Novel Key Storage and Management Solution for the Security of Wireless Sensor Networks

Ali Hassan Sodhro[1], Ye Li*[2], Madad Ali Shah[3]
[1,2]Center for Biomedical Information Technilogy, Shenzhen Institutes of Advanced Technology, Chinese Academy of Sciences
[3]Department of Electrical Engineering, Sukkur Instituts of Business Adminsitration, Pakistan
Corresponding author, e-mail: ali.hassan@siat.ac.cn, Ye.li@siat.ac.cn, madad@iba-suk.edu.pk

Abstract

As wireless sensor networks continue to grow in usage for distinct applications. Storage (memory) requirement and security are major problems for these resource limited networks. This paper present a novel and an efficient key establishment and management scheme for WSNs, named Random Initial and Master Key (RIMK).We showed that our proposed technique, manages keys randomly with less storage (i.e. only two keys), less communication and computation overhead compared to existing Localized Encryption and Authentication Protocol (LEAP), in which every node uses four different keys in a static pattern and occupy greater storage space, which increases overhead and complexity in the network. Simulation results show that RIMK is more efficient and robust than LEAP.

***Keywords**: WSNs, LEAP, RIMK, initial key, master key*

Copyright © 2013 Universitas Ahmad Dahlan. All rights reserved.

1. Introduction

Wireless Sensor Networks (WSNs) is a new and increasingly used technology because of their data acquisition and data processing processes. WSNs are special networks which provide useful interface to the real world. They are composed of hundreds and thousands of inexpensive, low-powered sensing devices known as nodes with limited computational and communication resources [1]. WSNs are cooperative environmental networks in which tiny sensor nodes communicate over a wireless medium [2]. These types of networks are extensively used in all fields due to their broader applications in urban and rural areas such as warehouses, healthcare, forest fire tracking, military, smart buildings, earthquake detection, security gates of five star hotels and very high buildings etc. As general wireless techniques cannot be used for WSNs because they embarrass the resources and need greater security and storage space. The method of their communication and distribution in different fields [3] make them very effective to several actions of an opponent and large storage requirements. Small sensor nodes that are deployed in the surrounding are collecting data for present and future use, due to their small size and less storage allocation they perform every action for very short period of time. Due to limited memory, processing power and battery life each sensor node utilizes resources very effectively. Many appropriate methods for node scattering, use matched techniques for key (i.e.public key, private key, initial key and master key) for memory management and security purposes. These methods also need many communication and counting techniques for transfer of information from base station to the neighboring nodes and vice versa. Therefore; it is very essential to find distinct performance parameters for the WSNs. These networks have diverse characteristics because they combine the small sensors with their computing elements to handle and attack the surrounding and manage the small memory. These networks are mostly classified by fixed power and storage requirements. However, WSNs suffer from many constraints, including low computation capability, small memory, limited energy resources, susceptibility to physical capture, and use of insecure wireless communication channels. These constraints make security in WSNs a challenge. So in order to provide strong security mechanism, we propose a novel security technique-RIMK, a public key cryptography technique for the authentication of WSNs, which is most appropriate cryptographic technique. Previous works have more focused on the key management techniques [4] for the

Received January 12, 2013; Revised April 18, 2013; Accepted April 26, 2013

security of WSNs and its routing protocols. Efficient security mechanism for large scale distributed networks, LEAP and LEAP plus [5] discussed. Secure in-network processing in LEAP[6] proposed. An efficient self key establishment protocol [16] presented. Security protocol for the neighborhood nodes [17] is described. A survey on the authentication protocol is conducted [18]. Distributed key management techniques [19] examined. A secure authentication scheme [20] for the WSNs is presented. Many researchers worked on the pairwise keys for the security [7]. B.Das, et.al.propose routing mechanism in ad-hoc networks [8].Jiyong et.al develop time based key management protocol [9] for the WSNs. Tree based protocol for the key management of sensor networks [10], is explored by M-L.Messai,etal. S.p.Bingulace propose key management scheme for the distributed sensor networks [11]. H.Chan, A.Perring and D.Song design random key predistribution scheme for sensor networks [12]. A pair wise key predistribution scheme for WSNs and more techniques proposed by W.Du et al. [11, 12, 13]. Techniques for establishing pairwise keys for the distributed sensor networks [14] proposed by D.Liu and P.Ning. Location-aware key management technique [15] is the resource managing key technique in WSNs on which research is carried out by D.Huang, M.Mehta, D.Mehdi and L.Harn. Zhihong liu, Jianfeng Ma, Qiping Huang, SangJee Moon, storage requirement for key distribution in sensor networks [21], Xiuyuan Zheng; Hui Wang; Yangying Chen design decentralized key management scheme via neighborhood prediction in mobile wireless networks [22].

