Volume 5, Issue 3, March 2015 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Survey on Various Key Management Schemes for LEACH in Wireless Sensor Networks

Gurpreet Kaur[*], Navdeep Kumar

CSE & Kurukshetra University

Haryana, India

Abstract— Wireless Sensor Network (WSN) are the network of sensor nodes which communicate with each other and with the base station using wireless channel. Due to extensive use of wireless sensor networks it is necessary to improve its security. WSN nodes are prone to physical attacks. Wireless sensor networks (WSN) face security threats so traditional key management schemes are no longer accurate for WSN. There should be some special key management schemes for WSN. The objective of this paper is to provide comparative study of various key management techniques for LEACH in wireless sensor networks with advantages and disadvantages of each scheme.

Keywords— WSN, LEACH, CH, SecLEACH, ESKMS, DKS-LEACH

I. INTRODUCTION

Wireless Sensor Network (WSN) are the network of sensor nodes which communicate with each other and with the base station using wireless channel. Sensor nodes can communicate with base station by single-hop or by multi-hop. In single-hop sensor send data directly to the base station and in multi-hop sensor data is send to intermediate node or data aggregate node which aggregate data coming from sensor nodes, then send to the base station[4]. A wireless sensor network is an Adhoc network which includes sensor nodes, sink nodes and cluster heads. Sensor networks are self organized networks. Wireless Sensor network consists of large number of tiny devices known as sensor nodes which are distributed to check environmental and physical conditions[17]. To get information about the environment, sensor nodes have to coordinate among themselves.

Wireless Sensor network can be applied in the field of military applications, e-learning and air traffic control. The main advantage of using Wireless sensor network is that it provides flexible communication between nodes in the network but energy consumption is a major issue in WSN. To save energy during communication in WSN researchers proposed Cluster based organization.

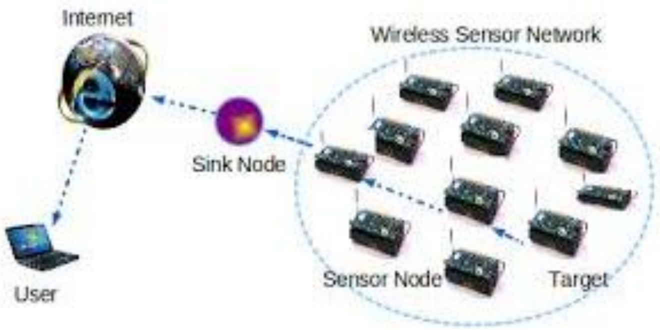

Fig 1.1 A Typhical Wireless Sensor Network

Security In Wireless Sensor Networks:

Recently Sensor network security issues are becoming the focus of industry. Due to extensive use of wireless sensor networks it is necessary to improve its security. WSN nodes are prone to physical attacks. In WSN we do not know before which nodes will be in communication range of each other after deployment. The traditional network security method is not suitable for sensor networks because of its limited storage space and computing power. In Wireless sensor networks different types of messages are exchanged having different requirements for security so a single keying method cannot satisfy all the security requirements. Wireless sensor networks (WSN) face security threats so traditional key management schemes are no longer accurate for WSN. There should be some special key management schemes for WSN. Most of the routing protocols for WSNs are vulnerable to a number of security threats.

II. LEACH PROTOCOL

LEACH is called Low Energy Adaptive Clustering Hierarchy. LEACH is the first protocol of wireless sensor networks based on clustering and layered structure technology. LEACH protocol was proposed to lower the energy consumption in sensor networks. It includes distributed cluster formation. Energy consumption is balanced by applying the clustered

hierarchy. Few sensor nodes are selected randomly to become cluster-heads according to a stochastic algorithm. LEACH can rotate this role to evenly distribute the energy load among sensors in the network[9]. In LEACH, the cluster-heads compress and aggregate the data which is arriving from the nodes that belong to their respective cluster, and send it to the BS to reduce the amount of information that must be transmitted to the BS. LEACH uses a TDMA/ CDMA (MAC) to reduce collisions within a cluster and within different clusters.
The working of LEACH protocol is divided into two phases[8]:

I. Set-up phase
II. Steady state phase

In set-up phase, the nodes are organized into clusters and some nodes are chosen at random to become cluster-heads. The cluster head(CH) broadcasts advertisement message to non CHs. After receiving the message the nodes can decide to join the cluster based on signal strength. The CH creates a TDMA schedule and broadcast it to all the members of its cluster. In the steady state phase, the actual data is transferred to the Base Station(BS). The CH receives data from its cluster members, aggregate the data and send the aggregated data to the BS. Energy is saved in LEACH protocol due to aggregation of data. The steady state phase is longer than the set-up phase.

