Localization and Key Management in Wireless Sensor Network: A Survey

Amar D. Rana
Research Scholar, IT Department
SCOE, Vadgaon (Bk)
Pune, Maharashtra. India
Amar.rana1601@gmail.com

Ganesh R. Pathak
Assistant Professor, IT Department
SCOE, Vadgaon (Bk)
Pune, Maharashtra. India
pathak.gr@gmail.com

***Abstract*— Wireless Sensor Network mentions a number of sensors for monitoring and recording the physical conditions of the environment. Sensors' location executes crucial role in many wireless sensor network. Localization and the movement of nodes creates security problem such as re-authentication and tracing the movement of the node. When the wireless sensor network is in hostile environment, location of the node may be estimated as a wrong one by the attacker and even the sensor node may be compromised. Many researchers conducted their work on Wireless Sensor Network along with particular issues of localization and proposed various methods to overcome those issues. In this paper we have discussed about localization process and key management methods what other researchers performed and focused on requirement of security of wireless sensor network.**

Keywords- Wireless Sensor Network, Key Management, Localization

I. INTRODUCTION

A wireless sensor network (WSNs) has gained global attention in recent days. It consists of small, low cost and less power sensor node [2]. It has short ranged wireless communication function. The sensors in the device gather information of the environment. The sensed information is then sent to the network i.e. the base station via wireless medium. Based on various sensing parameters and units, wireless sensor nodes can measure various physical characteristics such as sound, temperature, pressure, humidity etc. and due to this it mostly used in hostile environment like environment application or battlefield surveillance. [2].

The main issue in sensor network environment is nothing but security of network and security of particular sensor node. Our paper focusing on the security of sensor nodes in which distribution of authentication key is one of primary problem. As the sensor nodes are light-weighted devices and they have limited resources, utilizing the security protocol of other computer network is inadequate. Hence primary requirement in the security researches is to design a resource-efficient security protocol. For the efficient distribution of authenticated key many approaches have been introduced such as pre-distribution, pair wise key agreement, group key based key agreement and hierarchical key management [1].

When the WSNs are moved to an unfriendly environment, the attackers may attack to its localization process to make the estimated location incorrect. Incorrect location will lead to major consequences like providing wrong military decision on battlefield. Thus, the correctness of the sensor location must be safeguarded.

The correctness of sensors' location has to consider two facets. The first one is from the aspect of sensor, as the sensor has to acquire their correct location, so we need secure localization. The second is the aspect of the base station; the base station should also ensure that the sensors' location it is getting is correct. But when the base station needs to know about the location of the sensors', at that time the sensor nodes may be weaken and they deliberately report wrong location. We must verify that whether the reported location is correct or not which is collect location verification.

The main objective is to propose a well-organized re-authentication and key distribution model, which can reduce communication and computational overhead for the re-authentication of the mobile node between the sink and the base station. Using this protocol when the nodes changes its position and that node is previously authenticated by a sink then it can be re-authenticated with less communication and computational overhead and the node movement remains untraceable.

II. LITERATURE SURVEY

A. Localization and Key Management

When a node is initially connected to the network, the node gets connected with sink which is in the network and is authenticated by sink with the help of base station. Later when the node is moved to another location it needs to re-authenticate to other sink. This process of re-authentication continuous as the node keeps on changing its location. In practical, the re- authentication is needed when a node is moved and connected to other sink or when the connection is lost with the sink. Many researches on authentication and key distribution have been conducted assuming WSN as a static environment. So, they only have focused on efficient initial authentication and key setup.

1) Localization

Localization of sensor node in wireless network is very essential for many application either it should be deployed in hostile environment or not. Similarly it is used in number of engineering fields, so it is a separate and upcoming topic in research field such as robotics where to perform right task based on sensor, exact location is important thing. Basically this is rough use of localization, hence by considering such scenario the localization process is nothing but to find out area or location of particular node or batch of nodes. Wireless sensor network mainly contains two types of node, one is

common node and other is beacon node. Common nodes do not have any idea about their location, in contrast to this beacon nodes knows about its location by virtual Global Positioning System and their surrounding region. So here we say that localization is nothing but to estimate the location of common node also.
Classification of localization:

a) Range-Based v/s Range free

Range free method -

It does not require ranging information. This method uses radio connectivity to communicate between nodes in order to compute their location.

