International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 2 Issue 5, May - 2013

Enhancement In Alarm Protocol To Prevent Replay Attack In MANET

[1]RajinderKaur khera
[2]Rohit Sethi
[1] M.Tech Scholar, Lovely Professional University Jalandhar Punjab
[2] Assistant Professor Lovely Professional University Jalandhar

Abstract

Security has become an important concern in order to provide protected communication between mobile nodes Mobile Ad-hoc network is one of the most promising fields for research and development of wireless networks. Wireless ad hoc network has become one of the most vibrant and active field of communication in networks. As the Ad –hoc network technology has become widespread vulnerabilities in its security issue/problem are increasing which can be dangerous to the privacy of the user's personal information. To prevent the various inside and outside attacks mutual trust relationship between the mobile nodes should be maintained. In the alarm protocol some of the clocks are weakly synchronized .Hence replay attack is possible .Hence our new proposed technique is based in this paper to provide strong clock synchronization to prevent replay attack .Our new Technique in this paper is to provide strong clock synchronization to prevent replay attack in mobile ad hoc networks.

Keywords:- ALARM Protocol, Attacks, Clock Synchronization, GPS, NTP etc

1 Introduction:-

A MANET stands for mobile ad-hoc network it is a self configuring infrastructure less network. All devices in MANET are allowed to move freely in any direction. The complexity and uniqueness of MANETS make them vulnerable to security threats .Attacks on ad hoc wireless networks can be classified as passive and active attacks ,depending on whether the normal operation of the network is disrupted or not.

1. In inside attacks a node within the network becomes malicious node and it launched attack on network

2 .In outside attacks a malicious which is outside the network, it become the member of the networks and then launched the attack on network

Providing security in MANET is a challenge that needs to be approached at different levels .MANETS and their self Configuring mobile routers are vulnerable due to their wireless connectivity and their frequent topology changes. Ad –hoc networks are new networks for the wireless communication .Basically it is the network which is used in the emergency causes. No fixed infrastructure is required in the mobile ad-hoc networks. Mobile nodes can move freely.

Ad-hoc network uses Alarm Protocol It is an anonymous location aided routing in suspicious MANET. The nodes use by the ALARM indicates current locations to strongly distribute and forward data. With the help of group signature technique,

ALARM provides both privacy features and security including data integrity, node authentication, anonymity, and intractability.

. Alarm protocol works on two techniques. One is the technique which is used in the link state routing and the other is the group signature. The Alarm Protocol works by the following steps which are

1. The group manager is the manager which is responsible for the group signature scheme and enrolls all the legitimate MANET nodes as group members. During this phase each member creates a unique private key that is not revealed to anyone .This key is needed to produce valid group signatures .It also creates a public key (PK) member that is revealed only to the GM. In Addition to it each member learns the common public key that is used to verify the group signatures In Any case of dispute it is the group member who is responsible for the opening of the contested group signature and determining the actual signer..
2. The second phase is the operation online in which time is divided into equal slots of duration T. At the beginning of each node s generate temporary private –public key pair: PK-TMP and SK-TMP .Each node broadcast. Announcement Message (LAM) containing its location, timestamp, temporary public key. Upon receipt of a new LAM a node first checks that it has not received same LAM before, it then verifies the time stamp and group signature. If both of them are valid then the node rebroadcasts the LAM to its neighbor's .The location is included in the pseudonym in order to minimize required state and assist in the forwarding process. Whenever communication is needed it checks to see if any node currently exists at that location. This message is encrypted with Session key using symmetric cipher .The session key is in turn encrypted under the public key (PK-TMP) included in the destination latest LAM. When destination receives message it first recover session key and decrypt the rest .

2. Related Work:

S Karthiga and V.B.Rosy Christiana." (2012) Privacy in Suspicious Mobile Ad hoc Network Using Alarm:" In this paper they had reviewed the alarm protocol for mutual authentication .The Alarm protocol is to ensure data integrity and confidentiality .In Alarm protocol two approaches are there of group digital signature and link state routing The link protocol is for maintain link between mobile nodes and group signature to digitally sign the message to ensure message integrity and confidentiality The message is encrypted by the public key which is announced group manager and every group manager is having their private keys .to ensure digital signature group manager is responsible.[9]

Karim Ei Defrawy , Member , IEEE And Gene Tsudik " (2011) ALARM: Anonymous Location Aided Routing in Suspicious MANET. In the mobile ad hoc network ,mobile nodes can freely move in the environment ,the environment can be secure as well as unsecure .In the unsecure environment certain kinds of inside and outside attacks are possible To prevent these attacks we require mutual authentication .In this paper the alarm protocol is used for the mutual authentication in which certain packets are exchanged for mutual authentication in which packets are exchanged .The digital signature approach will leads to message integrity and confidentiality. It also offers protection against passive and active insider and outsider attacks [8].

