DEFENDING AGAINST WORHOLE ATTACKS IN POSITION BASED ENVIRONMENT IN MANET

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

Vinesh Kumar

Under the Supervision of

Dr. D.K.Lobiyal and Mr. Sushil Kumar

SCHOOL OF COMPUTER AND SYSTEMS SCIENCES
JAWAHARLALNEHRUUNIVERSITY
NEW DELHI–110067
INDIA

JULY 2012

JAWAHARLAL NEHRU UNIVERSITY

SCHOOL OF COMPUTER AND SYSTEMS SCIENCES

NEW DELHI – 110067, INDIA

CERTIFICATE

This is to certify that the dissertation entitled “**Defending against Wormhole attaks in position based routing environment in MANET”**being submitted by **Mr.Vinesh 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
(Supervisior)(Supervisior)(Dean)

SCHOOL OF COMPUTER AND SYSTEMS SCIENCES

JAWAHARLAL NEHRU UNIVERSITY

NEW DELHI-110067

DECLARATION

This is to certify that the dissertation entitled **“Defending Against Worhole Attacks In Position Based Environment In Manet”** 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.

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.

Vinesh Kumar

Dedicated To*God And My Well Wishers Who Gave Me All The Beautiful Things I Needed*.

Acknowledgement

I would to like to express my honest gratitude to my supervisor, Dr D.K.Lobiyal and Mr. Sushil Kumar of the School of Computer and Systems Science for their out standing help, support, guidance and efforts during my research. Successful completion of the present research effort not has been possible without them, who not only served as my guide but also encouraged and challenged me throughout my research program. they patiently guided me through the dissertation process, never accepting less than my best efforts.

I also thankful to Late Prof. G.V.Singh for hisunvaluable help and motivation during my work.

I would also like to choose this opportunity to express my respect to my parents and my family who always motivated me go forward and complete the task at hand. And finally, to my friends and colleagues who kept me sane during the long hours of work.

Vinesh Kumar

Abstract

Mobile ad hoc network is an infrastructureless network. MANETsare prone to various security threats posed due to the existence of some malicious nodes in the network. Vrious types of security attacks try to degrade the performance of the network and at times even modify/fabricate the data that is being communicated between various nodes. One of such attack is a collaborative attack, in which attacker nodes collaborate together to disrupt the activities of the network. In this work, we focus on one of the collaborative attacks,which is the Wormhole attack. A mechanism named Cell-based Open Tunnel Avoidance (COTA) scheme to manage the detectioninformation to classify the wormhole attack results high computation and storage power. Considering the limited resources available to the nodes in a MANET, this is a matter of great concern. In this work, we detect the wormhole attack using the cell based tunnel scheme with location added routing protocol. The algorithm for implementeation of COTA is proposed. The proposed work is simulated using GloMoSim network simulator. It has been observed from the simulation results that the performance of the network in terms of packet delivery ratio and average end-to-end delay are improved.

Table of Contents

Chapter 1: Introduction

Chapter 2 Security in MANET and Related Work

Chapter 3:COTA Mechanism and Algorithms

Chapter 4: Simulation and Results

Chapter 5: Conclusion and Future Work

List of figures

CHAPTER 1

Introduction

1.1 Background

The concept of ad hoc mobile networks has been developed on the basis of extending the notations of mobility to all the components of the environment. It may contain mobile platforms called nodes that can change their position freely and without any constraints.

Mobile ad hoc network or short live network operates in the absence of fixed infrastructure. They offer quick and easy network. Ad hoc is a Latin word, which means "for this or for this only"[25] is an autonomous system of mobile nodes connected by wireless links[25], each node operate as an end system and as a router as well for all other nodes in the network.

An ad hoc network is a collection of wireless mobile nodes which dynamically forming a temporary network without help of any established infrastructure or centralized administration. Mostly ad hoc network uses in military domain. Ad hoc networks outside the military domain have developed in academic environment but recently commercially oriented solutions started to appear e.g. mesh network, SPA network etc[25].

Many technical issues exist in designing of an ad hoc network. In this type of network multi hop relaying concept is used while forwarding data packets to communicate and share radio channels over which communication takes place, due to shared radio medium, mechanism for sharing common channel is major concern because the bandwidth is a real constraint in an ad hoc network.

In an ad hoc network environment medium access protocols are used for bandwidth reservation. So that it must be used efficiently and effectively, Nodes in this environment need to be more intelligent because, there nodes have not only to do their own management but also network management and their power and processing capabilities are also week.

1.2 Issues in Mobile Ad-hoc Networks

Mobile ad hoc network are formed dynamically by any system of mobile nodes that are connected via wireless links without using the existing network infrastructure or centralized administration. These nodes are free to move randomly and organize themselves arbitrarily; the network topology may change randomly. Such a network may operate in an internet fashion or may be connected to the larger internet. Mobile ad hoc network are infrastructure less network. Since, they do not require any fixed infrastructure such as base station for their operations. In general, routes between nodes in an ad hoc network may include multi hops and hence it is appropriate to call such networks as multi hop wireless ad hoc network. Each node will be able to communicate in order to use intermediate nodes to relay the message hop by hop. Each mobile node might have a different configuration and processing capabilities. Designing network protocol and algorithm for the heterogeneous network can be complex and require dynamic adaption to changing condition.

In an ad hoc network accessibility to any node is much convenient in comparison to any other network. An ad hoc wireless network faces the problem of wireless communication and wireless networking [24]:

a. The wireless medium has neither absolute nor readily observable boundaries outside of which stations are known to be unable to receive network frame and energy constraint operation because batteries carried by each mobile node have limited power supply and processing power is limited, which turn limited service and application that can be supported by each node. This become a bigger issue in mobile ad hoc network because as each node acting as both an end system and a router at the same time. The additional energy is required to forward packets from other nodes.

b. The channel is unprotected from outside signals

c. The wireless medium is significantly less reliable than wired media.

d. The channel has time varying and asymmetric propagation properties.

e. Hidden terminal and Exposed terminal problem may occur.

These problems and complexities in an ad hoc routing applications increase many folds due to the presence of large network size and high number of node. Scalability is critical to these networks. The step toward a large network consisting of nodes with limited resources are not straightforward and present many challenges that are still to be solved in areas such as

Security, high capacity wireless technology, addressing, routing, location management, configuration management, interoperability[25] etc.
The lack of fixed infrastructure adds a number of characteristics, complexity, design constraint and centralized administration. Each node operates in distributed peer to peer mode, acts an independent router and generates independent data. Network management has distributed across different nodes, which bring added difficulty in fault detection and management. In MANET every node acts as a router and forwards each other's packets to enable information sharing between mobile hosts.

1.3 Routing in MANET

Routing is the core problem in networks for delivering the data from one node to another node. Routing is used to discover and preserve the routes between the source and destination. In MANET Routing plays an important role. Here, we have several routing protocols named as DSDV,AODV,DSR,TORA,LAR, Position Based Routing etc. Here below a short introduction about above protocols is given [7]:

- **DestinationSequencedDistanceVector [37]**DSDVisatable-drivenproactiveroutingprotocol,whichisbaseduponBellman-Fordroutingalgorithm.Eachnodeinthenetworkmaintainsaroutingtableinwhichallthepossiblecombinationofdestinationnumberofroutinghopsarerecorded.DSDVupdatedroutingtablesaresentperiodicallythroughoutthenetworktomaintainthe consistency.

- **DynamicSourceRoutingProtocol(DSR)**

  [36]TheDynamicSourceRoutingprotocolissimpleandefficientroutingprotocol designedspecificallyforuseinmultihopwirelessadhocnetworksofmobilenodes. DSRallow thenetworktobecompletelyself-organizingandself-configuringwithouttheneedforanyexistingnetworkinfrastructureoradministration.Theprotocoliscomposedoftwomechanismofroutediscoveryandroutemaintenance whichworktogetherfor nodes todiscoverandmaintainsourceroutestoarbitrarydestinationintheadhocnetworks. Theuseofsourceroutingallowspacketroutingtobetriviallyloopfree and avoidtheneedforuptodateroutinginformationintheintermediatenodesthroughwhichpacketsareforwarded andallowsnodesthatareforwardingoroverhearingpacketstocachetheroutinginformationinthemfortheirownfutureuse.Theprotocolisbasedonon-demandsoitisanon-demandsourcerouting.

  ThelimitationofDSRprotocolisthatthisisnotscalabletolargenetworksandevenrequiressignificantlymoreprocessingresources.

- **Ad hocOnDemandDistanceVectorProtocol(AODV) [35]**Ad-hocOnDemandDistanceVectorroutingprotocolisavariationofDSDVroutingprotocolwhichiscollectivelybasedonDSDVandDSR.TheaimofAODVistominimizetherequirementofsystemwidebroadcaststoitsextreme.Itdoesnotmaintainroutesforeverynodetoeveryothernodeinthenetworkrathertheyarediscoveredasandwhenneededandmaintainaslongastheyarerequired.

  InAODV,thefourstepsarerequirednamedasroutediscovery,expendingringsearch technique,settingupforwardingpathandroutemaintenance.AODVsupportbothuncastandmulticastpackettransmissionevenfornodesinconstantmovement.It’srespondveryquicklytothetopologicalchangesthataffecttheactivenodes.

  ThelimitationofAODVisthatitrequiresthenodesinbroadcastmediumcandetecteachother’sbroadcast.

- **TemporallyOrderedRoutingAlgorithm(TORA)**

  [38]TORAisdistributedandloopfreereactivetyperoutingprotocolwhich,provide smultipleroutes,withlessroutingoverhead.Inthiseachstationneedsinformationaboutitsone-hopneighboronlythisshowsthedistributedoperationofthisprotocol,whichprovidesmultipleroutestowardsadestination.TORAprovidesthemechanismforroutediscovery,routemaintenanceandroutedetection.TORAisdependingonsynchronizedclocksamongnodesinadhocnetworks.

1.4 Position Based Routing

Mobile ad hoc network change its topology frequently without any prior information. Routing in such network is a challenging task so in such cases we have two approaches [6]:

1. TopologyBasedRouting
2. PositionBasedRouting

1.4.1 Topology Based Routing

In this routing the protocols use the information about the links that exists in the network to perform packet forwarding. In this routing, the topology can change randomly without prior information.

1.4.2 Position Based Routing

In position based routing protocols[27] packet forwarding based on physical location of the mobile nodes in the network. Packet forwarding decision is based on the position of the current node, its neighboring node position and the position of the destination node. Position based routing protocol require a little traffic than topology based routing protocol. Position based routing protocols do not require the establishment or maintenance the routes and thus eliminate the overhead of frequent topology updates and route acquisition of topology based routing protocols. Position based routing eliminate some of the limitations of topology based routing by using physical location or some additional information.

In position based routing[27] each node determines its own position through the use of GPS. Position based routing supports the delivery of packets to all nodes in a given geographical region in a natural way.