One of the key limitations of the existing research on the LEAP and key management in WSNs is that they focused only the securities but ignore the storage space management in WSN nodes. As WSNs are very resource constraints, because of low power, small size and less storage space (memory). So in order to resolve that issue of storage space management in the routing protocol of WSNs we proposed an efficient key storage and management scheme, Random Initial and Master Key (RIMK) in which every sensor node uses two keys on the random basis to save the storage space.

Our main contribution in this paper is that, we proposed a novel technique, RIMK to reduce the excess storage problem in LEAP and proved through simulation results that our proposed technique occupies less storage than the LEAP. The remainder of the paper is organized as follows. Section II, presents LEAP and its excess storage problem, Section III, describes our proposed technique-RIMK, flow chart for generating initial (primary) and master keys for RIMK and operation performed by RIMK.Section IV, provides simulation environment and discussion of simulation results. In section V, storage requirement of RIMK and LEAP is discussed and verified with experimental and mathematical operations. Section VI, concludes paper and directs to future research.

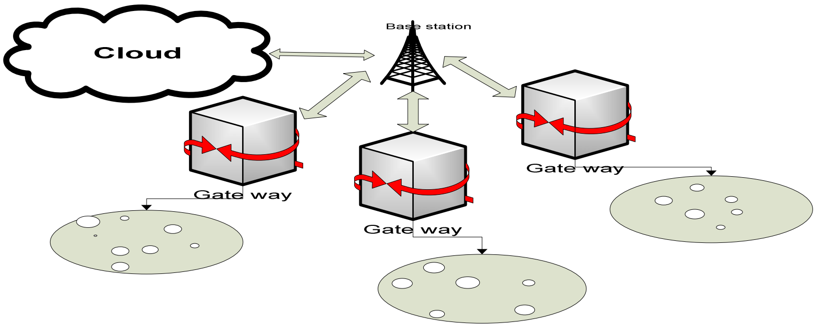

Figure 1. Architecture of Wireless Sensor Networks

2. Localized Encryption and Authentication Protocol

LEAP is a key management protocol in wireless sensor networks [4, 5]. It was intended to help in In-network processing [6] technique and at the same time restrain the nodes from sharing unauthorized or false information. As in all wireless networks distinct entities sharing multiple data, so for that reason we need separate methods for distributing and securing that information. For that purpose LEAP uses four different types of keys such as, individual key shared with base station, pairwise key [7] shared with another sensor node, cluster key shared with multiple neighboring nodes, and a group key shared with all the nodes in the network. A prominent characteristic of this routing protocol [8] is that it helps in finding authorized or legal entity beyond the involvement of in-network mechanism and to find an opponent affected environment. LEAP is based on the rule of using large key pattern to provide privacy and authentication but with larger storage requirement.

The information shared between sensor nodes is broadcasted in the whole network and categorized by distinct ways and unique conditions. For example, control information versus data information, information to multiple users versus to a single user, prerogative versus sensor self-information. The security position [9] of the sensor nodes is based on the condition in which these lies, authentication [10] is important for whole network while confidentiality is needed to few nodes in the network. For instance, confidentiality [11] is not important for schedule ordered data but is important for problems faced by individual nodes and base station [12]. As persuaded that use of distinct key algorithms is not good for efficient distribution and secluding information transfer techniques, which are very important in WSNs [13, 14]. LEAP is efficient for the security purpose but main problem of it is that every node stores four keys [15], so large storage space is required, as sensor nodes are already small in size and resource constraint [16, 17]. In order to resolve that issue of larger storage and memory usage by every node in the LEAP, we proposed a novel key management technique, which is a lightweight scheme for security and storage management in WSNs.