Jacek Cicho n Rafal Kapelko ,Jakub Lemiesz and Marcin Zawada." (2011) On Alarm Protocol in wireless sensor networks": They had discussed the problem of efficient alarm protocol for ad-hoc radio networks .The problem arises in tasks that sensors have to quickly inform the target user about alert situation such as presence of fire dangerous radiation In this paper we show a protocol which uses (o(logn) time slots and show that (logn=logn) is lower bound.[7]

3. Problem Definition: -

. The complexity and uniqueness of MANETS make them vulnerable to security threats..Attacks on ad hoc wireless networks Assumption in Alarm protocol is mobility range, location and time .We are working on this

assumption if the clock are strongly synchronized then the various type of replay attacks are prevented. High time synchronization between mobile nodes is required.

When the high clock synchronization is maintained between the mobile nodes, then various types of replay attack are prevented .Hence we provide strong clock synchronization in MANET to prevent replay attack. In MANET. Various inside and outside attack occurs so to prevent them we provide them strong clock synchronization. .Hence some clocks in mobile Ad-hoc network are weakly synchronized.

Suppose there are number of nodes present in a network from source to destination through node X. All the nodes are weakly synchronized with each others. When the data is send from source to destination through the node X then at the node it will take some time to send to the further node or destination node. Here this node shows weak synchronization with each other's nodes. Node X is a malicious node. At the malicious node attack can be easily possible. At this scenario replay attack is performed at the malicious node which takes the information from the node or either change it suppose 5seconds late than other nodes. After taking information malicious node send data to the destination.

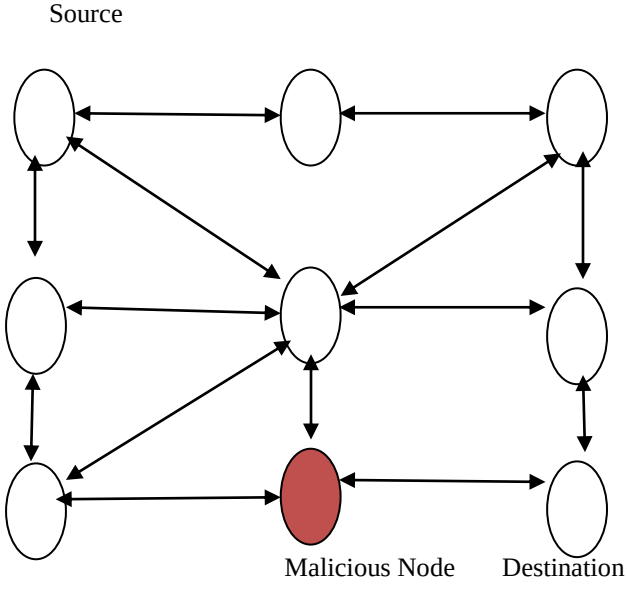

Figure 1 Shows the replay attack at the malicious node

In the Fig. 1 the information is transfer through the malicious node from source to destination and replay attack is performed at the malicious node only because of weak synchronization between all the nodes. So to avoid attack at the malicious node strong synchronization should be provided. In strong synchronization, mutual authentication is present between all the nodes. GPS system is also used in it. A master node is present in the network. With the master node all the other nodes in the network synchronized their clock so that strong synchronization is present between all the nodes. It is the solution of the problem. In the network where trust relationship, mutual authentication and strong synchronization is present then replay attack is not possible there.

4 Proposed Technique:

In the proposed work main concern is about the strong synchronization should be present between the nodes so that replay attack should be prevented. In weak synchronization system where replay attacks are easily possible at the malicious node which may harm the useful data.

So according to our work mutual authentication is the key point which is used to prevent replay attack. If the weak synchronization is present then the data can be easily encrypted the whole information is passed through the malicious node which is weak synchronized as compare to other nodes.

Then it delays some time to transmit it further which becomes responsible for the replay attacks. This problem can be solved by using strong synchronization between the nodes and a node should be there which act as a master node and all other node synchronized their selves with the help of master node. ALARM protocol merge with NTP protocol concept is used for the prevention of the replay attacks.

ALARM protocol uses the current location for the communication between the nodes. To provide authentication and integrity are the features of the

ALARM protocols. GPS system is also used in it. GPS is a Global Positioning System which senses the current location of the system. Group Signature is also used in it to provide security and integrity to the system.

We use NTP protocol which stand for Network Time Protocol. As a consequence, isolated networks may run their own wrong time, but as soon as you connect to the Internet, effects will be visible. Just imagine some E Mail message arrived five minutes before it was sent, and there even was a reply two minutes before the message was sent. Even on a single computer some applications have trouble when the time jumps backwards.

Following are the various steps by which NTP protocol is used to synchronize the clocks of computers to sometime reference. Time usually just advances. If you have communicating programs running on different computers, time still should even advance if you switch from one computer to another. Obviously if one system is ahead of the others, the others are behind that particular one. From the perspective of an external observer, switching between these systems would cause time to jump forward and back, a non-desirable effect. Following are the steps by which NTP protocol works .The algorithm used to prevent replay attack has following steps

.1 The network is deployed with the finite number of mobile nodes.

