Designing of Energy Efficient Cluster Based Scalable Key Management Technique to Improve the Lifetime of Wireless Sensor Network

K VIMAL KUMAR STEPHEN
Research Scholar
Computer Science and Engineering Department
AMET University, Chennai, India

MATHIVANAN V
Research Supervisor
Computer Science and Engineering Department
AMET University, Chennai, India

Abstract - **In the recent times, the demands of Wireless Sensor Networks (WSN) increase the challenges in terms of scalability and energy efficiency. Research has made a significant progress recently in the area of key management for protecting data during communication plays a prominent role in wireless sensor networks. A good key management strategy ensures secure sharing of information among the group. To achieve data confidentiality, scalability and improving lifetime of the sensor, static and movable mobile sinks are deployed. Here, movable sinks are used to receive sensed data from the sensor where it is located. The static mobile sinks act as a trusted third party for computing and distributing keys between sensor nodes and the clusters. It is not necessary to chose new cluster head often because of trusted third party sink, it performs all the computations of cluster head. The energy is retained when computation is reduced in cluster head thereby increases the life time of the particular cluster. The experimental result shows that the lifetime of the network is improved and computational overhead reduced are proved.**

Keywords – **Sensor Networks, Mobile Sink, Clusters**

I. INTRODUCTION

In sensor networks, the data are very crucial and to maintain secrecy in data communication is a toughest task. The process of establishing an authentication and secured communication could be achieved by a suitable key management scheme plays an important role in current scenario of security. A hierarchical sensor network consists of base station, cluster head and sensor nodes and it consists of three keys namely public and private key, cluster key and group key. In the research, Public-private key is employed for encryption and decryption, cluster key is for intra cluster communication and group key id for inter cluster communication should be shared among all members in the group in order to multicast information among a certain group securely.

Before transmitting, every data packages must be encrypted with a common shared group key. The users with the shared key can decrypt these packages and receive the data. Then the illegitimate user can decrypt the package without the key. Designing any kind of secure key management scheme requires a secret to set up a trust relationship between two or more communicating parties. Hence, the communication among the members in the group can be said to be secure.

Some of the issues in WSN in the area of key management are,

A. Security

Forward Secrecy: It implies that whenever a sensor leaves the group, the key will be changed and no node is able to encrypt or decrypt further messages in that group.

Backward Secrecy: It implies that a new node joining the group should not be able to encrypt or decrypt the previous messages in that group.

B. Efficiency

i. Computation Cost: It should be efficient for any group key management, which is the cost required to generate and update the keys for all members within a group.

ii. Communication Cost: It is the cost required to distribute the keys to every member within a group.

C. Distribution

Key distribution plays a major role in case of any network communication. All the key distribution protocol should be efficient and need to be more secure against the adversary attacks. The proposed key distribution scheme should be reliable to the large network size.

D. Scalability

As network sizes increase, scalability must be ensured in any key management protocol when multiple joins and leave's takes place in the network at the same time. The protocol should be capable of handling frequent key updates within very large, widely distributed groups.

In the scenario of energy efficiency, wireless sensor network encounters with loss of battery power during communication. Sensor node senses the data in the environment and transmits to the

base station through the cluster head. Battery is drained when the data is sensed and also during transmission of sensed data. The battery is drained in cluster head during computation of keys and data transmission.

The issue present here is during data transmission from one sensor node to another sensor node, it takes more hops to reach cluster head/other sensor node/base station hence the energy is drained. In cluster head, for the intra and inter cluster communication need secure transmission thereby computation of keys are necessary to ensure secure communication. The data transmission of cluster head takes place in three ways as follows

1. One sensor node to another sensor node within a cluster(Intra cluster Communication)
2. One cluster head to another cluster head
3. Sensor node to base station.

Due to this, energy is drained to the maximum. In order to retain the energy of the cluster head, energy efficient cluster based scalable key management technique has been proposed with mobile sinks to increase the lifetime of the cluster head which in turn increasing the lifetime of the network. The current scenario generally noticed problems in Wireless Sensor Networks are, 1) Security breach needs to be solved, 2) Scalability of sensor node and 3) Energy efficiency is still need to be improved. This research helps to overcome the above mentioned problems and issues thereby increases network lifetime and it is energy efficient.

