HCTL Open Int. J. of Technology Innovations and Research
HCTL Open IJTIR, Volume 4, July 2013
e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-132-1

Detection and Prevention of Wormhole Attack in ALARM Protocol (MANETs)

***Mahesh Gour*[*], *Amrit Suman*[†] *and Ankur Kulhar*[‡]**
amrit.it@gmail.com

Abstract

Mobile Ad-Hoc Networks are gaining popularity to its peak today, as the users want wireless connectivity irrespective of their geographic location. There is an increasing threat of attacks on the Mobile Ad-hoc Networks (MANET) such as passive attacks and active attacks. A passive attack does not disturb the functions of the network; snooping of exchanged data is done by the attacker without any modification of it. An active attack attempts to modify the data that have been exchanged in the network. Therefore this disturbs the operations of network. Active attacks can be categorized as: external and internal attacks. Internal attacks are most powerful attack because these are the nodes that are actually

[*]Department of Computer Science & Engineering, ABV-IIITM Gwalior India
[†]Department of Computer Science & Engineering, LNCTS , Bhopal, M.P., India
[‡]Department of Computer Science & Engineering, ABV-IIITM Gwalior India

HCTL Open Int. J. of Technology Innovations and Research
HCTL Open IJTIR, Volume 4, July 2013
e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-132-1

part of the network which has all keys and authorization. Wormhole attack is one of the active internal attacks in which two or more attacker nodes tunnel the traffic from one location to another location in the network. Anonymous Location-Aided Routing in suspicious MANET (ALARM) is a location based protocol, provides protection against passive attack, active insider and active outsider attacks. The main goal of ALARM protocol is providing security and privacy features in the MANET. ALARM does not overcome the problem of wormhole attack and sink hole attack. This paper shows the detection and prevention of the wormhole attack in the ALARM protocol. Firstly point out which link has wormhole tunnel, then verify actually which link is suffering from the wormhole attack.The impact of wormhole attack on the performance of ALARM is compared. The results studied on the basis of throughput, packet delivery ratio and routing load in network.

Keywords

ALARM protocol, Routing protocol, Wormhole attack and Location Aided Routing (LAR).

Introduction

Mobile Ad-Hoc Network (MANET) [6, 8, 9] is an autonomous and distributed wireless system. As the nodes in MANET are mobile, they are free to move in and outin the network. Nodes in a MANET may be cell phone, laptop, PDA, personal computer. MANET's node can act as host or router or both at the same time. MANET is having ability of self-configuration and because of that, they can be deployed rapidly without the requirement of base station. Network topology [14] of MANET is fully dynamic because of mobile nodes. In MANET, nodes are able to communicate with each other without any existing infrastructure. In early days Ad-Hoc research was mainly focuses on military networks, but now Mobile Ad-Hoc networks can be used in environments like conference room, disaster relief, battle field communication and it is also useful, where deployment of infrastructure network is either costly or difficult. MANET is also useful in environments such as search and rescue operations, vehicle networks, tactical networks, entertainment,sensor networks [16], military and law enforcement [17]. Security in MANETs is the most important concern for

e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-132-1

the proper functionality of network. Because of its features like open channel, dynamically change topology,lack of central security mechanism, co-operative algorithms and no effective security mechanism, MANETs frequently suffer from security attacks. These factors are big issues in the MANETs against the security threats. Due to absence of centralized administration in MANET, nodes communicate with each other on the basis of mutual trust. This characteristic of ad-hoc networks makes it more susceptible towards security threats and can be exploited by an attacker in the network. Wireless channel also makes the MANET more vulnerable to attacks; attacker can enter into the network and get access to the information which is to be transferred.In MANETs, information must be transmitted in secure way. This is a challenging and difficult issue because, it uses open wireless channel to transmit data. In order to prevent security attacks, the researcher must know about attacks can happen and their effects on the MANET. In the MANET, attacks such as Wormhole attack, Black hole attack [20], Sybil attack [21], flooding attack, routing table attack, DoS, selfish node, impersonation attack can take place. Communication is based on mutual trust and this makes MANET more sensitive to these attacks.

Motivation

Rapid growth of MANETs, due to usefulness in various applications where security and privacy-preserving networking operation MANET becomes important. This is main reason why MANETs playing an incredible role in many infrastructure less environments and applications such as: Search and rescue operations, vehicle networks, tactical networks, entertainment, sensor network, military and law enforcement.Now location information is easily available through small and cheaper global positioning system (GPS) receivers. An evolutionary natural step is to adopt such location-based operation in MANETs. These results in what then call location-based MANETs.Security in MANET [10] is unavoidable concern for the proper functioning of network. MANET frequently suffer from security attacks because of its features like open channel, infrastructure-less network, dynamically change topology, lack of central security mechanism, co-operative algorithms and no effective security mechanism.These factors are big issues in the MANETs against the security threats.

