ISSN 2229-5518

Dynamic key establishment and management to improve the scalability in heterogeneous sensor networks (HSN)

Premamaydu B, Venkatarao K, Suresh varma P

Abstract-Key management is the most important in wireless sensor network to achieve secure data transmission between nodes in the wireless sensor networks. However, sensor nodes have most insufficient resources in terms of hardware, power, processing capacity, storage capacity. As a result, the key management and distribution of keys in the network could be an efficient in all aspects. This paper address the efficient key management method uses the dynamic key generation schemes for heterogeneous sensor networks (HSN). The proposed scheme preloads a one way collision-resistant hash function into the base station, cluster heads and sensor nodes. All the nodes in the network including cluster heads generate their key chains. The pairwise keys establish by cluster heads and cluster sensor nodes and group keys to provide the confidentiality over the data transmission in the network which are preloaded by the base station. This scheme addresses efficiency in number of keys, storage space required for sensor nodes, scalability and key revocation in the network.

Key Terms- Key management, Heterogeneous sensor networks, Scalability, rekeying, wireless connectivity, communication overhead.

1. Introduction

A wireless sensor networks build with a large number of sensors, which are equipped with batteries, sensing, communication unit, data processing and radio communication unit. At present any real time applications implementing on wireless sensor networks, like home automation, environment monitoring, military or security areas, targeting and target tracking systems, agriculture monitoring system and battlefield surveillance. However all the applications need protection in all the level of the sensor network.

Key management is the mechanism to provide the security in all the levels of the wireless sensor networks. Since sensor nodes in WSNs have constrains in their computational power and memory capability and security. The solutions of traditional networks like computer networks, ad hoc networks, and wired networks are not suitable for WSNs. The goal of key management in WSNs is to solve the problem of creating, distributing and protecting those secret keys. Hence, the feasible and reliable techniques for key management and distribution of these keys are of major importance for the security in WSNs.

Due to their importance, numerous key management schemes have been introduced or proposed for WSNs and many researches are proposed the different key management systems [2, 3, 4, 6]. Depending on the ability of the key management scheme that can be classified into two different categories: Static and Dynamic. The static key management, the keys are fixed for the entire life of the network. This idea may increase the probability of attacks significantly. Instead, in dynamic key management, the keys used for cryptographic operations are modified throughout the lifetime of the sensor network. Dynamic key management is the most suitable key management in sensor networks. Dynamic key management schemes adopt many processes form the traditional network key management, but those processes are light weight in terms of processing, consuming memory and power, and computing needs. They perform rekeying either periodically or on demand as needed by the network. Since the keys of compromised sensor nodes are revoked in the rekeying phase. The dynamic key management schemes enhance the network survivability, stability, scalability and resilience of network dynamically.

- Premamayudu B is currently pursuing Ph.D. in Computer Science and Engineering in JNT University, Kakinada, India, PH-919440006478. E-mail: prem_it@vignanuniversity.org .
- Venkata rao is working as Prof. and HOD Department of CSE, Vignan's Institute of Information Technology, Visakhaptnam (Dt), Andhra Pradesh, India, E-mail:vrkoduganti@gmail.com.
- Suresh Varma p is currently working as Dean CDC & Professor, Adikavi Nannaya University, Rajahmundry, W. Godavari (Dt), Andhra Pradesh, India. E-mail: vermaps@yahoo.com.

2. Related work

Eschenauer and Gligor[2] first introduced a key management procedure for sensor networks based on probabilistic key predistribution. Chan et al. [8] extended this scheme and improved the metrics of key management. Liu et al. [9] proposed two key distribution schemes based on bivariate polynomials. They use the random subset assignment scheme and key predistribution scheme in which the key pool contains multiple instances of selected polynomial. Oliveria et al. [10] proposed random key predistribution for secure message and data communication in hierarchical (Cluster-based) protocols such as LEACH. Du et al. [3] implemented the asymmetric predistribution method for heterogeneous sensor networks which gives tuff security with less complexity and storage space enough for more number of keys. Liu et al. [11]

ISSN 2229-5518

propose a complete framework for key management in distributed wireless networks and heterogeneous wireless sensor networks. Bulusu et al. [12] propose two key predistribution based schemes for heterogeneous networks which contain the static and mobile sensor nodes.

3. Proposed Method

This paper proposes a Dynamic key management that is designed for heterogeneous sensor networks (HSNs). Each cluster head generates its own key-chain, which encrypts messages and communicates with the other sensor nodes in the cluster. In this architecture, each cluster consists of several sensor nodes and cluster head. Many clusters and a base station form the heterogeneous sensor networks. Fig. 1 shows the architecture of heterogeneous sensor networks (HSNs).