II. LITERATURE SURVEY/STATE OF ART

Efficient Group Key Management using Symmetric Key and Threshold Cryptography scheme [1] considers a hierarchical cluster structure of sensor network adopts the pair-wise group key management and keys are updated periodically. It prevents dangerous attacks from malicious nodes and mitigates the node compromise. The communication overhead is negligible for keys establishment with low memory overhead and energy savings. Provision of better connectivity and scalability is improved based on deterministic approach with few messages. In this research, energy savings increase the network lifetime and achieves efficient security with low key storage overhead.

Weight-balanced 2-3 tree [2] is proposed to address the balance between security and limited resources is formed in every subgroup. Maximum Distance Separable (MDS) code technique is used to distribute the multicast key dynamically. The superior problem is to solve security. This method takes advantage of both centralized and distributed key group management method which is organized as irregular tree and every subgroup is organized as a weight-balanced 2-3 tree. This method shows superiority on security, scalability and performance.

A new Cluster-based Mobile Key Management Scheme [3] shows less computational overheads and energy consumption. The new CH is selected based on its efficiency and trust ability by the moving CH for the cluster. Mobility management is improved in this method and also increases the network lifetime and efficiency of the wireless sensor network. The algorithm proposed in this research shows 20-23 percent improvements over existing algorithm.

Blind factor is used to compute group key in this method [4] that ensures an attacker will not be able to get the group key when the cluster head broadcasts the group key. MAC is used along with the partial keys to guarantee authentication. Group key is generated by using partial keys in this research. The energy consumption is very small compared to the total available energy for generating the partial keys and the group key.

III. PROPOSED SCHEME

Considers a cluster structure of sensor network is illustrated in Figure 1.

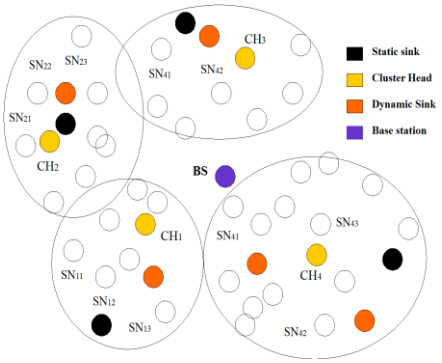

Figure 1 Proposed Architecture

In figure 1, SN_{11},SN_{12}….SN_{ij} represents number of sensor nodes in the cluster(i represents cluster and j represents sensor nodes , CH_1,CH_2…..CH_n represents number of Cluster Heads (CH_i) in a network and base station is represented by BS. Clusters are formed based on the transmission range.

1. A trusted and safe place available with unlimited resources is established for Trustworthy Base Station (BS). BS has authentication system, a sensor node table and an intrusion detection system for any node in the network.
2. Cluster head (CH) is solely accountable for receiving sensed data within a cluster and sends to the base station.

3. Sensor node (SNs) senses the information of an environment where is it located and transmits to the CH.

Initially, sensor nodes are dynamic after deployment during the network operation. Cluster head is also dynamic which can be chosen by cluster head formation algorithm. Initially the cluster head is chosen among on sensor node which is having highest battery power. The new cluster head is selected by the algorithm only when the already exiting cluster head reaches the threshold value. Before sending the sensed data, the sensor node enters in to the network should be authenticated by the BS.

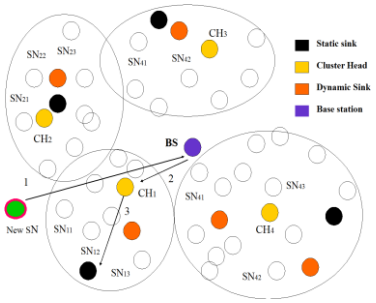

Figure 2: Joining Of New Sensor Node

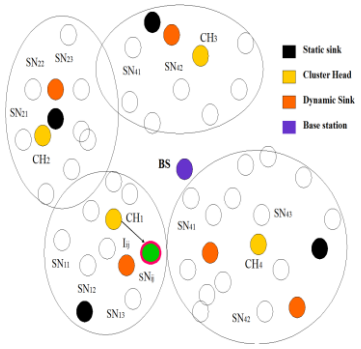

Figure 3: New Sensor Node Receiving Variable Length Identity

To ensure authenticity, identity for each sensor is assigned with the help of variable length Huffman coding algorithm by the CH. Identity I_{11} ,I_{12} …..I_{ij} is of variable length binary numbers such as 001, 00010, 100010, 100101, etc. The use of variable length coding is to avoid the illegitimate user in finding out guessing identities. Each sensor node is assigned with variable length so that no two nodes can have same identity i.e., each sensor node is provided with unique identity. This identity is used by the respective sensor nodes for further data transmission as well as for generating other keys.