We can distinguish three main packet forwarding strategies for position based routing[27]:

1. Greedyforwarding
2. Restrictedforwarding
3. Hierarchicalforwarding

1.4.2.1 Greedy forwarding

In the greedy packet forwarding the sender of a packet includes the approximate position of the recipient in the packet. This information is gathered by an approximation location service. There are different strategies a node can use to decide to which neighbour a given packet should be forwarded [27].

a. Mostforwardedwithradius*R*(MFR):MostforwardedwithradiusRtriestominimize thenumberofhops.Apackethastotraverseinordertoreachatdestination.MFRisgood strategieswherethesenderofapacketcannotbeadoptthesignalstrengthoftransmissiontothedistancebetweensenderandreceiver.

b. Nearestwithforwardprogress (NFP):InNFR,thepacketistransmittedtothenearestneighbourofthesenderwhichis closertodestination.

Greedy routing may fail to find a path between sender and destination, even though one does exist. In Greedy routing problem of looping of packets may occur.

1.4.2.2 Restricted Directional flooding

With directed flooding nodes forward[27] the packets to all neighbor that are located in the direction of destination. DREAM and LAR apply the above principle. LAR uses directed flooding only for route discovery while DREAM applies a restricted flooding for packet delivery.

1.4.2.3 Hierarchical routing

In traditional networks the complexity of each node has to handle can be reduced tremendously by establishing some form of hierarchy. Hierarchical routing [27]allows that network to scale very large number of nodes.

1.5 Location Based Routing

A localization Scheme Known as the coordinate system involves the work done by Nagpal, Shrobe and Bachrach at MIT. It uses a subset of GPS nodes to provide nodes without GPS a sense of relative location. HU et. al. [10] have consider packet, geographic and temporal lasses.

HU and Evansdeveloped a protocol using directional antennas are able to detect the angle of arrival of a signal[11]. In a survey of potential application of GPS, Dommetry and Jain briefly suggest the use of location information in Ad hoc networks[1], they do not elaborate on how the information may be used. Most current research in MANET routing is focused on topology-based protocol[27]. Location based routing[13] is a subset of topology based routing.

Location aware routing protocols[13] uses during the forwarding operations, the node’s position provided by GPS or other mechanism. Location based routing[13] does not require routes establishment and maintenance. The use of geo location information avoids network wide searches as both control and data packets are sent towards the known geographical co-ordinates of the destination node. Location based routing is typically used for long distances[13].

Position based routing protocols[27] offer the following advantages. Due to recent developments, they provide better scalability and performance by using geographical position to improve routing decisions and efficiency. Many of the current protocols have a low packet overhead meaning they use small packets and a reduced number of signaling packets. There are several advantages of GPS technology. GPS technology is owned and maintained by the US Government. It is global satellite systems that provide reliable location information in all types of weather. It is by design, the best option for tracking and identifying nodes. It is a free service to any device with a receiver. The technology first became available for mobile phones in November of 2004. There are currently thirty satellites available and a plan for increasing the number to thirty six.

With the help of location information service for mobile hosts one can decrease overhead of route discovery. The LAR[13] is used to reduce the search space for desired route location information used in LAR [13]protocols may be provided by Global Position System. It may be possible that the location information provided by Global Position System has some error. The error is the difference between Global Position System Calculated Co-ordinates and the real co-ordinates[13]. In the location added routing, we have two zones named as Expected zone[13] and Request zone[13].

1.5.1 Expected zone[13] let us assume a node S that needs to find a route to node D. We assume that S knows the location L of node D at time t_0 and the current time is t_1.

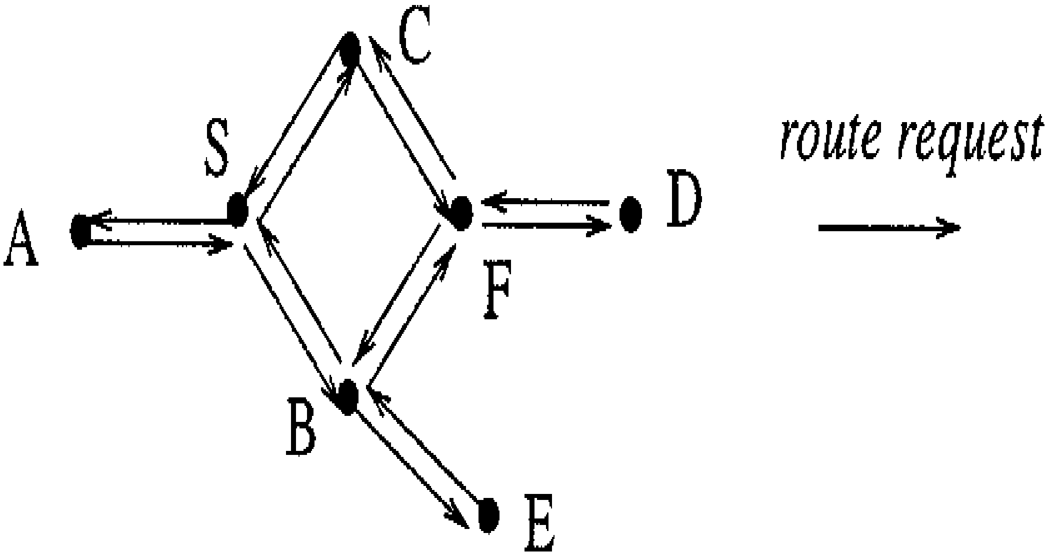

Figure 1-Example of flooding [13]

So the Expected zone of node D from the view point of node S at time t_1, is the region that node S expects to contain node D at time t_1. S may assume the Expected zone is the circular region of radius V (t_1-t_0) centered at location L.

If node S does not know the location of D then S cannot determine the Expected zone so the entire region may be Expected zone for the ad-hoc networks[13]. If S knows that destination D is moving north then the Expected region reduces to semi circle as in the figure 2.

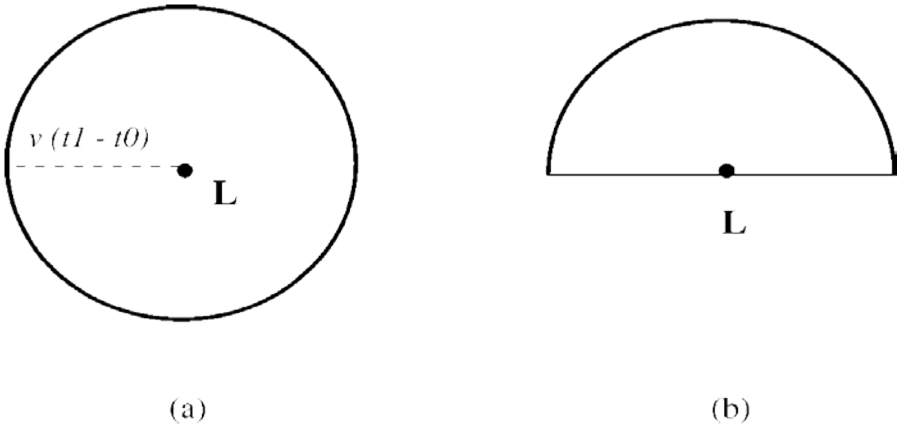

Figure 2-Examples of Expected zone [13]

1.5.2 Request zone [13] The LAR algorithm uses flooding with one modification. Nodes S define a request zone for the route request. A node can forward a route request only if it belongsto request zone. To increase the probability of the route request will reach at node D; the request zone should include the Expected zone,so the request zone can be used for the finding a path route discovery overhead also increases with the size of route request zone.

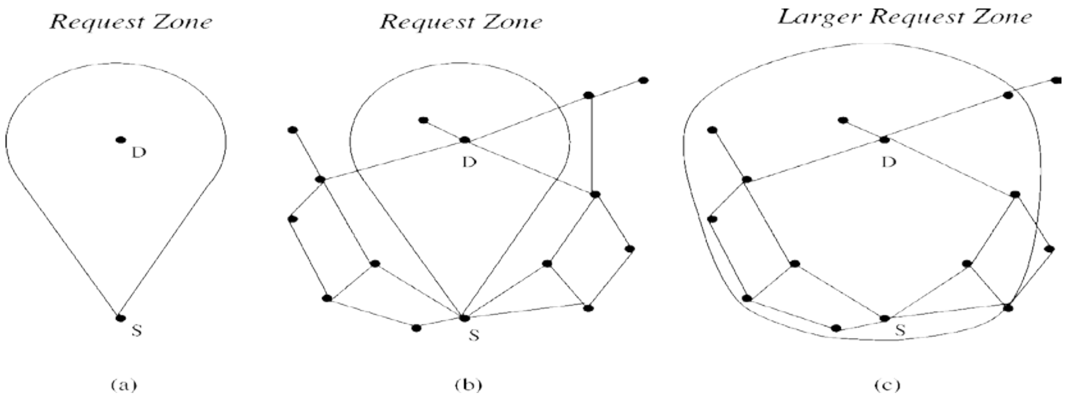

Figure 3-Example of request zone [13]

1.5.3 LAR Scheme [13]in the location added routing, we have two scheme named as LAR1 and LAR 2. Now we can briefly explain these two schemes.

1.5.3.1 LAR 1[13] In LAR 1, we usearequestzonethatisrectangular inshape as in figure3. Let node Sknow thatnodeDwasatlocation(X_d,Y_d)attimet$_0$.Attimet$_0$ nodeS initiateanewroutediscoveryfordestinationD.We assumethatnodeSalsoknows theaveragespeedvwith whichDcanmove.Usingthis,nodeSdefinethe expected zone to the circle of radius R =v(t_1-t_0) centred at location (X_d,Y_d).InthefirstLARalgorithm,we definethe requestzoneto bethesmallestrectanglethatincludescurrent locationofS andtheexpectedzone(thecircularregiondefined above), suchthatthesidesoftherectangleareparalleltotheXand Yaxes[13]. As In figure 4,therequestzone istherectangle whosecornersareS,A,BandC,whereasinfigure4 b, therectanglehascornersatpoint A,B,CandGnote that,inthisfigure 4, currentlocationofnodeSisdenotedas (X_s, Y_s)[13].

