Survey on Key Pre Distribution for Security in Wireless Sensor Networks

T.P. Rani[1] and C. Jaya Kumar[2]

[1] Faculty, Department of Information Technology, Sri Sairam Engineering College
Sai Leo nagar, west Tambaram Chennai-44
ranitp.2010@gmail.com
[2] Faculty, Department of Computer Science and Engineering, R.M.K. Engineering College
Kavarapettai, Chennai
Cjayakumar2007@gmail.com

Abstract. Wireless sensor networks (WSNs) consists of small nodes with constrained capabilities to sense, collect, and disseminate information in many types of applications. As sensor networks become wide-spread, security issues become a central concern. In this paper, we identify the Security requirements of key management in WSN. The secure management of the keys is one of the most critical elements when integrating cryptographic functions into a system. An outline of hybrid cryptography, one way hash and Key infection schemes are discussed in this paper. Along the way we analyze the advantages and disadvantages of current secure schemes. Finally, we aim to provide efficient key management operations for secure communications in WSN.

Keywords: Security, Key management, Wireless Sensor Networks.

1 Inroduction

Sensors are inexpensive, low-power devices which have limited resources [1]-[2]. They are small in size, and have wireless Communication capability within short distances. A sensor node typically contains a power unit, a sensing unit, a processing unit, a storage unit, and a wireless transmitter / receiver. A wireless sensor network (WSN) is composed of large number of sensor nodes with limited power, computation, storage and communication capabilities. In recent years, major advances have been made in the development of low-power micro sensor nodes. The emergence of such sensor nodes has allowed practitioners to envision networking a large set of nodes scattered over a wide area of interest into a wireless sensor networks (WSNs) [1] for Large-scale event monitoring and data collection and filtering. So when WSNs are deployed in a hostile management plays a central role in data encryption and authentication. The prime problem in key management is to establish the secure keys between the sensor nodes. This problem is known as the key agreement problem.

Key agreement protocol of WSNs includes three types in the existing schemes: trusted server, public key, and key predistribution.

N. Meghanathan et al. (Eds.): CCSIT 2012, Part I, LNICST 84, pp. 248–252, 2012.

1) Third Party Trusted Server protocols depend on a trusted server (also called a base station) for key agreement between the sensor nodes.

2) Public-key Cryptography requires a public-key infrastructure that would impose additional computational costs as well as increased storage requirements. However, the limited computational and communication resources of nodes make it infeasible to use public-key protocols in WSN.

3) Key pre-distribution: The third strategy to establish the secret keys is key predistribution, where keys are distributed to all sensor nodes prior to deployment. Such schemes are proved to be most appropriate for WSNs

2 Key Management

The Sensor nodes cannot practically use a third party trusted server because of the high communication cost and deployment cost. The Public Key protocols involve high computation cost. Hence the Symmetric Key Cryptography involving is considered to be the better method of cryptography system in WSN. Sensor network dynamic structure, easy node compromise and self organization property increase the difficulty of key management and bring a broad research issues in this area. Due to the importance and difficulty of key management in WSNs, there are a large number of approaches focused on this area. Based on the main technique that these proposals used or the special structure of WSNs, we classify the current proposals as key predistribution schemes, hybrid cryptography schemes, one way hash schemes, key infection schemes, and key management in hierarchy networks, though some schemes combine several techniques.

A. KEY PRE-DISTRIBUTION SCHEMES

In the key predistribution schemes, sensor nodes store some initial keys before they are deployed. After deployed, the sensor nodes can use the initial keys to setup secure communication. This method can ease key management especially for sensor nodes that have limited resource.

Two types of key predistribution schemes suited for WSNs have been developed: random key predistribution and deterministic key predistribution.

1) Random Key Predistribution

According to this scheme, each sensor node receives a different random subset of keys from a large key pool as the node’s key ring before deployment and then stores the key ring in its memory [3]-[5]. After sensor nodes have been deployed in the designated area, secure direct communication between two nodes requires that they share at least one common key.

2) Deterministic Key Predistribution

Combinatorial designs [6]-[9] are applied to key predistribution. They presented two classes of combinatorial designs. The combinatorial designs are associated with the distinct key identifiers and nodes, respectively. Though the probability of key establishment has been increased, this scheme is limited in network resiliency and network size.

B.HYBRID CRYPTOGRAPHY SCHEMES

Though most framework use one type of cryptography, there still exist some schemes that use both asymmetric-key and symmetric-key cryptographs. For example, a hybrid scheme proposed by Huang[11], balances public key cryptography computations in the base station side and symmetric key cryptography computation in sensors side in order to obtain adorable system performance and facilitate key management. On one hand, they reduce the computation intensive elliptic curve scalar multiplication of a random point at the sensor side, and use symmetric key cryptographic operations instead On the other hand; it authenticates the two identities based on elliptic curve implicit certificates, solving the key distribution and storage problems, which are typical bottlenecks in pure symmetric-key based protocols.

C. ONE WAY HASH SCHEMES

To ease key management, many approaches use the one-way key method that comes from one-way hash function technique. For example, Zachary[12] propose a group security mechanism based on one-way accumulators that utilizes a pre-deployment process, quasicommutative property of one-way accumulators and broadcast communication to maintain the secrecy of the group membership. Another group security mechanism proposed by Dutta, also use one-way function to ease group node joining or revocation. Their scheme has self-healing feature, a good property that makes the qualified users recover lost session keys over a lossy mobile network on their own from the broadcast packets and some private information, without requesting additional transmission from the group manager. The one-way hash function can also adapt to conduct public key authentication. To ease the joining and revocation issues of membership in broadcast or group encryption, many approaches use predistribution and/or a local collaboration technique.

