EPKM:An Efficient and Practical Key Management Scheme for Hierarchical Wireless Sensor Networks

Yang Wei, Qi Yue , Luo Xinqiang , Wang Qin
School of Computer and Communication Engineering
University of Science and Technology Beijing
Beijing, China
ustbyangwei@139.com

***Abstract*—Wirless sensor networks are becoming increasingly attactiv for military,wildlife monitoring and other applications. Usually the sensor nodes are deployed in a dangerous and untrusted area.Therefore,network security becomes very important.Key management is the core areas of the security. In this paper,we describe EPKM(Efficient and Practical Key Management Scheme),a key management protocol for the hierarchical wireless sensor networks. EPKM adopts the main idea of multiple keying mechanism which includes key establishment and updating procedures.It supports four types of keys for each node–an individual key shared with the gateway, a data encryption key shared with another node, a cluster key shared with the cluster head,and a global key that is initially preloaded by all the nodes. Compared to other key management schemes,our scheme used for establishing and updating these keys is efficient and practical as well as low storage and communication.**

Keywords-wireless sensor networks; key management; hierarchical

I. Introduction

A Wireless Sensor Network (WSN for short) is composed of hundreds, even thousands of small sensor nodes, and can be widely used in many applications, for instance, military sensing, environment monitoring, medica treatment and industrial monitoring. WSN are usually deployed in a dangerous and untrusted area. Hence, security mechanism becomes very important for the operation of sensor applications [1]. Due to the characteristics of WSN, it has such limitations as limited battery power, finite computing and memory capability. Public key algorithms are typically considered to be too computationally intensive for resource constrained WSN nodes [2]. Thus, most of key management protocols for WSN are often based on symmetric key algorithms.

In this paper, we design a multiple keying mechanism for the hierarchical WSN based on symmetric key algorithms.It is suitable for meeting different security requirements. It supports four types of keys for each node–an individual key shared with the gateway, a data encryption key shared with another node, a cluster key shared with the cluster head,and a global key that is initially preloaded by all the nodes.The process of establishing and updating these keys is discussed in detail. Compared to other key management schemes,our scheme used for establishing and updating these keys is efficient and practical as well as low storage and communication.

The paper is organized as follows. Some existing key management approaches are reviewed in Section II. In Section III, details of EPKM approach are presented. In Section IV, the security and performance of EPKM are analyzed. Finally, it concludes the paper and outlines our future research plan.

II. Related Work

In order to meet the need of practical applications,researchers have proposed a number of key management schemes for the hierarchical WSN. For example, Sencun et al.[3] proposed LEAP+(Localized Encryption and Authentication Protocol) scheme.It used different keys to secure different types of communication messages in the WSN.Also it supported Inter-node Traffic Authentication.It can lead to prevent the difficulty of launching many security attacks.But the entire network would suffer a severe loss if the aninitial key was exposed to an attacker.Jang et al.[4] proposed a Time-Based scheme.It proposed a secure scheme with a new notion of probabilistic time intervals.But its assumption of security in the initial deployment phase is not viable in many cases.Jia et al.[5] proposed a novel key management scheme.It adopted the main idea of threshold secret sharing scheme to divide the master key into several sub keys.It can provide strong security.But it increased computation complex.

Though these schemes have their own advantages, they can not apply to all situation in the hierarchical WSN.Our scheme provide different security requirements according to different message exchanged in WSN. It supports four types of keys for each node based on multiple keying mechanism. Furthermore, our scheme is very efficient and practical.

III. Key Management Scheme

Before introducing our protocol, we must describe some assumptions regarding the sensor network scenarios in which our protocols will be used:

(1) The sensor network is static and the topology is a hierarchical network .

(2) The gateway nodes is located in a well protected place and supplied with long-lasting power.It have sufficient memory resources .Also it is capable of detecting intrusion.

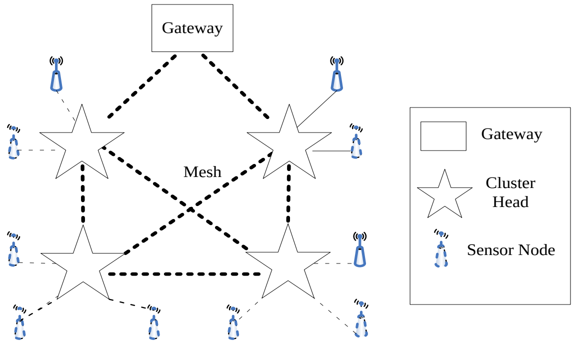

Figure 1. Hierarchical wireless sensor network model

A. *Overview*

We adopt the sensor network model proposed by Wireless Networks for Industrial Automation (WIA)[6].As illustrated in Fig.1, Our network supports a hierarchical network topology that is hybrid star and mesh. The first level of the network is in mesh topology where gateway nodes(GW) and cluster head nodes(CH) are deployed. The second level of the network is in star topology where cluster head nodes(CH) and sensor nodes(SN) are deployed.

