VOL. 10, NO. 4, MARCH 2015 ISSN 1819-6608
ARPN Journal of Engineering and Applied Sciences


www.arpnjournals.com

# SECURITY KEY MANAGEMENT AND AUTHENTICATION SCHEME FOR WIRELESS SENSOR NETWORKS

S. Jayapraba[1] and A.F.Sheik Hakkani[2]
[1]Department of MCA, Jayam College of Engineering and Technology, Bharathiyar University, Dharmapuri. Tamilnadu, India
[2]Department of MCA, Er.PMC TECH, Hosur. Periyar University,Tamilnadu, India.
E-Mail: jayaprabamca@gmail.com

**ABSTRACT**

Wireless Sensor Networks (WSN) is vulnerable to node capture attacks in which an attacker can capture one or more sensor nodes and reveal all stored security information which enables him to compromise a part of the WSN communications. Due to large number of sensor nodes and lack of information about deployment and hardware capabilities of sensor node, key management in wireless sensor networks has become a complex task. Limited memory resources and energy constraints are the other issues of key management in WSN. Hence an efficient key management scheme is necessary which reduces the impact of node capture attacks and consume less energy. In this study, we develop a cluster based technique for key management in wireless sensor network.

**Keywords:** wireless sensor network, cluster, key management, authentication.

## 1. INTRODUCTION

### 1.1. Wireless Sensor Network

A network comprising of several minute wireless sensor nodes which are organized in a dense manner is called as a Wireless Sensor Network (WSN). Every node estimates the state of its surroundings in this network. The estimated results are then converted into the signal form in order to determine the features related to this technique after the processing of the signals.

Based on the multi hop technique, the entire data that is accumulated is directed towards the special nodes which are considered as the sink nodes or the Base Station (BS). The user at the destination receives the data through the internet or the satellite via gateway. The use of the gateway is not very necessary as it is reliant on the distance between the user at the destination and the network (Lina *et al*. 2008).

For supervising the physical world, the wireless sensor networks are the promising technology. In order to collect the data from the surrounding in a sensor network application, several minute sensor nodes are organized and collaborated. Sensing modals like image sensors are placed in every node and this possess the ability to communicate in materials. Whereas in case of the inside threat, the attacker will be possess some key materials and trust of some sensor nodes.

Compromising the sensor nodes is an easy task due to the absence of the expensive tampering resistant hardware. Even if it possesses the tampering resistant hardware, it may be very reliant. Modification, forging the wireless environment (Lee and Aghajan, 2005). Military sensing and tracking, environment monitoring, patient monitoring and tracking are the fields where the sensor networks are utilized. Several low power sensors are distributed across the location that is to be monitored in the sensor network (Saravanan *et al*. 2011).

### 1.2. Attacks in Sensor Networks

The threats and challenges of sensor networks are:

- Spoofed, altered, or replayed routing information
- selective forwarding
- sinkhole attacks
- Sybil attacks
- Wormholes
- HELLO flood attacks
- Acknowledgement spoofing (Clark *et al*. 2007)

### 1.3. Network Security in Sensor Networks

In wireless channels, the communication is not completely secure and is subjected to security hazard. In the wireless channels, the possible security threat can be divided into two threats: Inside threat and outside threat. In case of outside threat in the sensor network, the attacker does not possess control over the cryptographic and discarding the messages is possible in case of a compromised node (Sang *et al*. 2006).

In vulnerable locations, maintaining the security of the sensor nodes is a major task. In WSN, the encoding and the authentication of the communication carried out is necessary, to ensure security. For communication between the sensor nodes, few solutions have been developed to attain stability in communication. Distribution key method, dissymmetric encryption method and key predisposition method are the three kinds of key management techniques (Jeong and Lee, The attacks like jamming and spoofing are very destructive to the sensor networks. Whenever the cluster heads are responsible for the transmission and reception of the data, this nature of the Cluster Hierarchy distribution networks makes it susceptible to destructive networks. So, the network will get destructed if a hacker tries to become the cluster head of the cluster. Examples of this type of attack are the selective forwarding and the sinkhole attacks (Abuhelaleh and Elleithy, 2010).