Advantages Of LEACH:

a) The selection of path and routing information is easy in LEACH so the sensor nodes don’t have to keep large routing information and there is no need of complex functions.
b) The CH is selected randomly so each node has an equal opportunity for being selected as CH, thus balancing the network load.
c) Due to data fusion mechanism in LEACH protocol the energy consumption of data transmission is reduced by the CH, and thus the network life cycle can be extended.

Disadvantages Of LEACH:

a) LEACH does not take into account the residual energy of each node.
b) The distribution of cluster head depends on random number, so there is a possibility that at some regions the CH are large whereas at other regions the CH may be small.

III. KEY MANAGAMENT IN WIRELESS SENSOR NETWORKS

WSNs are applied in some of the sensitive areas such as defense, battle field surveillance, target tracking. As WSNs are composed of sensor nodes, so an intruder can capture a sensor node to become a CH and further propagate attacks such as sinkhole and selective forwarding. The entire network could be disrupted by this. Therefore, it is necessary to establish encryption keys among sensor nodes, so that the security impact of a node compromise could be restricted[3]. The key management is one security aspect that receives a great deal of attention in cluster based WSNs. The data sent to the base station must be encrypted using some encryption techniques to make it secure. Key management is used to make data secure in WSNs. Key management is one of the application of wireless sensor network. Key management in wireless sensor network is a complex task. Wireless sensor network consists of large number of sensor nodes having different hardware abilities. Since sensor nodes have limited memory resources and are energy constrainted so complex security algorithms cannot be used in sensor networks. Hence, an energy efficient key management scheme is necessary to mitigate the security risks.
Key management can be defined as a mechanism that consists of key establishment and the maintenance of ongoing keying relationship between valid parties according to a security policy[11]. The key management in WSNs consists of creating, distributing and maintaining the secrete keys. So to generate techniques for key management for encryption, which can make data communication more secure and at a same time make less resource utilization, have vital importance in WSNs. Depending on the ability of key management schemes to update the cryptographic keys of sensor nodes during their run time, these schemes can be classified into two different categories:

- Static
- Dynamic

In static key management, the keys are pre-distributed in the network which means that the keys remain fixed for the whole lifetime of the network. In this case since the key is same so the probability of attacks increases in the network. But in dynamic key management, the keys are not fixed instead they are changing throughout the lifetime of the network. So Dynamic key management is most important type of key management in sensor networks. Dynamic key management is a processes in which keys are distributed either periodically or on demand as needed by the network. The dynamic key management schemes can enhance network survivability and network resilience since the keys of compromised nodes are revoked in the rekeying process.
Generally the key management schemes can be classified as:

- Distributed
- Centralized.

Distributed dynamic key management is a set of process, in which no central key controller, such as a base station or third party, is involved in rekeying process of sensor nodes. Basic idea behind distributed dynamic key management scheme is to avoid a single point of failure by managing key using multiple key controllers. But these schemes are prone to design errors as compromised sensor nodes can participate in node eviction process. Whereas, centralized dynamic key management is a set of mechanisms that that uses a single central key controller, such as a base station or any third party, to manage and replace key materials on the network's nodes. Compared with distributed dynamic key management, the compromised sensor nodes cannot damage the node eviction process in centralized key management scheme. It is further divided into flat, hierarchical and heterogeneous network based key management.

IV. RELATED STUDY

A) Provide security in LEACH

Leonardo B. Oliveira,Hao C. Wong and M. Bern in 2005 [1], proposed a modified version of LEACH called SecLEACH. SecLEACH is a random key distribution solution for securing clustered Sensor networks. The author described main ideas behind key distribution schemes and showed that how it can be used to secure node to CH communications in LEACH. The author showed how SecLEACH can yield different performance numbers on efficiency and security depending on parameter values.

Mandicou Ba, Ibrahima Niang, Bamba Gueye [12], proposed a deterministic key management scheme, known as DKS-LEACH, to secure LEACH protocol from malicious attacks. A theoretical evaluation of security model is designed which secures the setup and study phases of LEACH protocol. An evaluation of the power consumption of DKS-LEACH is performed using the TOSSIM simulator. The advantage of this approach is in the prevention of the election of untrustworthy cluster head as well protection from different kind of attacks from malicious sensor nodes.