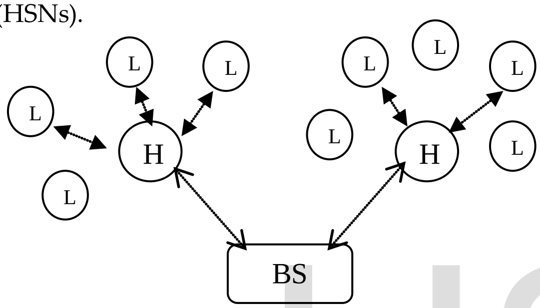

Fig. 1: Architecture of heterogeneous Sensor Networks (HSNs)

All the nodes are randomly distributed in the environment. They are static and their locations are identified using any one localization technique.

3.1 Initialization Phase: the Base Station generates a very large key pool of size $S \cong 2^{20}$ before deployment of sensor nodes in the network. The base station selects the distinct key for each cluster head (H-Sensor), which is referred as HK. After that Base Station generates the sub key $K_{sub}=HK \oplus R_s$ using HK and random number R_s. Using sub key K_{sub} and $R_1 \sim R_n$ to generate key chain with n keys for each H-sensor as given below

$K_{n-1}=(K_{sub} \oplus R_n)$

$K_{n-2}=(K_{n-1} \oplus R_{n-1})$

.

.

.

.

$K_1=(K_2 \oplus R_2)$

$K_0=(K_1 \oplus R_1)$

Hence, each H-sensor will get the unique key chains, Ks and random numbers $R_1 \sim R_n$ from Base Station Bs. All the nodes the network store the same hash function and temporary session key K_T. Here session and HK are not same in the Cluster Head. All the generated stuff for each sensor node will preload from Base Station through a secure channel before deployment.

3.2 Pairwise Key Establishment

Step 1: H-sensor HID_j broadcast the sample message to the entire cluster L-Sensors using the maximum power. The position of H-Sensor and random number R_H is encrypted by session key K_T. The format of the sample message is as follows.

HID_j ǁ sample message ǁ Position of the H-Sensor ǁ $\{R_H\}$

Step 2: The L-Sensor LID_i may receive one or more sample message offers from H-Sensors. The LID_i sensor selects an H-Sensor as its cluster head based on the signal strength of message and distance of H-Sensor to it. L-Sensor backups all other H-Sensors information which are offer the sample messages. These H-sensors are used in case the selected H-Sensor is disabled or compromised. After selecting the H-Sensor, L-Sensor LID_i generates a pairwise key $LK_{ij}=\{H(R_H \parallel LID_i)\}K_T$ and send to the H-sensor in the following format

HID_j ǁ replay message ǁ position of the LID_i ǁ $\{MAC(LK_{ij}) \parallel LID_i\}K_T$

Step 3: After getting the replay message from the L-Sensor LID_i, the H-Sensor HIDj generates the pairwise key $HK_{ij}=\{H(R_H \parallel LID_i\}K_T$. if $MAC(LK_{ij})=MAC(HK_{ij})$ is satisfied, then the H-Sensor authenticate validity of the L-Sensor LID_i. Hence $HK_{ij}=LK_{ij}$ becomes the pairwise key between HID_j and LID_i. This key is used to establish confidentiality between cluster head and sensor node over the data transmission.

3.3 Group Key Establishment

Step 1: The H-Sensor HID_j selects the group key K0 in the cluster and transmits using the associate pairwise key of L-Sensor. The format of Group key message is as follows

HID_j ǁ position of the L-Sensor ǁ $\{K_0\}LK_{ij}$

Step 2: After identifying all the clustering sensor nodes, the H-Sensor HID_j broadcast the ID of members to all the sensor nodes using the Group key K0. The format of members ID message as follows.

HID_j ǁ {list of all neighboring nodes ID}K_0

3.4 Normal Operation of HSNs: In the proposed method, the BS generates the pairwise keys and groups keys between BS and Cluster Heads. This process is similar to the above process which is used between cluster heads and sensor nodes. For example, in this scheme the Base station Generated HKj as a pairwise key and K_{BS} as Group key for all cluster heads.

We address two normal operations in the Heterogeneous wireless sensor network. Operation 1 is that BS asks the H-Sensors to get the data from all the sensor nodes. Operation 2 is that BS asks the H-Sensor to get the data from particular L-Sensor node.