GW is a control center and used to connect the WSN with the other network. CH is responsible for constructing the star network and management of all the nodes in the cluster. Meanwhile, CHs can communicate with each other and forwarding data between its cluster members and the BS. SN can collect field data and send the data to its CH. It only communicate with its CH directly.

The packets exchanged by nodes in WSN can be classified into several categories, e.g. beacons packets , control packets ,data packets and broadcast packets. Different type of packets requirements for Different security which depend on the category it falls in.

Global Key(KG) : Every node is initially preloaded with it before the network deployment. It is a globally shared key that is used by the GW and CH for encrypting securing broadcast messages.For example, A new node which wants to successfully join to the network have to listen to beacons from the GW or CH according to IEEE 802.15.4 standard[7].So only the legal node can decrypt the beacons and successfully join to the network.However, since the KG is shared among all the nodes, we have to design an effcient rekeying mechanism i for updating it if a compromised node is revoked.

Individual Key (KI): Every node has a unique key that shares with the GW. The key is used for secure communication between a node and the GW. For example, a node may send an alert data to the GW if it observes any abnormal network conditions. Similarly, the GW can use the key to encrypt some sensitive information, e.g. special command or keying material.

Data Encryption Key(KED): In the EPKM, it supports a hierarchical network topology that is hybrid star and mesh. Every node which in mesh topology shares a KED with its immediate neighbors.However,the SN only shares a KED with its CH. The keys are used to protect data and check integrity during the data transport. For example,a CH can use its KED to secure the distribution of its KC to its SN, or to secure the transmissions messages to its neighbors CH.

Cluster Key(KC): In the EPKM,The second level of the network is in star topology where cluster head nodes(CH) and sensor nodes(SN) are deployed.A KC is a key shared by a CH and all its SN, and it is mainly used for securing locally broadcast messages. Although we can use KED to encrypt the messages to every SN,it may cost to much energy consumption. Similarly,our purpose is for saving energy consumption in WSN.

Descriptions of the notations involved in this paper are listed as Table I.

TABLE I. NOTATION USED IN OUR SCHEME

Notion	Description
GW	gateway node
CH_i	cluster head node i
S_i	the sensor node i
KG	Global Key
KI_i	Individual Key of device i
$K_{ED(i,j)}$	Data Encryption Key shared between device I and j
KC	Cluster Key
MAC(K,M)	message authentication code for M using key K
N_A	A nonrepeating value,such as an increasing counter
E(K,M)	the symmetric encryption for M using key K
||	concatenation operator

B. *Key establishment*

Before network deployment, each node is initially preloaded with an initial KG , 64-bit Unique Identifier address and CBC-MAC(Cipher Block Chaining-Message Authentication Code) function.

1) Establishing KI: Each node has a unique key that it shares with the GW. It is generated as follows:KI=MAC(KG,M).Here M is a node 64-bit Unique Identifier address combin with GW 64-bit Unique Identifier address.KG is pre-loaded into each node.So the node and GW can computer the same KI use the MAC function.Here MAC is the abbreviation of CBC-MAC function.

2) Establishing KED: Every node shares a KED with its immediate neighbors.However,the SN only shares a KED with its CH.The keys are used to protect data during the data transport.

