IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-6, Issue-6, June 2018 E-ISSN: 2347-2693

An Efficient Key Management Scheme for Secure WSN

K. Derashri[1*], N. Chaudhary[2]

[1] Department of CSE, MPUAT College of Technology and Engineering, Udaipur, India
[2] Department of CSE, MPUAT College of Technology and Engineering, Udaipur, India

Available online at: www.ijcseonline.org

Accepted: 13/Jun/2018, Published: 30/Jun/2018

***Abstract*—** WSN is a wireless sensor network. It is the multi-hop network where large numbers of sensor nodes are connected together by wireless medium. WSN network used in various application like Military, Whether Detection, Agriculture etc. In this network data transfer occurs through wireless medium so we always need an efficient security scheme for this type of network which provides better security. WSN is a network contains low power sensor nodes so we need an efficient scheme which requires less power. In this security scheme implementation key management phase plays an important role because security of any scheme depends on key security. Many Key Management Scheme proposed in previous years like LEAP, PANJA, SEHKM etc. We explored these schemes and proposed a scheme for general purpose sensor networks which provide region able security level with less time requirement. The performance is measure in term of time requirement.

***Keywords*—** Wireless Sensor Network [WSN], Key Management.

I. INTRODUCTION

Wireless sensor network is a network in which large numbers of sensor nodes are distributed autonomously in the field to sense environment physical condition. It is the advancement of communication network [1]. Wireless Sensor Network [WSN] is widely used in many application areas like military, healthcare, agriculture etc. [2]. Security is the major key challenge in WSN deployment in hostile environment. WSN cannot implement same security schemes which are designed for normal wireless network due to physical limitation of nodes. Sensor nodes work on the battery and have limited memory. Public Key Encryption is the most secure scheme for any network but due to it's high resource requirement not suitable for WSN[3].

Security of any scheme is dependent on the key management. If Keys are secured then Security schemes can implement efficiently. So we need a key management scheme for WSN.

Key Pre-distribution Scheme provides a solution for WSN. Laurent Eschenauer, Virgil D. Gligor proposed an earliest scheme based on it. This Scheme suitable for earliest network but with time the security attacks increase rapidly and due to which new schemes proposed. But due to resource limitation and real time work we need always a scheme which provides security with limited resources utilisation [4].

Many Schemes proposed like LEAP, PANJA and SEHKM etc. But every scheme has such limitation. My proposed Scheme provides solution for all the general purpose WSN which demand reliable security level with low time cost.

A. Network Architecture

WSN can be implemented in distributed and hierarchical network. In HWSN we have three types of nodes Base Station, Cluster Head and sensor nodes. Base station connects at top level of network. Cluster Heads connect at the second level and at third level low level sensor nodes are connected. Each Cluster Head connected to fix number of low level sensor nodes and form a cluster. Low level sensor nodes do not directly communicate with base station. There is a fixed routing algorithm can implement so it is suitable for general purpose sensor network and also easy to implement.

II. LITERATURE REVIEW

In past years many key management schemes were proposed for WSN. Key Management is the most important task in security implementation in any network.

Laurent Eschenauer and Virgil D. Gligor 2002 proposed a key management scheme for distributed sensor network. This scheme based on key pre-distribution technique in this technique a large set of key pool is generated and then from this pool small subset of keys are generated and distributed

among low level sensor nodes. When two nodes want to communicate and if they have same key in their subset then they directly communicate by using this key and if not then they communicate by using third node which have common key with both nodes. This scheme did not have greater scalability. [4]

Wenliang Du, Yunghsiang S. Han, Pramod K. Varshney, Jonathan Katz and Aram Khalili 2005 proposed a pair-wise key pre-distribution scheme for WSN this uses blom's key matrix model is based on symmetric key multiplication. This scheme generates a pool of key matrix and then each node take subset of key matrix pool. When two nodes want to communicate they need common key matrix and calculate the private key by Blom's scheme. [5]

Biswajit Panja, Sanjay Kumar Madria and Bharat Bhargava 2006 proposed energy and communication efficient group key management protocol. This is developed for hierarchical sensor network. In this architecture base station at top level that followed by cluster heads and after that at least level low level sensor nodes are connected. All nodes have initial symmetric key for key transportation this is pre-installed. Every node generates group key by using partial key. The low level sensor nodes use random number to calculate partial keys. The upper level nodes use lower level node's partial keys to generate partial key of self. Nodes have two group keys Intra Cluster and inter cluster. [6]

