ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 5, May 2012

A Survey on Key Management Issues in WSN

Tahira Laskar, Debasish Jena

Abstract: - Wireless sensor networks (WSN) with low cost, low energy consumption and high utilization are becoming practically feasible through recent advances in wireless communication and microelectronics. The security concerns of the sensor nodes becomes a challenging issue since the nodes are often placed in hostile or adverse environment. Key Management is a critical security service for communication in WSNs. The key management system should be substantially secure, robust and efficient for a secure communication protocol. Many key establishment techniques have come up to address the tradeoffs between limited memory and security but choosing an effective scheme is debatable. In this paper, we provide a survey of various key management schemes in WSNs. choosing a key management scheme depends upon the target applications requirements and the resource of the sensor network.

***Index Terms*: Asymmetric cryptography, Confidentiality, Key Management, Wireless Sensor Network.**

I. INTRODUCTION

Wireless sensor networks (WSN) consist of a large collection of sensor nodes with each node equipped with sensors, processors and radio transceiver. Large number of sensor nodes can be deployed in a variety of situations capable of performing both military and civilian tasks owing to their low cost. Key Management is a security aspect that gets a great deal of attention in Wireless sensor networks. Key Management establishes the keys that are required for providing confidentiality, integrity and authentication requirements. Key Management establishes secure connection between nodes at network formation stage, ensures that messages are encrypted and communicating nodes are authenticated. Asymmetric cryptography is not suitable for most sensor networks because of increased energy consumption and large code computation and storage requirements. Hence several alternative approaches have come up for performing key management in wireless sensor networks.

II. NEED FOR KEY MANAGEMENT

Key Management in WSN is an important research area. It provides very critical security service in wireless sensor networks. It provides the crucial security of authentication and confidentiality. But implementation of Key Management schemes in WSN is a difficult task because of the vulnerabilities of the sensor nodes and their resource limitations. Key management is the process by which cryptographic keys are generated, stored, protected, transferred, loaded, used, and destroyed[1].

Key pre-distribution phase is an important starting phase where keys are distributed before the deployment of the network, i.e. during the node's manufacturing time. This is followed by the key establishment phase which refers to how nodes will establish a secure session. The network formation phase is then initiated. Node addition or Node deletion phase deals with establishment of secure sessions with new nodes being added or removed from the network.

Authenticity, confidentiality, scalability, integrity and flexibility must be provided in a secure application through various key establishment techniques [2].

Authenticity: The communicating node should have a method of verifying the authenticity of the node with which it is communicating through the key establishment techniques.

Confidentiality: An adversary may try to access the network if it manages to obtain the secret keys to obtain the data. Confidentiality refers to the ability to protect the disclosure of data from unauthorised access. Key establishment techniques should provide confidentiality and in case of a node being compromised, it tries to keep the data from being further known.

Scalability: Key establishment techniques should provide high-security features not only for small networks but also for network of large size. Key establishment techniques if scalable can support variations in the size of the network.

Integrity: Access to the keys should be available only to the nodes within the network and only the authenticated base station should be allowed to change keys. This would stop unintended nodes from obtaining knowledge about the secret keys or from trying to change it.

III. SOME EXISTING KEY MANAGEMENT SCHEMES:

A. Random Key Pre-Distribution Scheme --- Eschenauer and Gligor

Eschenauer and Gligor [3] proposed a random key predistribution scheme based on probabilistic key sharing among the nodes of random graph. Distribution of keys consists of three phases: key pre-distribution, shared-key discovery, and path key establishment. Nodes randomly chose keys from key pool during the key pre-distribution phase. The sensor nodes then trace the keys that are shared with its neighbors within its range of transmission. Upon deployment, every sensor node can only communicate with those sensor nodes with which it shares a secret key [10].In case of nodes not sharing keys, they will establish a shared key through more links in path key establishment phase. In case of nodes being compromised, the shared key will be removed from other key rings and the key ring will be revoked. This causes weakening of link connectivity of the

ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 5, May 2012

network and it becomes the duty of the affected node to reconfigure the connections. This scheme has the advantage that less than N-1 keys are to be stored, where N is the total number of nodes in the network. The scheme also makes it feasible for the network to be scalable since the size of the key ring and the number of keys in the ring is not fixed but can be adjusted. This scheme has the disadvantage that it does not have the authentication process and there is no method for refreshing the keys. Also, some nodes may become unreachable since there is no guarantee that every node will have common keys with all its neighbors. Eschenauer and Gligor [3] stated that with a pool size S = 1000 keys, to have 50% probability of sharing keys with the key rings, 75 keys must be kept in the node's memory. If the pool size is increased by ten times, i.e., S = 100,000, then nodes need to store only 250 keys. Hence this scheme is flexible and can also be used for large networks [2].