Operation 1:
Step 1: BS Sends the request message to all its H-Sensors using group key K_{BS}
BS || request message { MAC(M) || M} K_{BS}
Step 2: H-Sensor HID_j forwards the request message to all cluster nodes using Group key K_i(i.e K_0)
HID_j || request message {MAC(M) || M}K_i
Step 3: Each L-Sensor replys the data to its cluster head using Group key K_i
LID_i || reply message { MAC(M || C) || M || C}K_i
Step 4: Finally H-Sensor HID_j sends gathered data from all L-Sensors to Base Station Using Group key K_{BS}
HID_j || {MAC(C_1 || C_2 || C_3….)|| C_1 || C_2 || C_3…..}K_{BS}
Operation 2:
Step 1: Base Station BS Sends request message to a particular Cluster Head using pairwise key HKj
BS || request message { MAC(LID_i) || LID_i}HK_j
Step 2: H-Sensor HID_j forward the request message to a specific L-Sensor using pairwise key KH_{ij}
HID_j || request message || {MAC(M) || M}HK_{ij}
Step 3: L-Sensor LID_i sends the data to a requested cluster head HID_j using pairwise key LK_{ij}
LID_i || {MAC(M||C)||M||C}LK_{ij}
Step 4: H-Sensor HID_j forward the received data from L-Sensor LID_i to Base Station using pairwise key HK_j
HID_j || {MAC(M || C) || M || C}HK_j

4 Adaptability of the Proposed Scheme

Our proposed Scheme addresses the adaptability of the Proposed Scheme, which includes the Key Revocation (resiliency), Adding new node (Scalability) and Extending the key chain.

4.1 Key Revocation: Base Station has the capability of identifying compromised sensor nodes or adversary. When the BS identified the malicious sensor node, it broadcasts the malicious message to the entire H-Sensors using group key K_{BS}.
Malicious node message || {MAC(LID_x) || position of the node x || LID_x } K_{BS}
H-sensor HID_j will transmit the revocation message to all the members of its own cluster. After that, H-Sensor HID_j sends the revocation message to malicious sensor node using pairwise key. The old key of compromised sensor will be revoked with new key using new random number.
HID_j || revocation message || {R_{i+1}}LK_{xj}

4.2 Addition of a new node (Scalability): When a new node is deployed in the network, it needs to establish the pairwise and group keys with its cluster head. Firstly new L-Sensor node establishes the pairwise key with its H-Sensor node. Hence, H-Sensor forwards the group key of cluster using pairwise key. Before placing the new node in the environment, this new node preloads with hash function and session key K_T. After deployment of new node, Bs broadcast the addition of new node message to all H-Sensors.
Addition of new node || {MAC(LID_x) || LID_x || K_T}K_{BS}
In this method, L-Sensor LID_x placed randomly in the network. After that L-Sensor LID_x broadcast a request message to all its neighboring H-Sensor. One or more H-Sensors may give reply to the LID_x sensor. L-Sensor LID_x selects the one of H-Sensor as a cluster head based on the signal strength and distance of cluster head, other H-Sensors are make them as backup cluster heads. H-Sensor HIDJ will reply with random number R_H to the node x using K_T. Hence, H-Sensor j and L-Sensor x generates the pairwise key LK_{xj}=HK_{xj} using RH, LIDx and K_T. After generating pairwise key LK_{xj}, H-Sensor sends the group key K_0(i.e K_i) to the L-Sensor LID_x using LK_{xj}. Finally H-Sensor broadcast the neighbor message to all the members of the cluster once again.

4.3 Extension of key-chain: When all the keys in the key chain have been used in the cluster, still H-Sensor has sufficient power, it generates a new key-chain for the L-Sensor in the cluster. The H-Sensor HID_j uses the pairwise key LK_{ij} to send the new key for the L-Sensors. The format of the new extended key-chain message that H-Sensor j sends to the L-Sensor i is as follows
HID_j || position of L-Sensor || {MAC(k_0) || k_0}LK_{ij}

5. System Analysis

In our Experiment, they are 1000 L-Sensor nodes and 50 H-Sensors in the network. The ration between these two types is 20:1. The key-chain length of H-Sensor is 50 keys. L-Sensors gather the data from the environment and send to the H-Sensor nodes. Then H-Sensor nodes forward the data to Base Station.