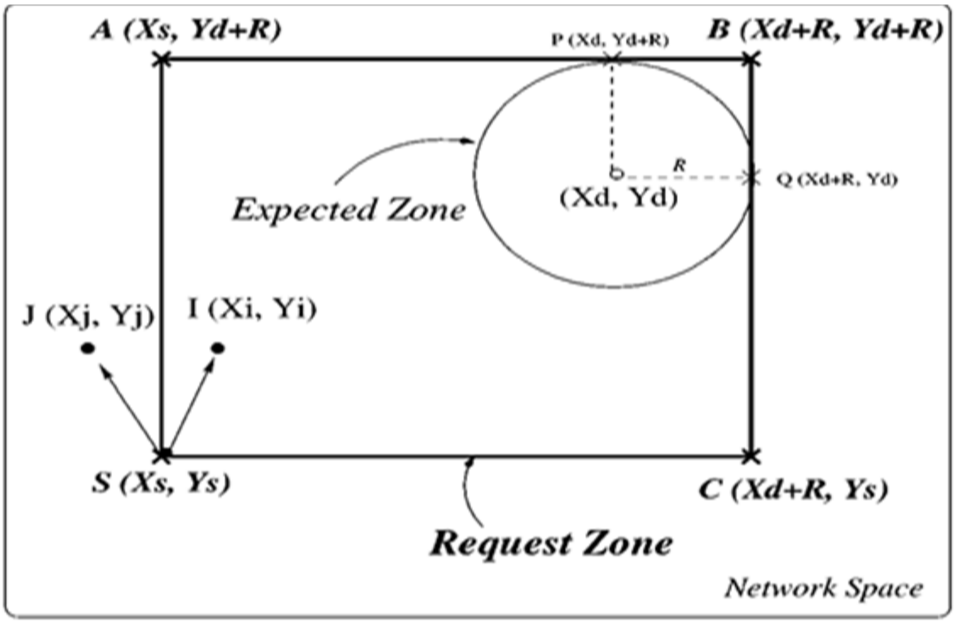

Figure 4a- Source node outside the Expected Zone[13]

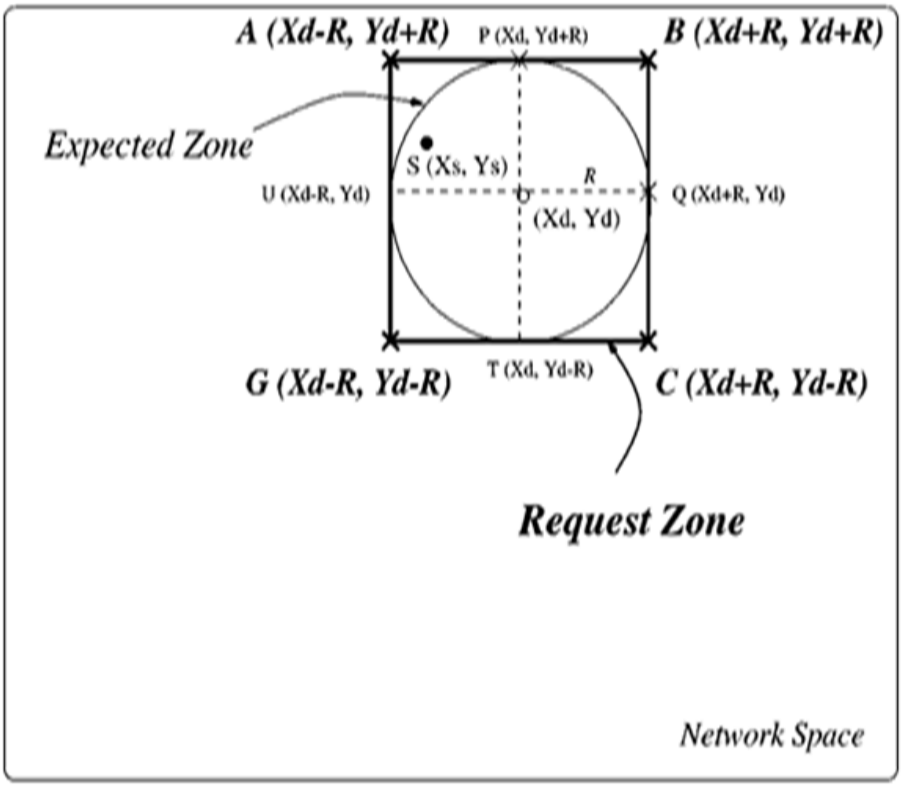

Figure 4b- Source node within the Expected Zone[13]

ThesourcenodeScandeterminethefourcornersoftherequestzone. Sincludes theircoordinatewith the route requestmessage transmittedwheninitiating routediscovery. Whenanodereceivesarouterequest, itdiscards therequest ifthenode isnotwithintherectangle specified bythefourcornersincludedintherouterequest.

Asinthefloodingalgorithm[13],nodeD receivestherouterequestmessage and itrepliesbysending aroutereplymessage.But incaseofLAR,nodeDincludesitscurrentlocationandcurrenttimeintheroutereplymessage. WhennodeSreceivesthisroutereplymessage, itrecordthelocationofnodeD.NodeS canusethisinformationtodetermine therequest zoneforafutureroutediscovery[13].

Thesizeoftherectangularrequestzoneaboveisproportional to(1)averagespeedofmovementvand(2)timeelapsedsincethelastknownlocationofthedestinationwasrecorded. Smallerrequestzone mayoccuratspeed that isneithertoosmallnortoolarge.Forlowspeed, it ispossibletoreducethesizeoftherequestzonebypiggybacking thelocationinformationonotherpackets,in additiontoroute replies.

1.5.3.2 LAR Scheme 2[13] InLAR2,nodeSincludestwopiecesof informationwithitsrouterequest[13]-

(1).AssumethatnodeSknowsthelocation(X_d,Y_d)ofnodeD at sometime$t_0$the timeat whichroutediscoveryisinitiatedbynodeSist_1,where$t_1>t_0$.NodeS calculatesitsdistance fromlocation(X_d,Y_d),denotedas$DIST_s$,andincludesthisdistancewiththerouterequest message.

(2).Thecoordinates(X_d,Y_d)arealsoincludedwiththeroute request.Whenanode I receivetherouterequestfromsendernodeS,nodeIcalculateitsdistancefromlocation(X_d,Y_d),denotedas$DIST_i$,andForsomeparametersαandβ,if$\alpha(DIST_s)+\beta>DIST_i$, thennodeIforwardtherequesttoitsneighbor.Whennode I forwardstherouterequest,itnow includes$DIST_i$and(X_d,Y_d)intherouterequest.Else$\alpha(DIST_s)+\beta<DIST_i$.Inthiscase,node Idiscard therouterequest[13]

Whensome nodes J receivetherouterequestfromnodeI thanitappliesacriterion.IfnodeJhasreceivedthisrequest,itdiscard therequest.Otherwise, node Jcalculateitsdistancefrom(X_d,Y_d)denotedas$DIST_j$.Now,therouterequestreceivedfromnodeIincludes$DIST_i$.If$\alpha(DIST_i)+\beta>DIST_j$,thennodeJforwardstherequesttoitsneighbours.Beforeforwarding therequest,J replacesthe$DIST_i$intherouterequestby$DIST_j$.Else $\alpha(DIST_i)+\beta<DIST_j$, inthiscase,nodeJdiscards therequest[13].

1.6 Problem statement

In MANETs, a pair of attacker nodes can collaborate to form a tunnel resulting in fabricating a scenario falsely, thus implying that the shortest path between the sender and the receiver nodes exists through these collaborating nodes. This fake path will then attract the data traffic i.e the packets will be routed through a wormhole path being either compromised or dropped. In [1], a mechanism was proposed to classify the wormhole attacks. This mechanism resulted in a high computation and storage powerthat form the important drawbacks of this mechanism. In this, the Cell-based Open Tunnel Avoidance (COTA) scheme [1] was proposed to manage the detection information.

In our Dissertation, we propose to implement the COTA mechanism over the position based routing environment using alocation based routing protocol. We further, provide a detailed analysis of the performance of COTA through simulations carried out using the Glomosim simulator[29].

1.7 Organization of Dissertation

In this dissertation the whole content is organize in the following manner; In chapter 1, we discuss about MANET, issues in MANET, routing in MANET and our problem statement. In chapter 2, we discuss the Security in MANET and related work. In chapter 3, we present the COTA mechanism [1] and our implementation algorithms. In chapter 4, we discuss the simulation setup and result analysis. In chapter 5 , we give the conclusion and future work.

Chapter 2

Security in MANET and Related work

2.1Security in MANET

Mobile ad-hoc network is more vulnerable than traditional wired network. Security is very difficult to maintain in this environment due to unreliability of wireless link between nodes and consistently changing topology. There are many security criteria[26]:

- **Confidentiality-**Theinformationmust reach; whoareentitledtoreceivetheinformation,notonlydata,Routinginformationmustremainsecure.
- **Integrity-** Oneshouldnottobeabletomodifythedataduringtransit.Integrityisthemostimportantcriteriaforsecurity.
- **Availability-** ThenetworkcanstilloperatewhenfacedwithaDoSattack.Thesetypesofattackcanbelaunchedatanylayerofthenetworkcausingphysicaljamming,disconnectionandroutingprotocol.
- **Authentication-**The receivershouldbeabletoidentifythesendercorrectly.Nootherpersoncantochangetheappearanceasthesender.
- **Non-repudiation-** Thisisusefultodetectionandisolationofcompromisednodes.
- **Accesscontrol-** In access control, the informationisbeinghandledbyauthorizednodes.
- **Authorization-**Rulesandregulations define restrictionofresponsibilityofnetworkandindividualnodes.

2.2 Types of security attacks

- **External and internal attacks**External attacks, in which the attacker aims to cause congestion, propagate fake routing information. Internal attacks, in which the adversary wants to gain the normal access to the network and participate in the network activities either by some malicious impersonation to get the access to the network as a new node or briefly compromising a current node and using it as a basis to conduct its malicious behavior**.**

  The security attack in MANET can be classified into two categories, namely passive attacks and active attacks [26]:

- **Passive attacks**A passive attack does not disturb the normal operation of the network. In passive attacks the requirement of confidentiality gets violated. Detection of passive attacks is very difficult and since the operation of network does not get affected. One of the solution to the problem is to use powerful encryption mechanism to encrypt the data being transmitted.
- **Eavesdropping** it is another kind of attack that usually happen in the mobile ad hoc networks. It aims to obtain some confidential information that should be kept secret during the communication. The information can include the location, public key, private key or passwords of the node. Because such data are very important to the security state of the node, they should be kept away from the unauthorized access.
- **Traffic Analysis and Monitoring**Traffic analysis attack monitor packet transmission for important information such as a source, destination, and source destination pair.

- **Active Attacks**An active attack attempts to destroy the data being exchanged in the network there by disrupting the normal functioning of the network. Active attack can be internal or external. External attack carried out by nodes that not belong to the network. Internal attacks are from compromised nodes that are part of the network. Since, attacker is already part of the network. Internal attacks are more severe and hard to detect than external attack. Active attacks, whether carried out by an external advisory or an internal compromised node involves actions such as impersonation, modification, fabrication and replication.

2.3 Collaborative attacks

A Collaborative attack[28] in Mobile wireless ad-hoc network is a homogeneous attack involving two or more colluding nodes. The collaborative attack is classified as internal active attack, We can categorize the collaborative attack into two different attack named as Direct Collaborative attack and Indirect Collaborative attack[28]. Now we give a brief introduction of the Direct Collaborative and Indirect Collaborative attack as given blow[28]-

2.3.1 Direct Collaborative attack

Here, the attacker nodes are already in existence in the original network or a malicious node join the network or an internal node is compromised in the network. This kind of collaborative attack can be referred to as direct collaborative attack. Block hole and Wormhole attack belong to this class[28]. The reason for this classification is based on the nature behavior of these attacks. In the block hole attack, one or more malicious nodes try to disturb the network routing operation by advertising itself as on the shortest path to the destination node. Therefore, there will be at least three physical node must be involved in this attack, namely; the source node, the black hole node(malicious node) and the destination node. The second attack is belonging to this class is Wormhole attack; there always exists two clouding malicious nodes. Since they can tunnel data packets back and forth even packets not addressed to them without being known by other nodes. Thus, the Wormhole attack involves at least two physical nodes.[28].