Sencun Zhu, Sanjeev Setia and Sushil Jajodia 2006 proposed LEAP key management protocol with the operation of four types of keys. The individual key shared between general sensor node and the base station. Pair Wise keys shared between two nodes. Cluster Key shares between cluster head and it's member nodes. Group Key is used by the base station to communicate with all sensor nodes of the network. These four keys are generated by the initial pre-distributed key is called initial key. [7]

Jiyong Jang, Taekyoung Kwon, and Jooseok Song 2007 proposed a time based key management protocol for WSN this is the advancement of LEAP protocol. In this scheme the network lifetime divided into p time slots. All nodes deployed in the same slot i are in the same group N_i, They have same initial key IK_i and n master keys for n time slots which are chosen randomly. The master keys help to generate initial key in different time slots. [8]

Boushra Maala, Hatem Bettahar and Abdelmadjid Bouabdallah 2008 proposed a scheme "TLA: A Tow Level architecture for key management in WSN" in this scheme network divided into two types of clusters supervised cluster and unsupervised cluster. Master Key and pair wise key technique used in supervised cluster and Key pool technique used in unsupervised cluster. [9]

Xinyang Zhang and Dr. Jidong Wang 2015 proposed an efficient key management scheme for hierarchical WSN. In this at top level base station available at second level cluster heads are connected and at last low level sensor nodes are connected. The low level sensor nodes have four types of keys network key, group key, pair-wise key and one extra pair wise key with assistant node. Assistant node works as cluster head in any cluster when cluster head stopped working.[10]

III. PROPOSED WORK

The proposed scheme works for general purpose sensor network it provides the reliable security level with fast key management which suitable for many real time applications. This scheme proposed for the hierarchical sensor network. In it's network architecture at top level base station is available at second level cluster heads are available and at the third level low level sensor nodes are available.

In this scheme we used two types of keys Pre-Distributed Key and Pair-wise key.

Pre-Distributed Key:- Pre-distributed key(PDK) is 64 bit key which is initially installed in nodes by the node establisher. This key only exist on the node until it not create pair wise key after that it is deleted from all nodes except Base station and Cluster Heads because higher level nodes are always physically secured. They always have Pre-Distributed Key.

Pair-Wise Key:- Pair-Wise key (PWK) is 64 bit key it's establish between Base station and each cluster heads. Cluster head also establish pair-wise key with it's lower level sensor nodes which are connected in it's cluster.

A. Establishment of Pair Wise Key between BS and CHs:-

The pair wise key distribution between cluster heads and the base station happened with help of pre-distributed key. This process includes following steps:

1. First Cluster Head establisher loads Pre-distributed key in Cluster Head.
2. After that Cluster Head use Diffie Hellman approach to establish key. For this it generates the value of A.

A=power(g,x);

A=mod(A,p);

Where

x= random integer number
g=prime integer number
p=prime integer number

3. After that we calculate the message digest (md) of value of A.
4. Then After Encrypt the value of A by using Pre-distributed Key. And send the request message to the Base Station.

A=encrypt (A,PDK);
req_msg=f(Id,A,md);

5. Base station put request in request queue and after one by one process request.
6. Base station first decrypt the value of A by using pre-distributed key and then calculate message digest of value of value of A. If the value of message digest (md1) matches with the received message digest (md) then except request another way remove it from queue.
7. Cluster head calculate value of B and then generate pair wise key (PWK_cb) value of B after that encrypted and send to Cluster Head.

B=power(g,y);
B=mod(B,p); …(i)
A=power(A,y);

Final Key

PWK_cb=mod(A,p);

Use equation (i) for reply message

B=encrypt(B,PDK);
rpy_msg=f(ID,B);

8. Cluster head receive message and then decrypt it and find out value of B and generate the corresponding pair wise key.

B=decrypt(B,PDK);
B=power(B,x);
PWK_cb=mod(B,p);

9. At last both cluster head and base station has pair wise key.

Fig.1:- PWK establishment b/w BS & CHs

B. Establishment of Pair Wise Key between CH and SNs:-

The Low level sensor nodes establish the pair wise key with it's corresponding cluster Head. For this following steps are performed.