If a sensor SN_{12} is ready to send the sensed data to BS, it is done through by means of cluster head. Nodes need cluster key and Group key to transmit data to BS. The cluster key is calculated by the CH by getting partial keys P_j from all the nodes in it. The partial key is any random number generated by random number generation algorithm in SNs. After generating partial key P_j , the SN computes secret partial key called S_{ij}

$$S_{ij} = P_j \oplus I_{ij}.$$

Assume CH is going to compute its Cluster key (CK_i), all the secret of S_{ij} is sent to the CH. In CH_1, it receives all the S_{ij} from the SNs and it computes CK (CK_i) by computing its own partial key K_i as below

$$CK_i = h (S_{11} \oplus S_{12} \oplus S_{13} \oplus \ldots\ldots S_{ij} \oplus K_i)$$

h is the hash function. Equation 2 is invoked by all the CH and performs the computation. Similarly the Master Key (MK) is generated by getting partial keys of all CHs L_i and BS,s own partial key.

$$MK = h (K_1 \oplus K_2 \oplus K_3 \oplus \ldots\ldots K_i \oplus L_{BS})$$

MK is computed by BS when sensor nodes joins and leaves the cluster in the network in order to maintain secrecy (both forward and backward secrecy). Further this cluster key and master key is used for communication between the nodes, sinks, base station and the clusters. When new node connects to the existing network, it should be authenticated with identity, partial key should be generated, CKs and MK generation need to be done.

When any of the SNs leave the group, it is necessary to generate CK and MK to ensure secrecy. During each joins and leaves, the above computation needs to be done. Each time, computation such as identity generation and cluster key generation is being done by CH, drains the energy present in the short span of time.

To avoid this, two or more movable mobile sinks and one static mobile sink is placed in the network. This movable sink moves around the cluster and receives the sensed data and transmits directly to the CH/BS. If the SN is far away from the base station, it needs to transmit the data through multiple nodes. If it happens again and again hence there is a more chance of energy drain. If any of the SNs is ready to transmit the data when the sink is moving around the clusters, it gets the data and transmits to the BS. Hence loss of energy is reasonably avoided because sink gets the data directly from the SNs and move towards BS and delivers the data. This sink helps in saving battery power of CHs and all other SNs. The static sink is a trusted node deployed for computing the above mentioned key management system so that the computation overhead is reduced drastically in the CH. It acts as a proxy for CH in such a way that it prevents energy loss.

Both the variable length Huffman coding algorithm for generating random number identity and CK generation algorithm for generating cluster key are implemented in trusted third party static sink. This

static sink computes identity and CK upon the request of CH about the join and leaves of SNs. This static sink concept helps to prolong the life of CH to the certain extent. The cluster head election algorithm is executed to select the new cluster head once the old one reaches the threshold level and also, the same is followed for sinks.

Once the sink reaches the energy level below threshold level, new sink is elected based on highest energy level among the SNs. The authenticity had been done efficiently using key management strategy. In order to ensure forward and backward secrecy, four scenarios such as single node join, multi node join, single node leave and multi node leave should be explored.

Single Node Join

In figure: node SNij connects under cluster Chi , the SNij request to CH and it informs the BS about its join in the cluster. CH sends request to sink, it provides variable length identity to SNij. Then it requests all the SNij to generate and send secret partial key. Upon receiving the Sij of all the SNs by CH in the cluster, it sends the same to static sink. The sink computes new CKi and multicast it to the group. All the SNs in the cluster decrypt the new CKi with the help of old CKi and the old CKi is dropped once new key is decrypted. Further all the communication is done with the help of new CKi. The SN does not have enough storage to store all the keys. Hence, the SNs should be automatically dropped the secret partial key once the CH acknowledges the Secret partial key.

Finally SN is implemented to store its Identity and CK alone. The sink can store maximum of 20 cluster keys for a particular threshold time. When it reaches the threshold time, it should be automatically resetted. Nevertheless sink will not receive any new request. The table in the sink consists of CK with its time on request. Time taken to reset the sink table should be in milliseconds. During each joins and leaves, GK can be generated as same as the cluster key generation by the BS and Multicast it. All the communication is done with the help of CK and MK.