2.3.2 Indirect Collaborative Attack

The attack in this category use different nonexistent nodes in order to fake other nodes to redirect data packets to malicious node. This kind of collaborative attack can be referred to as indirect collaborative attack. The attacker nodes are not already in existence in the original network but created along the line of their attack. Sybil attackbelongs to this category of collaborative attack. The malicious node in Sybil can generate arbitrary number of additional identities for itself while using only one physical node. This physical node may be a legitimate node or an already compromised or malicious node by Sybil attack in the MANET.[28]

Routing table overflow is another attack in this category in which the malicious node tries to create as much as possible routes to non-existent nodes. It aims to prevent new routes from being produced or to overpower the routing protocol.

2.4 Wormhole Attack

Wormhole attacks on mobile Ad hoc networks were independently discovered by Dahil et al, Hass et al and Hu et al[1]. To defend against them, some Effort has been put on hardware design and signal processing technique.

In physics, a wormhole is a hypothetical short cut through space and time that connect two distant regions. In cyber security, the term wormhole means to describe an attack on MANET routing protocols in which colluding nodes create the illusion that two remote regions of a MANET are directly connected through nodes that appear to be neighbours but are actually distant from one another. The wormholes thus create three artificial traffic choke points that are under the control of the attacker and can be utilized at an opportune future time to degrade or analyze the traffic stream.

Wormhole attack can be launched using several modes. Some of these describe blow [1]-

- **Wormhole using Encapsulation**In this mode a malicious node at one part of the network and hears the RREQ packet. It tunnels it to a second colluding party at a distant location near the destination. The second party then rebroadcast the RREQ. The neighbor of the second colluding party receive the RREQ and drop any further legitimate request that may arrive later on legitimate multi hop path. The result is that the routes between the source and the destination go through the two colluding nodes that will be said to have formed a wormhole between them. This prevents node from discovering legitimate path that are more than two hops away.
- **Wormhole using Out-of-Band Channel**The second mode for this attack is the use of an out of band channel. This channel can be achieved by using a long range directional wireless link or a direct wired link. This mode of attack is difficult to launch than the previous one since it need specialized hardware capability.
- **Wormhole with High Power Transmission** Another method is the use of high power transmission. In this mode a single malicious node get a RREQ; it broadcast the request at a high power level capability which is not available to other node in the network. Any node that hears the high-power broadcast rebroadcast it towards the destination. By this method, the malicious node increase its chance in the route established between the source and the destination even without the participation of a colluding node.
- **Wormhole using Packet Relay**Wormhole using Packet Relay is another mode of the wormhole attack in which a malicious node relay packet between two nodes to convince them that they are neighbor. It can be launched by even one malicious node. Cooperation by a number of malicious node serve to expand the neighbor list of a victim node to several hop.
- **Wormhole using Protocol Deviations**A wormhole attack can also be done through protocol deviation. During the RREQ forwarding, the node typically back off for a random amount of time before forwarding reduce MAC layer collision. A malicious node may create a wormhole by simply not complying with the protocol and broadcast without backing off. The purpose knows the request packet it forward arrive first at the destination.

In this attack, an attacker receives packets at one point in the network, tunnel them to another point in the network and then replay them into the network from that point. it is simple to the attacker to make the tunneled packet arrive with better metric than a normal multi hop route for example through use of a single long range directional wireless link or through a direct wired link to a colluding attacker. It is possible to the attacker to forward each bit over the wormhole directly without waiting for an entire packet to be received before beginning to tunnel the bits of the packet. If the attackers perform this tunneling honestly and reliably then no harm is done. The attacker provides a useful service in connecting the network efficiently. The attack can also still be performed even if the network communication provides confidentiality and authenticity and if the attacker has no cryptographic key. A pair of attackers can form a long tunnel and fabricate the false scenario that sort paths exist between the source and destination[1]. The fake path will attract the data traffic as soon as the packets are absorbed to the Wormhole, the attacker either drop the packet or compromise them. The attacks may harm the hierarchical routing protocols.

The wormhole attack is very dangerous against many Ad hoc network routing protocols in which the nodes that hear a packet transmission directly from some node considers themselves to be in range of that node. If a wormhole controls the link between two cluster heads or link close to the root of the routing hierarchy, it can partition the network. Wormhole Attacks put severe threats to both Ad hoc routing Protocols and some Security enhancement.

2.5 Classification of wormhole attack

There are varies type of the wormhole attack as Open wormhole attack, closed wormhole attack, Half open wormhole attack[1], Wormhole using out of band channel, Wormhole with high power transmission, Wormhole using Encapsulation, Hidden Wormhole and Exposed Wormhole etc [1,4,28].

Now we explain the above different type of wormhole attacks. The most important of them are Open wormhole attack, closed wormhole attack, half open wormhole attack[1] etc.

2.5.1 Open wormhole attack-In this attackboththemaliciousnodesarevisibleinthepathfromsourcetoDestination.

2.5.2 Closed wormhole attack-

InitbothmaliciousnodesareinvisibleinPathfromsourceanddestinationhencethisinvisibilitymakesthisattackmodemorechallengingtocaterwith.Boththenodesbehaveascompromisingnodesanddohencetheclosedwormholeattackisdifficulttodetect.

2.5.3 Half open wormhole attack-

InthiswormholeoneoutofthesetwomaliciousnodesisvisibleinPathfromsourcetodestination.HerethemaliciousnodeneednottoCompromisewithanyotherhostnodehenceitiseasytoperform,andevencryptographicsolutionsforsecuritycan’trestricttheattacker [1].

There are many other wormhole attacks ,which are not discussed here because in my work, I mostly use the above three wormhole attacks in my dissertation work.

In broader way, if we look wormhole then in positive perspective . it is not a problem because it may beprovide a best path between source and destination, provided no node in this path is compromised. But the irony is that, this situation puts the nodes in path on such a position that it could be exploited.

In reactive routing it could mislead and thus set up a false route where compromise node can selectively discard some data packets or can completely block the forwarding of these packets leading to denial of service attack. Malicious nodes can modify the content of certain data packets and even in replay attack. Even for nodes with cryptographic keys for authentication it is difficult to counter this attack.

In proactive routing protocol also it can affect the periodic neighbor, discovery mechanism which result into maintaining wrong topological record in routing table and hence routing is affected. Due to this wormhole impact distant node may be treated as neighbors, hence through this wormhole data traffic is lured towards these malicious nodes and then this position can be exploited to do eavesdrop.

2.6 Related work

Hu et al. Introduce geographic packet leash [1]. By appending the location information of the sending nodes in each packet, they verify whether the hop-by-hop transmission is physically possible and accordingly detect the wormhole. Wang et al.instead verify the end-to-end distance bounds between the source and the destination node. Zhang et al. proposed location-based Neighborhood authentication scheme to locate the wormhole[1]. Such approaches require the pre-knowledge of node locations to capture the distance mismatch.

Hu et al.[1] introduce temporal packet leash, which assumes tight global clock synchronization and detect wormhole from exception in packet transmission latency. Capkun et al. [1,] propose SECTOR which measures the round-trip travel time (RTT) of packet delivery and detects extraordinary wormhole channels. SECTOR eliminates the necessity of clock synchronization, but assumes special Hardware on each node that enables fast sending of one-bit challenge messages without CPU involvement. True Link proposed by Eriksson et al. is another RTT based approach. It relied on the exchange of vast Nonce’s between neighboring node[1].

In [11] directional antenna is used to prevent against wormhole attack. Each node in the network share a secret key with every other node and broadcast HELLO message to discover its neighbors using directional antenna in each direction.

In [30], the proposed DelPHI protocol allows a sender to observe the delays associated with the different paths to a receiver. a sender can check, there are any malicious nodes sitting along its path to a receiver trying to launch wormhole attack. The obtained delay and hop count information of some disjoint path is used to decide whether a certain path among these disjoint path is under a wormhole attack.

Qian et al. [31] present a scheme to detect wormhole attack based on data analysis. Here the values of routing and connectivity data before the attack are compared with the corresponding value after the attack. These assume that the wormhole does not exist at the time they congested the statistics and that the statistics do not change due to other causes.

In [32], the authors propose a mechanism to detect Byzantine behaviors during packet forwarding in MANET. Using the acknowledgement from the destination, the source can find change in packet delivery. Then a binary search based query procedure is adopted to locate the faulty link in the path. The method can detect both individual and collusive Byzantine behavior.

Lite Worp [33] detects wormhole attack based on local traffic monitoring at some selected nodes. This detection method may introduce other attacks such as blackmail attack through impersonation [34].

Chapter 3

COTA Mechanism and Algorithms

3.1Cell Based Open Tunnel Avoidance

COTA[1] divides the whole area into same-sized cells (hexagon) and divides the time into same length slots. In the COTA mechanism[1] we have to store the (time, position) pairs of the intermediate nodes in destination nodes data structure likewise the end-to-end detection mechanism with a little difference that it only stores the first received (time, position) pair of every node that falls into same cell and same slot. Through adjusting the cell size and slot length we can control the efforts that it wants to put on the wormhole detection. .

3.1.1 Advantages of COTA

As we know that COTA[1] divides the whole area into same sized cells so we have the following advantages of COTA-

1. 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 $\mathbf{(T_{life}}+\Delta\mathbf{)/T+1}$recordfor every intermediate node.

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

3. 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.

3.1.2 Wormhole Detection

Now T_{life} = the lifetime of a packet (a few seconds). In our case, clocks are loosely synchronized .COTA can estimate the packet traveling time.
If **$T>T_{life}$**then the packet is discarded by the destination node. Let the packet arrives at destination D within its lifetime, the sending time at S and the receiving time at D must satisfy [1]**:** **$(T_{Drecv} - T_{Ssend)} \leq T_{life}$**$+ \Delta$, where Δ= estimated clock error.

