Key Pre-Distribution Methods of Wireless Sensor Networks – A Survey

S.Sibi, Thamizarasi A R

Abstract—Wireless Sensor Networks (WSN) consists of numerous small nodes which observe the environment that they are deployed in and transmit information like temperature, sound, movement etc. The security of this information is of top priority. There are many security mechanisms that are available and many researches being conducted on improvising these mechanisms. Various studies imply that the key management is one of the most efficient methods in providing a better security against various types of attacks. In this paper, the major key pre-distribution methods are discussed along with their advantages and disadvantages and how each method is different between other methods.

Index Terms— information transmission, key management, key pre-distribution, nodes, security, security mechanisms, studies

1 INTRODUCTION

Nodes form the integral part of a wireless sensor network. They contain small amount of memory in which they perform computation and transmission of messages. Since communication is the important function of the node, all it's communication should be properly secured. An intruder's main goal is it to compromise the network, so the security should be strong enough to neutralize any kind of attacks. The common threats posted by the intruder are denial of service, Sybil attack, traffic analysis attack, node replication or node duplication, eavesdropping, camouflage, physical attacks and natural attacks like flood, fire, earth quacks etc.

There are many techniques for establishing a secure transmission between the nodes. The most effective technique is key pre distribution. The major distribution methods are further discussed. The wireless network sensor could be deployed in any environment even that in a place that could pose a threat to them. Security mechanism should be implanted in such a way that they can withstand any environment and any possible attacker. A nodes memory is very limited. So it should be efficiently used in transmission and computation.

- *S.Sibi is currently pursuing bachelors' degree program in Information Technology engineering in Vellore institute of Technology, India, PH-09789732932. E-mail: sibisenth@gmail.com.*
- *Thamizarasi A R is currently pursuing bachelors' degree program in computer science engineering in Vellore Institute of Technology, India.*

Security mechanism should only take less memory space and provide greater security. If a security protocol is big and labors, it not only takes up the very essential memory space but also increases the amount of energy consumed which in turn will increase the cost of the establishment of a wireless sensor network.

2 METHODS OF KEY PRE-DISTRIBUTION

2.1 Eschenauer & Gligor's Random key pre-distribution [1]

This method consists of a three step working phase. In the first phase called pre-distribution phase it selects a random set of keys from all available keys. Each node receives m keys that are stored in the memory of that node. These selected set of keys are called as key-ring. This phase is called key selection phase. The second phase, key discovery phase involves in the nodes broadcast their key –king to find out which of their neighbors have common keys. This is done by challenge.-response protocol. The common key that is recognized by both of the nodes (neighboring nodes), becomes the key for that link. The third phase is the path key establishment phase. After each node establishing link with its neighbors, if the path is connected form the source and destination then source node can transmit information security via the path to the destination.

2.1.1 Disadvantages of Eschenauer & Gligor's Random key pre-distribution

The area when the nodes are deployed could have extreme erotic physical obstacles which decrease the possibility of a successful establishment of fully connected network. Despite all odds there is always a possibility that the link is not properly formed and fully connected to all the required nodes. The major reason is that the formation of link between the two nodes depends of only one shared key from the key ring of those nodes. If the network detects a link failure or a disconnection, the network should do range extension (Increasing the power of transmission is called Range extension) or multi-hoping (sending request to their neighbors to forward their communication to a certain no of hops).

2.2 q- Composite random key pre-distribution [2]

This is a modified method of Eschenauer & Gligor's random key pre distribution method [1] to minimize its disadvantages. In Eschenauer & Gligor's random key pre distribution method [1] only one key from key ring is used. Whereas here the modifications proposed is to have 9 common keys between the communication nodes where Q is >1. Since it increases the number of keys shared between each node, it decreases the chances of an intruder breaking in and there by considerably increasing the resilience of the network. In this method it is necessary to increase the size of the pool or number of keys form which the key-ring is selected and decreasing the key–ring size thus making it harder for the attacker. This follows the same three phases of Eschenauer & Gligor's random key pre distribution method [1]. Everything is similar except for the multiple common key usage and size of key pool. Each node is assigned with a set of random keys, that they store it in memory called as key ring. In second phase, the key discovery phase, each node identifies all common keys that it contains with each of its neighbor. It can be achieved by broadcast - response method (or) Markel puzzle-solve-response method. Broadcast-response easy but very vulnerable to eaves dropping. So if a strong security is required alternative method, the Markel puzzle-solve–response method is suggested. A node issues m number of puzzles (one for each key) to all its neighbors, the node which solves the puzzle and responds with a correct answer, a path key is established. This is more secure but much slower. Neighbors are identified and key set up is only performed it both the nodes have at least q common keys. Then the connection/link between the nodes is established. This is the third and final step called path key establishment.

2.2.1 Disadvantages of q- Composite random key pre-distribution

This method holds no good towards node duplication or node replication. This is because there is no constrain on node degree. Once a key is established it can be used many number of times.