HCTL Open Int. J. of Technology Innovations and Research
HCTL Open IJTIR, Volume 4, July 2013
e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-132-1

Anonymous Location-Aided Routing in MANETs (ALARM)

Anonymous Location-Aided Routing in MANETs (ALARM) [4] has considered privacy-preserving secure communication in location-based MANETs. It is proactive based routing protocol. ALARM gives strong privacy and provides security properties in Mobile Ad-Hoc scenario. ALARM use node's locations to securely propagate and build topology snapshots and send data. With the help of advanced cryptographic techniques like group signatures, ALARM provide both security and privacy and also provides node authentication, data integrity, anonymity, and untraceability. It also provides protection against passive attack and active attack.This is first protocol that offers security, privacy, and performance trade-offs in the optimized link-state MANET routing. For privacy ALARM show how some advanced cryptographic techniques can be used to reconcile them. The main goal of ALARM protocol is to prevent attacks such as passive outsider and passive insiders attack. Passive insiders are most powerful attacks because they possess necessary cryptographic keys that used to decrypt routing control information.

A: Group Signature

Group signature [1] is a traditional public key signature which includes additional privacy features. In a group signature technique, each group member has its own private key and a group public key. Each group member can sign a message,thereby producing a group signature. Verification of group signature is done by anyone who has a group public key. A valid group signature implies that the signer is a valid group member. But it is computationally harder to find out when two signatures are given whether signature is generated by the same or different group members. When dispute over a group signature take place, a special group member called a Group Manager (GM) forcefully opens a group signature and recognizes who is the actual signer. Based on this features ALARM uses group signature for privacy preserving. A group signature scheme consists of the following algorithms:

1. `Setup`: This algorithm runs by the GM, and it outputs a cryptographic condition for the group, including the group manager's public and private keys.

2. `Join`: Join is protocol between the GM and a new user that want to join the group. The output of this protocol is group manager's key (its public

e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-132-1

membership key) and private output for the user - its secret membership key.

3. `Sign`: Sign is an algorithm that executed by any group member for generating signature whose input consists of: a message, a group's public key and a member's private key.

4. `Verify`: This algorithm is executed by any group member for validation of the signature.

5. `Open`: This algorithm, executed by the GM, when any dispute in signature occurs.

6. `Revoke`: This algorithm is executed by the Group Manager to remove(revoke) a member from the group and to generate new group public key and other a set of support information.

B: ALARM Basic Operation

The basic steps in the operation of ALARM are as follows:

1. `Initialization`: The group manager (GM) starts the group signature scheme and adds all valid MANET nodes as group members. Then all member/node creates a private key that is not exposed to anyone. The private key is used to produce a group signature. Each nodes also creates a corresponding public key that is exposed only to the GM. Group public key is known to all members.

2. `Operation`: (A) Time is divided into slots of length T. At the beginning of each slot, a no degenerates a temporary public private key pair: PK-TMPs and SK-TM, respectively. Temporary public is used by other members to encrypt a session key.
(B) All member broadcast a Location Announcement Message (LAM) which containsits location (GPS co-ordinates), time-stamp, temporary public key (PKTMP's)and a group signature computed over these fields. LAMs are flooded throughout the MANET. This operation is shown in the figure 1.
(C) When a new LAM is received at the node then node first checks whether this LAM is received or not, if not, then verifies the group signature and the time-stamp. If both are valid, then LAM re-broadcasts to its neighbours by the receiving node. And also collect all current LAMs of each node then construct a geographical map of the MANET and node

e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-132-1

connectivity graph. Flow chart of this operation is given in figure 2.
(D) If any node wants to communicate to a certain location node then it first checks if there is a node at that location. If so, it transmit a message to the destination's current location and uses its temporary ID (TmpID).The data is encrypted with a session key and session key is also encrypted under the public key (PK-TMP), Destination's latest LAM is integrated with it. At the receiving end receiver node first decrypts the session key and then decrypt the message. This operation is shown in the Figure 3.
(E) Forwarding: In the ALARM current topology, information disseminates periodically on the basis of OLSR routing. Once each node gets the entire topology view then it decides whether (or not) to communicate with a certain location node.Message forwarding is not dependent on the topology dissemination.

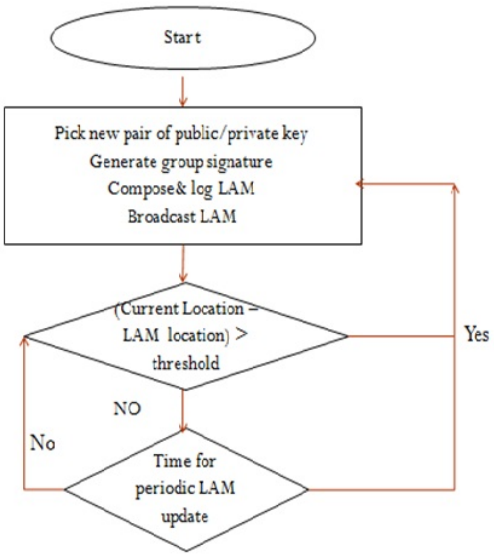

Figure 1: *ALARM sender process flowchart*

Security issues in MANETs

Developing foolproof security protocol for MANETs [24] is tough task. This is mainly because of certain uniqueness of Ad-hoc mobile network, namely, common broadcast radio channel, insecure working environment, lack of central

