To Enhance the Security in Terms of Malicious node attacks by using Alarm Protocol in WSN

Neelam Shekhawat[1], Moumita Ghosh[2]

[1]*Faculty of Engineering, Mody University of Science & Technology, Laxmangarh (Sikar), India*
er.neelamshekhawat@gmail.com

[2]*Faculty of Engineering, Mody University of Science & Technology, Laxmangarh (Sikar), India*
mom2001@gmail.com

ABSTRACT

The wireless sensor network is the self configuring type of network .In these kinds of networks mobile nodes can leave or join the network when they want. In such type of networks many active and passive attacks are possible. To prevent from these active and passive attacks trust relationship between the mobile nodes must be maintained. The trust relationship between the mobile nodes is provided by mutual authentication. ALARM is the protocol for providing trust relationship between the mobile nodes. In this protocol the clocks of the mobile nodes are weakly synchronized by using GPS. In such case reply attack is possible. To prevent reply attack clocks of the mobile nodes must be strongly synchronized. In our new proposed technique, we are enhancing t the ALARM protocol to provide strong clock synchronization between the mobile nodes. Our new technique will be based on the network time protocol.

Keywords: ALARM, Attacks, clock Synchronization, GPS, NTP.

1. INTRODUCTION

Wireless sensor network is a decentralized type of wireless network. In wireless sensor network there is no pre-existing infrastructure, such as routers in wired networks or access points in wireless networks. Sensor networks are massive numbers of small, inexpensive, self-powered devices pervasive throughout electrical and mechanical systems and ubiquitous throughout the environment that monitor sense and control most aspects of our physical world. In wireless sensor network each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. Wireless networks refer to those networks that make use of radio waves or microwaves in order to establish communication between the devices. The complexity and uniqueness of MANETs make them more vulnerable to security threats than their wired counterparts. Attacks on wireless sensor network wireless networks can be classified as passive and active attacks, depending on whether the normal operation of the network is disrupted or not.

- Passive attacks: A passive attack does not disrupt the normal operation of the network; the attacker spoof the data exchanged in the network without altering it. Here the requirement of confidentiality gets violated.
- Active attacks: An active attack attempts to alter or destroy the data being exchanged in the network there by disrupting the normal functioning of the network. Active attacks can be internal or external. External attacks are carried out by that do not belong to the network. Internal attacks are from compromised nodes that are part of the network. Impersonation, modification, fabrication, and replay of packets. [1]

To prevent inside, outside active and passive attack mobile nodes must be mutually authenticated. To provide mutual authentication between the mobile node ALARM protocols is used. ALARM protocol have many assumptions among all one is that clock of the mobile nodes are weakly synchronized by using GPS .In such case the reply attacks can be Possible. ALARM protocol use two technique first is link state routing and other is group signature to provide mutual authentication. If the clocks are strongly synchronized various reply attacks can be prevented .In our work we are using NTP (network time protocol) to provide strong clock synchronization between the mobile nodes.

In this paper, Literature Review is presented in the section 2. ALARM protocol is discussed in the section 3. New proposed technique is written in the section 4. In the last section future work and conclusion is discussed.

2. LITERATURE REVIEW

Sushma Yalamanchili and K.V. Sambasiva Rao. In this paper they had proposed a two stage authentication scheme for wireless networks. They discus that in wired network we can use the authentication protocol which is having large computations but in wireless networks we require less computation and energy efficient authentication protocol .[2] Because in wireless networks the hand held devices are having limited battery and limited computational resources also wireless networks on suffer from packet losses and bit errors and offers low bandwidth. In the paper, they presents a two-stage authentication scheme for wireless networks that uses a computationally intensive but highly secure strong authentication in Stage 1 and a lightweight symmetric key based protocol in Stage 2. The cost of the strong authentication adopted in Stage 1 is amortized over N sessions thus reducing the overall cost of the scheme. We adapt the Dual-signature based IKE authentication that we proposed in our earlier work and employ it as Stage 1 authentication. The Symmetric key protocol in Stage 2 authentication that we propose uses the symmetric keys that are generated in Stage 1.

Karim El Defrawy,Member, IEEE, and Gene Tsudik. In the mobile ad hoc network ,mobile nodes can freely mobile in the environment ,the environment can be secure as well as unsecure .In the unsecure environment ,the certain inside and outside attacks are possible .To prevent the inside and outside attacks we require mutual authentication. If the mobile nodes are mutually authenticated they the inside as well as outside attacks can be prevented .The mobile nodes are traced from its current location .To establish the communication with the other node ,the mobile presents its current location to the other mobile nodes .This approach will leads to the security attacks .In this paper they had presented the ALARM protocol for mutual authentication in which the mobile presents its secondary identity which will leads to identity untraceable. In this paper the ALARM protocol is for mutual authentication in which certain packets are exchanged for mutual authentication and messages are digitally signature .The digital signature approach will leads to message integrity and confidentiality. It also offers protection against passive and active insider and outsider attacks. To the best of our knowledge, this work represents the first comprehensive study of security, privacy, and performance tradeoffs in the context of link-state MANET routing [3].