Now we calculate the average moving speed of a node. Let **P_{new}**and **P_{select}** be the position of the nodes and **T_{new}** and **T_{select}** of the time at that position and δ is the maximum error distance and Δ is the clock error then we define[1]:

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

Let V be the average moving speed of the previous node.
If ***V*** **> V**, it means the selected node sent the false information so there is a wormhole on the route.[1]

3.1.3 Detection Capability of COTA

As we know that COTA [1]avoids to store and compares all the pairs < time, position>. Due to that COTA can miss the detection of some anomaly.For removing these anomaly, we define an offset **2r+vT** where r=radius of cells, v=highest speed of the nodes, T=length of the time slot
If COTA[1] uses the following equation

$$V=\max((0,\|P_{new}-P_{select}\|)-\delta+2r+vT)/(\|T_{new}-T_{select}\|+\Delta)(3.2)$$

Using the above equation COTA[1] can detect all wormholes that can be detected by end-end mechanism. COTA will give the guarantee the detection capability but in some cases COTA introduce false positive alarms.[1]

3.1.4 Parameters in COTA

Now we define the required parameter which is used to implement the COTA[1] mechanism. There are three parameters named as

1. Packet life
2. Cell size
3. Slot length

3.1.5 Storage space in COTA

Now let the position of a node be with in a circle with [1]

Diameter=2r= v (T_{life} + Δ) so r= v(T_{life} + Δ)/2 (3.3)

If there is no wormhole then the number of cells that have active records for the node is at most

Area of circle/area of cell= (Π(v(T_{life} +Δ)/2)^2)/1.5√3r^2(3.4)

We already known that in each cell at most [(T_{life}+Δ)/T]+1 records are stored.

The total number of records stored by destination for one node is at most

((Π(v(T_{life}+Δ)/2)^2)*(((T_{life}+Δ)/T)+1))/1.5√3r^2≡(πv^2(T_{life}+Δ)^3)/6√3T*r^2 (3.5)

Now if the path length is l then the destination node store at most

L* (πv^2(T_{life}+Δ)^3)/6√3T*r^2 records for one route.[1]

3.1.6 Number of operations in COTA

Let there are m COTA packets for one route and the path length is l then the total number of operations required by COTA is[1]

$((2\Pi ml(v(T_{life}+\Delta)/2)^\wedge 2)*(((T_{life}+\Delta)/T)+1))/1.5\sqrt{3}r^\wedge 2$ Operation[1].

Now if number of packets>number of records stored i.e

$$m> (Pv^\wedge 2(T_{life}+\Delta)\ ^\wedge 3)/6\sqrt{3}T*r^\wedge 2 \qquad (3.6)$$

In this case, COTA will save space and computation both.[1]

3.1.7Sensitivity of COTA

For detection of wormhole in equation 2, we add an offset **2r+vT** where r, v, T has its usual meaning as in equation 2. the offset **2r+vT**[1]is called sensitivity of COTA.

3.1.8 Effect of sensitivity of COTA

if the sensitivity of COTA 2r+vT is predetermined. We can choose suitable values of r and T to minimize the required storage and computational overhead.[1]

Let **2r+vT =X[1]** where X is constant. On putting the values of v in equation 3, we get the equation

$$\mathbf{r^\wedge 2/(X-2r)} \qquad (3.7)$$

on differentiate the equation 7 partially with respect to r and find the value of r by setting

$$\frac{\partial}{\partial r}(r^2(X-2r)^{-1}=0 \qquad (3.8)$$

The optimal value of r=X/3 [1].

3.2 Difference between End To End Mechanism and Cell Based Open Tunnel Avoidance

1. End to End mechanism works keeping in consideration the continuity in space and time while COTA works with discrete time and position space.
2. To make space discrete, whole area is divided into number of same size Hexagon.

3. To make time discrete, whole simulation time is divided into number of slots with slot length t**. number of slots= [simulation time /t]**.
4. As in case of End to End mechanism, the destination node checks for all detection packets. Where as in case of COTA it stores (destination) nodes the first received (time, position) pair of every node that falls into the same cells and the same slot.
5. **T_{life}=packet life time**
6. **Array size=T_{life}+Δ/T+1** where T is the slot length.
7. Destination nodes maintain data structure. All nodes that have active records are put into a linked list. Destinations remember the expiration time of the latest (time, position) pair of every node.
8. Every node has cell structure link list which stores the cells that have active records (each cell remember the expiration time of latest record pairs in it).
9. In each cell, an array of records is maintained. **Array size=T_{life}+Δ/T+1** where T is the slot length.
10. When a new (time, position) pair of a node arrives, the destination first locates the cell list of that node then for each cell of that node, it uses a linear search to locate the record that has the shortest time difference from the new time slots. Then compares through that formula node is lying or not. Then simultaneously after n hopes run detection algorithm using same data structure maintain by destination node.
11. In real world scenario, many routing paths may exists, hence simultaneously many detection algorithm needs to operate on different paths i.e high computation.
12. Space recovery can also be done while searching for latest records in cell array. during this , as we know the expiration time of new records and as well as started records in cells, the obstelete records at that time can be deleted and memory space can be recovered.
13. Create data structure; data structure algorithm run in every slot and detection algorithm run on receive of new records.
14. Detection process keeps on working while route is in progress. The frequency of detection packets is depending on slots. Now for any route in progress, the detection nodes maintain data structure once in every slot. Onthe receive of

detection packet then run the detection algorithm. Detection packet frequency could be once in two slot time or four slot time etc.

15. Destination gets (time, position) pair of intermediate nodes

3.3 Algorithm to Implement COTA

```
COTA ( )
{
Hexagon(X,Y)  /* X and Y are  simulation coordinate.
/* using CBR we find the destination node N. then for N create data structure */
Node X= Create data structure (node-N);
/*then maintain this data structure in all slots*/
While (system time is equal to next slot time)
{
Maintain data structure (node N);
Next slot time= System time +Slot length;
}
/*now detection of arrival of new packets or once in two slot length*/
While (event raise for packet arrival || system in two slot length)
{
Boolean X=Wormhole detection (position p, node N)
}
};
```

3.4 Algorithm to Create Hexagon

```
Create-Hexagon (queue Q, int n)
{
Take first element from Queue Q; /*these are in x and y*/
If (((x>=0 && x<=X)|| (y>=0 && y<=Y))|| (again check all other five coordinate
is any one exists inside the simulation area))
{
Struct Hex H ;
H.a.x=x;
H.a.y=y;
H.a.z=0;
H.b.x=(x+rcos 30);
H.b.y=(y+rsin 30);
H.b.z=0;
H.c.x=(x+rcos 30);
H.c.y=(y+rsin 30);
H.c.z=0;
H.d.x=(x);
H.d.y=(y+2r);
H.d.z=0;
H.e.x=(x-rcos 30);
H.e.y=(y +r +rsin 30);
H.e.z=0;
H.f.x=(x-rcos 30);
H.f.y=(y +rsin 30);
H.f.z=0;
H.i=n;
Store the coordinates in Queue Q;
}
Else
Return;
};
```

3.5Algorithm to Divide the COTA mechanism

We divided the mechanism into three functions:

1. Node create data structure(Node N)
2. Node maintain data structure (Node N)

3. Boolean wormhole detection (Packet p, Node N)

Now, we define the static variable as listed below:

1. T_{life} /* Depends upon end to end delay in the network*/
2. Δ /* Clock error*/
3. Δ /* Position error*/
4. T /* time slot length*/
5. Simulation time ST

3.6Algorithm to Creating data structure for destination N

```
Node* create-data structure (Node N)
{
Step 1: To find the active nodes for the destination nodes.
Step 2: To make a link list of these active nodes and stores in it’s structure, the expiration time of it’s latest pair.
Step 3: Then step by step take each node and from it point towards another cell link list which are active for this node.
Step 4: In each cell structure, it should point towards an array of size $T_{life}+\Delta/T+1$, which store the actual (time, position) pair of that node in this cell at various slot time or length. Each cell structure should have a position to store the expiration time of the latest record in the pointed array.
Step 5: return pointer to the first node.
};
```

3.7 Algorithm tomaintain data structure for Node N

```
Void maintain data structure (Node N)
{
While (system time is equal to next slot time)
{
Maintain data structure (Node N);
Next slot time=system time + slot length
}
```

```
Void maintain data structure (Node N)
{
    Step 1: from node N structure take a pointer to that data structure.
    Step 2:  for (each node)
    {
        For (each cell)
        {
            Store the time position pair in each cell array and update it in cell structure.
        }
    Step 3: return;
};
```

3.8 Algorithm to wormhole detection

```
Boolean_wormhole_detection (Packet P, Node N)
{
    Step 1: Take the pointer to data structure using Node N structure.
    Step 2: using packet p take all (time, position) pair of each node associate with this packet.
    Step 3: for (all those nodes simultaneously)
    {
        1. Select the (time, position) pair from each arrays and take $p_{select}$ which is latest pair associated with packet.
        2. Then calculate velocity $v^-$ for all pairs with latest pair.
        3. If $v^- > v$ for any pair then raise alarm or return or find new path
           Else
           Return 0;
        4. In meanwhile when searching latest pair detection obsolete pair in array.
    }
};
```

Chapter 4

Simulation and Results

4.1Simulation setup

This chapter provides a description of the simulation of a wormhole attack and its defense in a position based routing protocol[27]. The position based routing protocol chosen to study the behavior of the network under the wormhole attack situation is LAR1[13]. The simulations are performed using the public domain simulator Glomosim[29]. The simulation parameters used are as below:

Parameter	**Value**
Simulation duration	10 minute
Simulation area	1000*1000 meter
Number of mobile nodes	50
Transmission range	15 db
Mobility model	Random waypoint
Traffic type	CBR
Data payload	512 bytes
Mobile speed	0-20 m/s

Table-4.1Simulation parameter

The defense mechanism used to defend against the wormhole attack is the Cell Based Open Tunnel Avoidance (COTA) scheme[1]. The simulations also analytically analyze the behavior of COTA defense mechanism with LAR1.

4.2Simulation Result Discussion Parameters

In this we compare the result achieved through simulations in terms of the packet delivery ratio, End-to-End delay and throughput for various scenarios against the number of packets sent. We also compare the number of false positive alarms i.e. the number of times the COTA mechanism raises a fake alarm of having a wormhole even when there is no wormhole existing, against the parameter Sensitivity which is the maximum distance a node can move in one unit distance times and then its added offset.

4.3 Assumptions

Here, we assume the behavior of collaborative malicious nodes. A malicious node, here is acting intelligently without dropping all the packets coming to it. It drops packets randomly, so that, the destination and the sender are not able to figure out the malicious behavior in the path.

4.4 Results

4.4.1 Scenario 1- LAR1 without Wormhole

This scenario considers the normal LAR1 protocol operation when there exists, no wormhole in the path. Here, we compare LAR1 protocol results in Static as well as the Mobile Ad hoc environment which acts as our base result to compare the scenarios accordingly.