1. First low level sensor establisher loads pre-distributed key(PDK) in it.
2. The low level sensor node uses diffie hellman approach and generates value of A and then calculate message digest of value of A after that encrypt value of A and send it to the cluster Head.

A=power(g,x);
A=mod(A,p);

Where

x= random integer number
g=prime integer number
p=prime integer number

A=encrypt (A,PDK);
req_msg=f(Id,A,md);

3. Cluster head receives message and then load it into request queue and process one by one. Cluster head decrypt the value of A by using pre-distributed key and then encrypt it by it's own pair-wise key with the base station.

A=decrypt(A,PDK);
A=encrypt(A,PWK_cb);
req_msg=F(C_Id, Id,A,md);

4. Base station receives the request and then put it into request queue then process one by one. First base station check the C_ID which identify that this request for low level sensor node and send by the particular cluster head and then by using corresponding pair-wise key with that cluster head decrypt the value of A.

A=decrypt(A,PWK_cb);

5. Base station now calculate the message digest (md1) by using the value of A. if the md=md1 then authentication complete and

then in the corresponding cluster table at base station the node ID and the value of A save.

6. Now base station send accept message to cluster head for the particular node.
7. Cluster head now generate the value of B by using diffie hellman approach. It also generates pair-wise key(PWK_sc) by using the value of A for that node.

B=power(g,y);
B=mod(B,p); ……(i)
A=power(A,y);
Final Key PWK_sc=mod(A,p);
Use equation (i) to calculate reply message

8. Then cluster head encrypt the value of B by using pre-distributed key and send it to the corresponding low level sensor node.

B=encrypt(B,PDK);
rpy_msg=f(ID,B);

9. Sensor node decrypts the value of B and generates the pair-wise key (PWK_sc). And now pre-distributed key delete from low level sensor node.

Fig.2:- PWK establishment b/w CH & SNs

C. *Key Updatation*

The key updation is only done when any node compromise it's security or deleted from network which also impact the security of another node. The low level sensor node when remove from network then cluster head and base station remove only it's details from it's database but not any key updation requires because this node not have any data which effect other nodes security. We assume that the higher level nodes cluster head and base station are highly secured node they do not compromise it's security. But cluster head can damage or stop working at that time the member nodes that are connected to that cluster head are required to connect with another cluster head. In this condition we require to update keys. Key updation happens in the following manner.

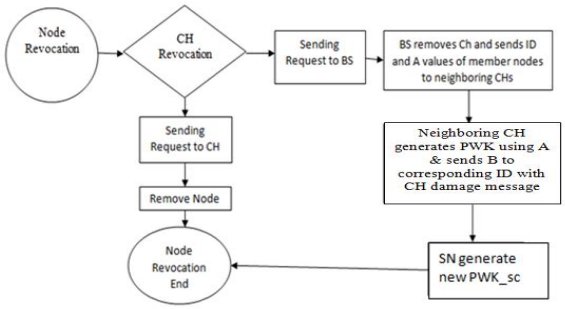

Fig.3:- Key Updation in WSN

IV. PERFORMANCE EVALUATION

In the performance evaluation of proposed scheme we simulate it with DES (64-bit) encryption with two level hierarchical wireless sensor network. The 64-bit key used for the encryption and decryption. The performance is measured in terms of time require for the key distribution in the complete network. The result of the proposed scheme compare with SEHKM scheme within the same environment.

Time Require for Pair-Wise Key establish b/w CHs and BS:

S. No.	No. of Cluster Heads	Time(Sec.) SEHKM	Time (Sec.) Proposed Scheme
1.	100	39.752	19.797
2.	200	70.119	42.447
3.	300	99.608	68.463
4.	400	130.4	85.279