B. Q-Composite Random Key Pre-distribution scheme -- Chan, Perrig and Song

This scheme [4] does not need to establish pair-wise key between every pair of nodes in a sensor network for a secure key management scheme for the wireless sensor networks. Communicating nodes should share at least Q number of keys. Thus in case of a key compromise, the nodes can communicate with the other keys. The value Q should be so selected such that the network maintains a certain desired level of connectivity. The size of the random key pool is reduced but this gives an advantage to the adversary. Only a few nodes need to be compromised to compromise the entire network.

C. Leap — Zhu, Setia, and Jajordia In 2003

Zhu, Setia, and Jajordia introduced the localized encryption and authentication protocol (LEAP) [5] that offers different types of data switching schemes for nodes with different security requirements. It's based on symmetric key algorithms. It offers varied services like network-wide, cluster/group, and pairwise keying capabilities. This is possible due to the fact that LEAP offers four distinct types of keys namely: (i) an individual key shared with the base station (pre-distributed), (ii) a group of key shared by all the nodes in the network (pre-distributed), (iii) pair-wise key shared with immediate neighbour nodes, and (iv) a cluster key shared with multiple neighbour nodes. A pre-distribution key is used by LEAP to help establish the four types of keys. The broadcast authentication of the sink node is done by an authentication mechanism known as µTimed Efficient Streaming Loss-tolerant Authentication Protocol, µ-TESLA [6]. The source packets are authenticated by using one-way hash-key mechanism. LEAP protocol is suitable for nodes which does not have very high security requirements. It cannot guarantee to avoid DOS attacks in case of nodes with very high security requirements.

D. Leap + :-- Zhu, Setia, and Jajordia In 2006

Zhu, Setia, and Jajordia [7] further came up with LEAP+ in 2006 which is not targeting any specific type of sensor network but almost equally applicable to all class of static network. Every node in the sensor network maintains four types of keys according to this scheme. Every node establishes keys with all its neighbors after deployment. Of the four keys, one of the key is shared with the base station, another key is shared with all its neighbors for broadcast reasons. A single network-wide key is used for broadcasting in the entire network. The neighboring nodes of a compromised sensor node remove the pair-wise key shared with the compromised node. The group keys are then refreshed followed by the refreshing of the network-wide key. LEAP+ is not suitable for dynamic network since the energy consumption overhead in establishing communicating links is high.

E. Shell — Younis, Ghumman, and Eltoweissy

The Scalable, Hierarchical, Efficient, Location aware, and Light-weight (SHELL) protocol [8] is a complicated key management scheme for large scale clustered sensor network. Multiple types of keys are used and also a new distributed key management entity is being presented. The role of distributed key management is handled by a non cluster head node thus separating the operational responsibility from key management responsibility. This increases the resilience of the network. There are multiple different entities and over seven types of keys. For the purpose of key management, SHELL involves multiple cluster heads of nearby clusters and makes use of EBS matrix[9]. EBS matrix maintains global information about keys stored on every node. Out of a total of k+m keys, the nodes in the network are aware of a distinct set of k keys. In case of a node being compromised, the m keys not known to the compromised node are used to refresh its k compromised keys to evict the compromised node. In SHELL, cluster head node of a cluster generates the EBS matrix, breaks it up into different parts and sends those parts to its neighbouring cluster head nodes. Neighbouring cluster head nodes manage keys for the cluster. The EBS matrix is divided in such a way that the compromise of a neighbouring cluster head node does not compromise too many keys. On a cluster head's request, neighbouring cluster heads generate keys and refresh them. However, the cluster head node does not get to know the actual key values [10].

