A Survey on Key Distribution Schemes in Wireless Sensor Networks

He Liu
School of Computer Science and Technology
HanKou University
Wuhan, China
e-mail:leuher@gmail.com

***Abstract*—in this paper, we propose the criteria and classifications of key management schemes in wireless sensor networks, and provide a survey on the key distribution management schemes including basic key pre-distribution schemes, polynomial based key distribution schemes, location based key distribution schemes and key management in hierarchy networks, and make a discuss and analysis of different key management schemes. Finally, we indicate the new research directions of key management schemes in wireless sensor networks.**

Keywords-Wireless Sensor Networks(WSNs); key management; Key Pre-distribution; security

I. INTRODUCTION

Wireless sensor network are consists of number of sensor nodes conjoin to monitor temperature, sound, pressure, and etc. The WSNs are application-oriented usually used in battlefield, environment monitoring, etc. [1]. Attacks from outside or inside of the network may destroy the sensor network, so it is important to make nodes trusted before a WSN exchange data, effective key management strategies among nodes, Cluster Heads and Base Station are the key methods to enhance the security of WSNs. Key management is one of the critical and basic issues in WSNs security [2].

Due to the limited capability of power and computation, the traditional security strategies in wire networks can’t be used directly in WSNs. In this paper, we analysis and compare the existing key pre-distribution schemes. And finally discuss the future researches on the key management in WSNs.

II. BASIC FEATURES AND SECURITY REQUIREMENTS

The sensor nodes of WSNs have many constraints in limitation of power, transmission and calculation capability [3][4]. To enhance the security of WSNs using key management schemes, there many indicators must be considered [4].

A. Features of sensor nodes

- **Limited energy.** Usually the battery power carried in the sensor nodes are very limited.
- **Limited transmission bandwidth and capability.** Typical sensor network’s bandwidth is low, the transmission capability of each node is also very limited, and therefore a large amount of data transmission will cause a great power loss.
- **Limited computation and storage capacity.** A sensor node with low power energy has weaker processor capability and less storage capacity.
- **Weak security.** Because sensor nodes have low battery and low calculation capability, the wireless sensor networks are more susceptible to network attacks and physical capture.

B. Desirable features of key management scheme

There are many qualitative indicators to evaluate a key management scheme [4]. Due to the characteristics and limitations of WSNs, the traditional security indexes such as connectivity, authentication, and, etc. can still be used to evaluate the key management schemes. Desirable features of key management schemes.

- **Connectivity**. Connectivity is the probability to set up session key directly between nodes. It is prerequisite of playing the proper function in WSNs to keep a high connectivity.
- **Security.** Authentication and intrusion tolerance are primary in sensor networks.
- **Robustness.** The key management system should survive despite denial-of-service attacks and unavailable nodes. The key management operations should be able to be completed despite faulty nodes and nodes exhibiting Byzantine behavior; Key management operations should not require network wide and strict synchronization.
- **Scalability.** Key management scheme must be able to adapt to different scale of wireless sensor networks and to support the dynamic changes in the network.
- **Simplicity.** The limitation of power, computation capability and storage must be considered in designing a key management scheme. Communication energy consumption is greater than calculation.

III. KEY MANAGEMENT SCHEMES

Key management deals with generating, distributing and storing encryption and decryption keys to implement secure communication. The simplest solution to key management is to use a global key for all the sensor nodes. However, if any node in the network is compromised, then the whole network security is defeated. Another simple solution is to have each node store N − 1 different keys, with each key corresponding to a different node in the network. However, sensor nodes may be insufficient to store the N−1 keys because of limited memory, especially for a large network.

There have been extensive research works done in the area of key management schemes. In this paper, we discuss four categories of key management schemes: basic key pre-distribution schemes, polynomial based key distribution schemes, location based key distribution schemes and key management schemes in hierarchy networks.

A. *Basic Key Pre-Distribution Schemes*

In key pre-distribution schemes, sensor nodes store some initial keys before the nodes are deployed [5]. Key pre-distribution schemes can be categorized into probabilistic schemes and deterministic schemes.

In probabilistic schemes, the existence of common pre-distribution keys between intermediate nodes is not certain, but instead guaranteed with probability.

Eschenauer and Gligor [6] proposed an earlier probabilistic schemes. In their scheme, a ring of keys is distributed to each sensor node before deployment. Each key ring consists of a randomly chosen *k* keys from a large pool of *P* keys, which is generated offline. A pair of nodes can communicate if they share any key among their key rings. Although a pair of nodes may not always have a shared key, if a path between them exists, they can use that path to exchange a key that establishes a direct link.

