# Key Management in Wireless Sensor Network A Survey

**Ms. Nimisha Chunilal Chaudhari**

LDRP Institute of Technology and Research, Gandhinagar

## ABSTRACT

***Key management has become a challenging issue in the design and deployment of secure wireless sensor networks. Key management is a fundamental cryptographic primitive upon which other security primitives are built. Basically, key management includes two aspects: key distribution and key revocation. Key distribution refers to the task of distributing secret keys between communicating parties to provide secrecy and authentication. Key revocation refers to the task of securely removing compromised keys. By revoking all of the keys of a compromised sensor node, the node can be removed from the network. Compared to key distribution, key revocation has received very little attention. In this paper, we have discussed several existing methods for key revocation.***

**Keywords:** Key distribution, Key revocation, heterogeneous atmosphere, wireless sensor node, Security Requirements

## 1. INTRODUCTION

Wireless Sensor Networks have become popular in recent past. The use of sensor networks is not limited to military applications, but also in civilian applications such as health monitoring, industry, wildlife monitoring and so on. A lot of research has been carried out in this field to improve hardware specifications, protocols for communications and information security [1]. Previous research on sensor network security mainly considers homogeneous sensor networks. Research has shown that homogeneous sensor networks have poor performance and scalability compared to heterogeneous sensor networks [2-3]. Many security schemes designed for homogeneous sensor networks have high communication overhead, computation overhead and large storage requirement. Sensor network applications mainly designed and developed for military [4] but now it has civilian applications too. Applications vary in scope from military applications to vehicular applications to medicine applications [5-6].

Wireless sensor network is differing from other wireless ad-hoc network in the sense that they are resource limited, they are prone to failures, and they are deployed densely. The number of nodes in wireless sensor network is several orders higher than that of ad hoc networks. In wireless sensor network, network topology is constantly changing. They use a broadcast communication medium. The major components of a typical sensor network are: sensor nodes, the sensor field, the sink and the task manager. Sensor nodes are made up of four basic components: a sensing unit, a processing unit, a radio transceiver and a power unit [7].

When you submit your paper print it in two-column format, including figures and tables. In addition, designate one author as the “corresponding author”. This is the author to whom proofs of the paper will be sent. Proofs are sent to the corresponding author only.

## 2. SECURITY GOALS

All the applications use intermediate node to send and receive data or can directly send and receive data. Sensor nodes send and receive data through wireless media and thus signals can be received by other nodes also. Broadcast nature requires that data must be sent securely so that no unauthorized node gets the data. This section is related to the security of sensor networks.

Secure communication is required for transmitting data securely between sensor nodes. Secure communication can be done using public key cryptography or symmetric key cryptography. Public key cryptography can not be used for sensor nodes due to high memory requirement, high energy consumption and computation requirement. Symmetric key cryptography can be used to setup pair wise keys between nodes.

Setting security goals for sensor networks will depend on knowing what it is that needs protecting. Sensor networks share some of the features of mobile ad hoc networks but also add some unique challenges. The security goals encompass both those of the traditional networks and goals suited to the unique constraints of sensor networks.

Among all security issues, key management has become a challenging issue in the design and deployment of secure wireless sensor networks. Key management is a fundamental cryptographic primitive upon which other security primitives are built. It contains two parts: key distribution and key revocation. Key distribution refers to the task of distributing secret keys between communicating parties to provide secrecy and authentication. Key revocation refers to the task of securely removing compromised keys. By revoking all of the keys of a compromised sensor node, the node can be removed from the network. Compared to key distribution, key revocation has received very little attention.

## 3. Security Requirements for Key Management Scheme

A good key distribution or establishment and management schemes for sensor networks needs to consider few security points.

1. The scheme must work without prior knowledge of which nodes will come into communication range of each other after deployment.
2. Deployed nodes must be able to establish secure node-to-node communication.
3. Additional legitimate nodes deployed at a later time can form secure connections with already deployed nodes.
4. Unauthorized nodes should not be able to take entry into the network or become members of the network.
5. Sensor nodes have limited resources so computational and storage requirements of the scheme must be low.
6. If a node becomes compromised, the key management scheme must be able to securely remove the compromised node from the network.

## 4. Related Work

A lot of work has been done in sensor networks related to key distribution. However, key revocation has received relatively little attention. The task of securely removing the compromised keys is known as key revocation. This chapter provides brief overview and analysis of the current key revocation schemes for sensor networks.

### 4.1 Eschenauer and Gligor's scheme

Eschenauer and Gligor [8] proposed the probabilistic key pre-distribution scheme. In most of papers this scheme is referred as basic scheme. In this scheme, three phases are needed to set up the secret keys between sensor nodes. These phases are key predistribution, shared key discovery and path key establishment. In first phase each sensor node randomly assigned k different keys from a big key pool. This is shown in figure 1 where nodes A, B, C, D, E are randomly assigned k keys from the key pool.