D.KEY INFECTION SCHEME

Contrary to most of key management using pre-loaded initial keys, Anderson[13], propose a key infection mechanism. In a key infection scheme, different from key pre-distribution schemes, no predistribution key is stored in sensor nodes. This type of schemes establishes secure link keys by broadcasting plaintext information first. This type of schemes is not secure essentially. However, Anderson, show that their key infection scheme is still secure enough for non- critical commodity sensor networks after identifying a more realistic attacker model that is applicable to these sensor networks. Their protocol is based on the assumption that the number of adversary devices in the network at the time of key establishment is very small.

E. KEY MANAGEMENT IN HIERARCHY NETWORKS

In this type of key management, some use the physical hierarchical structure of networks, while others implement their hierarchy key management logically in physical flat structure sensor networks[14], which only include a base station and sensors. For example, LKHW (Logical Key Hierarchy for Wireless sensor networks), proposed by Pietro [16]-[18], integrates directed diffusion and LKH (Logical Key Hierarchy) where keys are logically distributed in a tree rooted at the key distribution center

(KDC). A key distribution center maintains a key tree that will be used for group key updates and distribution, and every sensor only stores its keys on its key path, i.e. the path from the leaf node up to the root. In order to efficiently achieve confidential and authentication, they apply LKHW: directed diffusion sources are treated as multicast group members, whereas the sink is treated as the KDC.

3 Conclusion

Thus, we provide features of various key management schemes for establishing secure communication in a wireless sensor network .Security can be accomplished by adapting the type of Key Management based on the environment of WSN. In this paper, efficient cryptographic techniques have been proposed which ensures confidentiality, authenticity, availability and integrity of wireless sensor network that are deployed in hostile environment. Since key management plays a major role in encryption and authentication various schemes have been summarized by us. We have presented a nearly comprehensive survey of security researches in wireless sensor networks.

References

[1] Akyildiz, I., Su, W., Sankarasubramaniam, Y., Cayirci, E.: A survey on sensor networks. IEEE Commun. Mag. 40(8), 102–114 (2002)

[2] Perrig, A., Szewczyk, R., Wen, V., Culler, D., Tygar, J.D.: SPINS: Security protocols for sensor networks. Wireless Netw. 8(5), 521–534 (2002)

[3] Eschenauer, L., Gligor, V.D.: A key-management scheme for distributed sensor networks. In: Proc. 9th ACM Conf. Comput. Commun. Secur., New York, USA, pp. 41–47 (2002)

[4] Chan, H.W., Perrig, A., Song, D.: Key distribution techniques for sensor networks. Wireless Sensor Networks (2004)

[5] Chan, H.W., Perrig, A., Song, D.: Random key predistribution schemes for sensor networks. In: Proc. IEEE Symp. Res. Secur. Privacy, pp. 197–213 (2003)

[6] Du, W., Deng, J., Han, Y.S., Varshney, P.K., Katz, J., Khalili, A.: A pairwise key predistribution scheme for wireless sensor networks. ACM Trans. Inf. Syst. Secur. 8(2), 228–258 (2005)

[7] Blom, R.: An optimal class of symmetric key generation systems. In: Proc. EURORYPT 1984 Workshop Adv. Cryptol.: Theory Appl. Cryptographic Tech., pp. 335–338 (1985)

[8] Liu, D.G., Ning, P., Li, R.F.: Establishing pairwise keys in distributed sensor net-works. ACM Trans. Inf. Syst. Secur. 8(1), 41–77 (2005)

[9] Çamtepe, S.A., Yener, B.: Combinatorial Design of Key Distribution Mechanisms for Wireless Sensor Network. In: Samarati, P., Ryan, P.Y.A., Gollmann, D., Molva, R. (eds.) ESORICS 2004. LNCS, vol. 3193, pp. 293–308. Springer, Heidelberg (2004)

[10] Chakrabarti, D., Maitra, S., Roy, B.: A Key Predistribution Scheme for Wireless Sensor Networks: Merging Blocks in Combinatorial Design. In: Zhou, J., López, J., Deng, R.H., Bao, F. (eds.) ISC 2005. LNCS, vol. 3650, pp. 89–103. Springer, Heidelberg (2005)

[11] Huang, Q., Cukier, J., Kobayashi, H., Liu, B., Zhang, J.: Fast authenticated key establishment protocols for self-organizing sensor networks. In: Proc. 2nd ACM International Conf. Wireless Sensor Networks Applications, pp. 141–150 (2003)

[12] Zachary, J.: A decentralized approach to secure group membership testing in distributed sensor networks. In: Proc. IEEE Military Commun. Conf. (2003)

[13] Anderson, R., Chan, H., Perrig, A.: Key infection: Smart trust for smart dust. In: Proc. 12th IEEE International Conf. Network Protocols (ICNP) (2004)

[14] Eltoweissy, M., Younis, M., Ghumman, K.: Lightweight key management for wireless sensor networks. In: Proc. IEEE International Conf. Performance, Computing, Commun., pp. 813–818 (2004)

[15] Shi, E., Perrig, A.: Designing secure sensor networks. IEEE Commun. Mag. 11, 38–43 (2004)

[16] Djenouri, D., Khelladi, L., Badache, N.: A survey of security issues in mobile ad hoc and sensor networks. IEEE Commun. Surveys Tutorials 7, 2–28 (2005)

[17] Wang, Y., Attebury, G., Ramamurthy, B.: A survey of security issues in wireless sen-sor networks. IEEE Commun. Surveys Tutorials 8, 2–23 (2006)

[18] Carman, D.W., Kruus, P.S., Matt, B.J.: Constraints and approaches for distributed sensor network security, NAI Labs Technical Report (2000)