An enhancement probabilistic scheme is proposed by Chan et al [7]. This scheme requires *q* keys ($q > 1$) instead of just one common key among the key rings of a pair of communicating nodes. The authors showed that the *q*-composite key scheme strengthens the network's resilience against node capture when the number of captured nodes is small.

GKMPSN is a probabilistic scheme proposed by Zhu and Zhang [8]. It is a centralized group key distribution scheme, in which a network controller broadcasts new group keys, as well as node revocation information, to all the nodes whenever a compromised node is detected. Prior to the deployment of the network, each node stores a random set of keys out of a common large key pool. The group re-keying operation then takes two steps. In the first step, the pre-deployed random keys at each node are used to create secure channels between nodes in order to deliver new keying materials to legitimate nodes. In the second step, each node uses the received keying materials to update both the group key and the pre-deployed keys that are invalidated by the compromised nodes. GKMPSN has an attractive property of partial statelessness, in which a node can decode the current group key, even if the node missed a few previous group re-keying operations. This is an attractive feature as: (1) typically packet losses are high in WSN due to unreliable communication, and (2) the scheme facilitates new nodes joining the network after initial network deployment.

In deterministic schemes, any two intermediate nodes are guaranteed to share one or more pre-distributed keys.

Zhu et al. [9] proposed a deterministic scheme named LEAP. LEAP supports four types of keys for each sensor node: an individual key shared with the sink node, a pairwise key shared with another sensor node, a cluster key shared with multiple neighboring nodes, and a group key that is shared by all the nodes in the network.

B. *Polynomial based Key Distribution Schemes*

The idea of key distribution using polynomial first proposed by Blundo [11], the scheme contains two phases: polynomial pre-distribution phase and session key establishment phase. In pre-distribution phase, any two nodes who want to communicate with each other substitute both the node ID into a polynomial function, by which can get the session key that is used to ensure communication security. According to the Lagrange interpolation, as the number of captured node not more than that the polynomial cannot be restored and the session key between nodes is secure. Consequently, as the value of increased the resilience will be better, but the node needs more storage, which is a complex problem.

Liu et al [12] proposed two improved schemes based on Blundo's scheme, one is polynomial key pool based, and the other is grid based. In the scheme, before network deployment, the deployment server establishes polynomials on the finite field GF (q), and then each node selects polynomials from the pool randomly. After the deployment, if the Neighbor nodes share same polynomial, a pair key will be created directly. According to Lagrange interpolation, it is very difficult to capture so many nodes having the same polynomial, so the scheme has a good resistance.

Kong B. et al proposed a scheme of Polynomial key distribution based on hexagon grid [13]. In the scheme, first, the entire region is divided into t × n equal size of the regular hexagon group of nodes, and in each group the node obeys Gaussian distribution; each group selected |SC| polynomials from the polynomial pool constitute a sub polynomial pool, there is |SC| polynomials same in each sub polynomial pool, in group (1, 1) is certain to 1, but in other group is related to the parity of t. In the key establishment phase, two nodes as long as there is a shared polynomial can establish a session key. This scheme has a better connectivity than the scheme of square grid based, and in the same connectivity the key storage is less and the anti-attack capability is stronger.

C. *Location based Key Pre-Distribution Schemes*

Location based key management schemes can improve networks' connectivity, reduce the key computation and the memory consumption comparing to the basic key distributions. Location based key distribution usually divided the topology into geometric figures like square and hexagon, .etc. using deployment knowledge and other types of Key management schemes. Bellow follows some location based key pre-distributions schemes.

A square based key management scheme [14] was proposed by Wenliang Du. etc. They assume that sensor nodes are static once they are deployed. Keys in pools was shared by sensors in the same grid cell. They show that key pre-distribution with deployment knowledge can substantially improve a network's connectivity and resilience against node capture, and reduce the amount of memory required.

An enhanced scheme using pre-deployment knowledge was proposed by Ngo, etc. [15]. They take advantage of hexagonal grid and expect location information not only to reduce the memory cost but also get better resilience against capture attacks.

Mohammed F.Younis and Mohammed Eltoweissy[16] propose a Location-Aware Combinatorial key management scheme based on Exclusion Based System (EBS). Since it is Scalable, Hierarchical, Efficient, Location-aware and Light-weight, this scheme is termed SHELL. Result demonstrated that the proposed scheme can reduce the potential of collusion among compromised sensor nodes, reduces energy and memory over trading off the number of keys and rekeying messages, reducing the potential of collusion by factoring the geographic location of nodes, eliminates the need of storing a large number of keys at each sensor node, support for addition and expulsion of nodes and thereby performs key refreshing through the exchange of considerably few messages.