e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-132-1

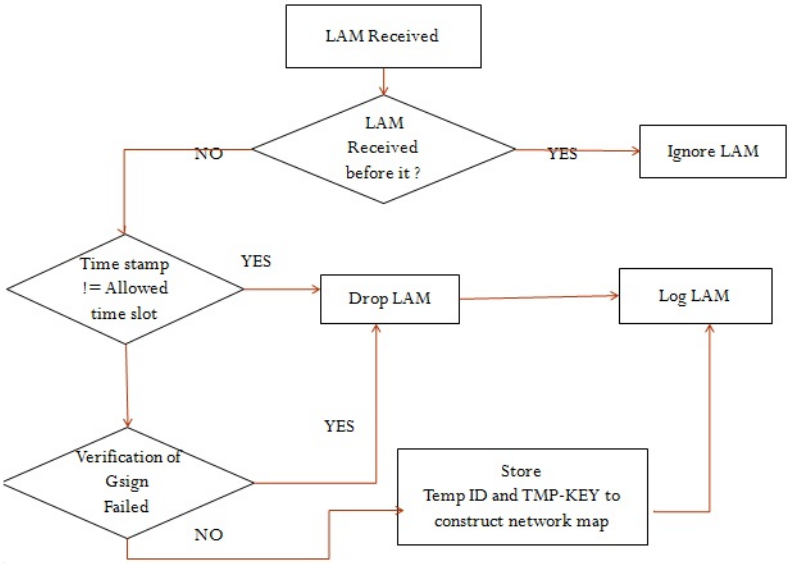

Figure 2: *ALARM LAM receiver process flowchart*

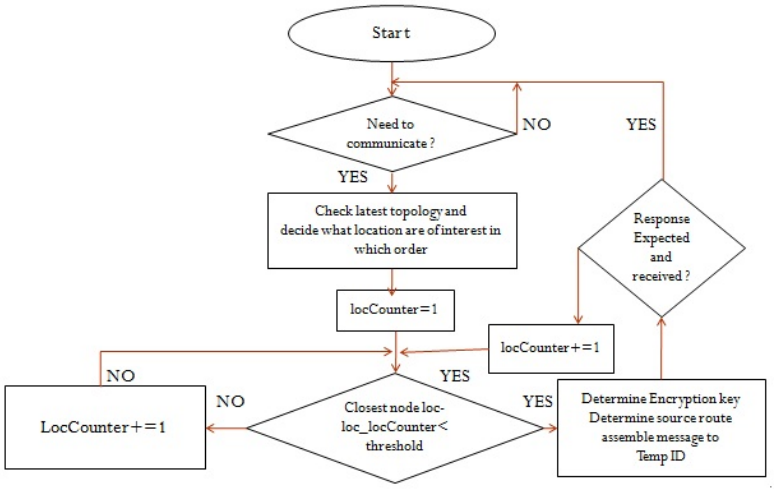

Figure 3: *ALARM communication decision Flowchart.*

administration and limited availability of resources.

`I. Common Broadcast Ratio Channel`: Disparately in wired networks where may be a single dedicate transmitting wire used between a two or more nodes but in the MANET wireless medium is used for communication which has

e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-132-1

broadcasting nature and it is shared by all user nodes. So an attacker can easily find data being transferring in the network.
`II. Insecure Working Environment`: The functioning Environment where MANET networks are used may not always be secure like in the military network, search and rescue operation and battlefields. In such applications, nodes may join in and leave out in the hostile and insecure area, where they would be highly susceptible to security threats.
`III. Lack of Central Administrations`: In wired networks and infrastructure networks uses monitoring and traffic control mechanism by special central point such as base station, router and access points but in MANET there is no such central point for implementing this mechanism.
`IV. Lack of Association`: MANETs is dynamic in nature and nodes are mobile. They any time can leave and join the network. Node authentication mechanisms are not there for joining new node with a network so a malicious node can easily join the network and carry out its attacks.
`V. Limited Resource Availability`: Resource such as bandwidth, battery power, and computational power are limited in MANETs. So it is difficult to implement complex algorithm for security.

MANETs Security Attacks

MANET's attack can be divide in major categories, as passive attack and active attacks. A passive attack does not disturb the functions of the network; snooping of exchanged data is done by the attacker without any modification of it. This attack violates the confidentiality and also analysed the data that gathered by snooping. Passive attack is harder to detect because it does not

