Volume 4, Issue 8, August 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Survey of Key Pre Distribution Schemes for Wireless Networks

Hitesh Matre
Svits Indore (M.P)
India

Abstract: The security in wireless sensor network is a burning issue. There are many researchers, who are working on the security requirements of the wireless sensor networks. In this paper, we are presenting a survey for pre key distribution in the wireless sensor network. Key management is a challenging issue in the WSNs. While designing a key management scheme, the parameters like network scalability is needed to be considered. The key management scheme should be able to support a large number of nodes. It also contains an introduction to key distribution. It also elaborates various challenges in establishing an efficient key distribution scheme.

Keywords: wireless sensor network, key distribution, scalability

I. INTRODUCTION

A wireless sensor network (WSN) [3,4] consists of spatially distributed autonomous sensors to *monitor* physical or environmental conditions and to cooperatively pass their data through the network to a main location. The more modern networks are bi-directional they also enables *control* of sensor activity. The research of wireless sensor networks was motivated by military applications such as battlefield surveillance. Today such wireless networks are used in many industrial and consumer applications. Such application includes industrial process monitoring and control, machine monitoring, and so on.

Key distribution is an important issue in wireless sensor network (WSN) design. It is a newly developing field due to the recent improvements in wireless communications.

Wireless sensor networks are networks of small, battery-powered, memory-constraint devices named sensor nodes, which have the capability of wireless communication over a restricted area.[1]Due to memory and power constraints, they need to be well arranged to build a fully functional network.

Key pre distribution is the method of distribution of keys onto nodes before deployment. Therefore, the nodes build up the network using their secret keys after deployment, that is, when they reach their target position.

Key pre distribution schemes [5,6,7] are various methods that have been developed by academicians for a better maintenance of key management in WSNs. Basically a key pre distribution scheme has 3 phases:

1. Key distribution
2. Shared key discovery
3. Path-key establishment

During these phases, secret keys are generated, placed in sensor nodes, and each sensor node searches the area in its communication range to find another node to communicate. A secure link is established when two nodes discover one or more common keys (this differs in each scheme), and communication is done on that link between those two nodes. Afterwards, paths are established connecting these links, to create a connected graph. The result is a wireless communication network functioning in its own way, according to the key pre distribution scheme used in creation.

There are a number of aspects of WSNs on which key pre distribution schemes are competing to achieve a better result. The most critical ones are: local and global connectivity, and resiliency.

Local connectivity [6] means the probability that any two sensor nodes have a common key with which they can establish a secure link to communicate.

Global connectivity is the fraction of nodes that are in the largest connected graph over the number of all nodes.

Resiliency is the number of links that cannot be compromised when a number of nodes(therefore keys in them) are compromised. So it is basically the quality of resistance against the attempts to hack the network. Apart from these, two other critical issues in WSN design are computational cost and hardware cost. Computational cost is the amount of computation done during these phases. Hardware cost is generally the cost of the memory and battery in each node.

There is a most-cited key pre distribution scheme [2] which is usually called "the main scheme" that introduced the ides of random key distribution, whereby the randomness factor drastically improves resiliency.

II. LITERATURE SURVEY

Eschenauer and Gligor [8] proposed the probabilistic key pre-distribution scheme. It became popular and most referred method by the subsequent researchers. . This scheme requires three phases are needed to set up the secret keys between sensor nodes. These phases are key pre distribution, discovering shared key and path key establishment. The first phase randomly assigns k different keys from a big key pool each sensor node randomly.

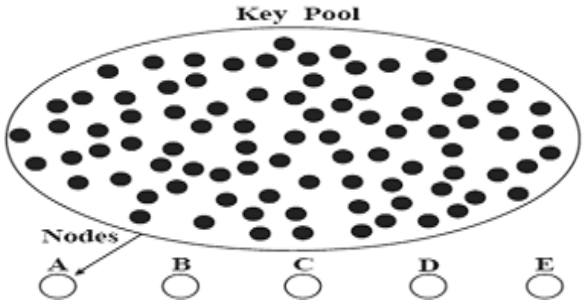

Figure 1: Key pool[8]

Stored keys in each sensor node are called keyring of the node and each key has a corresponding id. Next two phases are done when nodes are deployed. The shared key discovery phase nodes find the common key between them and establish a secure connection. Each node discovers its neighbors in communication range with which it shares common keys. The sample graph after shared key discovery is shown below in figure. The node pairs A and B or A and C can set up secure links through their common keys.