Jacek Cicho ´ n, Rafal Kapelko, Jakub Lemiesz, and Marcin Zawada: They discussed the problem of efficient alarm protocol for ad-hoc radio networks consisting of devices that try to gain access for transmission through a shared radio communication channel. The problem arises in tasks that sensors have to quickly inform the target user about an alert situation such as presence of fire, dangerous radiation, seismic vibrations, and more. In this paper, we show a protocol which uses O (log n) time slots and show that (log n= log n) is a lower bound for used time slots [4].

3. ALARM PROTOCOL

Following are the various assumptions of ALARM protocol

- Location. Universal availability of location information: Each node is deployed in such way that provides accurate positioning information. For example GPS.
- Mobility. Sufficiently high mobility: A certain minimum fraction (or number) of nodes move periodically, such that tracking a given mobile node from one topology snapshot to the next requires distinguishing it among all nodes that have moved in the interim [7].
- Time: All nodes maintain loosely synchronized clocks. This is easily obtainable with GPS [7].
- Range: Nodes have uniform transmission range. Once a node knows the current MANET map, it can determine node connectivity [7].

A. Goals of ALARM Protocol

Following are the various Goals of ALARM

- Privacy: There are no public node identities or addresses. Each node is anonymous and its occurrences at different locations cannot be linked [7].
- Performance: Security and privacy goals must be achieved without undue sacrifices in performance (i.e., without requiring excessive computations and/ or high delay) [7].
- Security: The network must be resistant to passive and active attacks stemming from both outsiders and malicious e.g. compromised insiders [7].

B. Detail of ALARM

Following are the two operations of ALARM protocol

1. Initialization (Offline)

A. The group manager (GM) initializes the underlying group signature scheme and enrolls all legitimate MANET nodes as group members. During this phase, each member (node) creates a unique private key that is not revealed to anyone. This key is needed to produce valid group signatures. It also creates a corresponding public key (PK member), that is revealed only to the GM. In addition, each member learns the common group public key (PKGM) that is subsequently used to verify group signatures. In case of a dispute and for offline forensics, GM is responsible for opening any contested group signatures and determining actual signers.

B. Depending on the specific group signature scheme, GM might also handle future joins for new members as well as revocation of existing members. Revocation might not be feasible or desired, since it would require propagating in real time update revocation information to all legitimate nodes. Dynamic membership is necessary.

2. Operation (Online)

Time is divided into equal slots of duration T. At the beginning of each slot, each node s generates a temporary public-private key-pair: PK-TMPs and SK-TMPs, respectively [7].

Each node broadcasts a Location Announcement Message (LAM), containing its location (GPS coordinates), time-stamp, temporary public key (PK-TMPs), and a group signature computed over these fields [7].

Upon receipt of a new LAM, a node first checks that it has not received the same LAM before; it then verifies the time-stamp and group signature. If both are valid, the node rebroadcasts the LAM to its neighbors. The location is included in the pseudonym in order to minimize required state and assist in the forwarding process. Here the current location concatenated with the group signature in the last Location Announcement Message (TmpID = {Location||GSig}). Including location in the pseudonym speeds up the forwarding process and requires fewer look-ups [7].

Whenever the communication is needed, it checks to see if any node currently exists at (or near) that location. This message is encrypted with a session key using a symmetric cipher. The session key is, in turn, encrypted under the current public key (PK-TMP) included in the destination's latest LAM. When the destination receives the message, it first recovers the session key and uses it to decrypt the rest. ALARM is not restricted to any specific public key technique [7]. One obvious choice is Diffie-Hellman half-key.

Forwarding: Message forwarding is independent of topology dissemination. The actual path can be computed using the shortest path algorithm or any other location-aided routing algorithm, such as [7]. It generates a session key (Ks) and encrypts data with that key using a symmetric cipher for example AES.