Zhen yu and etc. [17] also use deployment knowledge to proposed a key management scheme based on Blom's scheme[10] and compared the key deployment scheme in clusters of triangle, square and hexagon grids.

A novel key pre-distribution scheme based on hexagon deployment model [18] was proposed by Xueli Yan and Xiaohi Ye. This scheme combines bivariate polynomials and node expected deployment knowledge. This scheme has following three phase, key pre-distribution, direct key establishment and indirect key establishment. This scheme eliminates the probability of additional key compromises between non captured sensor nodes, high network connectivity, low communication overhead, and memory requirement.

D. Key Management schemes in Hierarchy Networks

Some key management schemes take advantage of the fact that nodes are often categorized into different types, such as sink nodes, gateway nodes, and sensor nodes, and different types of nodes have different computational resources.

Jolly et al [19] presented a key management scheme in a clustered sensor network. The method uses pre-deployed symmetric keying, in which sensor nodes store a minimum number of keys sharing with other nodes. Gateway nodes store a larger number of keys, and the sink nodes have no restrictions and store all the keys in the network. Simulation showed that the energy consumption for the key management is remarkably low.

Chorzempa et al. [20] proposed another hierarchical key management scheme named SECK. SECK has three tiers of nodes. The bottom tier consists of low-end sensor nodes, which are clustered. Each cluster is managed by a second-tier cluster head to perform data aggregation and forwarding. At the top tier there is a globally trusted sink node. Clusters are used for establishing and updating administrative keys. A session key between a pair of nodes can be obtained from administrative keys. Simulations suggested that the scheme is resilient against multiple node captures, and can efficiently recluster and salvage compromised nodes.

Zhao Huawei et al. [21] proposed a hierarchy cluster model and key management which has two stage of key management, establishment of pairwise key and delivering cluster key. In the hierarchy model, a sensor only establish pairwise keys with its vicinal nodes, and when these pairwise keys are divulged, only the secure communication its vicinal nodes are affected, and other communications between other nodes will not be affected, so the security affection to the whole network is little.

Random key pre-distribution scheme was proposed by Xueli and Xiaohui Ye [22]. In the scheme the whole application area is dividing into number of sub regions and divides the whole sensor nodes into different non overlapping subgroups, in which, the hash function is used to derive the relevant keys to subgroup's sensor nodes. Then subgroup's sensor nodes deployed into sub regions.

IV. Discussion and analysis

The key management schemes commonly use key chains (pools) or calculated polynomials combing with the location or hierarchy information to generate and distribute the keys.

Four kinds of key distribution schemes mentioned above are each has advantages and disadvantages, specific as follows.

In basic key distribution schemes, nodes select several keys from the key pool randomly; nodes can establish communication links only when the intermediate nodes share the same key. This kind of scheme is relatively simple, usually requires very small computational load, but in large networks, nodes need sufficient memory to storage enough keys, otherwise the authentication for the neighbor cannot be supported. Because the key is directly stored by the node, when a certain number of nodes are captured, the keys of the entire network is likely to be revealed.

In polynomial based key pre-distribution schemes, each node stores the polynomial used to produce keys. So nodes need high computational capability and enough storage, which both affect the WSN's life.

In the location based key pre-distribution schemes, nodes are usually static after deployment, neighbor nodes establish secure link using sharing keys from prior key pool or keys generating by polynomial. The network's ability to resist physical attacks will be better. But the addition of extra nodes will be more difficult, and the key updating would cost more. This scheme is suitable for the networks that sensor node’s position can be predicted after the deployment.

In hierarchy networks, nodes in a cluster share same key pool, nodes can communicate within the same cluster, cluster heads can aggregate data from common nodes, and transmit to the base station. This kind of schemes has greater scalability and low calculation.

V. CONCLUSIONS AND FUTURE WORKS

Key management will be surely more and more important in WSNs. Based on the analysis of existing key management schemes, the following seven aspects will be the focuses and research directions.

(1) How to update and revoke the key effectively while the network working will be an important means to improve the resistance and security of WSNs.

(2) As the developing of hardware technology of sensor nodes. The public key technology used in WSNs will be a research hot spot.

(3) According to the actual need, selecting and modifying the existing key management schemes will be an important research direction.

(4) Combination of different key management schemes, such as key pool and hierarchy key distribution, is a new direction of research.

(5) Key management cross the cluster in hierarchy networks and location based network will attract more attentions.

(6) Using different key distribution schemes in a WSN to achieve different security goals, such as nodes’ trust and secure transmission, will be a research spot.

(7) Key update scheme combining with secure routing and transmission will be new research spot.