Multi Node Join

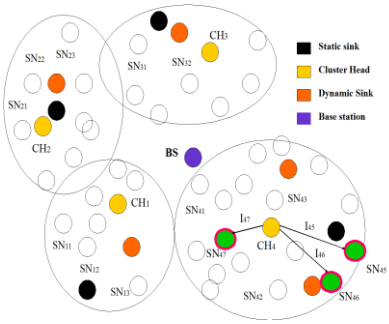

Figure 4: Multiple Node Join In Cluster 4

In Figure.4, Multiple nodes SN_{45}, SN_{46} and SN_{47} connects under same cluster or under different cluster in a network, all the SNij request to CH and it informs the respective BS about its join. CH sends request to its corresponding static sink, it provides variable length identity to all the SNij under particular cluster. Then it requests all the SNij to generate and send secret partial key under the particular cluster. Upon receiving the Sij of all the SNs by CH in the cluster, it sends the same to static sink. The sink computes new CK_4 and multicast it to the group. All the SNs in the cluster decrypt the new CK_4 with the help of old CK_4 and the old CK_4i is dropped once new key is decrypted.

Further all the communication is done with the help of new CK_4. The SN does not have enough storage to store all the keys. Hence, the SNs should be automatically dropped the secret partial key once the CH acknowledges the secret partial key. Finally SN is implemented to store its Identity and CK alone. The sink can store maximum of 20 cluster keys for a particular threshold time. When it reaches the threshold time, it should be automatically resetted. Nevertheless sink will not receive any new request. The table in the sink consists of CK with its time on request. Time taken to reset the sink table should be in milliseconds.

Single Node Leave

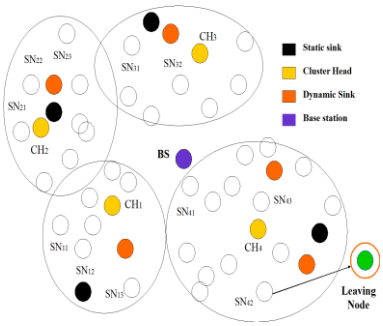

Figure 5: Single node leave from cluster 4

In Figure 5, SN_{42} leaves from cluster CH_4 , the SN_{42} request to CH and informs the BS about its leave from the cluster. CH sends request to sink about SNs leave. Then CH requests all the remaining SNij to generate and send a new secret partial key. Upon receiving the Sij of all the SNs by CH in the cluster, it sends the same to static sink. The sink computes new CK_4 and multicast it to the group. All the SNs in the cluster decrypt the new CK_4 with the help of old CK_4 and the old CK_4 is dropped once new key is decrypted. All the remaining operation is same as single node join.

Multi Node Leave

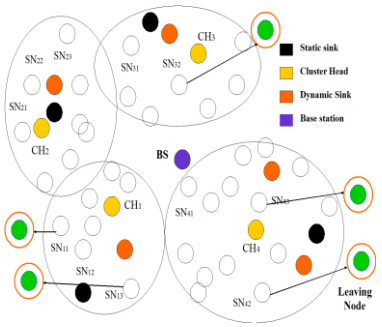

Figure 6: Multiple node leave from cluster 1,3 and 4.

In Figure 6, multiple nodes SN_{11}, SN_{13}, SN_{32}, SN_{42}, SN_{43} leaves from the same cluster or from different cluster in a network, the SNij request to respective CH_i about its leaves. CH_i sends request to BS and sink about SNs leave. Then CH requests all the remaining SNij to generate and send a new secret partial key. Upon receiving the Sij of all the SNs by CH_i in the cluster, it sends the same to static sink. Upon receiving the Sij of all the SNs by CH in the cluster, it sends the same to static sink. The sink computes new CKi and multicast it to the group. All the SNs in the cluster decrypt the new CKi with the help of old CKi and the old CKi is dropped once new key is decrypted. Further all the communication is done with the help of new CKi. All the remaining operations are same as multi node join.

IV. BENEFITS OF THE SYSTEM

The system enhances security through variable length coding in which key management overhead is reduced in terms of key size. The additional advantage is reduction in complexity, execution time and storage space. The most-frequently occurring source symbols are provided with shortest bit lengths, hence, number of bits used for encryption and decryption is reduced. Illegitimate user cannot able to find the identity of another user by holding the UID of another user.