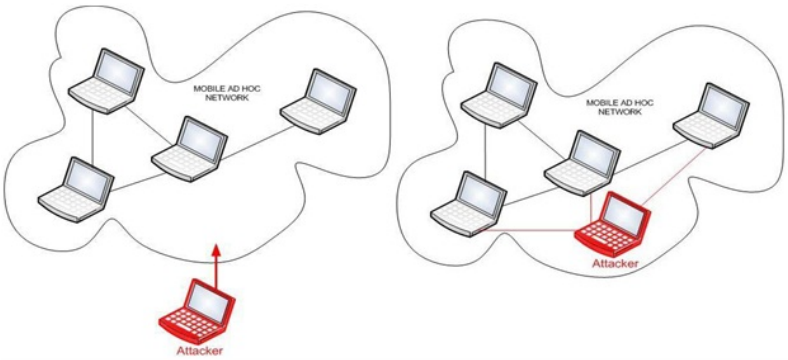

Figure 4: *External and Internal Attacks in MANETs*

HCTL Open Int. J. of Technology Innovations and Research
HCTL Open IJTIR, Volume 4, July 2013
e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-132-1

a affect the network operation. This kind of attack can be handled by use of a powerful encryption algorithm. An active attack attempts to modify the data that have been exchanged in the network. Therefore this disturbs the operation of network. Active attacks be divided into two categories: external and internal attacks, these attacks are shown in the figure 4. Internal attacks are most powerful attack because these are the nodes that are actually part of the network which has all keys and authorization so it is difficult to find out.

Wormhole attack

In the wormhole attack, an attacker receives packet at one location in the network and then tunnel to another location in the network [13]. This tunnel between two attackers node is known as wormhole tunnel. It can be establish by a single long range wireless link or even by a wired link added between the two attackers. Attacker make the use of their location i.e. they have shortest path between the nodes as shown in the figure 5. They advertise their path letting the other nodes in the network to know they have the shortest path for the transmitting their data.

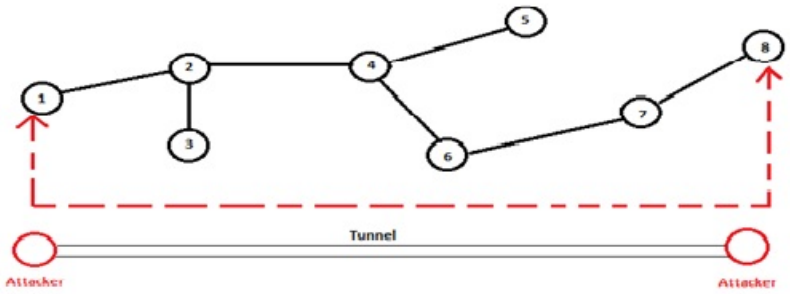

Figure 5: *Wormhole attack*

Related Work

MANETs gets popularity because of characteristic such as network's dynamic topology, no infrastructure and scalability. Even with the fact of popularity of MANET, these networks are very much open to the attacks [22, 12]. Radio channel also makes the MANET more vulnerable to attacks and make for the attackers to enter in the network and get access to the continuing communication [2]. Several kinds of attacks have been studied in MANET which

e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-132-1

affects on the network. Some attacks are like gray hole, where the attacker node behaves maliciously for the time till the packets are dropped and then behave normally [3]. MANETs routing protocols are also being demoralized by the attackers in the form of flooding attack or DoS attacks, which is done by the attacker by sending unnecessary request packet [15]. Every user wants its data to be sent secure and fast, many attackers, announce them-selves to have the shortest path and have high bandwidth for the transmission such as in wormhole attack and black hole attack, gets packet and discard it [18, 7]. One of the limitations of MANET is the limited battery, attackers take an advantage of this imperfection and tries to keep the nodes busy until it lost all energy and the node go down [23]. Location based routing in ALARM protocol is more secure but it has attack like wormhole and sink hole or black hole attack [16, 5]. This paper focuses on the impact of Wormhole attack in Anonymous Location based routing in suspicious MANET (ALARM).

Statement of Problem

Previously the work done on security issues i.e. attack (Wormhole attack) involved in MANET were based on routing protocol like Ad-Hoc On Demand Distance Vector (AODV) and proactive routing like OLSR. Wormhole attack is studied under the Location based routing protocol like LAR and ALARM and its effects are analysed by stating how this attack disturb the performance of MANET. Very little attention has been given to the impact of Wormhole attack in MANET. To compare the vulnerability effects of wormhole attack on the ALARM protocols against the attack, there is a need to address the location based protocols as well as the impacts of the attacks on the MANETs.

Objective

Objectives of this research work are summarized as follow:

1. To enhancing security in ALARM protocol by addressing wormhole attack.
2. The study focus on analysis of wormhole attack in MANET and its consequences.
3. Analysing the effects of Wormhole attack on basis of, network load, throughput and packet delivery ratio in ALARM.
4. Simulating the wormhole attack using proactive routing protocols.

HCTL Open Int. J. of Technology Innovations and Research
HCTL Open IJTIR, Volume 4, July 2013
e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-132-1

Methodology

In our literature survey we came to know that several approaches have been developed to defend against wormhole attack in mobile ad-hoc networks on that basis we have a technique for detection and prevention. Following algorithm is used to detection and prevention of wormhole attack.