Considering the memory used by every node in the LEAP, there are some parameters such as, L which shows the number of memory units required for storing random function F, A shows the number of neighboring nodes, and each cryptography key requires one 1 unit of memory storage, so memory used by each node is given by:

$$MemoryUnits = L + A + 2A + 1 + 1 \quad (1)$$

One individual key, one group key, A cluster keys, 2A pair wise keys, L is the random function storing unit. As each sensor node in the LEAP stores four types of keys; individual key, pairwise key, cluster key and group key [18]. Thus each node requires following number of memory units for storage: 1 unit for an individual key, 1 unit for the group key, A units for A cluster head keys, 2A units for 2A pairwise keys (i.e. 2 pairwise keys for each neighbor), and L units for its key chain (for the next key generation with F) [20]. Therefore, each node requires L+3A+2 units of memory [21, 22].

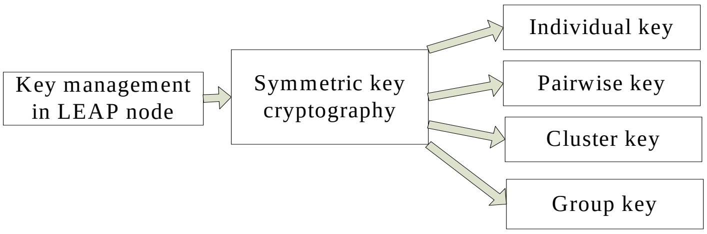

Figure 2. Key Distribution Pattern in LEAP Node

3. Our Proposal-random Initial Key and Master Key

Random Initial and Master Key (RIMK) is a very robust, energy efficient, dynamic, and low cost storage and secure key management technique in which newly added sensor nodes can join the network easily and secretly while malicious nodes will be separated at that time. This technique is based on the random function which helps in encryption of data, reduction of storage space and energy consumption in sensor networks which were not resolved by LEAP. RIMK is used only in the active portion of the network in order to decrease the amount of energy used and gives a very scalable approach to key management in the network.RIMK is also used for authentication of the network nodes; one novel feature of this technique is that it has the lowest storage cost because every node store only two keys, individual key and pair-wise key during communication as shown in Figure 3. Furthermore, in our proposed technique each node stores following number of memory units:

$$MemoryUnits = L + 1 + 2A \qquad (2)$$

One individual key, 2A pairwise keys. In RIMK each sensor node stores two keys; individual and pairwise key. Therefore memory units for every node are as: 1 unit for individual key, 2A units for pairwise keys (i.e. 2 pairwise keys for each neighbor), and L units for its key chain (for next key generation with F). So, each node requires L+1+2A units of memory, which is very small storage space than the each node in the LEAP. In our proposed technique no any additional resources are necessary for establishing other keys. Due to good security level in the RIMK, if any node stores an individual key than it will generate random master key, an encryption and authentication process is needed for every node to transfer information to the base station. RIMK is faster in computation as well as good in memory, energy and bandwidth savings, also it uses random function for the randomly assigned keys to each node in the network.

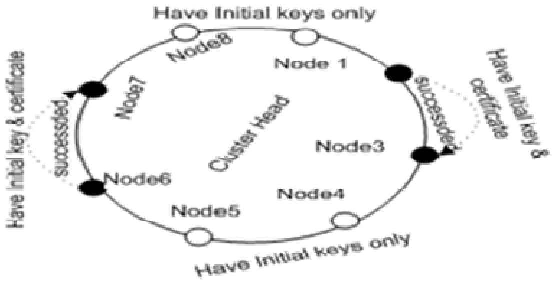

Figure 3. Key Distribution Pattern in RIMK Node

RIMK helps in maintaining/recovering the secure communication even when master key has been exposed/disclosed to intruders.The beauty of RIMK is that it supports key transformation in a random manner in order to avoid the whole network from compromise.