### 1.4. Key Management in Wireless Sensor Networks

Use of the pairwise keys between sensor nodes is the necessary requirement of the WSN for ensuring security.

The trusted-server scheme, the self-enforcing scheme and the key pre distribution scheme are the three classes of the key agreement schemes. A trusted server is assumed to exist in the case of trusted-server scheme for the establishment of keys between the nodes. But in case of distributed sensor networks, trusted server scheme is not appropriate due to the difficulty in developing a trusted network. Asymmetric cryptography, like that of public key certificate is utilized in the self enforcing scheme. But for sensor networks, use of the public key algorithm is inappropriate due to the restricted amount of power and resources for computation in the minute sensor node. In the key pre-distribution schemes, loading of the keying materials takes place at a prior basis in the sensor nodes (Jang *et al*., 2007).

In a wireless sensor network, the computation and communication capacity of every node is limited to a particular level. Node groups can be used for executing in network data aggregation and analysis. For instance, a vehicle can be tracked by a node group jointly via network. The nodes belonging to a group will keep varying repeatedly and at a faster rate in the network. In the wireless sensor network, most of the key services are executed by the groups. Hence, for admission of the new members to the group and to support group communication at a secure level, it is necessary to have a secure protocol for group management. After the omputation within the group, the result is transferred to the base station. In order to ensure the transmission from a legitimate group, the result must be authenticated (Perrig *et al*. 2004).

## 2. RELATED WORK

Jeong and Lee (2006) have proposed a new cryptographic key management protocol, which is based on the clustering scheme but does not depend on the probabilistic key. The protocol can increase the efficiency to manage keys since, before distributing the keys by bootstrap, the use of public keys shared among nodes can eliminate the processes to send or to receive keys among the sensors. Also, to find any compromised nodes safely on the network, it solves safety problems by applying the functions of a lightweight attack-detection mechanism.

Dwoskin *et al*. (2007) have proposed two low-cost secure-architecture-based techniques to improve the security against such node fabrication attacks. Their new architectures, specifically targeted at the sensor-node platform, protect long-term keys using a root of trust embedded in the hardware System-on-a-Chip (SoC). This prevents an adversary from extracting these protected long-term keys from a captured node to fabricate new nodes.

Jain and Jain (2011) have presented a security framework Wireless Sensor Networks Security Framework (WSNSF) to provide a comprehensive security solution against the known attacks in sensor networks. The proposed framework consists of four interacting components: A Secure Triple-Key (STKS) scheme, secure routing algorithms (SRAs), a Secure Localization Technique (SLT) and a malicious node detection mechanism. Singly, each of these components can achieve certain level of security. However, when deployed as a framework, a high degree of security is achievable. WSNSF takes into consideration the communication and computation limitations of sensor networks.

Maala *et al*. (2008) have presented a Two Level Architecture key management scheme for wireless sensor networks (TLA). Our scheme combines efficiently different key management techniques in each architecture level. This combination gives TLA good performances in terms of key storage overhead as well as in terms of resistance degree against node capture.

Shen and Shi (2008) in this study have presented a lightweight key management approach. A dynamic key management protocol is proposed to satisfactorily resolve the key distribution issues of WSN. The protocol assumes that the wireless sensor system has already been equipped with effective security detection mechanisms, which can decide if a sensor node is compromised or has used up its energy. Its analysis shows that this approach is an effective solution to the key management of hierarchical clustered wireless sensor networks. This protocol assumes that each sensor node is able to get its location information, which is currently a major restriction to its application.

Kim *et al*. (2007) in this study proposed a key distribution scheme which improves the resilience against node capture and reduces communication cost. This key establishment model is devised comparing the benefits and weaknesses of the EG scheme and LEAP. As a result, this scheme inherits the security of the EG scheme during key setup phase and the improved security of LEAP after that phase. Also, this scheme does not require the assumption in LEAP that no nodes are captured during that phase, meaning this scheme is more practical than LEAP. In addition, this scheme has low communication overhead.