Table 1: - Time Require for Pair-Wise Key establish b/w CHs and BS

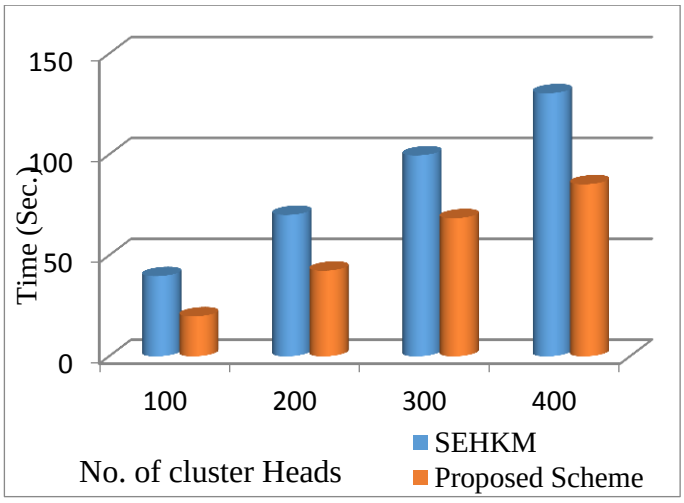

Fig. 4: - No. of Cluster Head & Time Graph

Time Require for Pair-Wise Key establish b/w CHs and low level Sensors:

[No. of Cluster Heads Fixed 5]

S. No.	No. of Sensor Nodes	Time (sec.) SEHKM	Time (Sec.) Proposed Scheme
1.	125	39.752	19.797
2.	250	70.119	42.447
3.	375	99.608	68.463
4.	500	130.4	85.279

Table 2: - Time Require for PWK b/w CHs and low level Sensors with fixed CHs

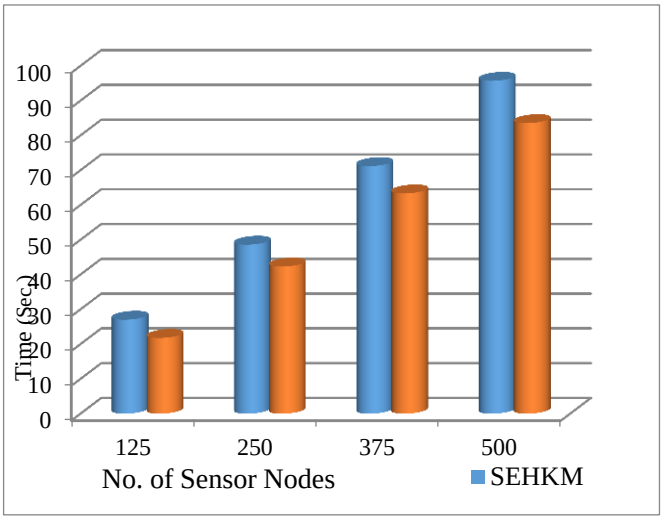

Fig 5: - No. of Sensor Nodes & Time Graph with fixed cluster heads

[No. of Sensor nodes 500 Fixed]

S. No.	No. of Cluster Heads	Time(Sec.) SEHKM	Time (Sec.) Proposed Scheme
1.	4	105.627	89.202
2.	5	95.703	83.54
3.	10	74.361	68.382

Table 3: - Time Require for PWK b/w CHs and low level Sensors with fixed SNs

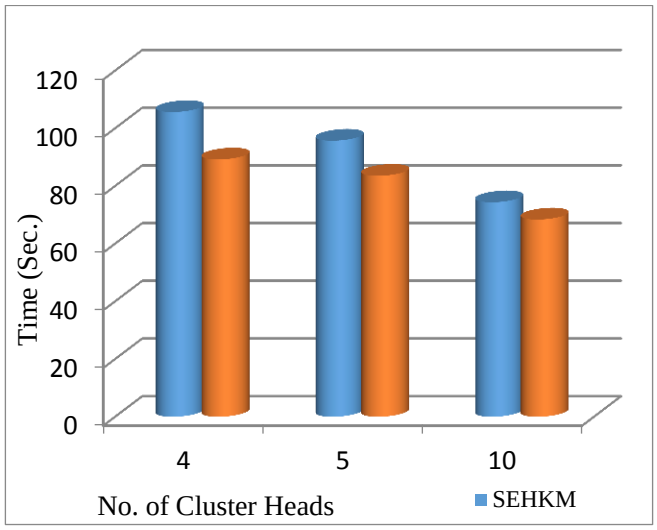

Fig 6: - No. of Cluster Head & Time Graph with fixed sensor nodes

V. CONCLUSION

In this Paper, an Efficient Key management scheme for WSN is proposed which provide the fast key establishment with reliable security level for general purpose WSN.