5.1 The number of messages between the H-Sensor and L-Sensor (Communication overhead): In the proposed scheme, H-Sensor establishes a pairwise key with its L-Sensor. H-Sensor exchanges 2 messages with L-Sensor: One message offers the Random number; other receives the pairwise key from L-Sensor. L-Sensor exchanges 2 messages with H-Sensor: one message receives the Random number form the H-Sensor; other sends the pairwise key along with L-Sensor ID.
In the group key establishment, H-Sensor uses the pairwise key to transmit group key K_0 form the key-chain of H-Sensor. H-Sensor only sends to messages to the L-Sensor using pairwise key: one message for group key and other for broadcasting all members IDs to their neighbors in the cluster. Total number of messages required to establishing broadcast and unicast communication is 6 messages. This

number is very less compare with other key establishment methods of HSN. Hence, this scheme consumes very less power. This method will give the long life for the HSN.

Sensor Type	Communication	Pairwise key Establishment	Group key Establishment
H-Sensor	Transmitted	1	2
	Received	1	0
L-Sensor	Transmitted	1	0
	Received	1	0

Table 2: Number of messages required for key establishment

5.2 The Key Sizes: In the experiment environment, H-Sensor node has an average of 24+n Keys, where 20 keys for pairwise keys for its L-Sensors, 4 keys are HK, K_{BS}, K_T, K_{sub} and n is the length of the key-chain. The length of key-chain at most 50 keys in H-Sensor. Therefore, H-Sensor should store 77 keys. The L-Sensor needs only 3 keys, which are K_T, LK_{ij}, K_i (Session Key, Pairwise key, and Group key).

Type	L-Sensor	H-Sensor	Base Station
Keys	3	77	$S(2^{20})$
Hash Function	1	1	1

Table 3: The number of functions & keys required for each member of HSN

6. Conclusion

This paper proposes the dynamic pre key distribution in HSN. The network itself divides into the clusters and headed by one cluster sensor to manage cluster. Cluster heads can generate the key-chain. Cluster heads and their sensor nodes themselves generate the pairwise key and group key provide the secrecy in the data transmission. The key-chain consists of continuous keys, and each key is dependent. This makes it possible for the sensor node to confirm the validity of each key. Sensor nodes or cluster heads change the key, and then sensor nodes can confirm the identity of cluster head and the validity of new key. This scheme uses the hash function to avoid the data collision while making the compressions. Sensor nodes themselves calculating the group key with the help of preloaded keys and hash function which is stored at the time of deployment. This scheme improves the scalability of the scheme and reducing the memory requirements of sensor nodes and ensuring the key security.

References:

[1] Hu W, Tan H, Corke C, Shih WC, Jha S. Toward trusted wireless sensor networks. ACM Transactions on Sensor Networks 2010;7:5:1-25

[2] Eschenauer L, Gligor V. A Key management scheme for distribution sensor networks. Smart wireless sensor networks. In TechOpen;2010;p18:1-18:6

[3] Du W, Deng J, Han YS, Varshney PK, Katz J, Khalili A. A pairwise key predistribution scheme for wireless sensor networks. ACM Transactions on information and system security 2005:8(2):228-58.

[4] Kim JM, Cho TH. A*-based key tree structure generation for group key management in wireless sensor networks. Computer and communications. 2008:31:2414-9

[5] Zhang X, He J, Wei Q. EDDK:energy-efficient distributed deterministic key management for wireless sensor networks, EURASIP Journal on wireless communications and networking 2011:1-11

[6] Zhou B, Li S, Li Q, Suna X, Wang X. An efficient and scalable pairwise key predistribution scheme for sensor networks using deployment knowledge. Computer and communication 2009:32:124-33.

[7] Xiaobing He, Michael Niedermeier, Hermann demeer. Dynamic key management in wireless sensor networks: A survey. Journal of network and computer applications. 36(2013):611-622.

[8] H Chan, A Perrig, and D song. Random key predistribution schemes for sensor networks. Proceedings 9th ACM conference computer and communication security. November 2002. 41-47

[9] Liu D, Ning P, Li R. Establishing pairwise keys in distributed sensor networks. ACM Transactions Information Systems Security. 2005.8(1):41-77

[10] Oliveira LB, Worg HC, Bern M, Dahab R, Loureiro. A Random key distribution solution for security clustered sensor networks. 5th IEEE international symposium on network computing and applications. 2006.pp 145-154

[11] Perrig A, Szewczyk R, Tygar JD, Victorwen. Security protocols for sensor networks. Seventh annual conference on mobile computing and networks. July 2001

[12] Bulusu V, Durresi A, Paruchuri V, Durresi M, Jain R. Key distribution in mobile heterogeneous sensor networks. Global telecommunications conference. 2006:1-5