Shaikh *et al*. (2010) have proposed two new identity, route and location privacy algorithms and data privacy mechanism that addresses the privacy problem. The proposed solutions provide additional trustworthiness and reliability at modest cost of memory and energy. Also, they proved that their proposed solutions provide protection against various privacy disclosure attacks, such as eavesdropping and hop-by-hop trace back attacks.

Abuhelaleh and Elleithy (2010) have proposed a special kind of architecture to the cluster hierarchy of wireless sensor networks. The most interesting protocol that has been proposed for this kind of architecture is LEACH. This proposal is a module of a complete solution that is developed to cover all the aspects of wireless sensor networks communication which is labeled Secure Object Oriented Architecture for Wireless Sensor Networks (SOOAWSN).

## 3. ENERGY EFFICIENT CLUSTER BASED KEY MANAGEMENT TECHNIQUE

### 3.1. Cluster Formation

In the wireless sensor network, after the nodes are deployed in the physical environment, they first report to the base station their physical locations and then the network starts to select cluster heads.

According to the cluster head selection algorithm, each node decides if it is capable of serving as a cluster head based on the following selection criteria:

- High energy resources
- Wide communication range
- High processing capacity

For the authentication process, the encryption mechanism is carried on.

When the selection criteria are satisfied by a particular node, it is capable of being the cluster head. So, this node, $N_i$ broadcasts a Cluster head beacon (CH_BEACON) packet. The CH_BEACON packet is encrypted with a key called as the primary key, $K_{pri}$:

$$N_i \xrightarrow{K_{pri}(CH\_BEACON)} broadcast$$

When the neighboring nodes $S_i$ receive this message, a Cluster Head Reply (CH_REPLY) message is sent to the node, $N_i$ by the nodes which intend to join the cluster. The reply message contains the ID and the response content Ack:

$$N_i \xleftarrow{CH\_REPLY} S_i$$

$$K_{pri}(ID_{\{S_i\}} \| Ack)$$

If the number of reply messages received by $N_i$ is greater than a threshold $R_{th}$, then $N_i$ can be selected as the cluster head, CH.

Finally, the cluster head assigns IDs to all its member nodes that intend to join the cluster.

### 3.2. Cluster Communication

**Figure-1** shows the architecture of the clustering system with every CH connected to the sink. In this figure, the network possesses three clusters. Each cluster possess a cluster head i.e., CH1, CH2 and CH3 are the cluster heads of clusters C1, C2 and C3, respectively.

CH1 contains the members 1 to 7, CH2 contains members 8 to 14 and CH3 contains members 15 to 21.

After the clusters are formed in the network, the CH sends the information of its members like <cluster id, member id> to the sink.

X1, X2 and X3 are the cluster information sent by CH1, CH2 and CH3 towards the sink, given by:

X1 = {<C1,1>, <C1,2>,…….. , <C1,7>}
X2 = {<C2,8>, <C2,9>,…… ….., <C2,14>}
X3 = {<C3,15>, <C3,16>,……..., <C3,21>}

The sink allots a cluster key, $K_{CH}$ to every cluster in the network. In Figure-2, the cluster keys obtained by the cluster heads CH1, CH2 and CH3 are $K_{CH1}$, $K_{CH2}$ and $K_{CH3}$, respectively.

After getting the cluster key from the sink, each CH receives the pairwise key set which is based on Exclusion Basis System (EBS) (Shen and Shi, 2008). (which will be explained in section 4):

Sink □□□□□□□□ $CH_i$ where i $K_{CHi}$ □EBS key set□

The EBS key set includes the pairwise keys, $P_{ij}$ for communication between the CH and its member and also the pairwise keys, $PH_{ii'}$ for communication between the CHs, encrypted by the cluster key. Hence EBS key set transmission can also be given as:

