International Journal of Wireless Networks and Communications.
ISSN 0975-6507 Volume 5, Number 1 (2013), pp. 1-8

http://www.irphouse.com

An Efficient and Secure Key Management Protocol for Wireless Sensor Network

Sanjesh Ghore and Mr Rakesh Kumar Khare

Department of Computer Science & engg
Raipur Institute of Technology, Raipur, India
ghore.sanjesh62@gmail.com
H.O.D., Department of Information Technology
Raipur Institute of Technology, Raipur , India
rakesh_khare2001@yahoo.com

Abstract

The design of optimal key management technique which provides higher security with lower complexity and reduced communication overhead and storage requirements is one of the important challenges for the security of the wireless sensor networks. Although many key management protocols are already proposed like Localized Encryption and Authentication Protocol (LEAP), µTESLA etc. but these protocols required large key updating overhead and key storing space while the key updating process is also produces the delay because the keys are updated node be node in sequential procedure. To overcome these problems we presented a new approach which not only maintains the security but also reduces the key updating overheads, storage space and a broadcasting based key updating which further reduces the time and communication overheads.

Keywords: Wireless Sensor Network (WSN), Key Management Protocol, Network Security.

1. Introduction

Key distribution is an important security and management issue in wireless sensor network (WSN) design. It is considered as relatively new and fast growing field because of the recent due to the recent advancements inwireless communications technology and their applications.

When looking as communication network the Wireless sensor networks can be classified as the networks of small, battery-powered, Memory-constraint devices called sensor nodes, which have the capability of wireless communication over a limited area. Due to memory, processing and power limitations, specialized deployment procedure and protocols are required to build a fully functional network. The protocol uses the key management schemes for ensuring the security of the network. Key distribution schemes are various techniques that have been developed by network engineers for a better maintenance of key management in WSN.

The rest of the article is organized as follows. The section 2 presents a brief review of the related literatures.Section 3 discusses the basic key management in WSN followed by section 4 which explains the working of PN sequence generator. The proposed algorithm is explained in Section 5 and its analysis on the basis of simulation in presented in Section 6, while in the section 7 the conclusion on the basis of simulation resultsare discussed.

2. Literature Review

This section presents a brief review of the some recent developments in the field of key management in WSN. Xing Zhang et al [1] present an energy efficient distributed deterministic key management scheme (EDDK) for resource constrained wireless sensor networks. EDDK mainly focuses on the establishment and maintenance of the pairwise keys as well as the local cluster keys and can fix some flaws in some existing key management schemes. Not only can the neighbor table constructed during key establishment provide the security for key maintenance and data transfer, but it can also be used to effectively manage the storage and update of the keys. By using the elliptic curve digital signature algorithm in EDDK, both new and mobile sensor nodes can join or rejoin a sensor network securely. Unlike some centralized and location-based key management schemes, EDDK does not depend on such infrastructure as base stations and robots and thus has a high level of flexibility.BimingTian et al [2] analyze the deficiency of the time based key management scheme and proposed a key management scheme for multiphase WSNs. The proposed scheme disperses the damage resulting from the disclosure of the initial key. We show it has better resilience and higher key connectivity probability through the analysis. An exclusion basis system-based key management scheme called MUQAMI+ for large-scale clustered sensor networksis proposed by Heejo Lee et al [5] the proposed scheme distributes the responsibility of key management to multiple nodes within clusters, avoiding single points of failure and getting rid of costly inter-cluster communication. The simulation result verifiesthe scalability and efficiency in terms of re-keying and compromised noderevocation. A Key Management Scheme for Body Sensor Networks is presented by Yee Wei Law et al [6] developed a new parameterized key management scheme that combines the best-suited cryptographic techniques in a seamless framework and named it KALwEN. KALwEN is user-friendly in the sense that it requires no expert knowledge of a user, and instead only requires a user to follow a simple set of instructions when bootstrapping or extending a network. One of KALwEN’s key features is that it allows sensor devices from different manufacturers,