A new CH that wants to establish KED shall undergo the following steps.

a) The GW and Online CH periodicity broadcast beacon(BE) frame according to IEEE 802.15.4 standard.The new CHi keeps scanning the available channels until it has successfully received BE from GW or Online CH.It then tries to discover its one-hop neighbors.

$$GW \rightarrow * : E(KG, BE \,||\, NA) \,||\, MAC(KG, E(KG, BE||NA))$$

$$CH \rightarrow * : E(KG, BE \,||\, NA) \,||\, MAC(KG, E(KG, BE||NA)\,)$$

b) For example,The new CH$_i$ discover two neighbors CH$_j$ and CH$_k$.It chooses an CH$_j$ as the temporal parent.It make use of the KI to encrypt the neighbors ID and N$_A$ then transmit to the CH$_j$.The CH$_j$ will forward a joining network request to the GW.

$$CH_i \rightarrow CH_j: E(KI_i, CH_i \,||CH_j\, ||CH_k \,||\, N_A) \,||\, MAC(KI_i,E(KI_i, CH_i \,||\, CH_j \,||\, CH_k \,||\, N_A)\,)$$

$$CH_j \rightarrow \ldots \rightarrow GW: E(KI_i, CH_i \,||\, CH_j \,||\, CH_k \,||\, N_A) \,||\, MAC(KI_i, E(K_{Jj}, CH_i \,||\, CH_j \,||\, CH_k \,||\, N_A)\,)$$

c) The GW receives the joining request from the CH$_i$.Then it have to complete authentication process.if the CH$_i$ has been authenticated to be a legal device.The GW will allocation of network resources and distributthe KED to it.Also,the neighbors CH$_j$ and CH$_k$ will receive the KED.

$$GW \rightarrow CH_i : E(KI_i, K_{ED(CHi,\, GW)} \,||\, \ldots|| \,K_{ED(CHi,\, CHj)} \,||\, \ldots \,||\, K_{ED(CHi,\, CHk)} \,||\, N_A) \,||\, MAC(KI_i,E(KI_i, K_{ED(CHi,\, GW)} \,||\, \ldots||\, K_{ED(CHi,\, CHj)} \,||\, \ldots \,||\, K_{ED(CHi,\, CHk)} \,||\, N_A)\,)$$

$$GW \rightarrow CH_j : E(KI_j, K_{ED(CHi,\, CHj)} \,||\, N_A) \,||\, MAC(KI_j,E(KI_j, K_{ED(CHi,\, CHj)} \,||\, N_A)\,)$$

$$GW \rightarrow CH_k : E(KI_k, K_{ED(CHj,\, CHk)} \,||\, N_A) \,||\, MAC(KI_k,E(KI_k, K_{ED(CHj,\, CHk)} \,||\, N_A)\,)$$

A new SN that wants to establish KED shall undergo the following steps.

a) The Online CH periodicity broadcast BE frame.The new S$_a$ keeps scanning the available channels until it has successfully received BE from Online CH.For example, The new S$_a$ discover CH$_i$ as the CH.The new S$_a$ make use of the KI to encrypt the joining request and send to CH$_{i.}$.

$$CH_i \rightarrow * : E(KG, BE \,||\, N_A) \,||\, MAC(KG, E(KG, BE \,||N_A)\,)$$

$$S_a \rightarrow CH_i: E(KI_a, S_a \,||\, N_A) \,||\, MAC(KI_a, E(KI_a, S_a|| \,N_A)\,)$$

b) The Online CH$_i$ receive the joining network request.Then it will forward encrypted message to the GW.

$$CH_i \rightarrow CH_j \rightarrow \ldots \rightarrow GW :E(KI_a, S_a \,||\, N_A) \,||\, MAC(KI_a, E(KI_a, S_a|| \,N_A)\,)$$

c) The GW receives the joining request from the S$_a$.Then it have to complete authentication process.If the S$_a$ has been authenticated to be a legal device.The GW will allocation of network resources and distribut the KED to it.Also,the CH$_j$ and S$_a$ will receive the KED.

$$GW \rightarrow CH_i :E(KI_i, K_{ED(CHi,Sa)} \,||\, N_A) \,||\, MAC(KI_i, E(KI_i, K_{ED(CHi,Sa)} \,||\, N_A)\,)$$

$$GW \rightarrow S_a : E(KI_a, K_{ED(CHi,Sa)} \,||\, N_A) \,||\, MAC(KI_a, E(KI_a, K_{ED(CHi,Sa)} \,||\, N_A)\,)$$

3) Establishing KC: A KC is a key shared by a CH and all its SN in the same cluster.We use a very straightforward way to establish the key.The cluster head CH$_i$ wants to establish a KC with all its SN.The CH$_i$ generates a random KC, then encrypts the key with the KED between CH$_i$ and SN and then transmits the KC to each SN. Here,we take CH$_i$ and S$_a$ for example.

$$CH_i \rightarrow S_a : E(K_{ED\ (CHi,Sa)}, KC \,||\, N_A) \,||\, MAC(K_{ED\ (CHi,Sa)}, E(K_{ED\ (CHi,Sa)}, KC||N_A)\,)$$

Node S$_a$ receive the message and decrypts the key KC. When one of the SN addition and deletion, the CH generates a new KC and transmits to all the remaining SN in the same way.