3.1. Operation Performed by RIMK

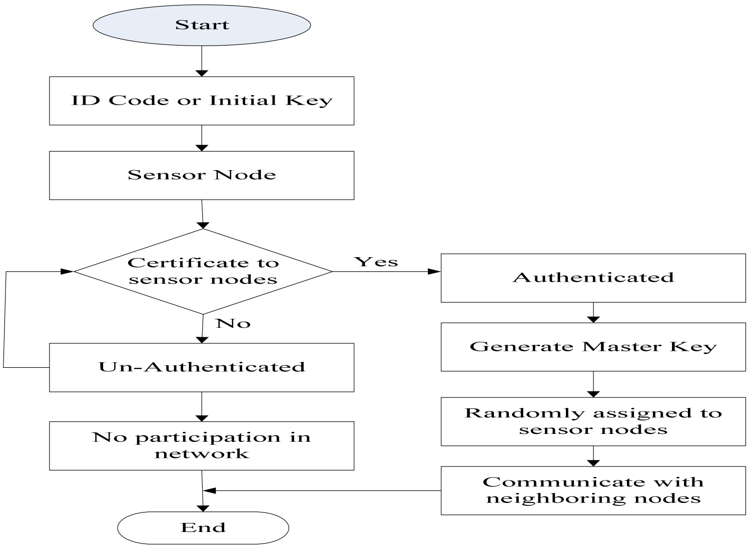
Start
ID Code or Initial Key
Sensor Node
Certificate to sensor nodes
Yes
No
Authenticated
Generate Master Key
Randomly assigned to sensor nodes
Communicate with neighboring nodes
Un-Authenticated
No participation in network
End

Figure 4. Proposed Method for Generating Initial and Master Key in the RIMK

First, an initial key or ID code is generated randomly by base station and assigned on the random basis to the sensor nodes in the group (i.e. cluster of nodes) of network, after this a certificate is assigned from the third trusted party known as Certificate Authority (i.e. cluster head node) on random basis to the nodes in the group of network which are holding initial key from base station. After combining the initial key and the certificate a sensor node will be authenticated and master key is generated, which is allocated on the random basis to the nodes in the group as shown in Figure 3, and a node can participate in the network for communication. Also these group nodes can communicate by sharing and exchanging information with the neighboring nodes.

On the other hand those nodes have got initial key from base station but not certificate from third trusted party will not be authenticated and cannot generate master key, so these nodes are not able to participate in the network for communication. They will return back to certificate authority to get certificate then generate the master key and will participate in the network, as shown in the Figure 4. That process of key transformation is iterated up to maximum number of times (μ) when a node finds new neighbor and participate in the network, than key shared information is exchanged. In Figure4 it is clear that if any node have not got initial key from base station and certificate from the certificate authority are not able to communicate with the neighboring nodes, but they will wait up to the time of getting initial key and certificate, if they are getting both then generate master key and can participate in the network for communication with the neighboring nodes.

The main goal of the RIMK is to perform shared key information exchange process with small number of keys and less storage by assigning initial and master keys randomly to each node to increase the connectivity between the nodes and decreasing the number of compromised nodes in the network.

4. Simulation Environment

There are three important parameters for the simulation of the LEAP and RIMK such as number of nodes, storage space in bits and number of rounds (i.e. number of times to transfer information from base station to the neighboring nodes and vice versa). Simulation is performed in MATLAB in Dell computer.

Table1. The Simulation Parameters

Parameter	Value
Number of nodes	20
Number of storage bits	70
Number of rounds(complexity)	400
Number of keys for LEAP	80
Number of keys for RIMK	40

4.1. Scenario1: Relationship Between Number of Neighboring Nodes and Storage Requirement

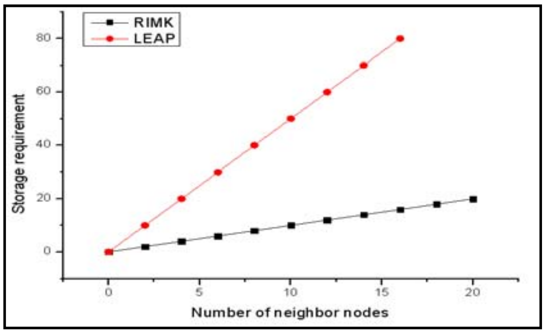

Figure 5. Relationship between Nodes and Storage Requirement

Figure 5. shows relationship between number of nodes and storage requirement. Here we have 20 nodes for both LEAP and RIMK while storage requirement is different for both because due to storage of four keys by every node in the LEAP and two keys by every node in the RIMK. Approximately 65 bits stored by LEAP and 22-bits stored by RIMK respectively. So, it is cleared from the simulation results that there is a direct relationship between storage space and the number of keys. As RIMK uses only two keys with less storage space than the LEAP so it is more efficient and robust than LEAP.