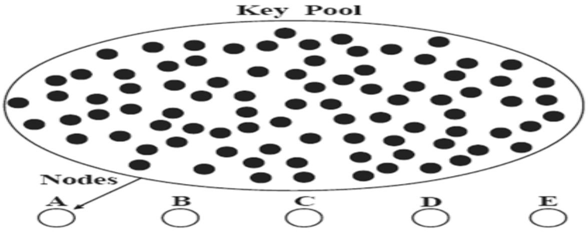

**Figure 1** Selection of keys from large key pool

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. In the shared key discovery phase nodes find the common key between them and establish a secure connection. In this phase each node discovers its neighbors in communication range with which it shares common keys. Figure 2 shows sample the sample graph after shared key discovery. In this network node pairs A and B, and A and C can set up secure links through their common keys.

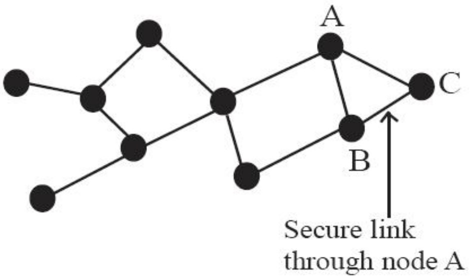

**Figure 2** Network graph after shared key discovery

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 path key establishment 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 pre-distribution schemes are based on this model.

In wireless sensor network base station is known as centralized authority. Base station is used to revoke the compromised nodes. Eschenauer and Gligor presented a key management scheme for wireless sensor network in [8]. It is a centralized key revocation scheme. If a node is compromised, the base station can send a message to all other sensors to revoke the compromised node's key ring. The revocation scheme 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 generates a signature key. The base station unicast a signature key to each node. 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 message contains a list of key identifiers for the key ring to be revoked. Each sensor verifies the signature of the key revocation message locates those identifiers in its key ring and removes the corresponding keys.

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. In a large scale sensor network, distributing the signature key might be a problem. Pre-distributing the signature key might be possible, however once the signature key is compromised, the adversary could use the signature key to duplicate the revocation messages from the base station.

### 4.2 Zhang et al. scheme

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

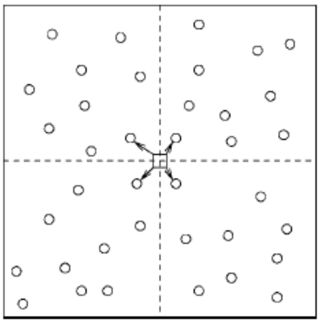

**Figure 3** Zhang et al. scheme

The revocation area is divided into sub-areas if the revocation area is large. Using GPSR protocol, a revocation message is sent to a certain node within each area [10]. After that for remaining sub-areas the revocation message is multicast. The revocation message includes two things: first the identifier of the sensor nodes to be revoked and the scope of the revocation area. If the sensor node is within the revocation area indicated by the revocation message, the sensor node records the identifier of the revoked sensor node and rebroadcast the message to its neighboring nodes. The message is dropped if it is outside the revocation area.

### 4.3 Chan et al. scheme

No centralized authority is used in a distributed key revocation scheme. Chan proposed a distributed key revocation scheme for sensor networks in [11] and further investigated this scheme in [12]. In this scheme, a vote is cast and collected among sensor nodes. If the vote tally against a sensor node exceeds a specified threshold, the sensor node will be revoked. In this scheme, first at the connection time neighboring nodes exchange the masks to decrypt the votes. Then in the current session, at least *t* sensor nodes cast their votes against the target node. In the next session, the voting nodes cast their votes against the target node. The compromised sensor node information needs to be broadcasted in the network if and only if a sensor node receives at least t revocation votes. Chan's scheme is built on some simplifying assumptions, such as each node knows its neighboring nodes and each node knows its neighboring node's neighboring nodes before deployment. It is hard to satisfy this requirement. The distributed key revocation scheme is faster compared with the centralized key revocation because it requires local broadcast. However, the 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].

## 5. CONCLUSION

The developments in sensor networks occurring at a very fast pace, but compared to that security within sensor networks has not gained significant interest. This is partially because of the lack of understanding of the potential of these tiny devices, and partially due to the lack of commercial motivation. In this paper, we have discussed various existing key management schemes for wireless sensor networks.

## 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.

[13] X. Zou, B. Ramamurthy, and S. S. Magliveras, *Secure Group Communications Over Data Networks*, Springer, 2005.

[14] D. Liu, P. Ning, and K. Sun, "Efficient self-healing group key distribution with revocation capability," in *CCS '03: Proceedings of the 10th ACM conference on Computer and communications security*. New York, NY, USA: ACM Press, 2003, pp. 231–240.