2.3 Master key

This is one of the most unsophisticated methods of key pre-distribution. A master secret is given to all the nodes present in the network. If any node wishes to communicate with any other node then; these communicating nodes make use of the global master key and establish a pairwise key. This technique has very poor network resilience when compared to all the other key pre-distribution techniques. This is because if any intruder hacks into the node and obtains the master secret key the integrity of the complete n/w is lost. This is the major disadvantage of this method to enhance this dis-advantage there were studies that advocated stocking the master key in tamper-resistant hardware that would comparatively abate the danger of exposure. But this in turn escalates the cost involves and also leads to higher and quicker energy depletion.

(N-I)Pairwise key method. This is a rhetoric method which is highly unfeasible to implement in a practical working wireless sensor network. Consider there are N nodes in a network. According to this method there will be (N-I) secret pairwise keys stored in the memory of each node. A unique separate key for every pair of nodes. This technique has "perfect resilience" because if the intruder manages corrupt one node. It will not affect the security of the rest of the network.

2.3.1 Disadvantages of Master key

Since the memory space in wireless sensor network nodes is very small it is impossible to store all N-1 keys in its very limited memory. If it requires adding new nodes to already deployed wireless network sensor, it is highly challenging because the other nodes present in the network will not contain the new nods key and vice-versa.

2.4 Blom's method (Matrix method) [4]

Bloms method considerable reduces the memory space required when compared to the memory space used (N-1)pairwise method. It requires λ+1 memory spaces, where threshold value λ is much lesser than N, where N is the total number of nodes deployed in a network. Blom's method follows λ-security property.

λ-security property *when an intruder disables less than or equal to λ nodes then the remaining nodes that are part of network will be untarnished. When an intruder disables more than y nodes then the security of the total network fails and complete connection collapses.*

In this method any two communicating nodes will be able to find their own pair wise key for their secret communication. It is given by

$$A = (D.G)\ T \quad (1)$$

When D is public Information so all the nods and including the attackers is allowed to know.

$$G = (\lambda + 1) + N \quad (2)$$

Where, λ is the threshold factor N is the size of the node and D is private information and secrecy should be maintained.

$$D = (\lambda + 1) + (\lambda + 1) \quad (3)$$

λ is the threshold factor.
The pairwise key obtained is

$$K = (D.G)\ T.G \quad (4)$$

This matrix key obtained will be symmetric in nature where Kji =Kji, where i corresponds to the row and j corresponds to Colum and kij is an element present in ith row and jth Colum. If node i computes row i and node j computes column j and finds kij=kji. Then they have a common key.

2.4.1 Disadvantages of Blom's method (Matrix method)

The disadvantage of blom's method is that a greater threshold factor (λ) is required for a greater security which in turn leads to high memory consumption.

2.5 LEAP - Lightweight Extensible Authentication Protocol) [3]

In a single global/master key method, if one node is compromised then it will lead to the down fall in security or the entire network. Also different types of messages that are exchanged between various nodes needs various types of security protocols. These two factors led to the rise of multi-keying mechanism. LEAP (Lightweight Extensible Authentication Protocol) is a multi-keying mechanism which supports in-network processing and also provides the same security that would protect the neighborhood of the surrounding compromising node.

They are four types of keys called Individual keys, Pairwise key, Cluster key and Group key.

2.5.1 Individual keys

An individual key is preloaded into each node before deployment that it shares it only the base station.

2.5.2 Pairwise key

A pair wise key is established between a node and its immediate neighbors.

2.5.3 Cluster key

The key that is established between a node and its all neighboring nodes is called a cluster key.

2.5.4 Group key

All the nodes in a n/w share a group key when the base station transmits a secure message it uses the group key.

2.5.5 Disadvantages of LEAP

Bigger the size of the network (high number of node) higher the cost becomes.

Leakage of group key poses a greater security threat.

3 CONCLUSION

Even though there are various security schemes the attackers constantly work on breaching the WSN. It is necessary to keep working on the development of new mechanism which is memory efficient and fuel efficient. These are most leading and efficient key pre distribution techniques that we discussed. Different environment require different type of security mechanisms. Pre-deployment knowledge plays an important role in security enhancements.

REFERENCES

[1] *L. Eschenauer and V. D. Gligor. A key-management scheme for distributed sensor networks. In CCS 02 : Proceedings of the 9th ACM conference on Computer and communications security , New York, NY, USA.ACM, 2002, 41-47.*

[2] *H. Chan, A. Perrig, and D. Song. Random key predistribution schemes for sensor networks. In SP 03: Proceedings of the 2003 IEEE Symposium on Security and Privacy, 197, Washington, DC, USA, IEEE Computer Society, 2003.*

[3] *S. Zhu, S. Setia, and S. Jajodia, Leap: efficient security mechanisms for large-scale distributed sensor networks. In CCS 03 : Proceedings of the 10th ACM conference on Computer and*

communications security, New York, NY, USA.ACM, 2003, 62-72.

[4] *R. Blom. An optimal class of symmetric key generation systems. In Proc. of the EUROCRYPT 84 workshop on Advances in cryptology: theory and application of cryptographic techniques, New York, NY, USA. Springer-Verlag New York, Inc, 1985, 335-338.*