4.2. Relationship Between Number of Neighboring Nodes and Number of Rounds

Figure 6 shows the relationship between number of neighboring nodes and number of rounds. Here we have 20 nodes for both LEAP and RIMK but different number of rounds for both due to different number of keys 80 and 40 respectively. As number of rounds (i.e.number of times information is transferred and exchanged between neighboring nodes and the base station, vice versa) are directly proportional to the number of keys. It is cleared from the simulation results that there are approximately 23 numbers of rounds for RIMK and 80 (number of nodes x number of keys in each node 20x4=80) numbers of rounds for LEAP. Due to the large number of keys by each node of LEAP, every node takes greater time to complete round (i.e. transfer and exchange information between each other and to the base station). While due to less number of keys and number of rounds in each node of the RIMK it takes less time to complete round. It is cleared that RIMK is more efficient than the LEAP.

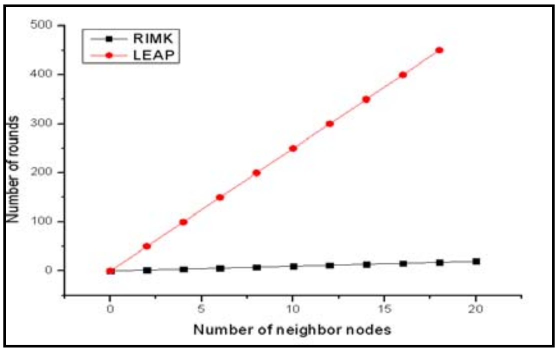

Figure 6. Relationship between Number of Nodes and Number of Rounds

5. Why RIMK is Better Than LEAP

In LEAP every node stores four keys, so more storage space is used because when number of keys increase the number of rounds and hence complexity in the network increase, while every node in the RIMK store two keys, so less storage space is used hence less number of rounds and less complexity. From simulation results it is clear that RIMK occupies one-third of the storage space as compared to the LEAP, so we can say that our proposed technique-RIMK is better than the LEAP, as shown in Figure 5 and Figure 6 . Another advantage of RIMK is in terms of memory cost, which is less than the LEAP as calculated by:
Let n be the number of neighbor nodes and k be the number of keys stored by each node.

$$LEAP : n \times k = 20 \times 4 = 80 bits \quad (3)$$

$$RIMK : n \times k = 20 \times 2 = 40 bits \quad (4)$$

From this mathematical calculation it is cleared that LEAP nodes occupy more storage while nodes in RIMK occupy less storage.

6. Conclusion and Future Work

In this paper, we proposed a novel key storage and management scheme RIMK for WSNs, based on random function, random distribution of initial key, master key and certificate from the third trusted party known as certification authority (CA). RIMK is lightweight storage management scheme manages keys with minimum transmission and storage requirement in order to resolve excess storage problem in the LEAP. It is also a base key management scheme because it keeps network security before start up, but here we have not discussed security of RIMK and LEAP in detail, only we have focused on the excess storage problem of the LEAP. Due to self-key establishment attribute of the RIMK, it can be applied to pervasive environment that needs self-configuration. The simulation results show that our scheme significantly reduces the storage requirement by one-third as compared to the LEAP.

In near future research will be carried out on security of WSNs by using RIMK, optimization of generation time of an initial key from base station to the cluster head node, optimization of transferring time of an initial key from base station to the cluster head node, optimization of generation time of master key by the nodes having initial key and the certificate from CA, optimization of transferring time of master key from cluster head node to the neighboring nodes in the network.

Acknowledgment

This work was supported in part by the National Basic Research Program of China (973 Program, No. 2010CB732606-6), the National S&T Major Project of China (No.2011ZX03005-001) and Key Basic Research Program of Shenzhen (No. JC201005270257A).