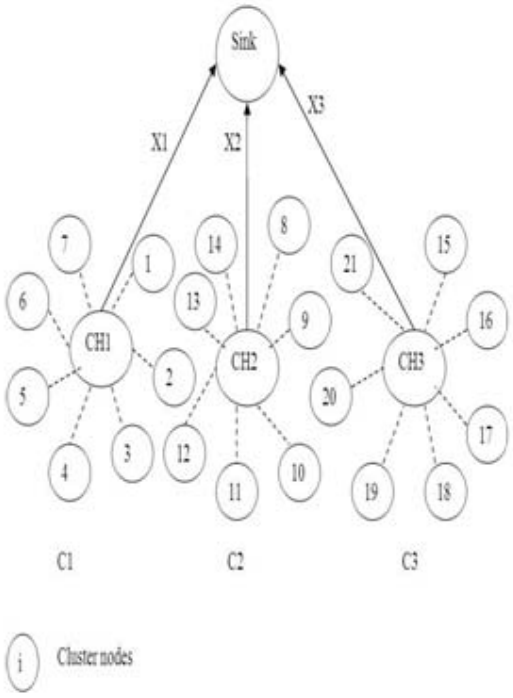


**Figure-1.**

#### 3.2.1. Intra Cluster Communication

The CH decrypts the pairwise keys sent by the sink, with its cluster key $K_{CH}$ and distributes them to its cluster members:

$$CH_i \rightarrow \{CM\}_j$$

$CH_1 \xrightarrow{K_{11}} \{CM\}_1$

$CH_1 \xrightarrow{K_{15}} \{CM\}_5$

Next a secure path is established between the two nodes; node 1 and node 5 after the exchange of hello message and acknowledgement message:

$\xrightarrow{\text{Hello message}} \{\quad\}$

$CH_1 \qquad CM_1$

$CH_1$

$\xrightarrow{\text{Hellomessage}} \{CM\}_5$

$CH_1 \xleftarrow{\text{Ackmessage}}$

$\{CM\}_1\ CH_1$

$\xleftarrow{\text{Ackmessage}}\ \{CM\}_5$

After receiving the acknowledgement message, a secure channel is set up between the node and the CH. Thus through the CH, a continuous path is established between the two nodes that need to communicate with each other:

### 3.2.2. Inter cluster Communication

If node 10 of C2 wants to communicate with node 15 of C3, then the following sequence of steps will take place.

Initially the CH2 distributes the pairwise key $K_{210}$ to the node10 and CH3 distributes the pairwise key $K_{315}$ to node 15 and then a secure channel is established in C2 between CH2 and node10 and in C3 between CH3 and node15.

In order to establish a secure channel between C2 and C3, the following steps are followed:

$$CH_2 \xrightarrow{K_{23}} CH_3$$

Next the hello message is sent by C2 to C3:

$$CH_2 \xrightarrow{\text{Hello message}} CH_3$$

$$CH_2 \xleftarrow{\text{Ackmessage}} CH_3$$

On receiving the acknowledgement message, a secure channel is established between the C2 and C3:

$$CH_2 \xleftrightarrow{\text{Securechannel}} CH_3$$

Where:

$i = 1 \dashrightarrow j = 1$ to 7

$i = 2 \dashrightarrow j = 8$ to 14

$i = 3 \dashrightarrow j = 15$ to 21

For example, in Figure-2, if node1 of C1 wants to communicate with node5 of the same cluster, then CH1

Whenever a node within a cluster wants to communicate with a node belonging to another cluster then the inter cluster communication takes place in the network. For communication between two clusters, the CH uses the pairwise keys, $PH_{ii'}$ obtained from the EBS key set:

$$CH_i \xrightarrow{H_{ii'}} CH_i$$

where,

$i = 1,2,3$; $i' = 1,2,3$ and $i \neq i'$

After the distribution of the pairwise keys between the CHs, the secure channels are established between the CHs. Initially the source CH sends a hello message to the CH with which the former wants to communicate. On reception of the Acknowledgement message from the target CH, the source CH establishes a channel between itself and the target CH:

$$CH_i \xrightarrow{\quad} CH_i$$

where,

$i = 1,2,3$; $i' = 1,2,3$ and $i \neq i$:

$$CH_i \xleftarrow{\text{Ackmessage}} CH_i$$

Then through CH2 and CH3, the node10 of C2 and node15 of C3 are connected to each other to form a secure path:

$$\{CM\}_{10} \xleftrightarrow{\text{Securechannel}} \{CM\}_{15}$$

## 4.1. Performance Metrics

The performance of EECBKM technique is compared with the SecLEACH (Abuhelaleh and Elleithy, 2010) scheme. The performance is evaluated mainly, according to the following metrics:

- Average Packet Drop: The number of packets dropped due to various attacks is averaged over all surviving data packets at the destination
- Average Packet Delivery Ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted
- Energy: It is the average energy consumed for the data transmission.