which expectedly do not have any pre-shared secret, to establish secure communications with each other. KALwEN is decentralized, such that it does not rely on the availability of a local processing unit (LPU). KALwEN supports secure global broadcast, local broadcast and local (neighbor-to-neighbor) unicast, while preserving past key secrecy and future key secrecy.WalidBechkit et al [7] proposed a Highly Scalable Key Pre-distribution Scheme for Wireless Sensor Networks. Their proposed work provides good secure connectivity coverage they use for the first time of the unital design theory and show that the basic mapping from unitals to key pre-distribution allows to achieve extremely high network scalability. They propose an enhanced unital-based key pre-distribution scheme providing high network scalability and good key sharing probability. The analysis results show that proposed approach enhances considerably the network scalability while providing high secure connectivity coverage and good overall performances. Moreover, the obtained results show that at equal network size, our solution reduces significantly the storage overhead compared to main existing solutions.Mandicou Ba et al [8] proposed A Deterministic Key Management Scheme for Securing Cluster-Based Sensors Networks called DKS-LEACH, to secure LEACH protocol against malicious attacks.

3. Basic Requirements and Constrains for Key Management Techniques

Key management schemes are various methods that are used for a better maintenance of key distribution in WSNs. Basically a key management scheme must have the following properties:

1. The protocol must establish a key between all sensor nodes that must exchange data securely.
2. Node addition / deletion should be supported.
3. It should work in undefined deployment environment.
4. Unauthorized nodes should not be allowed to establish communication with network nodes.

Bounds or constrains for key management protocols

1. Battery power
2. Computational energy consumption
3. Communication energy consumption
4. Transmission range
5. Memory Requirement
6. Network constraints

4. PN Sequence Generator

PRBS or Pseudo Random Binary Sequence is essentially a random sequence of binary numbers. It is random in a sense that the value of an element of the sequence is independent of the values of any of the other elements. It is 'pseudo' because it is deterministic and after N elements it starts to repeatitself, unlike real random

sequences.

The basic PN-sequences are generated by using linear feedback shift-register and exclusive OR-gate circuits (figure 1).A binary {0, 1} shift-register sequence $f_s(t)$ is a sequence that satisfies a linear recurrence relation of the form Linear generator polynomial g(x) of degree $m > 0$

$$\sum_{i=0}^{r} f_i s(t+i) = 0, \qquad \text{for all } t \geq 0 \ \ldots\ldots (1)$$

Where $r \geq 1$ is the degree of the recursion; the coefficients f_i belong to the finite field $GF(2) = \{0,1\}$ where the leading coefficient $f_r = 1$. A sequence satisfying a recursion of the form in Eq. (1) is said to have characteristic polynomial

$$f(x) = \sum_{i=0}^{r} f_i x^i \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots (2)$$

Since an r-bit binary shift register can assume a maximum of 2^r different states, it follows that every shift-register sequence $f_s(t)$ is eventually periodic with period $n \leq 2^r$, i.e.

$$s(t) = s(t+n), \qquad for\ all\ t \geq N \ldots\ldots (3)$$

The maximum period of a shift-register sequence is $2^r - 1$, since a shift register that enters the all-zero state will remain forever in that state.

5. Proposed Algorithm:

The proposed key management algorithm uses the symmetric key encryption while considering initially individual keys are distributed by secured pre deployment operations [3].The whole algorithm can be explained as follows:

Let there be N numbers of mobile station/nodes (MS) in the network and one base station (BS) there can be many BS but for simplicity only one is considered.

We consider that the symmetric key encryption is used for data encryption and the encryption sequence is E bits long.

It is known that to generate an E bit long PN sequence required shift register length (L) can be given by

$$L = log_2(E) \ldots\ldots\ldots\ldots (4)$$

However we need at least on feedback circuit with XOR gate. The complete configuration of PN sequence generator in the proposed technique is defined by N bit (where $N = L$) binary sequence where the ones indicate the locations of input connection location of XOR gate.

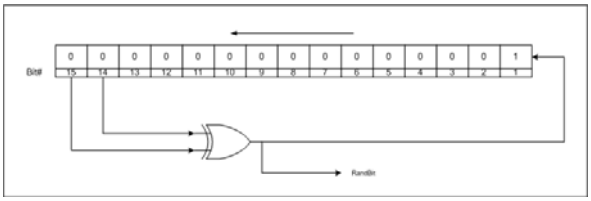

Figure 1: PN sequence generator

For example the configuration representation for the system shown in figure 1 can be defined as:

1	1	0	0	0	0	0	0	0	0	0	0	0	0	0

Figure 2: configuration bits for PN sequence generator.