B) Reduces network communication load for updating cluster keys

Jianli Wang, Laibo Zheng, Li Zhao, and Dan Tian in 2012 [2], proposed a LEACH-based key management scheme for wireless sensor networks based on Exclusion Basis Systems and μ TESLA. It is an efficient security routing algorithm for wireless sensor networks. The author used EBS for key generation and distribution, and used μ TESLA to guarantee the cluster head can update security key after the first round. The proposed scheme can decrease the storage requirements of keys, and the network communication load for updating cluster keys. The proposed key management scheme can enhance the survivability and ensure the security of WSNs.

C) Provides continuous authentication of nodes

Abdoulaye Diop, Yue Qi, Qin Wang, and Shariq Hussain in November 2012 [3], presented an Efficient and Secure Key Management Scheme for Hierarchical Wireless Sensor Network (ESKMS). This energy efficient key management scheme can mitigate the security risks. The proposed technique distributes the keys within a cluster efficiently and updates the pre-deployed keys to mitigate the node compromise attack. The author provided a detailed security analysis of ESKMS protocol and showed its advantages in avoiding different type of attacks from malicious nodes. Using simulation, the results showed that ESKMS is more energy efficient and provides a longer network lifetime compared to the existing key management schemes.

D) Protects the network from attacks

Namdeep Singh and Er. Jasvir Singh in July 2013 [4], provided an overview of some common WSNs concepts and proposed a security framework for LEACH protocols. Public key cryptographic techniques provide more security as compare to symmetric key cryptographic techniques at the cost of more energy consumption and more resource utilization. The Hybrid cryptographic techniques have been developed for Wireless Sensor Networks (WSNs) for balancing energy consumption and security level. By using Hybrid cryptographic techniques few security frameworks have been proposed in past few years to provide more security and with less memory requirements.

E) Provides more collaborative authentication security for key

Bi Jiana and E Xu in 2013 [5], proposed a security node-based key management protocol for cluster-based sensor networks. In this protocol generation of security nodes and different types of keys is described by the author. Performance analysis and simulation show that the by the proposed key management protocol energy consumption is less and key generation delay time is short. At the same time, more collaborative authentication security for keys is provided by the protocol. It can strongly recover against node capture, and can support large networks.

F) Provide WSN's dynamic security

Sai Ji, Liping Huang and Jin Wang in February 2013 [6], proposed a novel key management scheme for the dynamic WSNs. In the network deployment phase, the security authentication and random key distribution were initialized. During the network stable phase, the scheme proposed a dynamic updated key based on the AVL tree in order to ensure the real-time update security for the network topology. Simulation results showed that this program can ensure the WSN's dynamic security as well as achieve the energy efficiency goal.

Table1 Comparison of Various Key Management Techniques**:**

S.No	Key Management Technique	Proposed By	Based On	Advantages	Disadvantages

1	SecLEACH	Leonardo B. Oliveira	Random Key Predistribution	Secure CH-node communication in LEACH and protects the network from outside attacks	Resilience is less
2	LEACH-based Key Management	Jianli Wang	Exclusion Basis System	It decreases the storage requirements of storing keys and reduces network communication load for updating cluster keys	Collusion attack may occur in EBS
3	Efficient and Secure Key Management Scheme	Abdoulaye Diop	One way hash function, data encryption and MAC	Provides authentication of nodes in the network and reduces memory overhead	Cannot deal with malicious nodes
4	Solar Aware Distributed LEACH protocol	Namdeep Singh	ECC and AES cryptography	Protects the network from attacks such as spoofing, selective forwarding, Sybil, hello flooding	Solar powered nodes are selected as Cluster head
5	Security Node based Key Management	Bi Jiana	Pair-wise key and cluster key	Consumes less energy, provides more collaborative authentication security for key, has strong resilience against node capture and can support large scale network	Applicable only on static network and is not scalable
6	Novel key management scheme for the dynamic WSN	Sai Ji	Self-balanced binary search tree	This scheme has smaller memory and provide dynamic security	Only dynamic WSNs are considered
7	DKS-LEACH	Mandicou Ba	Deterministic key distribution approach	Provides authentication, integrity, confidentiality and also minimizes memory usage	Energy consumption is more

V. CONCLUSION

Various key management techniques have been studied for LEACH in wireless sensor networks with advantages and disadvantages of each scheme. From our work we conclude that Novel key management scheme for the dynamic WSN based on Self-balanced binary search tree has smaller memory and provide dynamic security. the scheme proposed a dynamic updated key based on the AVL tree in order to ensure the real-time update security for the network topology. DKS-LEACH scheme based on Deterministic key distribution approach provides authentication, integrity, confidentiality and also minimizes memory usage. This scheme secure LEACH protocol against malicious attacks.

