Maximizing the Lifetime and Data Security of WSNs – System Design

AbijithNayak M R[1]Akshay Kumar A[2] D P Santrupth[3] B N Kiran[4]

[1] Department of Information Science and Engineering, The National Institute of Engineering, Mysore, Karnataka,abhijithnayak95@gmail.com

[2]Department Information Science and Engineering, The National Institute of Engineering, Mysore, Karnataka,mail.akshay1504@gmail.com

[3]Department Information Science and Engineering, The National Institute of Engineering, Mysore, Karnataka,dp.santrupth@gmail.com

[4]Department Information Science and Engineering, The National Institute of Engineering, Mysore, Karnataka,bnkiran@gmail.com

Abstract-***Wireless Sensor Networks have gained wide popularity in the recent years for its important applications such as remote environment monitoring, target tracking, safety-critical monitoring applications etc. But WSNs have many constraints like low computational power, small memory, and limited energy resources. Two of the major issues associated with WSNs are the network lifetime and data security which we aim to address in this paper.Network lifetime maximization has become an essential system requirement for wireless sensor network which if maximized would contribute to the extensive usage of the capabilities especially for those used for safety-critical and highly-reliable applications. Clustering sensors into groups is a popular strategy to maximize the network Lifetime. In this paper, the High Energy First (HEF) clustering algorithm is chosen as a design reference model, which is proved to be an optimal clustering policy under certain ideal conditions. Further as an enhancement to avoid energy dissipation in WSNs, we use cluster node active/sleep algorithm. For protection of sensor data process from various kinds of attacks currently most of the WSN use hop by hop data security. But due to many decryptions performed by the intermediate nodes there is more consumption of battery power. End to end data security on the other hand can guarantee the end-to-end data confidentiality and result in less transmission latency and computation cost. In this paper we use privacy Homomorphism, which is one such encryption scheme that strives to provide data security.***

Keywords- Cluster head, base station, nodes, public key, private key.

1. INTRODUCTION

The Sensor Network can be described as a collection of sensor nodes which co-ordinate to perform some specific action. Unlike traditional networks, sensor networks depend on dense deployment and co-ordination to carry out their tasks. The architecture of the sensor network plays important role in the performance and lifetime of WSNs as well as data aggregation. In this paper we have chosen Hierarchical Clustering of WSNs. A typical HC-WSN is comprised of a Base Station, several Cluster Head nodes and Regular nodes. All the nodes are organized into clusters and a cluster head is chosen to head every cluster. Since the cluster head is responsible for most of the operations such as data aggregation from regular nodes and forwarding the same to the BS it requires possessing more energy than the regular nodes. Hence cluster head selection becomes an important process here. Unlike most of the clustering algorithms like LEACH, CIPRA which do not take energy information of the sensor nodes into consideration, our chosen High Energy First (HEF) gathers the residual energy of every sensor node in the network into account for cluster formation and also for cluster head selection. As an enhancement to this we propose here cluster node active/sleep algorithm in which, based on the energy information collected, a threshold energy level is computed and those nodes whose energy are extremely below this level will be sent to sleep and awaken only at the subsequent rounds where they would be useful. The optimality of HEF algorithm along with active/sleep ensures to balance the energies of all the nodes within a cluster thereby reducing energy depletion by efficiently forming clusters in set-up phase. During aggregation, data that is sensed by various sensor nodes are processed and encrypted for security purpose and sent to the aggregator node. Secure data aggregation can be classified based on encryption of data at specific nodes like hop-by-hop encrypted data aggregation and end-to-end encrypted data aggregation. In hop-by-hop encrypted data aggregation, all the intermediate sensor nodes has to decrypt the received encrypted data and apply aggregation function on it. Due to many decryptions performed by the intermediate node it's consuming more battery power and not provides end-to-end security. But in end-to-end encrypted data aggregation, intermediate nodes can aggregate the cipher text directly without decrypting the messages. Compared to the hop-by-hop one, it can guarantee the end-to-end data confidentiality and result in less transmission latency and computation cost. Hence we have chosen one such approach, the Paillier homomorphic cryptosystem where certain aggregation functions can be calculated on the encrypted data. The data is encrypted and sent towards the base station, while sensors along the path apply the aggregation function on the encrypted data. This is much better than end-to-end approach because the base station receives the encrypted aggregate result and decrypts it essentially allowing only the BS to know the gist of the data thus providing security to the data even at the aggregator level.

2. APPLICATION DESIGN

DESIGN PHASE

1. CLUSTER FORMATION USING HEF

The core idea of the HEF clustering algorithm is to choose the highest-ranking energy residue sensor as a cluster head. HEF is designed to select the cluster head based on the energy residue of each sensor to create a network-centric energy view.