ACKNOWLEDGMENT

This paper is supported by Foundation of Hubei (No. B20128012).

REFERENCES

[1] Barati A, Dehghan M, Barati H, et al. Key management mechanisms inwireless sensor network. Proceeding of the 2nd International Conference on Sensor Technologies and Applications. Cap Esterel, 2008: 81-86.

[2] Boyle D, Newe T, et al. Security Protocols for use with wireless sensor networks. Proceedings of the 3th International Conference on Wireless and Mobile Communications, Guadeloupe, 2007: 123-127.

[3] Cannan D W, Kruus P S, Matt B T. “Constraints and Approaches for Distributed Sensor Network Security”, NAI Technical Report, 2000, pp: 00-010.

[4] Weiming Tong,et al. A Suervey on Key Pre-distribution Scheme of Distribtuted WNS. Third International Conference on Instrumentation, Measurement, Computer, Communication and Control,2013.

[5] J. Jeong, Z.J. Haas, Predeployed secure key distribution mechanism in sensor networks: current state-of-the-art and a new approach using time information. IEEE Wirel. Commun. 42–51 (2008)

[6] L. Eschenauer et al.,Akey-management scheme for distributed sensor networks, in *Proceedings of Conference on Computer and Communications Security* (2002), pp. 41–47

[7] H. Chan et al., Random key predistribution schemes for sensor networks, in *Proceedings of IEEE Symposium Security Privacy* (2003), pp. 197–203

[8] S. Zhu,W. Zhang, Group key management in sensor networks, in *Security in Sensor Networks*, ed. by Y. Xiao (Auerbach Publications, Boca Raton, 2007)

[9] S. Zhu et al., LEAP: efficient security mechanisms for large-scale distributed sensor networks, in *Proceedings of 10th ACM Conference on Computer and Communications Security* (2003),

[10] R. Blom, An optimal class of symmetric key generation systems, advances in cryptology, in *Proceedings of EUROCRYPT84*, LNCS, Vol. 209 (1984), pp. 335–338

[11] lundo C, De Santis A, Herzberg A, et al. Perfectly-secure key distribution for dynamic conferences[C]. Advances in cryptologyCRYPTO’92. Berlin Heidelberg, 1993: 471-486.

[12] Liu D, Ning P. Establishing pairwise keys in distributed sensor networks[C]. Proceedings of the 10th ACM conference on Computer and communications security. New York, 2003: 52-61.

[13] Kong B, Chen H, Tang X, et al. Key pre-distribution schemes for largescale wireless sensor networks using hexagon partition[C]. Wireless Communications and Networking Conference (WCNC), Sydney, 2010:1-5.

[14] Du, J Deng, Y S Han, P K Varshney. A key management scheme for wireless sensor networks using deployment knowledge[C]. In IEEE Infocom, 2004

[15] Ngo Trong Canh,etc,Enhanced Group-Based Key Management Scheme for Wireless Sensor Networks using Deployment Knowledge,Consumer Communications and Networking Conference, 2009. CCNC 2009. 6th IEEE

[16] Mohamed F.Younis, Kajaldeep Ghumman and Mohamed Eltoweissy, "Location-aware combinatorial key management scheme for c1ustered sensor networks", IEEE Journals on parallel and distributed systems, vo1.17, issue.8, 2008.

[17] Zhen Yu, a key management scheme using deployment knowledge for wireless sensor networks,IEEE Transactions on parallel and distributed systems.VOL.19,NO.10,octorber 2008.

[18] Xueli Yan and Xiaohui Ye, "A novel key predistribution scheme for wireless sensor networks based on hexagon deployment model", In proceedings of ELSEVIER 2011.pp.8018-8026.

[19] G. Jolly et al.,A low-energy keymanagement protocol for wireless sensor networks, in *Proceedings of 8th International Symposium Computers and Communications (ISCC)*, Vol. 1 (2003), pp. 335–340

[20] M. Chorzempa et al., SECK: Survivable and efficient clustered keying for wireless sensor networks, in *Proceedings of IEEE Workshop on Information Assurance in Wireless Sensor Networks*(Phoenix, 2005), pp. 453–458

[21] Zhao Huawei, Hiberarchy Cluster Model and Key Management in Wireless Senosr Network,Wireless Communications, Networking and Mobile Computing, 2009.

[22] Xueli Yan and Xiaohui Ye, " A random key redistribution scheme for wireless sensor networks based on region security level", in the proceedings of ELESEVIER 2011, pp.9741-9749

[23] Habib M. Ammari,”The Art of Wireless Sensor Networks”, Volume 1: Fundamentals, Springer,2013.pp.578-582