Research Journal of Recent Sciences ISSN 2277-2502
Vol. **2(ISC-2012),** 158-161 **(2013)** *Res.J.Recent.Sci.*

Self-Healing Sensor Network Key Distribution Scheme for Secure Communication

Patel Jay Kumar Shantilal
Computer Science Department, Kadi Sarva VishwaVidyalaya, Gandhinagar, Gujarat, INDIA

Available online at: www.isca.in
Received 12th October 2012, revised 2012, accepted 2012

Abstract

Wireless sensor network (WSN) consists of a large number of small, low cost sensor nodes which have limited computing and energy resources. As the wireless medium is characterized by its lousy nature, reliable communication is difficult to assume in the key distribution schemes. Therefore, self-healing is a good property for key distribution in wireless applications. How to establish secure session keys is one of the central tasks for wireless sensor network communications. General Key distribution schemes for traditional computer networks could not be directly shifted to wireless sensor network environments. A self-healing key distribution scheme enables a large group of sensor nodes to establish a session key dynamically over an unreliable, or lousy wireless network. The main idea of self-healing key distribution scheme is that users are capable to recover lost session keys on their own, without requesting additional transmission from the group manager that saves the additional communication cost over the network and reduces the network traffic, even if during a certain session some broadcast messages are lost due to network faults.

Keywords: Self healing, Key distribution, secure communication.

Introduction

Self-organization, self-configuration and self-healing enable flexible integration, quick deployment, easy maintenance, low costs, high scalability, and reliable services[1]. Security of such a network has always been an issue[1]. The fundamental concept of self-healing key distribution scheme is to provide the session key to each member of the group; the group manager (GM) is responsible to broadcast a packet containing session key information when the session starts[2]. The register group members compute the session key by using a packet that is broadcasted by the group manager and some private information. The group manager has ability to dynamically register the group members[2]. The group manager periodically adds or removes the member from the group.

The main property of self-healing key distribution scheme is that users are capable to recover lost session keys on their own, without requesting additional transmission from the group manager[3]. That saves the additional communication cost over the network and reduces the network traffic. The only requirement to recover the lost keys through self healing is that, its membership requires in the group both before and after the sessions in which the broadcast packet containing the key is sent[3]. Self-healing approach of key distribution is stateless in the sense that a user who has been off-line for some period is able to recover the lost session keys immediately after coming back on-line.

Self Healing Sensor Network Framework: Self-healing sensor network frame work[4] is mention in above figure 1. In self healing frame work various Self Healing policies implemented using self healing engine. Self Healing Engine is responsible to provide an environment to implement specific policy. Sensing Driver enables the sensor device to sense and retort the event occurred. MAC-Message Authentication Code ensure authentication during communications. Sensing phase sense the event with the help of sensing driver. Routing specifies the specific route for the message passing with the help of routing table along with routing algorithms principles. Middleware provides the services to integrate these various phases to the specific application for which the sensor network built up.

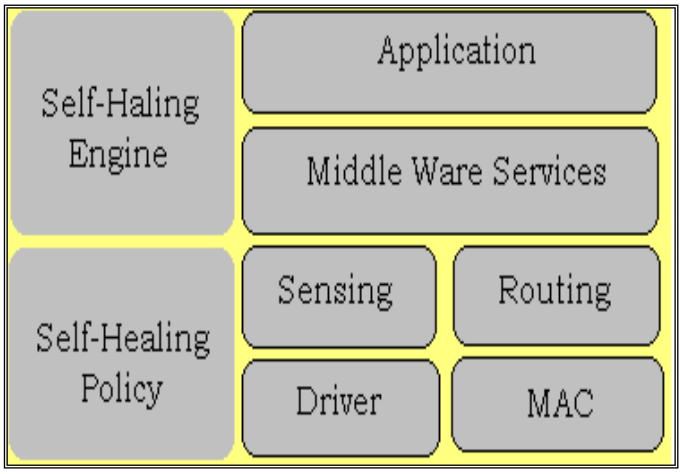

Figure-1
Self-healing Sensor Network Framework

Self Healing Routing: Self Healing multi-hop routing has three roles: i. to pass a packet towards the destination, ii. to

synchronize its recipients and iii. to signal to previous sender that their transmission was successful.

In Self Healing Routing, nodes do not maintain knowledge of neighbors' states to make routing decisions. Instead, packets are freely broadcast to all neighbors and they autonomously decide whether to forward packets further toward a destination based on some cost metric. *Cost Matrix* consists following entries:

Identity: It specifies the identity of a target node which may be either a source or destination.

Sequence number: It specifies the sequence number of the last packet observed from the target node.