I. Detection of Suspicious Links: In the Suspicious link detection process first we detect highly probable link which is involved in the attack. Latency of wormhole is relatively longer than the normal wireless propagation latency. This condition is enough to identify wormhole attack because latency depends upon various factors like congestion and intra-nodal processing. So for suspicious links detection we add two packets: `HELLOreq` and `HELLOrep` and doing following steps:

1. Sent `HELLOreq` to neighbours and set the Timer.
2. At the receiving a `HELLOreq` message, the receiver must respond with a `HELLOrep` message.
3. Check whether `HELLOrep` Packet is arrived before the timer out or not, if it got arrived before time out, status of link is set proven otherwise set is suspicious.
4. Stop communication with that node till the wormhole verification

Flowchart of the suspicious link detection is shown in the figure 6.

II. Wormhole Verification: In the verification procedure each link checks whether there is wormhole attack or not between source node and destination node. For this two more packet are added to protocol namely as `PROBreq` and `ACKprob` and do the following steps:

1. Sends a `PROBreq` to all of its suspect nodes.
2. Receiver replies with an `ACKprob` and it is also adds its own opinion about the status of node of sender.
3. Sender again checks whether the `ACKprob` arrived before the time-out and also decides status about possible suspicious links.
4. Sender compares its result of the status of the other endpoint of the suspicious link with the other node's results of its own status:

HCTL Open Int. J. of Technology Innovations and Research
HCTL Open IJTIR, Volume 4, July 2013
e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-132-1

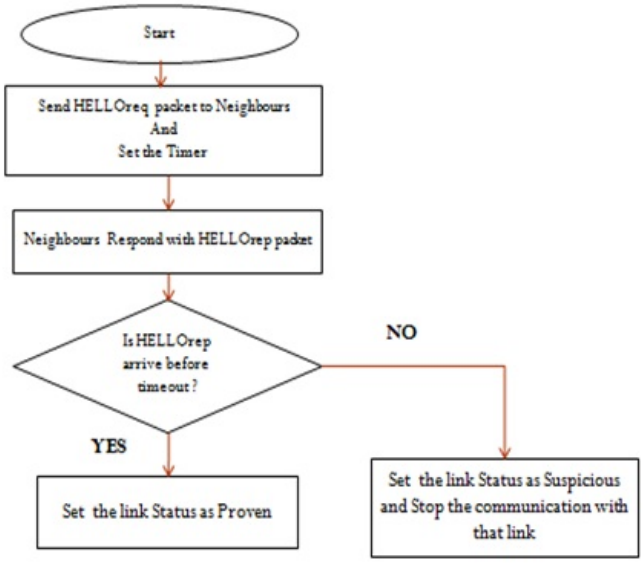

Figure 6: *Flowchart of Detection suspicious Link*

If**(Proved, Proved)**: If the evaluation of sender is proved and contents of `ACKprob` is also proved Then there is no Wormhole tunnel.

If**(Suspicious, Proved) or (Proved, Suspicious)**: Repeat the above procedure after a random amount time. If again one of them is Suspicious then treats this link as a wormhole tunnel.

If**(Suspicious, Suspicious)**: If status of remote node is suspicious, originator‘s status also Suspicious this concludes that the link contains a wormhole tunnel.

Design and Implementation

For the simulation purpose used NS-2 (Network simulator) [19, 11]. The simulation process is set-up in scenarios as: Objective of this scenario is to perform and prevent wormhole attack on ALARM protocol then collect ALARM related statistics and analyse the network dynamic changes. ALARM is as proactive routing protocol and uses multi-point relay (MPR) optimization for controlled flooding and operations. In the ALARM protocol when wormhole

e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-132-1

attack is launched during the propagation of link state packets, the wrong link information circulates throughout the network, leading to routing disruption. For the simulation study done on base of performance parameter like PDR (packet delivery ration), Network Throughput, Packet lost and Network Load.

Simulation Scenario

Figure 7 shows the simulation setup of a scenario there is 30 nodes.Number of nodes is fixed and simulation time has taken 100 seconds. Simulation area taken is `800 x 600` meters. Transmission Range is 100 meters.

Table 1: *Simulation Parameters*

Simulation	Parameters
Protocols	ALARM protocol and OLSR
Simulation time	100 seconds
Simulation area (m x m)	800x600
Number of Nodes	30 (Number as 0-29)
Traffic Type	TCP, CBR and UDP
Performance Parameter	Throughput, PDR , Packet Lost and Routing Load of the network

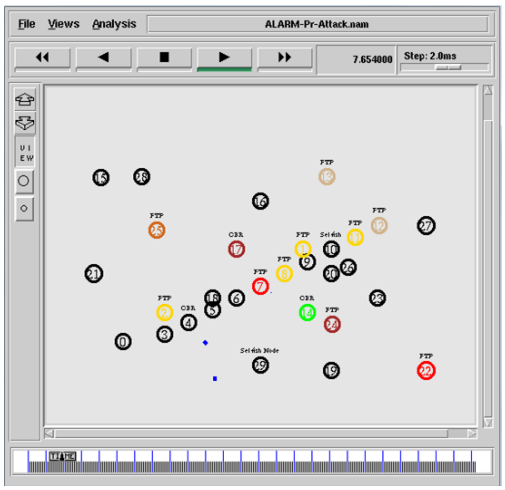

Figure 7: *Simulation topology*

In the figure 8, topology information is transmitted to within nodes and

e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-132-1

routing table updated. ALARM protocol is a proactive routing protocol, so MPR node periodically updated the topology information to its neighbour.