Range-Based method -

It requires ranging information. Range based methods are distance-estimation and angle-estimation. The techniques that are used in range based localization are received signal strength indicator (RSSI), angle of arrival (AOA), time difference of arrival (TDOA) and time of arrival (TOA). [6]

b) Node-centric v/s infrastructure centric

Node-centric method -

In this method node computed their location by themselves.

Infrastructure centric method -

In this method, the trusted node computes location of other node.

c) Centralized v/s Distributed

Centralized method -

In this method, all the information is passed to a central point/node which is generally known as "sink node" or "base station". Sink node is the one that computes the position of nodes and the information is forwarded to respective nodes.

Distributed method -

Sensors individually estimate and calculate their location and directly communicate with anchor nodes.

d) Region v/s Single point

Region method -

Verify sensor nodes of particular region.

Single point method -

Verify sensor node at position either batch of nodes or single node one by one.

e) GPS Based v/s GPS free

GPS Based method -

At every node GPS receiver are kept. In this method, accuracy in localization is high but the cost is also high.

GPS free method -

This method does not use GPS. In this method, node calculates the distance between nodes relative to local network. Cost is low compared to GPS based method.

f) Anchor Based v/s Anchor free

Anchor Based method -

In this method, the position of few nodes is known. Un-localized nodes use these known positions to localize their location.

Anchor free method -

In this method, nodes estimate their relative position instead of computing absolute node position.

g) Fine Grained v/s Coarse Grained

Fine grained method -

This method uses features of received signal strength for localization.

Coarse Grained method -

This method localize without using received signal strength.

2) Key Management

Zigbee [1] is a protocol that describes the key pre-distribution method used in commercial application which needs large key management in scalable network. It stores the secret between two entities. In this architecture, every node has their unique keys which are preinstalled. These unique keys are the master key and the link key and are shared to other entities. The producer shares the network key to entire network. To support the flexibility and localization of the node using the unique keys, each node must contain the key along with the number of nodes for communication. In totality it requires seven keys (three master keys, three link keys and on network key). Hence to deploy a Zigbee in to a large network needs large amount of storage for key management.

In 2002, [1] Eschenauer and Gligor presented a protocol with pair wise key agreement. It was based on pre-distribution of the random key and this pair wise key is shared form the pre-distribution key pool. In the first stage, every node stores certain number of keys. On deploying, the key information is shared between neighbour nodes. When the shared are found, a secure link is established among the sinks that share the keys. After the establishment of link, a pair wise key with the sink is generated via a secure link and no shared information.

Abraham and Ramanatha [1] [3] have proposed a protocol using authentication and initial shared key in hierarchical cluster networks. Ibriq and Mahgoub [1] proposed an efficient model that deployed a "partial key escrow table" for sink. A sink can generate by itself a shared key using the key escrow table for the nodes that are attached. But, all the sinks have to maintain the information of each node in the table to support movement of node.

Zhu [1],[3] proposed a model with group key based key agreement. It reduced the threads of compromised nodes. Each node has a unique key, pair wise keys with neighbour nodes, a cluster key which is shared with all neighbour nodes and a global key which is shared with complete network. But all these are assumed in static networks.

a) Authenticated key agreement protocol for Dynamic WSN

DISTRIBUTED AUTHENTICATION MODEL

Fantacci [3] presented an authentication model with distributed nodes. It does not require a base station to work as the centralized authenticator. In this model, partial authentication information of other nodes are shared among every nodes based on the secret sharing scheme. A node sends an authentication to other nodes which acts as a distributed authentication server. As there is involvement in the authentication process, there is overhead on all the nodes in this model. Each node has to act either as an authentication or as authenticator server so computational and the communication overhead is very high.

PKI (PUBLIC KEY INFRASTRUCTURE) BASED MODEL

Huang [3] proposed PKI based model by using Elliptic curve cryptography to reduce the overhead communication overhead from the key establishment. But PKI require larger computation power, in spite of enabling simplified key agreement procedure due to insufficient computational resources.

III. ATTACKS, DRAWBACKS AND SECURITY REQUIREMMENTS

A. Attacks on Localization

There are different attacks that would harm the localization in wireless network.