Hop distance: It specifies the hop distance from the target to the current node.

Research Methodology

Mutual healing: The self-healing key distribution mechanism addressed the fixed-number of broadcast messages loss. In other words, a node could not recover its new session keys if a node has missed more than fixed number broadcast messages. The mutual-healing key distribution scheme can enable a node in a wireless sensor network to recover its new session key although its last broadcast message was lost[5, 6]. The mutual-healing key distribution scheme is based on bilinear pairings[6]. The scheme is collusion-free for any alliance of non-authorized nodes. Each node's private key has nothing to do with the number of revoked nodes and can be reused as long as it is not disclosed.

Secrecy: Self-healing sensor network has two unique characteristics define with term secrecy. Secrecy divides in to two parts called forward secrecy and backward secrecy.

Forward secrecy[3,7,8]: preventing nodes from decrypting any secret messages after they left the network.

Backward secrecy[3,7,8]: preventing joining nodes from decrypting any previously transmitted secret message.

Encryption and Authentication: The distinguished characteristics of Wireless Sensor Networks compared to traditional networks such as wireless Ad Hoc networks make the security threats in Wireless Sensor Networks different from other networks. So the security research in Wireless Sensor Networks is more complicated and difficult. In order to ensure the security of Wireless Sensor Networks, we must make the communication safe among sensor nodes. Node-to-node secure communication service is necessary by key mechanism on the basis of data encryption and authentication. Thereby, encryption and authentication algorithms place the groundwork of achieving security issues. Because of the resource constraint in Wireless Sensor Networks, traditional key management schemes based on the third trusted part like Key Distribution Center and Asymmetric Key Cryptography are not suitable for Wireless Sensor Networks. The common perception of Asymmetric Key Cryptography is that it is complex, slow and power hungry, and as such not at all suitable for use in ultra-low power environments like wireless sensor networks. Currently, key management scheme is a hot spot in Wireless Sensor Networks security research and the study of key management pays more attention on the random key pre-distribution schemes based on symmetric key cryptosystems. However, they have some unsolved problems such as the shortcomings of connectivity and flexibility. Specifically, for example, there are remote sensors that cannot be connected to any other nodes in Wireless Sensor Networks and there are many useless pre-distribution key materials in nodes' memory. Also, many key materials may be disclosed after sensors being compromised by attackers. Besides, revocation of compromised nodes and key update tend to be overlooked in a lot of schemes. Key distribution policy works to solve all these problems.

Self-healing Key Distribution Policy: Key distribution policy[9] focuses on the research of three steps involving Key establishment for sensor-to-sensor key establishment. Key revocation of pair wise key after sensor nodes' distribution and compromised nodes revocation. And Key update during maintenance period. Besides, the distributed management strategy in cluster-based wireless sensor networks ensures that the communication overhead of the base station cannot increase extremely because of the key revocation scheme[10].

Key establishment: For sensor-to-sensor key establishment, a shared key is established by two communication nodes to protect communications. Thus, all sensed data transmitted between participants could be verified and protected even if an attacker eavesdrops on the communications between nodes or injects illegal sensed data into networks; this requirement still provides an adequate level of security.

Key revocation: When the back-end system or the manager node decides to terminate a sensor utilizing task, or when a sensor is lost, the sensor must not be allowed to make use of the credential which it stores to connect to networks.

Key update: By introducing a key update mechanism, a manager node can conveniently update a sensor's credential without the intervention of back-end system for the purpose of reducing the communication interactions and management burden on that back-end system.

Self-healing Key Distribution Schemes: Self healing key distribution scheme mainly classified into four classes[6] as follows: i. Polynomial secret-sharing-based self-healing key distribution schemes, ii. Vector space secret-sharing-based self-healing key distribution schemes, iii. SDR-based self-healing

key distribution schemes, iv. Hash chain-based self-healing key distribution schemes.

Originally every classes of self healing key distribution scheme include five procedures: i. Setup, ii. Broadcast, iii. Key recovery, iv Adding or revoking users, v. Self-healing.

Polynomial secret-sharing-based self-healing key distribution scheme[11] extends the lifetime of the basic self-healing key distribution scheme. It implements the concept of sliding window protocol to make error recovery consistently robust. It utilizes above mention five processes for successive implementation.

Vector space secret-sharing-based self-healing key distribution schemes[11] make the use of general monotone decreasing structure for the family of subsets of users that can be revoked instead of threshold one. Thus the scheme achieves more flexible performance than Polynomial secret-sharing-based self-healing key distribution scheme.