While the initial states of the register can be defined by another N bit binary sequence as:

0	0	1	0	1	0	0	1	1	0	0	0	0	1	0

Figure 3: initial states for PN sequence generator.

Hence required bits to be transmittedfor each node for both keys (individual and group) can be given as:

$$T_b = 2 * log_2(E_i) + 2 * log_2(E_g) \dots\dots\dots (5)$$

Where E_i and E_g are length of individual and group keys respectively.

However the required bits to be transmitted for dynamic key updating is further reduced by only sending the number of rotation from the previous initial states and can be given as:

$$T_b = log_2(log_2(E_g)) \dots\dots\dots (6)$$

1	0	0	0	1	0	1	0	0	1	1	0	0	0	0

Figure 4: Initial states rotation of figure 3 by 2 digits.

The proposed algorithm reduces the bits overhead because now only a few bits data are required to update all the keys, and broadcasting can also reduce the individual key updating.

6. Simulation Results

The proposed algorithm is simulated using MATLAB for the following scenario:

Table 1: Simulation Scenario Configuration

Properties	Values
Number of Nodes	50
Individual Key (IK) Length	128 bits
Group Key (GK) Length	128 bits
IK Configuration	16 bits
GK Configuration	16 bits
GK Rotation	8 bits
Nodes Arrival, Leaving Probability	0.5
Simulation Time	100 seconds

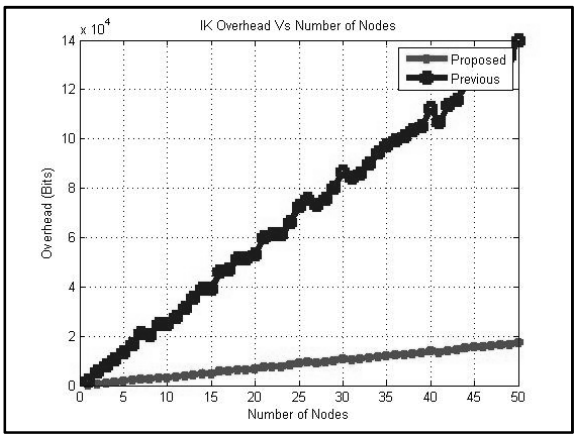

Figure 5: comparison of bits overhead required for updating IK for different number of nodes. The simulation result shows that the proposed algorithm reduces the overhead by 7 times.

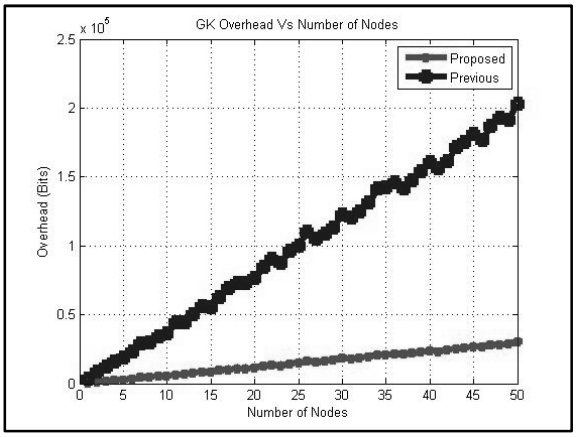

Figure 6: comparison of bits overhead required for updating GK for different number of nodes. The simulation result shows that the proposed algorithm reduces the overhead by 5 times.

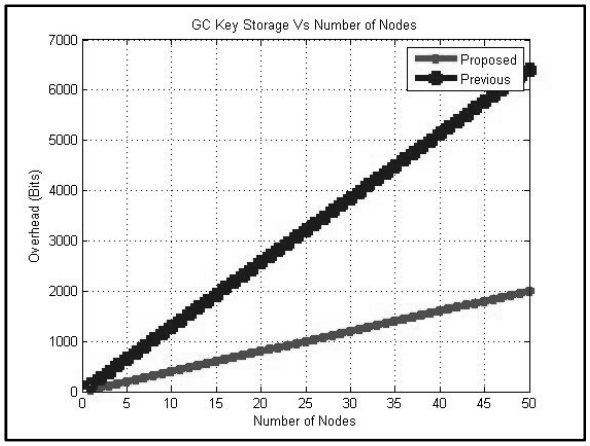

Figure 7: comparison of bits storage required for GK for different number of nodes. The simulation result shows that the proposed algorithm reduces the memory requirement by 3 times.