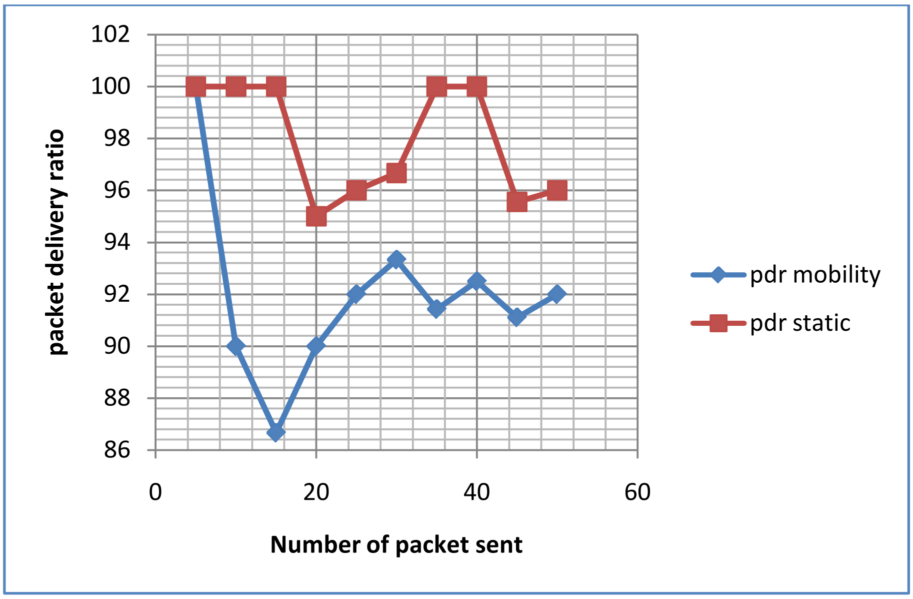

Figure 4.1: Comparison in PDR (Scenario 1)

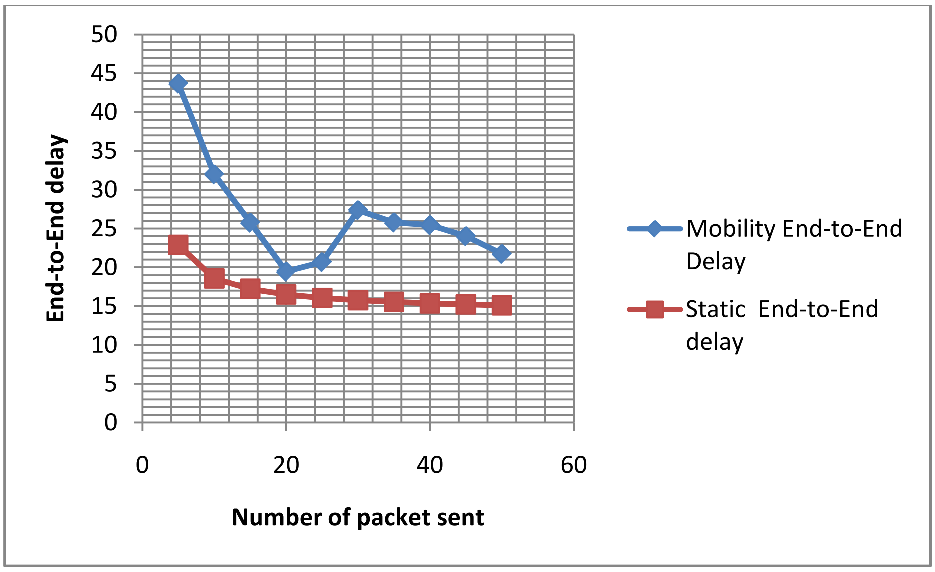

Figure 4.2: Comparison in End-to-End delay (scenario 1)

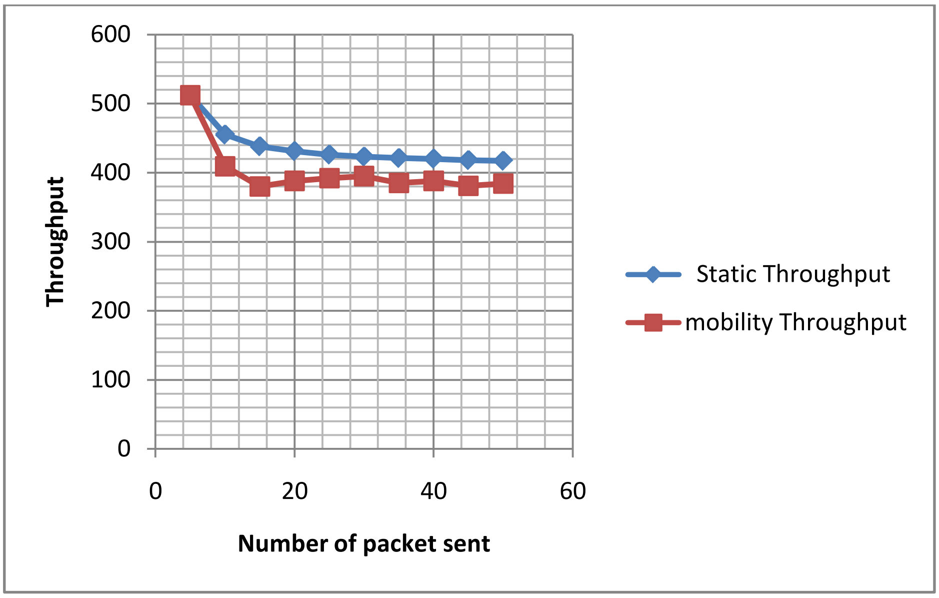

Figure 4.3: Comparison in Throughput (scenario 1)

Findings

Here, it is much obvious that in the static environment the packet delivery ratio is almost constant on 100% while as we introduce mobility into our system the PDR ratio drops and varies, between 87% to 98%. Likewise the End to End delay rises as the mobility is introduced, but as the number of packets sent increases the mobile scenario End to End delay and the static scenario End to End delay gap become less. In case of throughput as the number of packets sent increases, then the throughput for both the static and dynamic environment decreases with the mobile scenario throughput, that is somewhat less in comparison environment.

4.4.2 Scenario2 LAR1 with wormhole

This scenario, considers that there exists a wormhole in the environment and it's much possible that it comes in the route formed between the source and the destination in both static and mobile environment. The results show the impact of the wormhole nodes in the network and compare it in both static and dynamic environment.

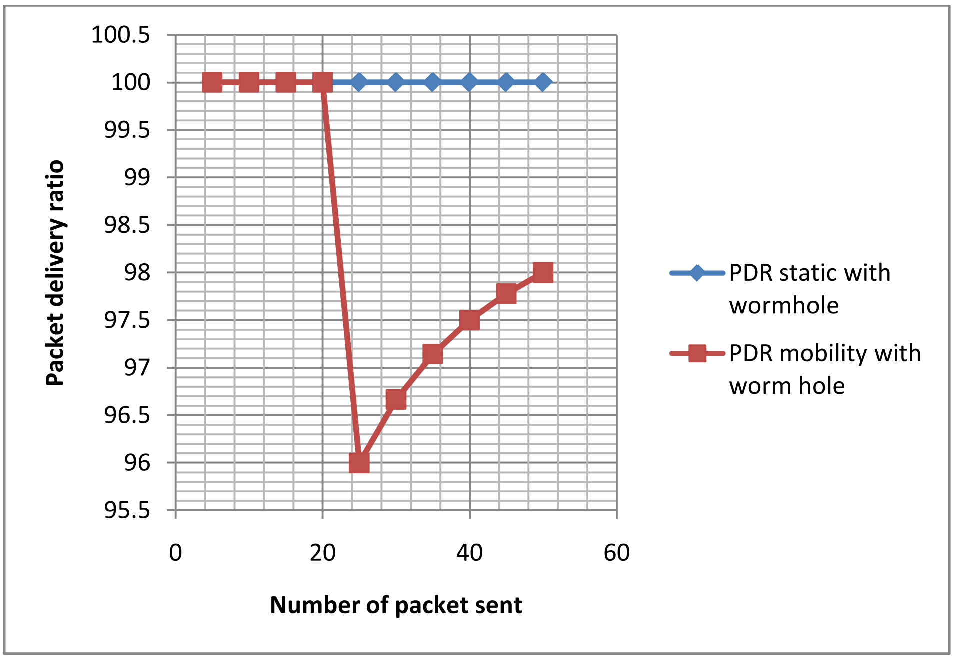

Figure 4.4: Comparison in PDR(Scenario 2)

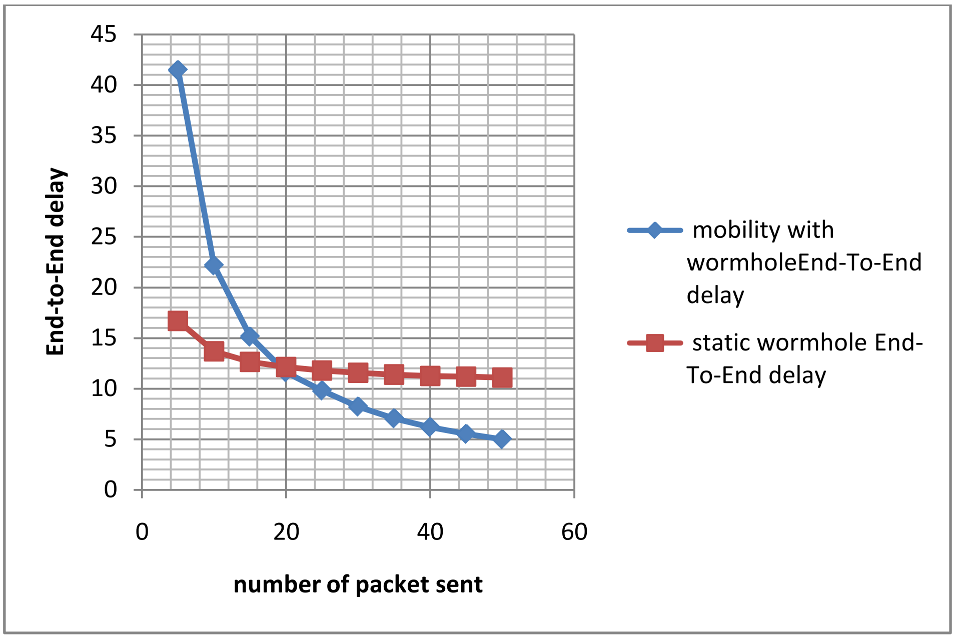

Figure 4.5: Comparison End to End delay(scenario 2)

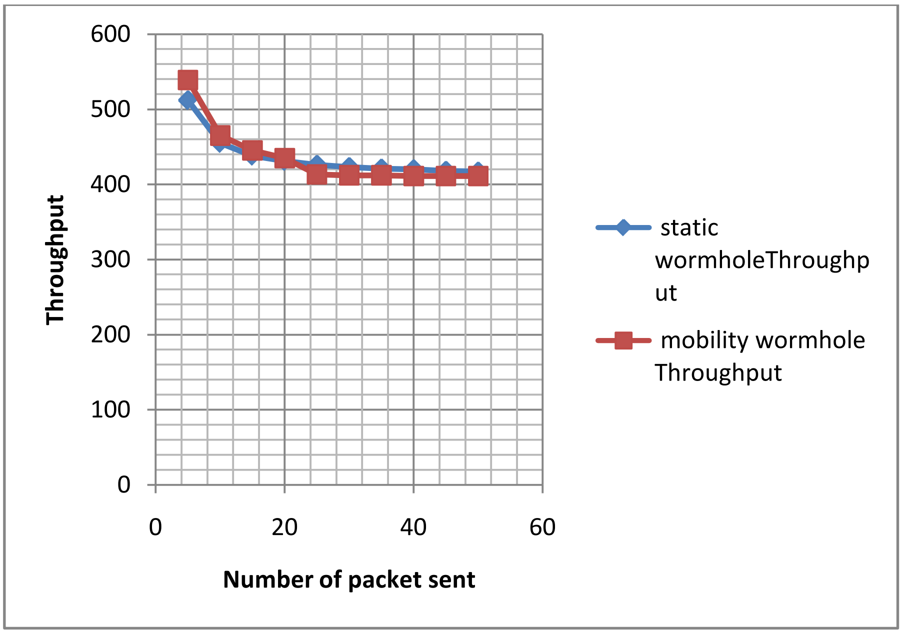

Figure 4.6: Comparison in Throughput (scenario 2)

Findings

In this scenario, a wormhole is introduced into the path from source to destination. In case of static environment the wormhole path is always chosen and it is like the previous scenario 1 with 100% PDR but in case of mobility, the probability of wormhole in the path from the source to the destination decreases as the time progresses and this activity is well observed in figure 4.6 whereas in case of mobility when packets sent is up to 20 then, the PDR for static and mobile is same but as the number of packets sent increases surely it is taking some other route resulting in a decrease in the PDR. In case of End to End delay, as the number of packets sent increases the End to End delay decreases. The End to End delay in case of mobility also decreases from 20 packets sent onwards in comparison to static wormhole environment. The throughput in case of mobility increases somewhat and approaches the static case throughput as the number of packets sent increases so with normal wormhole without maliciousness. Wormhole is an added advantage completely represented and observed in our graphs.