SDR-based self-healing key distribution schemes[11] are a stateless re-keying method. In this scheme, a key server maintains a logical key tree and every user are mapped to a leaf node of the key tree. In each re-keying operation[9], the key server partitions the current group into a minimal number of subsets, and then encrypts the new group key with the common key of each subset, respectively.

Hash chain-based self-healing key distribution schemes[11] proposed an efficient self-healing group key scheme with time-limited node revocation based on Dual Directional Hash Chains (DDHCs). The hash chain itself cannot be the only cryptographic primitive of a self-healing key distribution scheme. It forms a self-healing key distribution scheme together with other cryptographic primitives

Levels of Key Hierarchy: Key hierarchy is design with conjunction of various levels based on the task performed by the elements of the key distribution scheme.
Level 0: level 0 define as Group key. Sensor nodes deal with this Group key.
Level 1: level 1 defines as Manager Key. Group manager deals with this Manager Key.
Level 2: level 2 defines as Root Key. Base station deals with this Root key.

Approaches for Key Distribution: Of the many challenges facing real deployments of WSNs, the distribution of symmetric Keys in the network is one of the most difficult to address[12]. As there is no in-situ infrastructure for the wireless sensor nodes to interact with in order to obtain keys on the fly, like in a traditional Public Key Infrastructure (PKI) approach, novel techniques have to be employed. This section discusses different approaches[12, 10] to the key distribution problem.

Symmetric Keys: The simplest approach to deploy a symmetric system would be that all the wireless sensor nodes share the same key at the sender side as well as receiver side. As the wireless sensor nodes could be placed in a region where an adversary can capture them, it is likely that it could extract the secret key, and therefore would be able to monitor all communication in the network. For this reason, this method of ensuring privacy is not appropriate in a hostile environment.

Pair-Wise Keys: Another method would be for all the wireless sensor nodes to set up pair-wise keys between them before deployment. If there are N wireless sensor nodes in the network then each wireless sensor node would have to store N keys in its persistent memory. In a resource constrained device this would be a problem as storing the keys would use too much memory. The other main drawback to using this scheme is that it does not scale. If, after deploying the bulk of the wireless sensor nodes, it is required to add extra wireless sensor nodes then this is not possible unless the extra wireless sensor nodes' keys are already programmed in the deployed network. Upon capture of a wireless sensor node, however, only its N links will be compromised, which is a slight improvement on the system that uses only one symmetric key.

Probabilistic Key Sharing: Probabilistic key sharing is a kind of symmetric key technique. In this approach a large pool of keys is generated from which a smaller ring of keys is randomly selected and preloaded before deployment into each wireless sensor node. Each wireless sensor node thus has a separate ring of keys in which there may be a shared key. During the shared key discovery phase of the algorithm, the wireless sensor nodes determine whether or not there is secure path between them. However, this scheme is not secure against capture by an adversary. If one wireless sensor node is captured then there is a probability of the links in the network can be deciphered.

Public Keys: Another approach to key distribution is to employ an asymmetric or public key system. In these schemes there is a private/public key pair and it is considered computationally infeasible to calculate the private key from the public one. The wireless sensor nodes can be deployed with an embedded private/public key pair. They then broadcast the public key to their neighbors who can then use this public key to encrypt a message to them. This scheme has the added advantage that private key can be used to generate digital signatures. Asymmetric systems are secure against individual wireless sensor node capture and they are also scalable. In sensor network environment public key algorithms used like Elliptic curve cryptography algorithm, Elgamal Cryptography algorithm, NtruEncrypt algorithm etc.

Results and Discussion

The deployment of sensor nodes in a hostile environment makes the networks vulnerable. Wireless sensor networks are increasingly being used in military, environmental, health and

commercial applications. Sensor networks are inherently different from traditional wired networks as well as wireless ad-hoc networks[13]. Security is an important feature for the deployment of Wireless Sensor Networks. This paper summarizes the security mechanism widely used to provide robust security in sensor network environment.

In this paper the author proposed a new self-healing key distribution scheme. The proposed scheme enables a large and dynamic group of users to establish a session key for secure communications over an unreliable wireless network. The scheme also enables a user to recover, from a single broadcast message. The long-lived personal key schemes are provided by Staddon J. and Blundo C.[14, 15]. However, they do not properly fit for practical applications due to the very limited communication resources. The personal key can be reused without any alternation[16]. Scheme proposed over here has reserved forward security and backward security, which are crucial properties for group key distributions.

The author has anticipated four novel group-wise key distribution schemes - Polynomial secret-sharing-based self-healing, Vector space secret-sharing-based self-healing, SDR-based self-healing, Hash chain-based self-healing for secure group communications in Wireless Sensor Networks. The anticipated schemes offer self-healing group key distribution, which features periodic re-keying with implicit authentication and efficient tolerance for lost re-keying messages[10]; and time-limited group node revocation so that forward and backward secrecy can be ensured.