This Scheme require less time for the key establishment so we can establish any network in real time. It only includes pair-wise key so the memory requirement to store the key is also less. It provides a great option for those networks which require reliable network security with low resource cost. It also provides key updation which increases the security level.

VI. REFERENCES

[1]. Tanuja R, Souparnika P Arudi, S H Manjula, K R Venugopal, L M Patnaik, TKP : Three Level Key Pre-distribution with Mobile Sinks for Wireless Sensor Networks, 2015 IEEE.

[2]. Manel Boujelben, Omar Cheikhrouhou, Mohamed Abid and Habib Youssef, Establishing pairwise keys in heterogeneous two-tiered wireless sensor networks, 2009, Third International Conference on Sensor Technologies and Applications, IEEE.

[3]. Osman Yagan and Armand M. Makowski, Wireless Sensor Networks Under the Random Pairwise Key Predistribution Scheme: Can Resiliency Be Achieved With Small Key Rings?, December 2016, IEEE/ACM Transactions On Networking, Vol. 24, No. 6

[4]. L. Eschenauer and V. D. Gligor, A key-management scheme for distributed sensor networks. In : Proceedings of the 9th ACM conference on Computer and communications security, held at Washington, DC, USA during November 18 - 22, 2002,pp. 42-43.

[5]. Wenliang Du, Yunghsiang S. Han, Pramod K. Varshney, Jonathan Katz and Aram Khalili, A pairwise key predistribution scheme for wireless sensor networks. ACM Transactions on Information and System Security (TISSEC)8: 228-258.

[6]. Biswajit Panja, Sanjay Kumar Madria and Bharat Bhargava, Energy and communication efficient group key management protocol for hierarchical sensor networks. In: Proceedings of IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing, IEEE held at Taichung, Taiwan during June 5-7, 2006, pp. 8.

[7]. Sencun Zhu, Sanjeev Setia and Sushil Jajodia, LEAP+: Efficient security mechanisms for large-scale distributed sensor networks. ACM Transactions on Sensor Networks2: 500-528.

[8]. Jiyong Jang, Taekyoung Kwon, and Jooseok Song, A Time-Based Key Management Protocol for Wireless Sensor Networks. In : International Conference on Information Security Practice and Experience, Springerheld atHong Kong,China during May 7-9, 2007,pp. 314-328.

[9]. Boushra Maala, Hatem Bettahar and Abdelmadjid Bouabdallah, TLA: A Tow Level Architecture for Key Management in Wireless Sensor Networks. In : Proceedings of the 2nd International Conference on Sensor Technologies and Applications, SENSORCOMM, IEEE held at Cap Esterel, France during August 25-31, 2008, pp. 639-644.

[10]. X. Zhang, and D. J. Wang, An Efficient Key Management Scheme in Hierarchical Wireless Sensor Networks. In : International Conference on Computing, Communication and Security (ICCCS), IEEE held at Pamplemousses, Mauritius during December 4-5, 2015,pp. 2-5.

[11]. J. Zheng and A. Jamalipour. Wireless sensor networks: a networking perspective, 2009 John Wiley & Sons pp. 1-7.

[12]. S. Gajjar, S. Pradhan, and K. Dasgupta, Wireless sensor network: Application led research perspective .In :Recent Advances in Intelligent Computational Systems (RAICS),IEEE held at Trivandrum, India during September 22-24, 2011, pp. 25-30.

[13]. M. Steiner, G. Tsudik, and M. Waidner, Key agreement in dynamic peer groups. IEEE Transactions on Parallel and Distributed Systems11:769-780.

[14]. M. Steiner, G. Tsudik and M. Waidner,Key agreement in dynamic peer groups. IEEE Transactions on Parallel and Distributed Syst ems, 2000 11 : 769-780.

Author Profiles

Kuldeep Derashri pursued the B. Tech. degree in computer science engineering from rajasthan technical university, kota in 2016. He is currently pursuing the M. Tech. degree from maharana pratap university of agriculture and technology, Udaipur.

Dr. Naveen Chaudhary pursued the B.E. degree in computer science and engineering from Bangalore university. He pursued the M. Tech degree in computer science and engineering from IIT, guwahati. He pursued Ph. D degree in computer engineering from MNIT, jaipur. He is currently a professor and head of computer science & Engineering Department in CTAE college, Udaipur. His research interests are distributed system, operating system, interconnection networks and network-on-chip.