2 The mobiles nodes have the capability to move from one place to other. We have shown nodes in which communication takes place.

3. The ad hoc network is the self configuring type of network; mobiles can leave or join the network when they want.

4. In such type of network many types of inside and outside attacks are possible. Which degrade performance of network.

5. To prevent this type of attacks trust relationship must be maintained between the mobile nodes.

6. The ALARM protocol is efficient protocol for mutual authentication which provides mutual authentication between nodes.

7. The mobile node is weakly synchronized with GPS. The full form of the GPS is global positioning system.

8. The replay attack is possible in ALARM Protocol which is due to weak synchronization between nodes.

9. To prevent replay attack, clocks are strongly synchronized with the NTP protocol.

10. For clock synchronization master clock is deployed in the network, the master node Synchronize clock with GPS.GPS stand for Global Positioning System And act as master node and it synchronizes all other clocks to its clock.

12. All the node synchronize its clocks with the master clock and according to time of master clock .And hence by doing so our replay attack will be prevented ..

13. All the mobile nodes when strongly synchronize its clocks replay attack is prevented. In the proposed work main concern is about the strong synchronization should be present between the nodes so that replay attack should be prevented Firstly all the clocks were not strongly synchronize with each other but when we apply strong clock synchronization to the clocks then replay attack is prevented Hence replay attack gets prevented.

In the proposed technique nodes synchronized their clock according to the GPS which act as a master clock. So GPS is a master clock and all other nodes are like slaves which set their clock according to the master clock. Mutual authentication is also present between all the nodes. True relationship is maintained. ALARM Protocol is responsible for a Replay Attack. To prevent attacks synchronized ALRAM protocol with NTP protocol. Suppose information is send from source to destination through the intermediate nodes. First of all the nodes set their clock according to master clock or GPS

which sense about the location. In this way all the nodes are strongly synchronized when the data is transfer from source to destination through the intermediate node then these nodes send data immediately without any delay. So no delay means attack is hard to apply. In this way with the help of strong synchronization of the nodes with the master nodes clock replay attacks can be prevented.

5 Conclusions:-

In this paper, we conclude that mutual authentication is required to prevent various inside and outside attacks. We review the ALARM protocol for mutual authentication. In our work, we propose new technique to provide strong clock synchronization between the mobile nodes. Our new proposed technique will be based on the NTP protocol. In Future, we implement new proposed technique and compare the results with the previous techniques. Hence our work is used in military techniques .In Future various attacks will be prevented.

6 References -

[1 Rusha Nandy, "Study of Various Attacks in Manet and Elaborative Discussion of Rushing Attack on dsr with clustering scheme" Int. J. Advanced Networking and ApplicationsVolume: 03, Issue: 01, 2011

[2] Tein-Ho Chen and Wei-Kuan, Shih , "A Robust Mutual Authentication Protocol for Wireless Sensor TieNetworks" ETRI Journal, Volume 32, Number 5, October 2010

[3] Jacek Cicho, Rafał Kapelko, Jakub Lemiesz, and Marcin Zawada "On Alarm Protocol in Wireless Sensor Networks", IEEE Conference-Wcnc 2012

[4] Seung Yi, Robin Kravets, "Key Management for Heterogeneous Ad Hoc Wireless Networks" ,10th Ieee International Conference on Network Protocols (Icnp'02) 1092-1648

[5] Sushma Yalamanchi and K.v. Sambasiva Rao "Two Stage Authentication For Wireless Networks Using Dual Signature And Symmetric Key Protocol " International Journal of Computer Science and Communication (IJCSC), n Vol. 2, No. 2, July-December 2011, pp. 419-422

[6] Karim El Defrawy,Member, IEEE, and Gene Tsudik, Senior Member, IEEE." ALARM: Anonymous Location-Aided Routing in Suspicious MANETs"

7): S.Karthiga,V.B.Rosy christiana, "Privacy in Suspicious Mobile Ad Hoc Network By Using Alarm " International Conference on computing and control Engineering 12 April 2012. .

8 S. Mamatha and Dr. S. c. Sharma "Analyzing The Manet Variations , Challenges ,Capacity and Protocol Issues " 2010

9 Sunil Taneja, Dr. Ashwani Kush, Amandeep Makkar, "End to End Delay Analysis of Prominent On-demand Routing Protocols", IJCST Vol. 2, Issue1, March 2011.

10 Seung Yi, Robin Kravets, "Key Management for Heterogeneous Ad Hoc Wireless Networks" ,10th Ieee International Conference on Network Protocols (Icnp'02)

11 Yinxin Jiang, Chuang Lin, Senior Member, IEEE, Minghui Shi, and Xuemin (Sherman) Shen, Senior Member, IEEE." Multiple Key Sharing and Distribution Scheme With (n; t) Threshold for NEMO Group Communications"

12 Pradeep kyasanur et al ."MAC layer Misbehavior in wireless networks".