4.4.3 Scenario3 LAR1 with wormhole with malicious activity

This scenario considers the wormhole nodes as the malicious node's whose behavior pattern is random i.e sometime it may hold the packet for delay or may drop it. This randomness introduced by the malicious nodes also increases the complexity to detect the wormhole path. This result shows the impact of malicious activity done by a wormhole node with data packet sent.

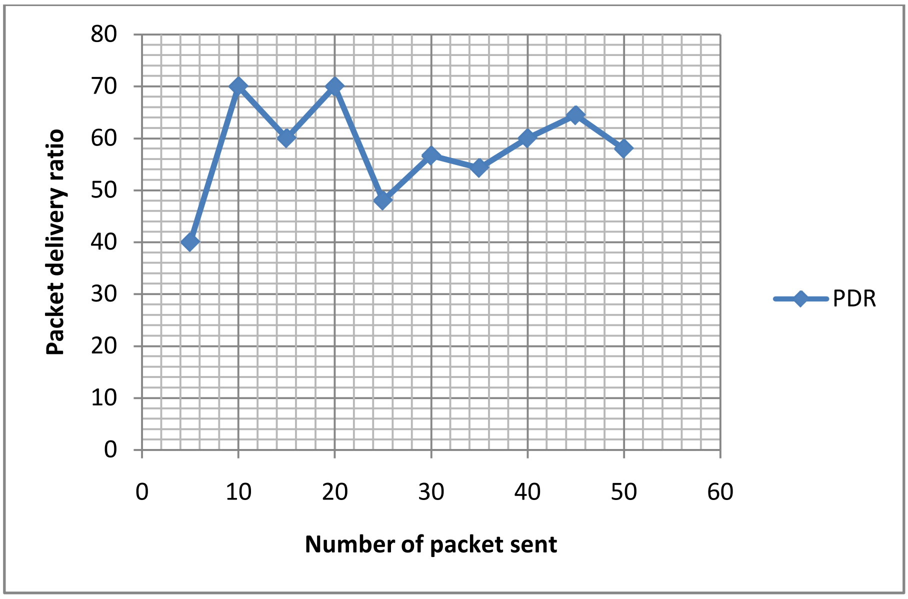

Figure -4.7: PDR (Scenario 3)

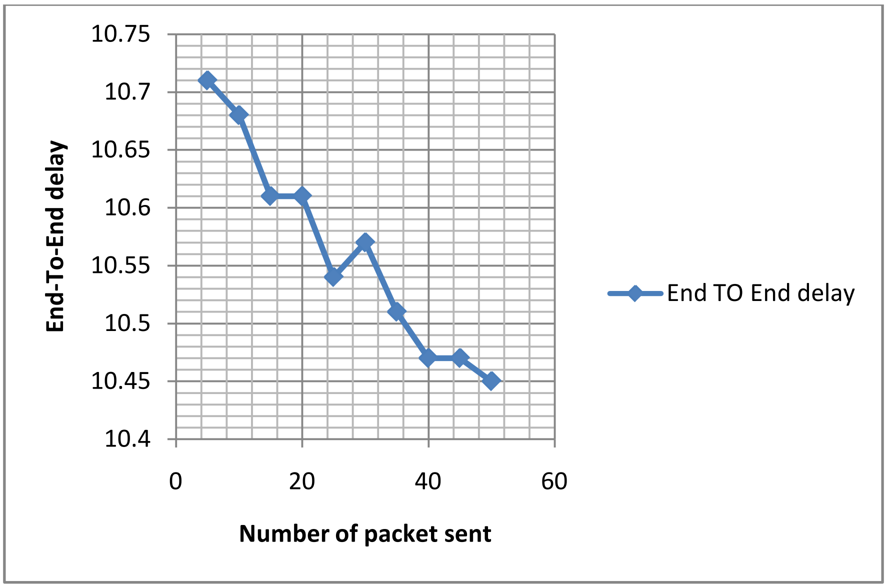

Figure -4.8: End-to-End delay(Scenario 3)

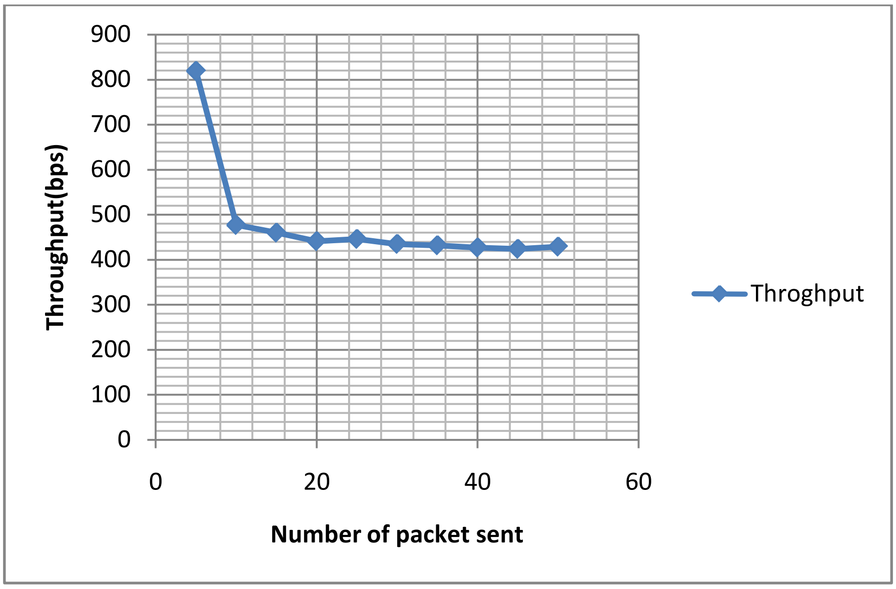

Figure -4.9: Throughput (scenario 3)

Findings

Here, the packet delivery ratio (PDR) becomes less and it values lies between, 40% to 70% depending upon the random behavior of the malicious nodes. The malicious nodes in our simulation only drop the packet, so End to End delay is not impacted at all, but if the malicious nodes introduce hold mechanism then it increases considerably. Due to the malicious activity the throughput also decreases as the number of packest sent increases.

COTA Analysis

The figure 4.10 illustrates the false positive alarms in an environment where no wormhole exists.

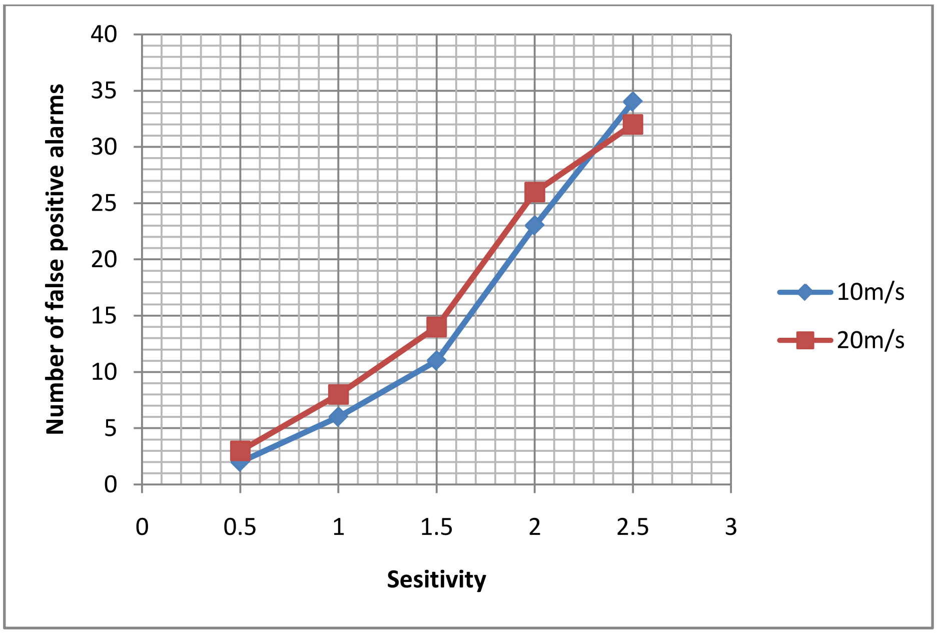

Figure-4.10: false positive alarm

The curves show the relation between the number of false alarms and the sensitivity. Here we compare it with two speeds viz. 10 m/s and 20 m/s and for both it is found that the false alarms decrease as the sensitivity parameter increase and the impact of velocity is not much on the values for false positive alarm. There are more or less for one sensitive value for both speeds.