F. Polynomial based key pre-distribution scheme

Blundo et al. [11] distributes a polynomial share (a partially evaluated polynomial) to each sensor node using which every pair of nodes can generate a link key. Symmetric polynomial P(x, y) (P(x, y) = P(y, x)) of degree, d is used. The coefficients of the polynomial come from GF(q) for sufficiently large prime q. Each sensor node stores a polynomial with d+ 1 coefficients which come from GF(q). Sensor node Si receives its polynomial share of $f_i(y) = P(i, y)$. S_i (resp. S_j) can obtain link key $K_{i,j} = P(i, j)$ by evaluating its

ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 5, May 2012

polynomial share $f_i(y)$ (resp. $f_j(y)$) at point j (resp. i). Every pair of sensor nodes can establish a key. The solution is d-secure, meaning that coalition of less than d+1 sensor nodes knows nothing about pair-wise keys of others [12]. Polynomial pool-based key pre-distribution scheme by Liu et al. [13] considers the fact that not all pairs of sensor nodes have to establish a key. It combines Polynomial based key pre-distribution scheme by Blundo et al. [11] with the key-pool idea in [[3], [4]] to improve resilience and scalability [12].

G. Panja, Madria, and Bhargava

Panja *et al.* [14] described group key management protocol for hierarchical sensor networks consisting of different groups, each with unique key. The sensor nodes in a group don't use pre-deployed keys but dynamically generate partial keys using a function that takes partial keys of its children as input. The partial keys in a group are used for computing the group key in a bottom up fashion. Groups of sensors at different levels are secured by using multiple level securities. The group key management protocol supports the establishment of two types of group keys: intra-cluster and inter-cluster. Intra-cluster group keys are used for encryption/decryption of messages for the sensor nodes within a group while Inter-cluster group keys are used within groups of cluster heads. The protocol handles freshness of the group key dynamically, and eliminates the involvement of a trusted third party (TTP). Panja *et al.* [14] introduced Tree-based Group Diffie-Hellman (TGDH) protocol which is a hierarchical group keying scheme. Each key in this scheme is made up of many partial keys. By breaking up the keys into smaller components, it makes rekeying an efficient and simple task by revoking, changing, or adding one or more partial key(s).[10] The hierarchical sensor node architecture consists of multiple levels consisting of sensor nodes, cluster heads and relay nodes. The data collection starts from a sensor node within a particular geographical area which then sends it to the nearest sensor node. If the receiving nodes are relay nodes, they further forward the data using appropriate routing path. The cluster head aggregates the data coming from different sensor nodes within its group and forwards it to the next higher level of cluster heads. This process is repeated until the data reaches the sink node.

IV. ANALYSIS

Eschenauer and Gligor's [3] scheme is simple and scalable and also offers flexibility and efficiency. This scheme has less storage requirements but it fails in situations requiring very high security. The Q-composite scheme [4] renders good security in case of small scale attacks but the reduced key pool size poses an adversary problem. LEAP [5] offers scalability and uses µ-TESLA for broadcast authentication. LEAP scheme can fight back many types of attacks on the network but the storage requirements are high with the four types of keys needing to be stored. LEAP+ [7] scheme offers high scalability, simplicity and resistance to collusion attacks and can be used for both clustered and homogenous wireless sensor network. But with extended features compared to LEAP, LEAP+ [7] has the drawback of having high computation overhead. SHELL protocol [8] offers high robustness against node capture by avoiding a single point failure having no such nodes whose compromise can lead to the compromise of the entire network. SHELL protocol [8] supports large scale cluster communication but its structure and operations are highly complex requiring many types of keys. Polynomial based key pre-distribution scheme [11] and Polynomial pool-based key pre-distribution scheme [13] improves the resilience and scalability of the network [12] with the security of the solution being proportional to the degree of the polynomial. The group key management protocol by Panja *et al.* [14] offers high scalability and flexibility with less storage and computation cost. But this scheme fails to guarantee a highly robust network unlike SHELL protocol.