Hash function used in this paper provides more security due to unique key generation. EX-OR operation used in generating cluster key and group key ensures accurate result i.e., no bit would be changed thereby error produced is negligible. The BS uses the partial keys received from each CH and its new own partial key to generate *CK*. Hence it takes *O(log C+1)* complexity for Master Key generation. In the same way, CH uses partial keys of its own and all the sensor nodes under it to generate CK. Hence it takes *O(log N+1)* operations for CK generation. During Node joins and leaves it takes computation cost O(1) for single and multiple joins and leaves.

V. CONCLUSION

Based on hierarchal wireless sensor network, energy efficient cluster based scalable key management technique has been proposed. A good key management strategy speaks about secure transmission of data. Hash function of Ex-OR operation with random partial keys provides us better result to ensure authenticity of a node. Variable code identity prevents attackers from acquiring the identity of the sensor node hence; compromising of sensor node is not possible. Effective security with low key storage overhead is achieved in this system. Long distance data transmission by sensor nodes is not energy efficient, since it is energy consumption. Deployment of static and dynamic sink in the network helps to prevent sensor nodes and cluster head form energy drain in turn it increases the lifetime of the sensor network. This leads to negligible storage overhead and communication overhead thus it saves energy. The experimental result proves that the proposed research works well to save the lifetime of a network.

VI. REFERENCES

[1]. Abdoulaye Diop, Yue Qi and Qin Wang , Efficient Group Key Management using Symmetric Key and Threshold Cryptography for Cluster based Wireless Sensor Networks, I.J. Computer Network and Information Security, 2014, 8, 9-18

[2]. Lin Yao, Bing Liu, Feng Xia, Guo-Wei Wu and Qiang Lin, A Group Key Management Protocol Based on Weight-Balanced 2-3 Tree for Wireless Sensor Networks,

[3]. M.Shainika and Mrs.C.Hema, Cluster Based Mobile Key Management Scheme to Improve Scalability and Mobility in Wireless Sensor Networks, National Conference on Research Advances in Communication, Computation, Electrical Science and Structures (NCRACCESS-2015) , 22-26.

[4]. Jyothi Metan and K N Narasimha Murthy, Group Key Management Technique based on Logic- Key Tree in the Field of Wireless Sensor Network, International Journal of Computer Applications, Volume 117 – No.12, May 2015, pp.0975 – 8887.

[5]. Yetgin, H., Cheung, K.T.K., El-Hajjar, M., Hanzo, L.2014. Cross-layer network lifetime optimization considering transmit and signal processing power wireless sensor networks. Wireless Sensor Systems, IET , Vol.4, No.4, pp.176-182

[6]. Alagheband, M.R., Aref, M.R.2012. Dynamic and secure key management

model for hierarchical heterogeneous sensor networks. Information Security, IET, Vol.6, No.4, pp.271-280

[7]. Seo, S-H., Won, J., Sultana, S., Bertino, E.2015. Effective Key Management in Dynamic Wireless Sensor Networks. Information Forensics and Security, IEEE Transactions, Vol.10, No.2, pp.371-383

[8]. J. Zhang, V. Varadharajan, "Wireless sensor network key management survey and taxonomy," Journal of Network and Computer Applications, vol. 33, no. 2, 2010, pp. 63-75.

[9]. A Diop, Y. Qi, Q. Wang "An Improved Key Management Scheme for Hierarchical Wireless Sensors Networks," in TELKOMNIKA Indonesian Journal of Electrical Engineering Science, vol. 12, 2014, pp 3969-3978.

[10]. Y. Zhang, C. Wu, J. Cao and X. Li "A Secret Sharing-Based Key Management in Hierarchical Wireless Sensor Network", Hindawi Publishing Corporation International Journal of Distributed Sensor Networks, vol. 2013, pp. 1-7.

[11]. Harn L, Lin C," Authenticated group key transfer protocol based on secret sharing", In Proceedings IEEE Trans. Comput, 2010, vol. 59 (6), pp, 842–846.

[12]. Klaoudatou, E., Konstantinou, E., Kambourakis, G. and Gritzalis, S., A Survey on Cluster-Based Group Key Agreement Protocols for WSNs. IEEE Communications Surveys & Tutorials, PP (2010), 1-14.

[13]. Kwang-Jin Paek, Jongwan Kim Chong-Sun Hwang And Sangkeun Lee, Group-Based Key Management Protocol For Energy Efficiency In Long-Lived And Large-Scale Distributed Sensor Networks, Computing And Informatics, Vol. 27, 2008, 743–756