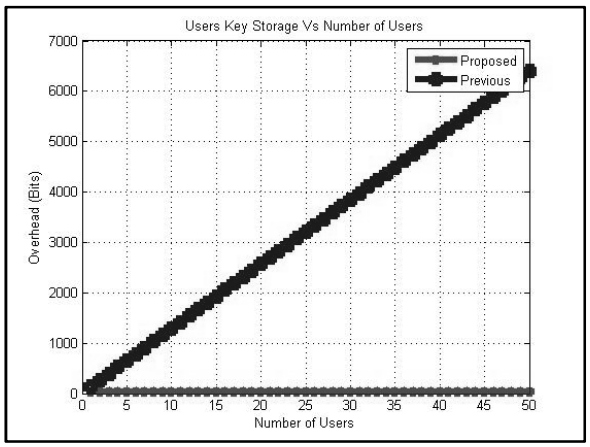

Figure 8: comparison of bits storage required for IK for different number of nodes. The simulation result shows that the proposed algorithm only small memory to manage IK.

7. Conclusion

In this paper we presented an efficient key management technique for securing communication in WSN and the simulation is performedfor analysis of proposed technique. The simulation results show that the overhead imposed by the proposed algorithm is very less compared to standard algorithm (LEAP). The proposed algorithm also reduces the energy consumption and the end-to-delayeven if the number of sensor nodes increases in the network.Furthermore, by using a limited number of keys (only configuration and initial states) minimize the memory usage in contrast to the previous works.As future works, we can consider the case wherea sensor node and/or the base station are affected by amalicious node.

References

[1] Xing ZhangJingsha He and Qian Wei "EDDK: Energy-Efficient Distributed Deterministic Key Management for Wireless Sensor Networks",EURASIP Journal on Wireless Communications and Networking Volume 2011, Article ID 765143, 11 pages.

[2] BimingTian, Song Han, SaziaParvin, Tharam S. Dillon "A Key Management Protocol for Multiphase Hierarchical Wireless Sensor Networks", 2010 IEEE/IFIP International Conference on Embedded and Ubiquitous Computing.

[3] Qi Mi, John A. Stankovic and RaduStoleru "Practical and secure localization and key distribution for wireless sensor networks", Ad Hoc Networks archive Volume 10 Issue 6, August, 2012 Pages 946-961, Elsevier Science Publishers.

[4] Shucheng Yu, KuiRen and Wenjing Lou "FDAC: Toward Fine-grained Distributed DataAccess Control in Wireless Sensor Networks", Parallel and Distributed Systems, IEEE Transactions on (Volume:22 , Issue: 4), April 2011.

[5] Muhammad Khaliq-ur-RahmanRaazi Syed, Heejo Lee, Sungyoung Lee and Young-Koo Lee "MUQAMI + : a scalable and locally distributed key management scheme for clustered sensor networks", Ann. Telecommun. Institut TELECOM and Springer-Verlag France 2009.

[6] Yee Wei Law, GiorgiMoniava, Zheng Gong, Pieter Hartel, MarimuthuPalaniswami "KALwEN: A New Practical and Interoperable Key Management Scheme for Body Sensor Networks", Security and communication networks, 4 (11). pp. 1309-1329. ISSN 1939-0122, 2010.

[7] WalidBechkit, YacineChallal, AbdelmadjidBouabdallah and VahidTarokh "A Highly Scalable Key Pre-distribution Scheme for Wireless Sensor Networks", IEEE Transactions on Wireless Communications 12, 2 (2013) 948-959.

[8] Mandicou Ba, IbrahimaNiang, BambaGueye and Thomas Noel "A Deterministic Key Management Scheme for Securing Cluster-Based Sensors Networks", Embedded and Ubiquitous Computing (EUC), 2010 IEEE/IFIP 8th International Conference on11-13 Dec. 2010.