4. PROPOSED TECHNIQUE

The ALARM protocol is used to provide mutual authentication between the mobile nodes. In this paper ,we are proposing a new enhancement in the ALARM protocol .One assumption of ALARM protocol is that clocks of the mobile nodes are weakly synchronized .When clocks of the mobile nodes are weakly synchronized reply attack will be possible. To prevent reply attack in wireless sensor network strong clock synchronization between the mobile nodes must there .In our work, we are using NTP (network time protocol) to provide strong clock synchronization between the mobile nodes. As:

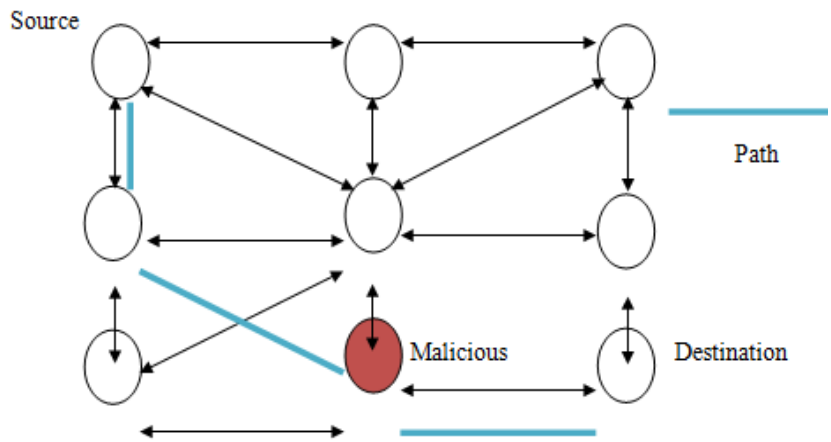


Fig 1: shows the replay attack at the malicious node

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 takes information malicious node send data to the destination.

In the Figure 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.

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

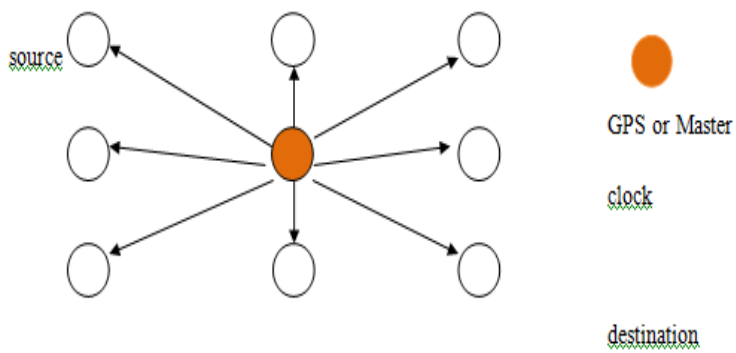


Fig 2: Nodes clock synchronization according to the GPS

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

In the figure 2 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.

Flow Chart of Proposed Methodology:

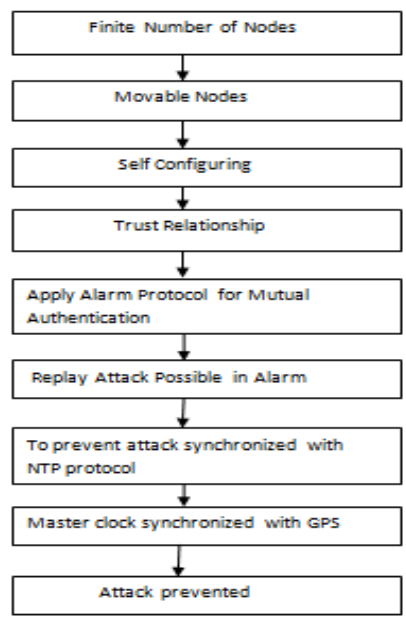
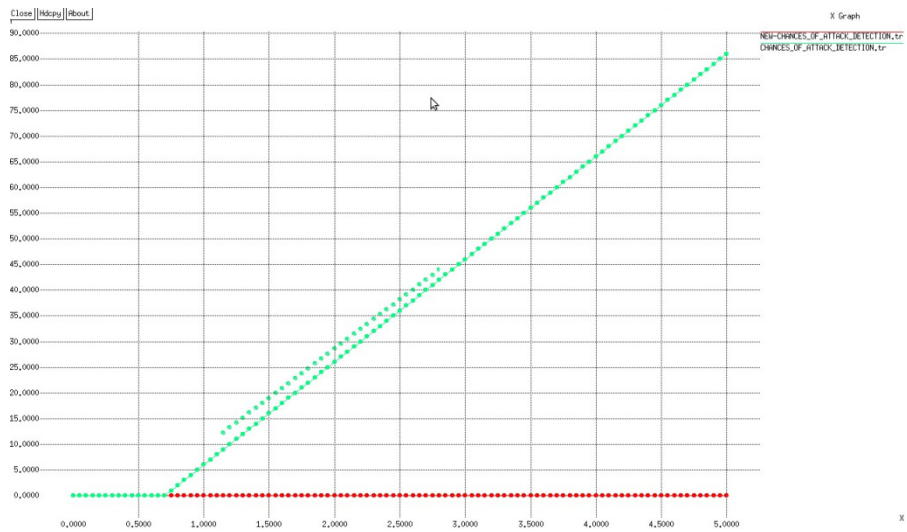