C. Key updating

Usually,the networks need periodic key updating mechanism to improve the security.Also,when a node is added or deleted ,it need to update the key.

1) Periodic Key updating: When the network exists for a certain period,it will start periodic key updating mechanism. The ISA100.11a which is a standard draft of industrial wireless measurement and control systems suggest that maximum lifetime of the keys is 48.5 days[8]. Surely,the lifetime of keys is configurable according to the application.In the EPKM,it suggest periodic update the KG and KC.The periodic updating the KG is determined by the GW.The new KG is encrypted by the KI,and the encrypted new KG is distributed to the network device by the GW.The periodic updating the KC is determined by the CH.The new KC is encrypted by the KED,and the encrypted new KC is distributed to all the SN in the same cluster.

2) Node Addition: When a SN want to join the network,it fristly choose an Online CH.The Online CH receive the joining network request. Then it will forward encrypted message to the GW.The GW will allocation of network resources and distribut the KED after it been authenticated to be a legal device.Also,The KC have to be updated in order to ensure backward confidentiality.The process of KC updating is the same as the establishing KC.

3) Node Deletion: In the EPKM,it considers two case about node deletion.One is the SN deletion,the other is CH deletion.When one of SN deletion,the GW can detect the case as the GW periodically collects the SN health report.In order to ensure forward confidentiality,the GW sends key updating command to the CH which is the head of SN.The CH receive the command and trigger thekey update mechanism immediately.The process is the same as the establishing KC.When one of CH deletion,the GW has a detection mechanism to know the case.If network have redundant CH,it can quick use redundant CH after detecting the CH deletion.In order to ensure forward confidentiality,it only have to update the KC.The process is the same as the establishing KC.However,most of WSN do not have redundant CH. For example,the S$_a$ and S$_b$ have be distributed to CH$_i$ using the clustering algorithm.The process is illustrated as follows.

a) The GW send command to tell the other CH.The other CH delete the key relation to it and do not trust the message from it.

b) The GW distribute its SN among the remaining CH.It should be noted that the CH distribute the SN using some existing clustering algorithm.The GW distributes the new KED to the CH$_i$,Sa and Sb.

$$GW \rightarrow CH_i :E(KI_i, K_{ED(CHi,Sa)}||K_{ED(CHi,Sa)}||N_A) \,||\, MAC(KI_i, E(KI_i, K_{ED(CHi,Sa)} \,||\, K_{ED(CHi,Sa)} \,||N_A)\,)$$

$$GW \rightarrow S_a : E(KI_a, K_{ED(CHi,Sa)} \,||\, N_A) \,||\, MAC(KI_a, E(KI_a, K_{ED(CHi,Sa)} \,||\, N_A)\,)$$

$$GW \rightarrow S_b : E(KI_b, K_{ED(CHi,Sb)} \parallel N_A) \parallel MAC(KI_b, E(KI_b, K_{ED(CHi,Sb)} \parallel N_A))$$

c) The KC have to be updated in order to ensure backward confidentiality beacuse of the SN addition.

$$CH_i \rightarrow S_a : E(K_{ED\ (CHi,Sa)}, KC \parallel N_A) \parallel MAC(K_{ED\ (CHi,Sa)}, E(K_{ED\ (CHi,Sa)}, KC \parallel N_A))$$

$$CH_i \rightarrow S_b : E(K_{ED\ (CHi,Sb)}, KC \parallel N_A) \parallel MAC(K_{ED\ (CHi,Sb)}, E(K_{ED\ (CHi,Sb)}, KC \parallel N_A))$$

IV. Security And Performance Analysis

This section analyzes security and performances of the keying mechanisms.It can provide sufficient security and achieve well performances.Also, the results of simulation show that our scheme have lower storage than LEAP+.