## 4.2. Results

### 4.2.1. Based on Attackers

In our initial experiment, we vary the number of attackers as 2, 4, 6, 8 and 10 from various clusters performing node capture attacks.

When the number of attackers is increased, naturally the packet drop will increase there by reducing the packet delivery ratio.

Since EECBKM reduces node capture attacks, the amount of packet drop is less, when compared with the existing schemes. Figure-3 and 4 give the packets drop and packet delivery ratio when the attackers are increased. Figure 5 gives the energy consumption when the number of attackers is increased .It shows that our proposed EECBKM technique achieves good packet delivery ratio with less packet drop when compared to SecLEACH scheme.

### 4.3. Simulation Results

The proposed Energy Efficient Cluster Based Key Management (EECBKM) technique is evaluated through NS2 simulation. In the Table-1, we consider a random network of 100 sensor nodes deployed in an area of 500×500 m. Two sink nodes are assumed to be situated 100 m away from the above specified area. In the simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. The simulated traffic is CBR with UDP. The number of clusters formed is 9. Out of which, we transmit data from 4 cluster heads to the sink. 3 sensor nodes in each cluster are sending data to their cluster head. The attacker nodes are varied from 2 to 10.

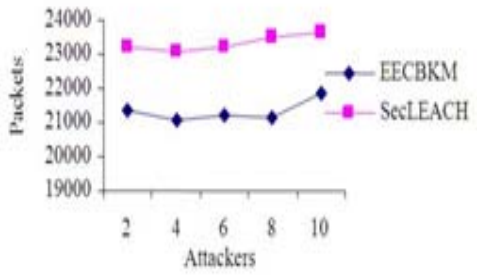


**Figure-3.** Attackers Vs delivery ratio.

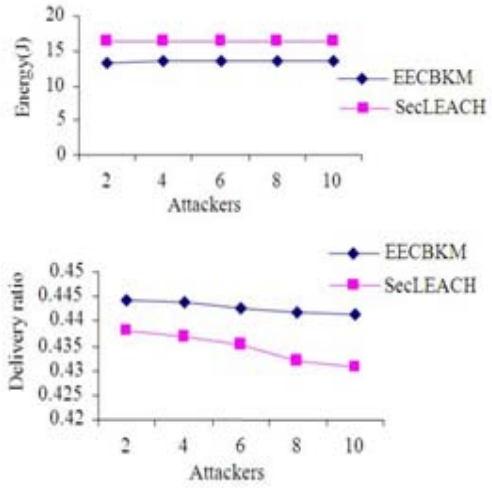


**Figure-4.** Attackers Vs packet drop.

**Table-1.** Summarizes the simulation parameters used.

| **No. of nodes** | **100** |
|---|---|
| Area size | 500×500 |
| Mac | 802.11 |
| Routing protocol | EECBKM |
| Simulation time | 50 sec |
| Traffic source | CBR |
| Packet size | 512 bytes |
| Rate | 250 kb |
| Transmission range | 250 m |
| No. of clusters sending data | 1, 2, 3 and 4 |
| No. of nodes per cluster sending data | 3 |
| Transmit power | 0.395 w |
| Receiving power | 0.660 w |
| Idle power | 0.035 w |
| Initial energy | 17.1 Joules |
| No. of attackers | 2, 4, 6, 8 and 10 |

## 5. AUTHENTICATION AND ITS ISSUES

In Wireless Sensor Networks (WSNs), authentication is a significant service for an unattended environment. It is a mechanism in which the identity of a node in a network can be identified as a valid member of the network. Hence the data authenticity is achieved. A Message Authentication Code (MAC) is appended to the data. It can only be viewed by valid nodes capable of decrypting the MAC, through some determinable means. The reliability of the message is ensured through authentication by identifying its origin. In the sensor networks, the attackers not only alter the packets but also the adversaries inject additional false packets. The identity of the senders and receivers are verified by the data authentication. It can be achieved through symmetric and asymmetric mechanism. Here the secret key is shared between the sending and receiving nodes. The major challenges faced in ensuring authentication (Yuan *et al*. 2005) are the wireless nature of the media and the unattended nature of sensor networks.