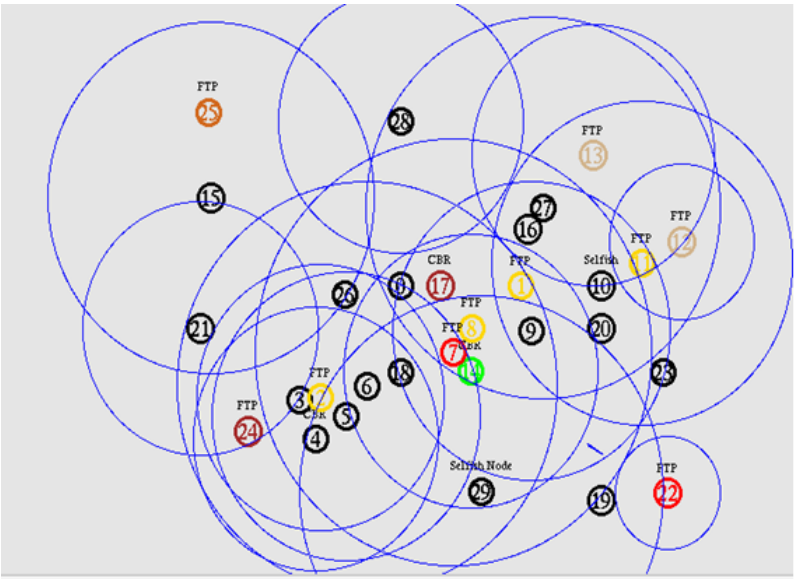

Figure 8: *Dissemination of Network traffic information topology*

Results

Here the comparison of the behaviour ALARM protocol in case without Wormhole attack, with Wormhole attack and after the prevention of wormhole attack, then considered the performance metrics of Packet Delivery Ratio (PDR), Network throughput, Packet lost and Network load.

Packet Delivery Ratio (PDR)

Packet Delivery Ratio is defined as it is ratio between no. of packet received to no. of packet transmitted in the network. Fig. 5.1 shows a graph in which comparison of PDR is given among the ALARM, ALARM with Wormhole attack and after Prevention of Wormhole attack.

In the graph at Y axis PDR in percentage and X axis shows the time in second. PDR is less compared to without wormhole attack. In case of wormhole attack maximum packets are either dropped or transmitted anywhere in the

e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-132-1

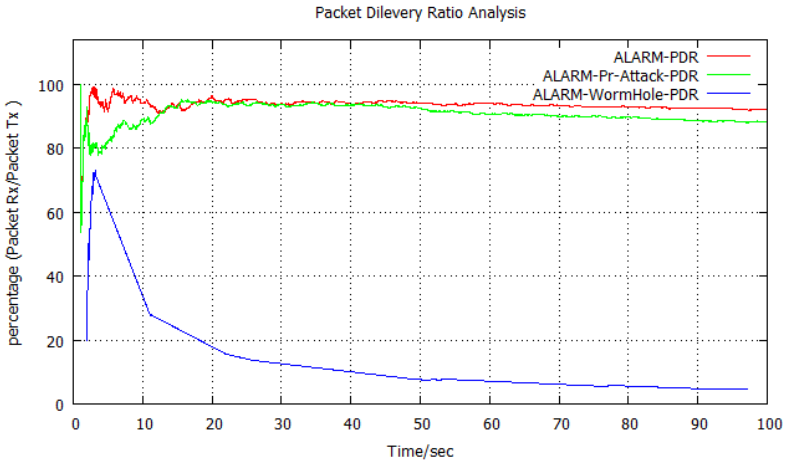

Figure 9: *Packet Delivery Ratio (in percentage)*

network so total no. of packet received packet is less compare to without wormhole.

Network Throughput

Network Throughput is second parameter of our study. Throughput is the average rate of successful packet delivery over a communication channel or successful packet delivery in per unit time or per second. Network throughput is decreased in case of attack because wormhole receives packet from one location and tunnel it to in the network, so successful packet delivery deceases. Throughput of network improves when we apply wormhole detection and prevention methodology (as shown in the figure 10).

Network Load

Load refers to amount of data or traffic being carried by the network, or total number of packet received by entire network. Network Load graph of ALARM, ALARM with attack and without attack is shown in figure 11. The network load of ALARM in case of attack is much high as compare to ALARM without attack. After the prevention of attack network load minimizes but still greater than ALARM without attack because in wormhole detection and prevention method we introduce four new packets.

