desired.

4.5 Results discussion

By comparing the results of above three scenarios, we find that wormhole existence in a path leads to low hop length which in turns results into low end to end delay for both static and mobile ad hoc network. Due to malicious activity packet delivery ratio goes down and varies randomly due to random behavior of the attacking nodes. When nodes is not an attacker then wormhole is a beneficial thing but control of whole network goes to them as mostly 70% of the route formed using them. Hence this added advantage may be a curse when collaborative nodes behave in a malicious manner.

Results on number of false positive alarm represent that as the sensitivity per unit distance increase results into increment of false positive alarm. This, results into high communication overheads. To minimize this equation Eq.7 is updated but, in our case its impact is only up to (1.2) sensitivity/distance.

Chapter 5

CONCLUSION & FUTURE SCOPE

5.1 Conclusion

In this work, we have studied the collaborative attacks and implemented the wormhole and it's implication on mobile ad hoc network was analyzed. There are many mechanism like End-to-end mechanism, Cell based open tunnel scheme etc to defend against wormhole attack. We have integrated COTA with Dynamic Source Routing protocol to defend against wormhole attack. In our analysis we have represented that due to wormhole attack the packet delivery ratio goes down which raises through COTA mechanism application by raising alarm about wormhole path in the network. Wormhole exixtence in the path results into smaller number of hop counts which leads to reduced average End-to-end delay. In positive sense wormhole is beneficial in respect of less delay associated but, malicious behaviour of wormhole nodes changes the whole scenario by misbehaving in the network. Our implementation of COTA mechanism gives us satisfactory results in respect of reactive routing environment .

5.2 Future work

This work can be extended in a way so that, COTA can be integrated with other routing protocols. The mechanism of COTA can be changed in order to minimize the number of false positive alarm which in turns leads to minimized communication overheads. The impact of more number of wormhole nodes in the network can be analyzed and its implications on network can guide us to modify the exixting defense mechanisms for dense malicious environment. Even the implementation of COTA can be modified to optimize computation and storage complexity.

Bibliography

1 G. Neelesh, G. Roopam, “Routing protocols in MANET an overview”, IEEE 2010.

2. I. Chlamtac et.al, “MANET: imperatives and challenges”, Elsevier, 2003.

3. Hu Yih-chun, p. Adrian et.al, “Wormhole attack in wireless networks”, IEEE journal on selected areas in communications, Vol. 24, No. 2, Feb 2006.

4. L. Hu and P. Evans, “using directional antennas to prevent wormhole attack”, in proceedings symp, netw, distrib, sust, security, Feb 2004.

5. D.B Johnson and D.A Maltz, “Dynamic Source routing in ad hoc wireless networks”, in mobile computing, Norwell M A KLUWER, 1996, ch5, pp. 153-181.

6. D. L Mills, “A computer controlled LORAN-C receiver for precision timekeeping”, Dept Elect. Comput. Engg., Univ delware Newark, DE, Tech, March 1992.

7. R. L Rivest, A. Shamir, and L. M Adleman, “A method for obtaining digital signature and public key cryptosysyem”, Communication ACM VOL. 21 No 2, pp. 120-126, Feb 1978.

8.M.A Azer, S.M El-kassas et.al, “Immuning routing protocols from the wormhole attack”, Conf. on System and Network communication IEEE 2009.

9.Y.C. Hu, A. perring, and D.B Johnson, “Packet leash: a defense against wormhole attack in wireless network ”, in proceedings of the 22nd annual joint conference of the IEEE computers and communication socities (INFOCOM), pp. 1976-1986, 2003.

10. R. Maheshwari, J. Gao, and S.R Das, “Detecting wormhole attacks in wireless networks using connectivity information”, In INFOCOM 2007 IEEE, pp. 107-115.

11. W. wang, B. Bhargava, Y.Lu, and X.wu, “ Defending against wormhole attacks in mobile ad hoc networks”, wireless communication and mobile computing, pp. 483-503, January 2006.

12. F. N Abdesselam, B. Bensaon et.al, “Detecting and avoiding wormhole Attacks in wireless Ad hoc networks”, IEEE communication magazine April 2008.

13. M. Jain and H. Khandwal, “ A survey on complex wormhole attack in wireless ad hoc networks”, International conference on advances in computing , control, and Telecommunication Technologies, IEEE 2009.

14. Xia. Wang, J. wung, “ An End-to-end detection of wormhole attack in wireless ad hoc network”, in COMPSAC, IEEE 2007.

15. M. Khabbazian et.al, “Severity analysis and countermeasures for the wormhole attack in wireless ad hoc networks”, IEEE transactions on wireless communication, Vol 8 No 2, Feb 2009.

16. M. corner and B. Nobel, “Zero Interaction Authentication”, In proceedings of 8th annual international conference on mobile computing and networking, IEEE 2002.

17. Manoj B.S and Siva Ram Murthy, C, Ad hoc wireless network:issues and challenges, Technical report, Department of computer science and engineering, IIT Madras. 2003.

18. Pradip M. JawandhiyaM. M Ghonge, M. S Ali, J. Deshpande, “A survey of Mobile ad hoc network attacks”, International journal of Engineering science and technology, Vol 2 issue 9, 2010, pp. 4063-4071.