REFERENCES

[1] Leonardo B. Oliveira, Hao C. Wong and M. Bern, “SecLEACH – A Random Key Distribution Solution for Securing Clustered Sensor Networks”, Supported by FAPESP under grant 2005/00557-9.

[2] Jianli Wang, Laibo Zheng, Li Zhao, and Dan Tian, “LEACH-Based Security Routing Protocol for WSNs”, Advances in CSIE, Vol. 2, AISC 169, pp. 253–258, © Springer-Verlag Berlin Heidelberg 2012.

[3] Abdoulaye Diop, Yue Qi, Qin Wang, and Shariq Hussain, “An Efficient and Secure Key Management Scheme for Hierarchical Wireless Sensor Networks”, International Journal of Computer and Communication Engineering, Vol. 1, No. 4, November 2012.

[4] Namdeep Singh, Er. Jasvir Singh, “A Security Framework for Wireless Sensor Networks”, Journal of Global Research in Computer Science, Volume 4, No. 7, July 2013.

[5] Bi Jiana, E Xu, “An Energy-efficient Security Node-based Key Management Protocol for WSN”, Proceedings of the 2nd International Symposium on Computer, Communication, Control and Automation, 2013.

[6] Sai Ji, Liping Huang and Jin Wang, “A Novel Key Management Scheme Supporting Network Dynamic Update in Wireless Sensor Network”, International Journal of Grid and Distributed Computing Vol. 6, No. 1, February, 2013.

[7] Mohammed A. Abuhelaleh and Khaled M. Elleithy, “Security In Wireless Sensor Networks: Key Management Module In SOOAWSN”, International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October 2010.

[8] Alisha Gupta, Vivek Sharma, “A Confidentiality Scheme for Energy Efficient LEACH Protocol Using Homomorphic Encryption”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013.

[9] Baiping Li**,** Xiaoqin Zhang, “Research and Improvement of LEACH Protocol for Wireless Sensor Network”, International Conference on Information Engineering, 2012.

[10] Nguyen Duy Tan, Longzhe Han, Nguyen Dinh Viet and Minho Jo, “An Improved LEACH Routing Protocol for Energy-Efficiency of Wireless Sensor Networks”, Smart Computing Review, vol. 2, no. 5, October 2012.

[11] Jaydeepsinh Barad, Bintu Kadhiwala, “Comparative study on dynamic key-management techniques for cluster-based sensor networks”, © IJEDR | Volume 2, Issue 2, 2014.

[12] M Ba, I Niang and B Gueye, “ A Deterministic Key Management Scheme for Securing Cluster-based Sensor Networks,” In : 8th International Conference on Embedded and Ubiquitous Computing IEEE 2010, pp. 422-227.

[13] Yi Liu, Shan Zhong, Licai You, Bu Lv, Lin Du, “A Low Energy Uneven Cluster Protocol Design for Wireless Sensor Network”, Int. J. Communications, Network and System Sciences, 2012, 5, 86-89, February 2012.

[14] Ms. Parul Tyagi, Ms. Surbhi Jain, “Comparative Study of Routing Protocols in Wireless Sensor Network”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 9, September 2012.

[15] Chunyao Fu, Zhifang Jiang, Wei Wei and Ang Wei, “An Energy Balanced Algorithm of LEACH Protocol in WSN”, IJCSI International Journal Of Computer Science Issues, Vol. 10, Issue 1, No 1, January 2013.

[16] Meena Malik, Dr. Yudhvir Singh , Anshu Arora, “Analysis of LEACH Protocol in Wireless Sensor Networks”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 2, February 2013.

[17] Neha Mehndiratta, Manju, Harish Bedi, “Wireless Sensor Network LEACH Protocol: A Survey”, International Journal of Emerging Research in Management &Technology,Volume-2, Issue-3, March 2013.

[18] Ajay jangra, Amisha Dhiman, “A Review on Low Energy Adaptive Clustering Hierarchy (LEACH) Routing Protocol in WSN”, International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 6, June 2013.