1. Distance fraud attack

It is an attack of hacking the measuring distance between two nodes. It contains one malicious node that is to appear closer or further to another legitimate node [4].

2. Mafia fraud attack

It is man-in-middle attack. It contains legitimate prover p, legitimate verifier v, malicious prover p (m), malicious verifier v (m). When p is about to make a verification protocol v(m), it establish a link with p(m) and sends information transmitted by p to p(m), which in turn sends it to v. When v tries to verify the identity of p (m), same occurs in reverse order. This makes distance between p and v to be calculated wrongly [4].

3. Spoofing attack

It contains a setting in which a malicious node pretends to a legitimate node in network and provide false localization information [4].

4. Jamming

It is caused by broadcasting a high- energy signal to disrupt network operation [4].

5. Wormhole attack

In the wormhole attack, at one location in the wireless sensor network a malicious node records packet, then it tunnels to another malicious at different location then retransmits it to distant sensor nodes. This makes sensor node to estimate wrong location [4].

6. Replay

It adversary plays back a past legitimate localization message to same or to some other recipient [4].

7. Manipulation

Modify the content of the message containing localization information [4].

B. Drawbacks of previous protocols

1. The Frequent re-authentication:

In order to increase the lifetime of the sensor, it is necessary to reduce communication and computational overhead since the sensor has limited battery power and low end processor. But, the mobile sensor node suffers from the problem of larger overhead, and this is because of the frequent request of re-authentication of node. The node will get connected to and get authenticated with sink. After the nodes' movement, the new sink has to authenticate with the node again. If the node is moving continuously, the process of re-authentication will occur repeatedly. This process of frequent re-authentication drains the resources in battery-based sensor nodes [1].

2. Tracing node movement:

Previous protocol does not considers the mobility of node. But when the sensor node moves, the tracking of node movement is one of the probable attacks. Tracking node movement is a threat to privacy [1]. Hence, it is necessary to have an authentication and key agreement protocol that provides privacy of the mobile node.

C. Security and Privacy Requirements

1.Re-authentication with less communication and computation overhead

2.Untracebility- In the process of re-authentication of the node with sink, the sink only knows that the node was previously authenticated but it can never trace the direction node.

3.Confidentiality- Communication packets between node and sink and between sink and base station will not be known to anybody else.

4.Message authentication is important to prevent the communication packet from getting forge by malicious attack.

5.Key freshness- The node and the sink should be able to verify the key which is been generated is in the current session.

6.Node/Sink Resiliency- The hostile adversary of either the node or the sink should not affect the network.

IV. CONCLUSION

In our paper we discussed about the process of localization and we have surveyed the technique of key management in wireless sensor network. Similarly we have discussed attacks on the localization process.

Based on this survey we say that very few work have been done in mobile or dynamic environment of sensors in wireless sensor network as well as some parameters like authentication of transferred sensor nodes, key management , robustness to highly effected attacks needs more attention which makes wireless sensor network more reliable and secure.

REFERENCES

[1] K. Han, K. Kim and T. Shon, "Untraceable Mobile Node Authentication in Wireless Sensor Network." KAIST, 119 Munjiro

Yuseonggn, Daejeon, Korea; SAMSUNG Electronics CO.LTD, Suwon Korea, April 2010.

[2] Y. Zeng, J. Cao, "Secure localization and location verification in Wireless Sensor Network", State Key Laboratory for Novel Software Technology Nanjing University, Nanjijg, 2009.

[3] Priya L C, Shantala Devi Patil, "A Survey on Sensor Authentication in Dynamic WSNs", Department of Computer Science and Engineering, April-June 2014.

[4] Waleed Ammar, Ahmed EIDawy and Moustafa Youssef, "Secure Localization in Wireless Sensor Networks: A Survey", Computer and Systems Engineering Department Alexandria University, July 2007.

[5] Chi-Chang Chen, Chi-Yu Chang and Yan-Nang Li, "Range-Free Localization in Wireless Sensor Network Based on Bilateration", Department of Information Engineering I-Shou University, December 2012.

[6] Guangji Han, Chenyu Zhang, Jaime Lloret,"A mobile Anchor Assisted Localization Algorithm Based on Regular Hexagon in Wireless Sensor Networks", Department of Information & Communication Systems, Hohai University, Changzhou 213022, China,July 2014