References

[1] F Lorenzelli, K Yao. *Arrays of randomly spaced sensors*. Pro.SPIE. 2009; 2846:122-133.
[2] Hill J. *System Architecture for wireless sensor networks master report*. University of California Berkeley. 2002.
[3] M Sohail. Introduction of wireless sensor networks. *Ambient Intelligence*. 2007.
[4] Sencum Zhu, Sanjeev Setia, Sushil Jajodia. *LEAP: Efficient security mechanisms for large scale distributed sensor networks.* In 10th ACM conference on computer and communication security CC'S3. ACM Press. 2003; 62-72.
[5] Sencun Zhu, Sanjeev Setia, Sushil Jajodia. *LEAP & plus: Efficient security mechanisms for large-scale distributed sensor networks*. ACM transaction on sensor networks (TOSN). 2009; 2(4): 500-528.
[6] T Dimitriou, D Foteinakis.*Secure In-Network Processing in sensor networks.* In proceedings of the 1st workshop on Broadband Advanced sensor networks. IEEE Basenets. 2004.
[7] Bin Saad H, Cao G, Kumar R, Laportal T, Trayonar P. *Establishing pairwise keys in the hetrogenous sensor networks*. In FOCOM IEEE 25th International conference on computer communication Proceedings. 2006; 1-12.
[8] B Das, V Bharghavan. *Routing in Ad-Hoc networks using minimum connecting dominating sets.* In Proceedings of ICC.1997.
[9] Jiyong Jangel. *Time-based key management protocol for wireless sensor networks*. Department of computer science, Yonsei University.
[10] ML Messai. Tree based protocol for key management in WSNs. *hindawi publishing corporation, EURASIP Journal on wireless communications and networking*. 2010.
[11] SP Bingulac. *Key management scheme for the distributed sensor networks*. Proc.of the 9th ACM conference on CCS. 2002; 41-47.
[12] H Chan, A Perring, D Song. *Random key Predistribution scheme for sensor networks.* IEEE symposim on security and privacy. 2003; 197-213.
[13] W Du, J Deng, YS Han, PK Varsheny. *Pair wise key predistribution scheme for wireless sensor networks.* Proceedings of 10th ACM Conference on computer and communication security (CCS), Washington, DC, USA. 2003; 42-51.
[14] D Liu, P Ning. *Establishing pairwise keys in distributed sensor networks.* Proceedings of 10th ACM Conference on computer and communication security. 2003; 52-61.
[15] D Huang, M Mehta, D Mehdi, L Harn. *Location aware key management scheme for wireless sensor networks.* Proc.of ACM workshop Security of Ad-Hoc and sensor networks (SASN'04). 2004; 29-42.
[16] Mohsen Sharifi. An efficient self key establishment protocol for WSNs. 2009.
[17] Di Zhang, Yi Zhao. *A robust and efficient neighborhood-based security protocol for wireless sensor networks.* IEEE computer society. 2010.
[18] Rasmita Aautray, Itun Sarangi. Survey on authentication protocols of WSNs. 2011; 3: 4253-4256.
[19] Kejie Lu. A frame work for a distributed key management scheme in heterogeneous WSNs. 2008; 7(2).
[20] Li Feng-Yu. Secure authentication scheme on IBE. 2010; 5(9).
[21] Zhihong liu, Jianfeng Ma, Qiping Huang. *SangJee Moon Storage requirement for key distribution in sensor networks*. IEEE SensorCOMM. 2008.

[22] Xiuyuan Zheng, Hui Wang, Yangying Chen. *Decentralized key management scheme via neighborhood prediction in mobile wireless networks.* IEEE 7th International conference on mobile adhoc and sensor system. 2010; 51-60.
[23] Qingsong Hu, Dian Zhang, Wei Liu. Precise Positioning of Moving Objects in Coal Face: Challenges and Solutions. *Journal of Digital Content Technology and its Applications*. 2013; 7(1): 213-222.
[24] Desheng Liu, Keqi Wang. Flow Meter online Compensation Based on Neural Network Algorithm. *IJACT: International Journal of Advancements in Computing Technology*. 2013; 5(1): 297-303.