V. CONCLUSION

Many researchers have worked on Key management for Wireless Sensor Networks (WSNs) which is a very critical issue from the security point of view. In this paper, we have presented an overview of some the schemes presented in various papers. The choice of deciding on a particular key management scheme should be based the requirements of that particular application. There are immense research opportunities in the field of key management in wireless sensor network. Further study on the security aspects of key management in WSNs will make the wireless sensor networks immensely useful in various aspects of life.

REFERENCES

[1] Lee, Victor C., M. Leung, Kirk H. Wong, Jiannog Cao, and Henry C. B. han(2007): "Key Management Issues In Wireless Sensor Networks: Current Proposals And Future Developments", Proceedings of IEEE Wireless Communications, p.p. 76-84.

[2] Yang Xiao, Venkata Krishna Rayi, Bo Sun, Xiaojiang Du, Fei Hu, and Michael Galloway "A Survey of Key Management Schemes in Wireless Sensor Networks"

[3] L. Eschenauer and V. D. Gligor, "A Key-Management Scheme for Distributed Sensor Networks," Proc. 9th ACM Conf. Comp. and Commun. Sec., 2002, pp. 41–47..

[4] Chan, H., Perrig, A., and Song, D. 2003. Random Key Predistribution Schemes for Sensor Networks. In Proceedings of the 2003 IEEE Symposium on Security and Privacy (May 11 - 14, 2003). SP. IEEE Computer Society, Washington, DC, 197-213.

[5] S. Zhu, S. Setia, and S. Jajodia, "LEAP: Efficient Security Mechanisms for Large-Scale Distributed Sensor Networks," Proc. 10th ACM Conf. Comp. and Commun. Sec., 2003, pp. 62–72.

[6] A. Perrig et al., "SPINS: Security Protocols for Sensor Networks," Wireless Network, vol. 8, 2002, pp. 521–34.

ISSN: 2277-3754
International Journal of Engineering and Innovative Technology (IJEIT)
Volume 1, Issue 5, May 2012

[7] Zhu, S., Setia, S., and Jajodia, S. 2006. LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. ACM Trans. Sen. Netw

[8] M. F. Younis, K. Ghumman, and M. Eltoweissy, "Location-Aware Combinatorial Key Management Scheme for Clustered Sensor Networks," IEEE Trans. Parallel and Distrib. Sys, vol. 17, 2006, pp. 865–82.

[9] Eltoweissy, M., Heydari, M. H., Morales, L., and Sudborough, I. H. 2004. Combinatorial optimization of group key management. J. Netw. Syst. Manage

[10] .Syed Muhammad Khaliq-ur-Rahman Raazi and Sung young Lee: "A Survey on Key Management Strategies for Di®erent Applications of Wireless Sensor Networks"

[11] Blundo, C., Santis, A., Herzberg, A., Kutten, S., Vaccaro, U., and Yung, M. 1992. Perfectly-secure key distribution for dynamic conferences. In Crypto 92.

[12] SEYIT A. C¸AMTEPE and B¨ ULENT YENER: Key Distribution Mechanisms for Wireless Sensor Networks: a Survey

[13] Liu, D. and Ning, P. 2003b. Establishing pairwise keys in distributed sensor networks. In 10th ACM conference on Computer and communications security CCS'03.

[14] B. Panja, S. K. Madria, and B. Bhargava, "Energy and Communication Efficient Group Key Management Protocol for Hierarchical Sensor Networks," SUTC '06: Proc. IEEE Int'l. Conf. Sensor Networks, Ubiquitous, and Trustworthy Comp., 2006, pp. 384–93.

AUTHOR BIOGRAPHY

Debasish Jena received the B.E degree in 1990 from Gulbarga University, the M.Tech degree in 2002 from Osmania University at Hyderabad and the Ph.D degree in 2010 from National Institute of Technology, Rourkela, India. His current research interest includes Information Security. E-mail: dr.djena@gmail.com

Tahira Laskar received her B.E degree (Computer Science Engineering) in 1998 from National Institute of Technology, Silchar, Assam, India. Currently she is pursuing her M.Tech degree from Department of CSE, IIIT Bhubaneswar, Odisha, India. Her area of research is Security in Wireless Sensor Networks.
E-mail: a110022@iiit-bh.ac.in