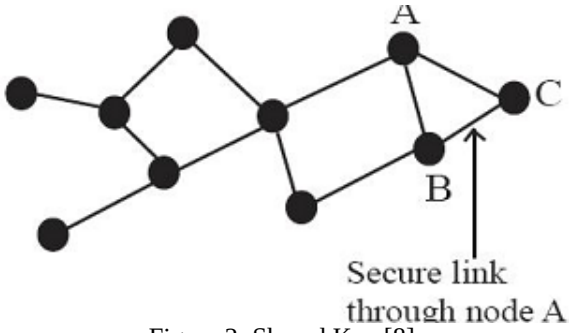

Figure 2: Shared Key [8]

It might happen that nodes are in communication range but do not share any keys, these nodes may be connected by one or more hops links through path key establishment phase. As shown in fig. 2, nodes B and C are in communication range but do not share a common key. The third phase assigns a path key to the sensor nodes via node A and then they can set up secure link between them. Most of the present pre-distribution schemes are based on this model. It is a very popular model

In wireless sensor network base station is known as centralized authority. Base station is used to revoke the compromised nodes. Authors presented a key management scheme for wireless sensor network in [8]. It is a centralized key revocation scheme. In this scheme if a node is compromised then the base station can send a message to all other sensors to revoke the compromised node's key ring. The work in [8] can be divided into three phases: signature key distribution, key revocation and link reconfiguration.

In the signature key distribution phase the base station is responsible for generating a signature key. To do the same the base station unicast a signature key to each node. Then the signature key is encrypted with a pairwise key shared by the base station with the sensor node.

In the key revocation phase the base station broadcast single key revocation message signed by the signature key. This broadcasted message contains a list of key identifiers for the key ring to be revoked. Some links may disappear if the keys are removed from the key rings and the affected nodes need to reconfigure those links by restarting the shared-key discovery and the path-key establishment phase.

The key revocation scheme in [8] requires n unicast messages and one broadcast message. Also in a large scale sensor network, the distribution of signature key might be a problem. Also the adversary could use the signature key to duplicate the revocation messages from the base station.

Zhang et. al. proposed a key revocation scheme which is commonly known as GPSRRev scheme [9]. It is also a centralized key revocation scheme.

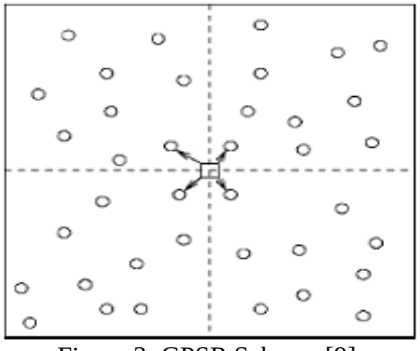
Figure 3: GPSR Scheme [9]

In this scheme [9], revocation area is divided into sub-areas if the revocation area is large. Then by using GPSR protocol, revocation message is sent to a certain node within each area [10]. Then the same message is multicast for the remaining regions. The revocation message contains two fields: the identifier of the sensor nodes to be revoked and the scope of the revocation area. If the sensor node falls within the revocation area indicated by the revocation message, then the sensor node records the identifier of the revoked sensor node and rebroadcast the message to its neighboring nodes. A message is dropped if it is outside the revocation area.

No centralized authority is used in a distributed key revocation scheme. Author Chan proposed a distributed key revocation scheme for sensor networks in [11] and further investigated this scheme in [12]. This scheme cast a vote & collect it using among sensor nodes. If the number of votes against a sensor node exceeds a specified threshold, then that particular sensor node will be revoked. First at the connection time neighboring nodes exchange the masks to decrypt the votes, then in the current session, at least *t* sensor nodes are required to cast their votes against the target node. In next session, voting nodes cast their votes against the target node. The information related to the compromised sensor node is to be broadcasted in the network if and only if a sensor node receives at least t revocation votes. This scheme has some assumptions. These are each node knows its neighboring nodes and each node knows its neighboring node's neighboring nodes before deployment. It is extremely hard to satisfy this requirement. But the main advantage is that he distributed key revocation scheme is faster compared with the centralized key revocation because it requires local broadcast. But this distributed key revocation scheme is more complex than the centralized key revocation scheme. Detail information about the distributed key revocation scheme is included in [11-12].