HCTL Open Int. J. of Technology Innovations and Research
HCTL Open IJTIR, Volume 4, July 2013
e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-132-1

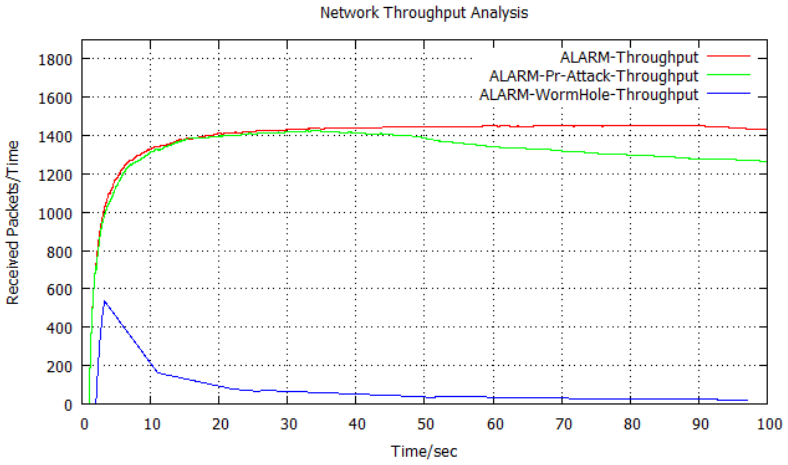

Figure 10: *Network Throughput (packet/sec)*

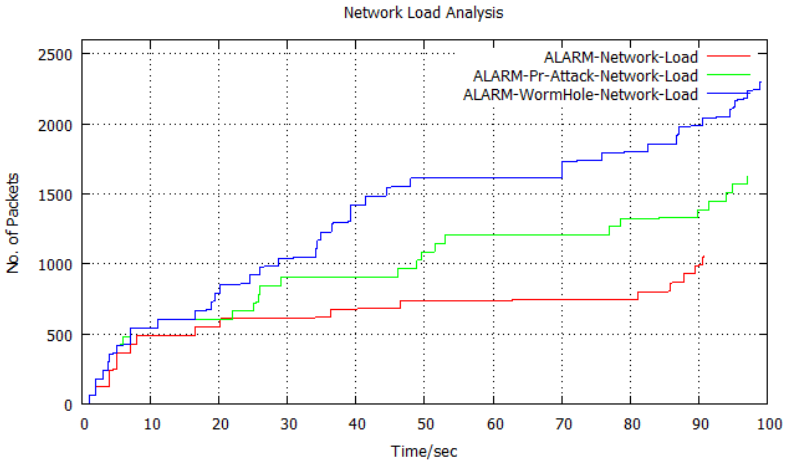

Figure 11: *Network Load*

Packet Loss

In the figure 12, a comparison graph of packet loss in case ALARM with and without attack and after prevention of Attack shown. Packet loss rate in case of attack is high, it is minimized in the attack prevention process but it is still more as compare to normal ALARM.

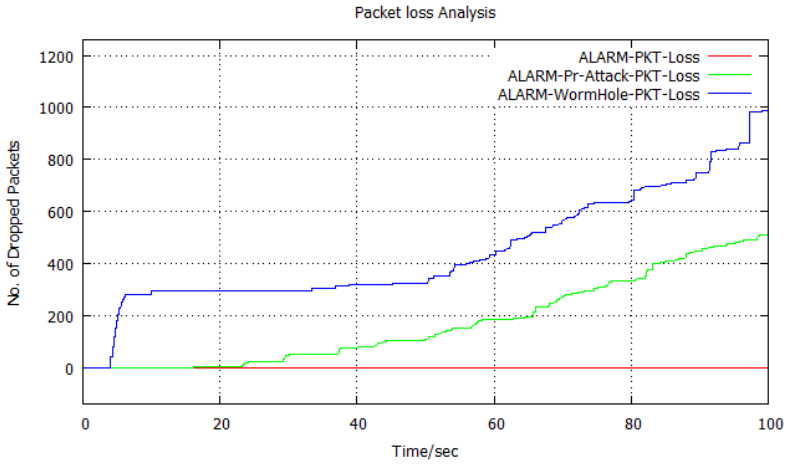

Figure 12: *Packet Loss in the Network*

Conclusion

Mobile Ad-Hoc Networks could be deploying in environment where wired network or infrastructure based network cannot possibly be deployed. With the importance of MANET and its enormous potential it has still many challenges to overcome.MANET Security is one of the most important requirement its deployment and development. There are many threats of security one of them is wormhole attack.Wormhole attacks are brutal attacks that can easily be launched in any network even networks has strong confidentiality and authenticity mechanism.

In this paper first perform wormhole attack at location based protocol(ALARM) then detect and recover the wormhole attack and also analyse the behaviour of protocol with attack and without attack. The Analysis is done on basis of network throughput, Packet delivery ratio, packet dropped rate and the network load.

References

[1] G. Ateniese and G. Tsudik, `Some open issues and new directions in group signatures`, In Financial Cryptography, pages 196-211. Springer, 1999.

[2] K. Biswas and M. Ali, `Security threats in mobile ad hoc network`,

e-ISSN: 2321-1814
ISBN (Print): 978-1-62776-132-1

University essay from Blekinge Teknisha Hogskola/Sektionen for Teknik (TEK), 2007.

[3] O. Chandure and V. Gaikwad. A Mechanism for Recognition and Eradication of Gray Hole Attack using AODV Routing Protocol in MANET.