Authentication may be either of the two namely, end-to-end or hop-to-hop. The source and destination share some secret and verifies each other in end-to-end authentication. The two secure routing protocols based on end-to- end authentication are SEAD and Ariadne. On receiving a routing update by the node, the sender of the update is verified before the accepting the update. Each message in transmission is authenticated hop by hop in hop-hop authentication. Hence the trust between the source and the destination is built upon the trust on all the intermediate nodes in the path. It is not as secure as end-to-end authentication. It is not so expensive. It does not require every pair of nodes share some common secret.

### 5.1. Authentication Issues in WSN

The outsiders are prevented from launching a Sybil attack on the sensor network by using authentication and encryption techniques. The participation of insiders in the network cannot be prevented. It can be only done using


the identities of the nodes which are compromised (Sharma and Ghose, 2010).

The SPINS protocol provides confidentiality, integrity, freshness of data. But the problem of information leakage in secret channel, processing of captured nodes, DoS attacks and other issues in the sensor network are not considered (Rautray and Sarangi, 2011).

The symmetric schemes mTESLA and its variations Code (MAC) are efficient in terms of processing and energy consumption. The following issues are suffered by them:

- Delayed authentication is provided
- It is not scalable in terms of number of senders
- It cannot broadcast multiple senders simultaneously
- It is very slow for large scale sensor networks
- The late authentication causes DoS attack against storage

## 6. CONCLUSIONS

In this study, we have developed an efficient technique for key management in the wireless sensor network. During the formation of a cluster, initially a clusterhead is selected based on eligibility criteria such as energy cost, coverage and processing capacity. After the clusterhead selection, the information about all the members of the cluster is sent to the sink by the clusterhead. The sink then provides the clusterhead with the cluster key and the EBS key set required for the communication between the nodes. These keys are distributed to the nodes by the clusterhead prior communication. After the key distribution, secure channel is established between the nodes and the clusterhead. During the data transmission from the cluster members to the sink, the data passes two phases. In the first phase the data is encrypted and transmitted to the clusterhead. In the second phase, the data is encrypted by another key by the clusterhead and then transmitted to the sink. Thus this technique allows inter cluster as well as intra cluster communication in a very efficient manner with high security.

By simulation results, we have shown that our proposed technique efficiently increases packet delivery ratio with reduced energy consumption.

## 7. REFERENCES

[1] Abuhelaleh M.A. and K.M. Elleithy. 2010. Security in wireless sensor networks: Key management module in SOOAWSN. Int. J. Netw. Security Applic. 4: 67-78.

[2] Clark J.A., J. Murdoch., J.A. McDermid. and S. Sen *et al*., 2007. Threat modelling for mobile ad hoc and sensor networks.

[3] Dwoskin J., D. Xu., J. Huang., M. Chiang. and R. Lee. 2007. Secure key management architecture against sensor-node fabrication attacks. Proceedings of the IEEE Global Telecommunications Conference, Nov. 26-30, IEEE Xplore Press, Washington, DC, pp: 166-171. DOI: 10.1109/GLOCOM.2007.39

[4] Jain Y.K. and V. Jain. 2011. An efficient key management scheme for wireless network. Int. J. Scientific Eng. Res., 2: 39-45.

[5] Jang J., T. Kwon. and J. Song. 2007. A time-based key management protocol for wireless sensor networks. Proceedings of the 3rd International Conference on Information Security Practice and Experience, May 7-9, Springer Berlin Heidelberg, Hong Kong, China, pp: 314-328. DOI: 10.1007/978-3-540-72163-5_24