A. Security analysis

In this section, we analyze the security of the keying mechanisms in EPKM.Every node is initially preloaded with a KG. So only the legal node can use it to successfully join the network. It prevents some illegal node to access. Every node has a unique key KI that shares with the GW. It can ensure secure communication between a node and the GW. So,any SN's compromise won't affect the secure communication between the other SN and CH.The adversary can not attack the whole network even though they obtaining the key.The GW distributes the KED to nodes by using of the KI to encrypt.So the KED is Secure.The KC is randomly generated and is distributed by using of the KED. The adversary can not easy to get it.It ensure secure the locally broadcast messages.In the node addition,The KC have to be updated in order to ensure backward confidentiality. The key updating mechanism is discussed in detail toin order to forward confidentiality.Conclusively, our scheme can provide sufficient security and can achieve perfect resilience.

B. Performances analysis

1) Storage cost analysis: In the EPKM,a node needs to keep four types of keys.The SN only storage one KG,one KI,one KED and one KC.The CH storage one KG, one KI, one KC and lots of KED. The number of KED is according the network size and the average number of node in a cluster.e.g. the network size is N and the average number of node in a cluster is B, the average number of keys for a CH have to storage is B+N/B+2. Compared to other key management schemes LEAP+,it have to storage 3B+2 keys. As shown in Fig.2,our scheme have lower storage than LEAP+ as the number of node in a cluster increasing.

2) Communication cost analysis: For updating the KC,The CH have to send it to all of SN in the cluster.The average number of keys a CH transmitsis equal to B-1 for a cluster of size B.For updating the KG,The GW have to send it to all of nodes in the network.So,the average number of keys the GW transmitsis equal to N for a network of size N.The CH have toforward the key message to the SN.The average number of keys a CH transmitsis also equal to B-1 for a cluster of size B.The average cost is not very large as the KG is periodic updating.

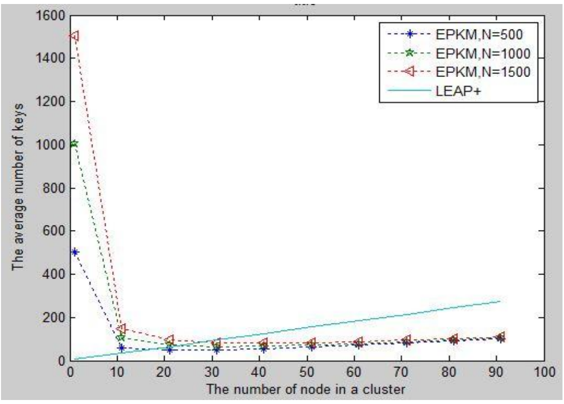

Figure 2. The average number of keys for CH

V. Conclusion

In this paper,we propose EPKM scheme for hierarchical WSN.It adopts the main idea of multiple keying mechanism,design four types of keys for each node according to different message exchanged.The key establishment and key updating procedures used by EPKM are storage and communication effcient.Also it has strong security and perfect practicability.In our further research, we are going to improve its security to defend against various attacks.

Acknowledgment

The paper is sponsored by the National High Technology Research and Development Program of China (863 Program) (No. 2011AA0401), National Natural Science Foundation of China (No. 61003251).

References

[1] Kavitha T, Sridharan D. Security vulnerabilities in wireless sensor networks: A survey[J]. Journal of information Assurance and Security, 2010, 5(1): 31-44.4

[2] Perrig A, Stankovic J, Wagner D. Security in wireless sensor networks[J]. Communications of the ACM, 2004, 47(6): 53-57.

[3] Zhu S, Setia S, Jajodia S. LEAP+: Efficient security mechanisms for large-scale distributed sensor networks[J]. ACM Transactions on Sensor Networks (TOSN), 2006, 2(4): 500-528.

[4] Jang J, Kwon T, Song J. A time-based key management protocol for wireless sensor networks[M].Information Security Practice and Experience. Springer Berlin Heidelberg, 2007: 314-328.

[5] Hu J, Bai E, Yang Y. A novel key management scheme for hierarchical wireless sensor networks[C].Communication Technology (ICCT), 2010 12th IEEE International Conference on. IEEE, 2010: 526-529.

[6] Liang W, Zhang X, Xiao Y, et al. Survey and experiments of WIA‐PA specification of industrial wireless network[J]. Wireless Communications and Mobile Computing, 2011, 11(8): 1197-1212.

[7] LAN/MAN Standards Committee. Part 15.4: wireless medium access control (MAC) and physical layer (PHY) specifications for low-rate wireless personal area networks (LR-WPANs)[J]. IEEE Computer Society, 2006.

[8] International Society of Automation. (2009). Wireless Systems for Industrial Automation: Process Control and Related Applications, ISA-100.11a-2009. [Online]. Available: http://www.isa.org