[4] K. Defrawy and G. Tsudik, Privacy-Preserving Location-based on-Demand Routing in MANETs, Selected Areas in Communications, IEEE Journal on, 29(10):1926-1934, 2011.

[5] P. Garg and A. Tuteja, Comparative Performance Analysis of Two AD-HOC Routing Protocols, In Proceedings of 2011, 1st International Conference onNetwork and Electronics Engineering (ICNEE 2011), 2011.

[6] S. Gupta, S. Gill and A. Joshi, Analysis of Black Hole Attack on AODV and OLSR Routing Protocols in MANET.

[7] D. Johnson, D. Maltz, Y. Hu, and J. Jetcheva. The Dynamic Source Routing Protocol for Mobile AD-HOC Networks (DSR), july 2004. http://www.ietf.org/internet-drafts/draft-ietf-manet-dsr-10.txt (Last visited: 10/2005).

[8] J. Kim and G. Tsudik, SRDP: Securing Route Discovery in DSR, In Mobile and Ubiquitous Systems: Networking and Services, 2005. MobiQuitous 2005, The Second Annual International Conference on, pages 247-258. IEEE, 2005.

[9] Y. Ko and N. H. Vaidya, Location-Aided Routing (LAR) in MANETs, Pages 66-75. Proc. ACM MobiHoc, Oct. 1998.

[10] S. Kurkowski, T. Camp, N. Mushell, and M. Colagrosso, A Visualization and Analysis Tool for NS-2 Wireless Simulations: Inspect, In Modeling, Analysis, andSimulation of Computer and Telecommunication Systems, 2005. 13th IEEE International Symposium on, pages 503-506. IEEE, 2005.

[11] S. Lu, L. Li, K. Lam, and L. Jia, SAODV: A MANET Routing Protocol that can with-stand Black Hole Attack, In Computational Intelligence and Security,2009. CIS'09. International Conference on, volume 2, pages 421-425. IEEE,2009.

[12] H. Nguyen and U. Nguyen, A Study of different types of Attacks on Multi casting mobile AD-HOC Networks, Ad Hoc Networks, 6(1):32-46, 2008.

[13] A. Perrig, R. Canetti, J. Tygar, and D. Song, The Tesla Broadcast Authentication Protocol, 2005.

[14] M. Refaei, V. Srivastava, L. DaSilva, and M. Eltoweissy, A Reputation-based Mechanism for Isolating Selfish Nodes in AD-HOC Networks, In Mobile andUbiquitous Systems: Networking and Services, 2005. MobiQuitous 2005, The Second Annual International Conference on, pages 3-11. IEEE, 2005.

[15] J. Ren, Y. Li, and T. Li., SPM: Source Privacy for Mobile AD HOC Networks, EURASIP Journal on Wireless Communications and Networking, 2010.

[16] R. Shah and J. Rabaey, Energy Aware Routing for Low Energy AD HOC Sensor Networks, In Wireless Communications and Networking Conference, pages 350-355, IEEE, 2002.

[17] N. Song, L. Qian, and X. Li, Wormhole Attacks Detection in Wireless ADHOC Networks: A Statistical Analysis Approach, In Parallel and Distributed Processing Symposium, Proceedings of 19th IEEE International, IEEE, 2005.

[18] Y. Sun, S. Kumar, and A. Jantsch, Simulation and Evaluation for a Network on Chip Architecture using NS-2, In 20th IEEE Norchip Conference, 2002.

[19] I. Ullah and S. Rehman, Analysis of Black Hole Attack on MANETs using different MANET routing protocols, Program Electrical Engineering with emphasis on Telecommunication, Type of thesis-Master Thesis, Electrical Engineering,Thesis no: MEE-2010-2698, 2010.

[20] I. Ullah and S. Rehman, Analysis of Black Hole Attack on MANETs using different MANET Routing Protocols, Program Electrical Engineering with emphasis on Telecommunication, Master Thesis, Electrical Engineering, Thesis no: MEE-2010-2698, 2010.

[21] A. Vani and D. Rao, Article: Providing of Secure Routing against Attacks in MANETs, International Journal, 24:16-25.

[22] D. Westhoff, `Method for Authentication`, Sept. 13 2006. US Patent App.11/519,929.

[23] H. Yih-Chun and A. Perrig, `A Survey of Secure Wireless AD HOC Routing`, Security and Privacy, IEEE, 2(3):2839, 2004.

[24] Preetam Suman and Amrit Suman, `An Enhanced TCP Corruption Control Mechanism For Wireless Network`, HCTL Open International Journal of Technology Innovations and Research, Volume 1, January 2013, Pages 27-40, ISSN: 2321-1814, ISBN: 978-1-62776-012-6.

[25] Raksha Mehra, Gourav Shrivastava and Amrit Suman, `NAODV: A Routing Protocol to Prevent Wormhole Attack in Ad-hoc Network`, HCTL Open International Journal of Technology Innovations and Research, Volume 3, May 2013, ISSN: 2321-1814, ISBN: 978-1-62776-443-8.