Each round comprises the following three phases:

1. CHS Phase (Cluster head selection)
2. CFM Phase (Cluster formation)
3. DCM Phase (Data communication)

- HEF selects cluster heads according to the energy remaining for each sensor node, and then the "setup" message is sent to the cluster head of each cluster.
- The cluster head of each group broadcasts the "setup" message inviting the neighbor sensor nodes to join its group.
- After receiving the "setup" message at this round, the regular sensors send the "join" message to its corresponding cluster head to commit to associate with the group.
- Each cluster head acknowledges the commitment, and sends TDMA schedule to its cluster members.

All sensors perform its sensing and processing and communication tasks cooperatively at this clock cycle. Each sensor sends its energy information to its cluster head at the end of this clock cycle.

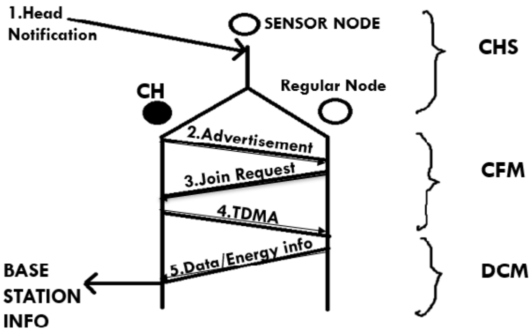


Fig 2.1 THREE PHASES OF HEF CLUSTER FORMATION

2. GENERATING SECURITY KEYS AND DEPLOYING IT

- At base station, public keys are generated using Paillier cryptography keys.
- Paillier Cryptography system uses two keys

1. Public key known to everyone.

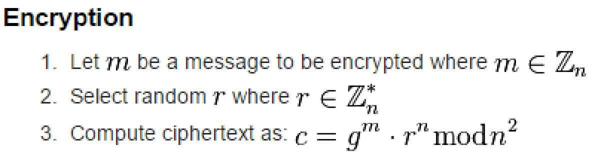
2. A Private key known only to recipient of the message.

Eg: When John wants to send a secure message to Jane, he uses Jane's public key to encrypt the message. Jane then uses her private key to decrypt it.

- An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them.
- Moreover, it is virtually impossible to deduce the private key if you know the public key.
- These keys are exchanged using UDP protocol.

3. DATA SENSING & ENCRYPTING AND FORWORDING

- The Sensor which has detected or responded to some types of input from the physical environment needs to be sent to cluster head.
- We encrypt the data before sending using Paillier cryptography for data security.
- The encryption is done as follows
- For forwarding the encrypted data we use TCP protocol as it is Serial port communication.



Encryption

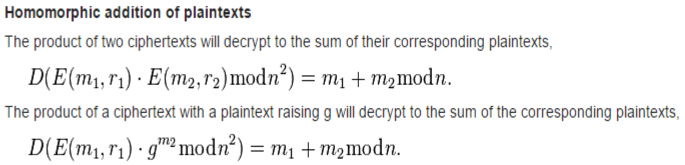
1. Let m be a message to be encrypted where $m \in \mathbb{Z}_n$
2. Select random r where $r \in \mathbb{Z}_n^*$
3. Compute ciphertext as: $c = g^m \cdot r^n \bmod n^2$

Fig 2.2 Encryption

4. AGGREGATION

- Since we are using End-to-End encryption which reduces battery consumption and gives more security.

We aggregate data in cluster head before sending it to Base station using Homomorphic properties either Additive or Multiplicative.



Homomorphic addition of plaintexts

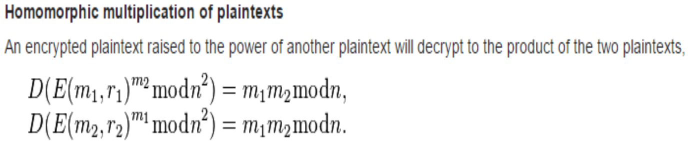
The product of two ciphertexts will decrypt to the sum of their corresponding plaintexts,

$$D(E(m_1,r_1)\cdot E(m_2,r_2)\bmod n^2) = m_1 + m_2 \bmod n.$$

The product of a ciphertext with a plaintext raising g will decrypt to the sum of the corresponding plaintexts,

$$D(E(m_1,r_1)\cdot g^{m_2}\bmod n^2) = m_1 + m_2 \bmod n.$$

Fig 2.3: Additive Homomorphic



Homomorphic multiplication of plaintexts

An encrypted plaintext raised to the power of another plaintext will decrypt to the product of the two plaintexts,

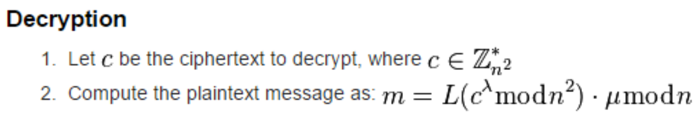
$$D(E(m_1,r_1)^{m_2}\bmod n^2) = m_1 m_2 \bmod n,$$
$$D(E(m_2,r_2)^{m_1}\bmod n^2) = m_1 m_2 \bmod n.$$

Fig 2.4: Mulitiplicative Homomorphic

5. DECRYPTION

- This is done at Base station.
- When all the cluster head sends the encrypted data to the base station, Base station decrypts it using private key.
- Decryption is done as follows

- After decryption the data is used for computation or observation.