III. RESEARCH OBJECTIVES

- To design a pre key distribution scheme for wireless sensor network with higher scalability
- To design a pre key distribution scheme for wireless sensor network with good key sharing probability
- To design a pre key distribution scheme for wireless sensor network with reduced storage overhead

IV. CONCLUSION

This paper contains an overview of wireless sensor network. Key management in WSN is also elaborated in an attractive manner. The literature survey of the most popular algorithms for the pre key distribution is the heart of this survey paper. All these algorithms have been analyzed. Their merits and demerits are discussed. At the end, we have identified a list of future research works in the area of pre key distribution in wireless sensor networks.

ACKNOWLEDGEMENT

This research paper is made possible through the help and support from everyone, including: parents, teachers, family, friends, and in essence, all sentient beings. Especially, please allow me to dedicate my acknowledgment of gratitude toward the following significant advisors and contributors:

First and foremost, I would like to thank Mr Anand Rajavat and Mr Rajesh Kumar Chakrawarti (Department of CSE in SVITS Indore) for his most support and encouragement. He kindly read my paper and offered invaluable detailed advices on grammar, organization, and the theme of the paper.

Finally, I sincerely thank to my parents, family, and friends, who provide the advice and financial support. The product of this research paper would not be possible without all of them.

REFERENCES

[1] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in wireless sensor networks," *IEEE Communications Surveys and Tutorials*, vol. 8, no. 2, 2006.

[2] X. Du, Y. Xiao, M. Guizani, H.H. Chen, An Effective Key Management Scheme for Heterogeneous Sensor Networks, Ad Hoc Networks, Elsevier, vol. 5, issue 1, January 2007, pp. 24–34.

[3] P. Traynor, R. Kumar, H. B. Saad, G. Cao, and T. L. Porta, "LIGER: Implementing efficient hybrid security mechanisms for heterogeneous sensor networks," in *Proc. MobiSys'06*, Uppsala, Sweden, 2006.

[4] Chee-Yee Chong and S. P. Kumar. Sensor networks: evolution, opportunities, and challenges. *Proceedings of the IEEE*, 91(8):1247–1256, 2003.

[5] I. F. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," *IEEE Communications Magazine*, vol. 40, no. 8, pp. 102–114, August 2002.

[6] S. Kroc and V. Delic. Personal wireless sensor network for mobile health care monitoring. In *Telecommunications in Modern Satellite, Cable and Broadcasting Service, 2003. TELSIKS 2003. 6th International Conference on*, volume 2, pages 471–474 vol.2, Oct. 2003.

[7] I. Akyildiz, W. Su, Y. Sankarasubramaniam, and E. Cayirci, "A survey on sensor networks," IEEE Communication Magazine, Aug. 2002.

[8] Zhang W, Song H, Zhu S, Cao G. Least privilege and privilege deprivation: towards tolerating mobile sink compromises in wireless sensor networks. In *MobiHoc '05: Proceedings of the 6th ACM International Symposium on Mobile Ad Hoc Networking and Computing*. ACM Press: New York, NY, USA, 2005; 378–389.

[9] Karp B, Kung HT. GPSR: greedy perimeter stateless routing for wireless networks. In *MobiCom '00: Proceedings of the6th Annual International Conference on Mobile Computing and Networking*. ACM Press: New York, NY, USA, 2000; 243–254.

[10] Chan H, Perrig A, Song D. Random key predistribution schemes for sensor networks. In *Proceedings of IEEE Symposium on Security and Privacy*, Oakland, CA, USA, May 2003, 197–213.

[11] Chan H, Gligor V, Perrig A, Muralidharan G. On the distribution and revocation of cryptographic keys in sensor networks. *IEEETransactions on Dependable and Secure Computing* 2005; **2**(3):233–247.

[12] O. Kachirski and R. Guha, "Effective intrusion detection uses multiple sensors in wireless ad hoc networks," in System Sciences, 2003. Proceedings of the 36th Annual Hawaii International Conference on, p. 8 pp., 2003.