Conclusion

With the wide application of wireless networks, as one of the basic security service self-healing key distribution scheme will receive more attention. In this paper, the author reviewed most existing self-healing key distribution schemes. The author clarified the security requirements of self-healing key distribution schemes according to their special application environment. Then the author classified the schemes according to different cryptographic primitives. The author has also discussed mutual healing and authentication techniques which can be used to strengthen the robustness of self-healing key distribution schemes.

Acknowledgement

The author expresses his sincere thanks to Prof. Dr. Vijay Chavda, N.P. College of Computer Studies and Management - Kadi (Gujarat-INDIA) and Prof. Dr. Manik Lal Das, Dhirubhai Ambani Institute of Information and Communication Technology - Gandhinagar (Gujarat-INDIA) for their invaluable guidance and unremitting support.

References

1. Mewada S. and Singh U., Performance Analysis of Secure Wireless Mesh Networks, *Res.J.Recent Sci.*, **1(3)**, 80-85 (**2012**)

2. Wang Q., Chen H., Lei X. and Wang K., Long-lived Self-healing Group Key Distribution Scheme in Wireless Sensor Networks, *Journal of Networks***, 7,** 1024-1030, **(2012)**

3. Firdous K., Sajid H., Jong H. and Ashraf M., Secure Group Communication with Self-healing and Rekeying in Wireless Sensor Networks, H. Zhang et al. (Eds.): MSN 2007, LNCS 4864, 737–748, 2007, and Springer-Verlag Berlin Heidelberg **(2007)**

4. Jingyuan L., Yafeng W., John A., Sang H., Zhong Z., Tian H., Bong W. and Seong Soon J., Predictive Dependency Constraint Directed Self-Healing for Wireless Sensor Networks, *IEEE Publication:* 978-1-4244-7910-8/10 **(2010)**

5. Biming T., Song H., Jiankun H. and Tharam D., A Mutual Healing Key Distribution Scheme in Wireless Networks, *Journal of Network and Computer Applications*, **34**, 80-88 **(2011)**

6. Biming T., Song H., Sazia P., Jiankun H. and Das S., Self-Healing Key Distribution Schemes for Wireless Networks: A Survey, *Oxford University Press on behalf of The British Computer Society*, March 20 **(2011)**

7. Wang H. and Zhang Y., Cryptanalysis of an Efficient Threshold Self-Healing Key Distribution Scheme, *IEEE Transaction on Wireless Communications*, **10(1) (2011)**

8. Roberto D., Claudio S. and Gene T., Self-Healing in Unattended Wireless Sensor Networks, *ACM Transactions on Sensor Networks*, **9(4),** 39:1-39:19 **(2010)**

9. Minghui S. and Xuemin S., Self Healing Group Wise Key Distribution Schemes With Time Limited Node Revocation for Wireless Sensor Network, Security in Wireless Mobile Ad Hoc and Sensor Networks, *IEEE Wireless Communications*, 38-46 **(2007)**

10. Seyed Hossein N., Amir Hossein J. and Vanesa D., A Distributed Group Rekeying Scheme for Wireless Sensor Networks, *ICSNC 2011: The Sixth International Conference on Systems and Networks Communications***(2011)**

11. Song H., Biming T., Mingxing H. and Elizabeth C., Efficient Threshold Self-Healing Key Distribution with Sponsorization for Infrastructure less Wireless Networks, *IEEE Transactions on Wireless Communication*, **8(4)**, 1876-1887 **(2009)**

12. Dr. Padmavathi G. and Shanmugapriya D., A Survey of Attacks-Security Mechanisms and Challenges in Wireless Sensor Networks, *International Journal of Computer Science and Information Security*, **4(1) (2009)**

13. Sasha S., Miodrag P., Vlasios T., Scott Z. and Srivastava M., On *Communication Security in Wireless Ad-Hoc Sensor Networks* **(2002)**

14. Blundo C., D'Arco P., Santis A., and Listo M., Design of self-healing key distribution schemes, *Design Codes Cryptography*, **32**, 15- 44 **(2004)**

15. Staddon J., Miner S., Franklin M., Balfanz D., Malkin M., and Dean D., Self-healing key distribution with revocation, *IEEE Symposium Security Privacy*, 224-240 **(2002)**

16. Dutta R. and Mukhopadhyay S., Improved self-healing key distribution with revocation in wireless sensor network, *Wireless Communication Networking*, 2963-2968 **(2007)**