Fig 3: Flow chart

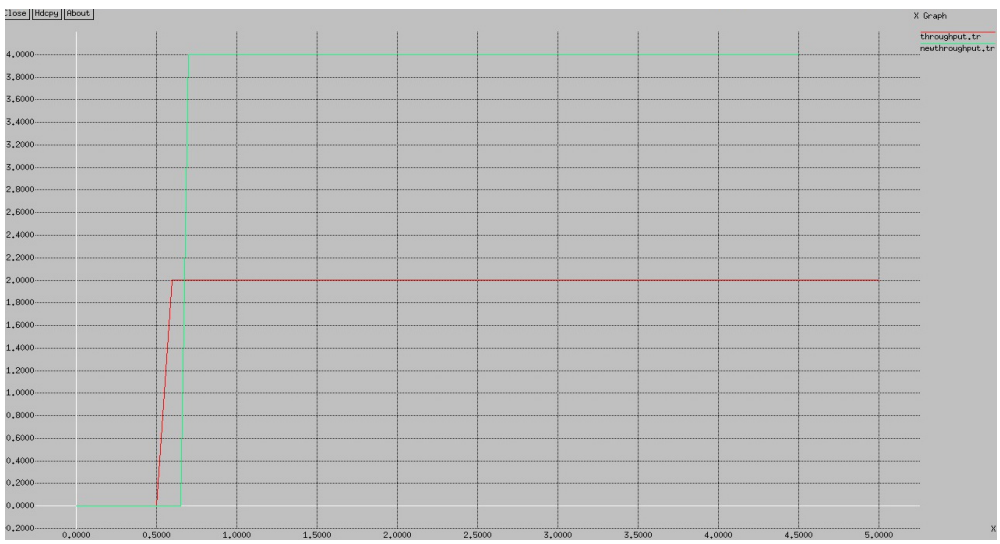
5. RESULTS

The results are shown in the form of graphs. Here we do the comparison between our work to the previous work, as:



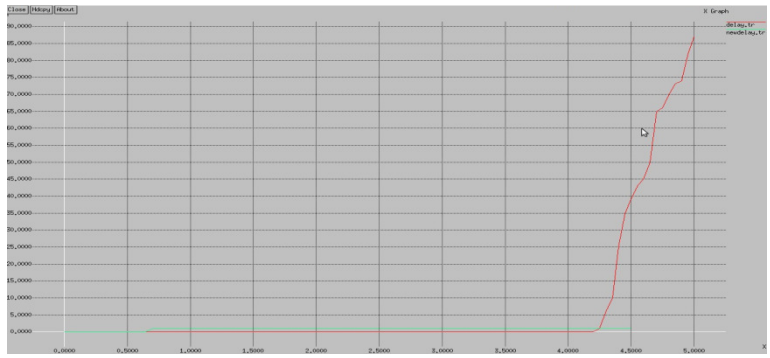
Graph 1: Prevention of attacks

In the above diagram a graph is shown which tells us about the prevention of attacks. Red and green lines show about the prevention of attacks of replay in WSN.



Graph 2: Throughput graph

In this above figure we compare the throughput of the old scenario and our scenario. In the above figure we shows the graph for both scenario, whether red line shows the throughput of the old scenario which is very low as compare to the new scenario which we have present. And green line shows the throughput of the new scenario which is quite high as compare to the old scenario.



Graph 3: delay of packets

In this above scenario which is shown in the figure we compare the packet delay and benefits due to the whole work. In the old scenario when the data move from source to destination there is high delay as shown in red lines In the above graph red line show more packet delay in old scenario, which is quite high and green graph shows the delay of packet which is quite low.

6. CONCLUSION AND FUTURE WORK

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. Presently not very much of the work has been done on the security of Alarm Protocol .This is because one would find it difficult to know the level of security to be provided to the Alarm Protocol. Hence in the future we can work upon that.

REFERENCES

[1] Jian-zhu Lu and Jipeng Zhou, "On the Security of an Efficient Mobile Authentication Scheme for Wireless Networks", International Journal of Computer Networking, Wireless and Mobile Communications (IJCNWMC), Vol. 3 Issue 2, 71-74, Jun 2013.

[2] Tien-Ho Chen and Wei-Kuan Shih, "A Robust Mutual Authentication Protocol for Wireless Sensor Networks", 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”

[5] System Steven M. Bellovin and Michael Merritt .”Limitations of the Kerberos Authentication”.

[6] K. El Defrawy and G. Tsudik, "Alarm: Anonymous location-aided routing in suspicious manets", IEEE ICNP 2007, pp. 304–313, Oct 2007.

[7] S.Karthiga and V.B.Rosy christiana, "Privacy in suspicious mobile ad hoc network by using Alarm", International Conference on Computing and Control Engineering (ICCCE 2012), April, 2012.