These false positive alarms need to be less so that the communication overhead becomes less. To lower the number of such mistakes, the following equation (1)[1] updated

$$\boldsymbol{V=\max((0,\|P_{new}-P_{select}\|)-\delta+ \text{offset})/(\|T_{new}-T_{select}\|+\Delta)} \qquad \textbf{(1)}$$

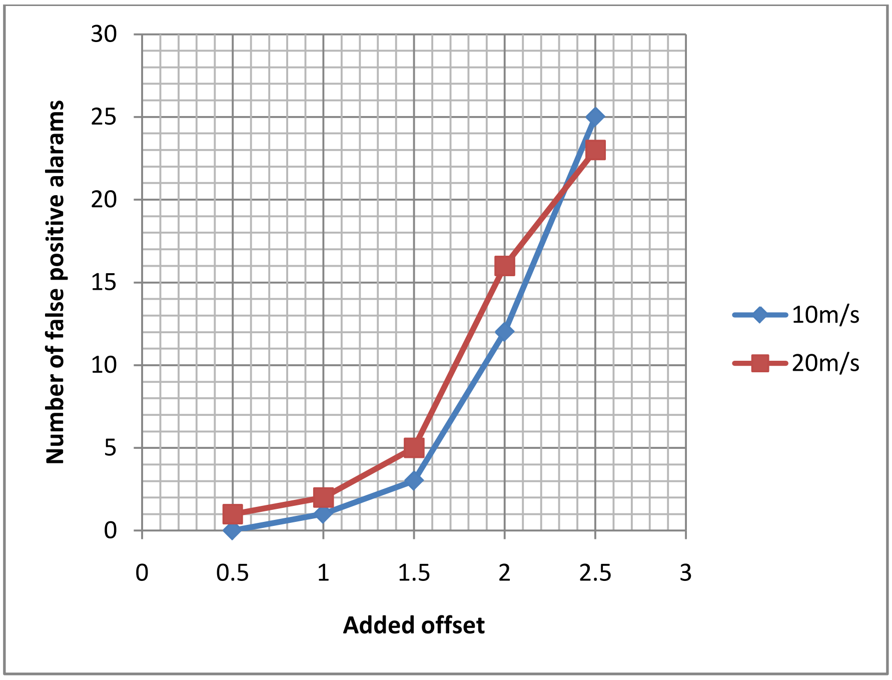

Figure-4.11: false positive alarm with added offset

The added offsets decrease the number of false positive alarms, but after (1.5) sensitivity the added offset does not create much impact on the network.

4.5 Result Discussion

By comparing the above results of the three scenarios, we noticed that the wormhole creation in static and mobile ad hoc environment leads to better path from source to destination in terms of hop length. This results in lower end-to- end delay and increasing throughput but the scenarios which implement wormhole with malicious activities leads to low packet delivery ratio and lesser throughput.

By analyzing the defense mechanism on the data received by implementing the above scenarios we find the number of false positive alarms with respect of sensitivity. This, increases with respect of sensitvity. To reduce the number of false positive alarm some offset is needed to add which improves our result but this improvement is only up to (1.5) sensitivity. Beyond this the affect of offset is not significant.

Chapter 5

Conclusion and Future work

5.1Conclusion

In this study, the wormhole attack is basically divided into three groups named as open wormhole, closed wormhole and half open wormhole attack. Most of the detection and prevention technique solutions focus on closed wormholes.

The End to End mechanism has the capacity to detect open wormhole, closed wormhole and half open wormhole. To reduce the storage and communication overhead, in [1] present cell based open tunnel avoidance scheme (COTA) to manage the detection information. COTA records and compares the (time,position) pairs. After introducing the offset 2r+vT , COTA has the same detection capability as End to End mechanism have. A node can control the resources to detect the wormhole by adjusting the cell size and time slot length.

It is observed that the wormhole creation in static and mobile ad hoc environment leads to better path from source to destination in terms of hop length. Which , results in lower end to end delay and increasing throughput but the scenarios which implement wormhole with malicious activities lead to low packet delivery ratio and less throughput.

In our work, we implemented COTA mechanism with LAR1. By result analysis, we see that in LAR1, the packet delivery ratio is going down because of wormhole attack. In figure 4.10, we see that as the ratio (sensitivity/unit distance) increases, false positive alarm increases. False positive alarm leads to breaks in existent routes in LAR1 and increase the communication overhead. The implementation of COTA mechanism gives us satisfactory result in respect of position based routing environment.

5.2 Future work

We may extend our work with other location routing protocol like DREAM, LAR2 etc. we may implement COTA mechanism with other reactive routing protocol and develop an environment in which packet delivery ratio and overhead must be reduced. In future, we can search the other detection mechanism in which frequency and communication overhead should be reduced.

Bibliography

[1]. Wang W, Bhargava B, Lu Y, Wu X, Defending Against Wormhole Attacks in Mobile Ad Hoc Networks, WCMC 2006, vol. 6, Issue 4, pp. 483-503, June 2006.

[2]. Wang W, Bhargava B, Defending Against Collaborative Packet Drop Attacks on MANET, In Proc. of IEEE DNCMS 2009 Workshop (in conjunction with SRDS 2009), Niagara Falls, New York, U.S.A, Sept. 2009.

[3]Hu Yih-chun, Yh-chunhu, David b. Johnson, "wormhole attacks in wireless Networks"IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 24, NO. 2, FEBRUARY 2006.

[4] Jain Mohit, KandwalHimanshu, A Survey on Complex Wormhole Attack in WirelessAd Hoc Networks, International Conference on Advances in Computing, Control, and Telecommunication Technologies 2009.

[5] N. Song, L. Qian., and X. Li, "Wormhole attacks detection in wireless ad hoc networks: A statistical analysis approach", in proceedings of 19th IEEE International Parallel and Distributed Processing Symposium, 2005. [6]Mauve M,WidmerJ.,asurveyonpositionbasedroutinginmobileadhocnetworks,IEEEnetworks2001.

[7] David b Johnson," routing in ad hoc networks of mobile hosts", IEEE 1995.

[8]. Wang Xia, Wong Johnny, an End-to-end Detection of Wormhole Attack in Wireless Ad-hoc networks, 31st Annual international computer software and applications conference (c0mpsac *2007)* IEEE.

[9]. M. Corner andB. Noble. Zero-interactionauthentication.In Proceedings of the EighthAnnual International Conference on Mobile Computing and Networking *(MobiCom)*, 2002.

[10] Y. Hu, A. Perrig, and D. Johnson. Packet leashes: A defense against wormhole attacks in wireless ad hoc networks. In *Proceedings of INFOCOM*, 2003.

[11] L Hu and D. Evans. Using directional antennasto prevent wormhole attacks. to appear in the Proceedings of Network and Distributed System Security Symposium (NDSS), 2004.

[12].A. Perrig, R. Canetti, D. Song, and D. Tygar. Efficient and secure source authentication for multicast. In Proc. of Network and Distributed System Security Symposium (NDSS), 2001.

[13] Y. KO and N. Vaidya. Location-aided routing (LAR) in mobile ad hoc networks. In Proceedings of MobiCom, 1998.

[14] YaXu, John S. Heidemann, and DeborahEstrin. Geography-informed energy conservation for ad hoc routing. In *Proc. of ACM Mobile Computing and Networking*, pages70–84, 2001.

[15] T. Hodes and R. Katz. Composableadhoc location based services for heterogeneousmobile clients. *Wireless Networks*,5(5):411–427, 1999.

[16]. S. Capkun, L. Buttyan, and J. Hubaux. Sector: Secure tracking of node encounters in multi-hop wireless networks. In Proceedings of the ACM Workshop on Security of Ad Hoc and Sensor Networks, 2003.

[17]. Y. Hu, A. Perrig, and D. Johnson. Ariadne:A secure on-demand routing protocol for adhoc networks. In Proc. of ACM MobiCom,2002.

[18]. D. Mills. A computer-controlled LORANC receiver for precision timekeeping. Technical report 92-3-1, Dept. of Electrical and Computer Engineering, University of Delaware, 1992.

[19]. D. Mills. A precision radio clock for wwv transmissions. Technical report 97-8-1, Department of Electrical and Computer Engineering, University of Delaware, 1997.

[20]. J. Elson, L. Girod, and D. Estrin. Finegrained network time synchronization using reference broadcasts. In Proceedings of theFifth Symposium on Operating systems Design and Implementation, 2002.

[21]. Jana van Greunen and Jan Rabaey. Light weight time synchronization for sensor networks. In Proceedings of ACM Workshop on Wireless Sensor Network sand Applications, 2003.

[22]. B. Dahill, B. Levine, E. Royer and C. Shields. A secure routing protocol for ad hoc networks. Tech report 02-32, Dept. of Computer Science, University of Massachusetts, Amherst, 2001.

[23]. P. Papadimitrato s and Z. Haas. Secure routing for mobile Ad Hoc networks. In Proceedings of SCS Communication Networks and Distributed Systems Modeling and Simulation Conference (CNDS), 2002.

[24].Manoj B.S, Siva Ram Murthy C, Ad hoc wireless network: Issues and challenges, Technical report, Department of computer science and engineering, Indian Institute of Technology, Madras, India, November 2003.

[25]. I. Chlamtac et.al, “MANET: imperatives and challenges”, Elsevier, 2003.

[26]. 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(9) 2010, 4063-4071.

[27]. Martin Mauve and Jörg Widmer, Hannes Hartenstein, a Survey on Position Based Routing inMobile Ad Hoc Networks, November/December 2011 , IEEE network.

[28] Cong Hoan Vu, Adeyinka Soneye, An Analysis of Collaborative Attacks on Mobile Ad hoc Networks, School of Computing at Blekinge Institute of Technology, SWEDEN

[29] Lokesh Bajaj, Mineo Takai, Rajat Ahuja, Ken Tang, Rajive Bagrodia, Mario Gerla GloMoSim: A Scalable Network Simulation Environment, University of California, Los Angeles.

[30]. H.S. Chiu and K.S. Lui, “DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks,” Proc. Int’l. Symp. Wireless Pervasive Comp., Phuket, Thailand, Jan. 2006

[31] L. Qian, N. Song, and X. Li, “Detection of wormhole attacks in multipath routed wireless ad hoc networks: a statistical analysis approach,” *J. Netw. Comput. Appl.*, vol. 30, no. 1, pp. 308–330, 2007.

[32] B. Awerbuch, R. Curtmola, D. Holmer, C. Nita-Rotaru, and H. Rubens, "ODSBR: An on-demand secure Byzantine resilient routing protocol for wireless ad hoc networks," ACM Trans. Inf. Syst. Secur. 10(4), 1-35, 2008.

[33] I. Khalil, S. Bagchi, and N. B. Shroff. Liteworp: A lightweight countermeasure for the wormhole attack in multihop wireless networks. In *IXN*, p.p 612-621, 2005.

[34] J. Eriksson, S. Krishnamurthy, and M. Faloutsos. Truelink: A practical countermeasure to the wormhole attack. In The 14th IEEE lnlernational Conference on Network Prolocols (ICNP), Nov. 2006.

[35]. C. E Perkins and E. M. Royer ,”Ad-hoc On-Demand Distance Vector Routing,” Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications, New Orleans, LA, pp-90-100, February 1999.

[36]. David B. Johson, David A. Maltz and Josh Broch, “DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad-Hoc networks“, in Ad-hoc Networking, Edited by Charles E. Perkins, Chapter-5, pp- 139-172, Addison-Wesley, 2001.

[37]. C. E. Perkins and P. Bhagwat. Highly dynamic destination sequenced distance-vector routing (DSDV) for mobile computers. In *Proceedings of the ACM SIGCOMM ’94 Conference,* pages 234–244, August 1994.

[38]. Vincent D. Park and M. Scott Corson, “Temporally Ordered Routing Algorithm (TORA) Version 1:Functional Specification”, Internet draft, draft-ietf-manettora-spec-01.txt, August 1998.