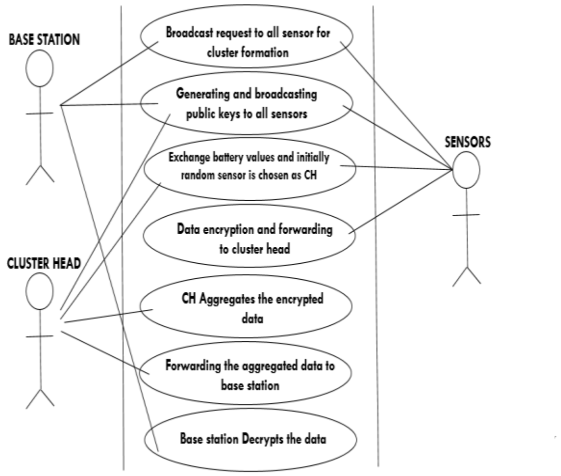


Decryption

1. Let c be the ciphertext to decrypt, where $c \in \mathbb{Z}^*_{n^2}$
2. Compute the plaintext message as: $m = L(c^{\lambda} \bmod n^2) \cdot \mu \bmod n$

Fig 2.5 Decryption

3. USECASE DIAGRAM


BASE STATION
CLUSTER HEAD
SENSORS
Broadcast request to all sensor for cluster formation
Generating and broadcasting public keys to all sensors
Exchange battery values and initially random sensor is chosen as CH
Data encryption and forwarding to cluster head
CH Aggregates the encrypted data
Forwarding the aggregated data to base station
Base station Decrypts the data

4. SEQUENCE DIAGRAM

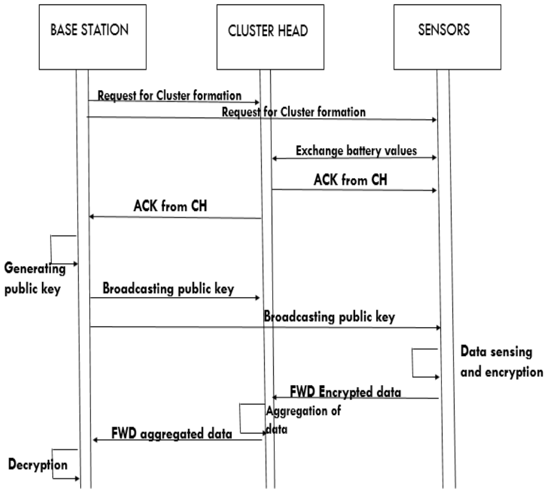


Fig 5.1: Sequence Diagram

5. CONCLUSION

A novel attempt to achieve maximum network lifetime by reducing energy consumption at the cluster head selection phase and at the data communication phase is introduced. A hierarchical cluster head selection algorithm which selects a node with the highest residual energy as the cluster head in every round is implemented. The HEF works on the residual energy of the sensor nodes which is gathered in priori in every round for cluster head selection. Thus it provides better predictability and utilization of battery for the sensor nodes. The threshold battery value calculation for every round and sending those nodes below this threshold battery value to the sleep state for later resumption prevents unnecessary battery consumption leading to premature death of the nodes. Further, a homomorphic encryption scheme to provide secure transmission of the sensed data using Paillier Cryptosystem is implemented. This not only provides the much needed security to the sensed data from eavesdroppers and intruders but also allows encryption to be done on the cipher text eliminating the need to decrypt/encrypt at every node through which it is transmitted. Thus further reducing the energy consumed for encryption and decryption at every node.

REFERENCES

[1] Balamurgan k etal, Maximization of lifetime and reducing power consumption in wireless sensor network using protocol, IJSCE, ISSN: 2231-2307, Volume 2, Issue 6,January 2013.

[2] U V Kulkarni etal, Comparative analysis of hop-to-hop and end-to-end secure communication, IJOART, ISSN: 2278-7763, Volume 2, Issue 7, July 2013.

[3]Abhishek Pandey etal, Cluster head election with node heterogeneity and recovery in WSN, IJARCSSE, ISSN: 2277-128X, Volume 5, Issue 6, June 2015.

[4] R Kumar etal, Analysis of data aggregation in wireless sensor network, IEEE, ISBN :978-1-4788-7225-8/15/$31.00, Issue 2015

Web references

[i]https://en.wikipedia.org/wiki/Paillier_cryptosystem

[ii]http://www.webopedia.com/TERM/P/public_key_cryptography.html