International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2018 IJSRCSEIT | Volume 3 | Issue 2 | ISSN : 2456-3307

Technique for Secure Data Aggregation in Wireless Sensor Network

Vaishali P. Latke, Amol N. Dumbare, Jameer G. Kotwal
Assistant Professor, Department of Computer Engineering, PCCOER, Ravet, Pune, Maharashtra, India

ABSTRACT

In wireless sensor the cost of energy is required for performing the operation on node is equal to the sending the single bit of information along with the distance to which it is sending. Therefore, data transmission in wireless sensor network reduce the network lifetime, while broadcasting the data in the sensor network, it is necessary to enhance the network lifetime by reducing the energy consumption. The cluster head is the aggregator node of the cluster which comes in frequent communication with all the cluster members thus requires more energy as compare to other members in the cluster. In the existing system cluster head is selected randomly from the cluster which cuts off that node from the network if not have enough energy hence results in reduced network lifetime of that sensor network. So to overcome this issue, the system introduces a method in which efficient cluster head is selected on the basis of, a distance from the base station and available energy. By selecting the efficient cluster head it consumes the less energy of the sensor network which enhance the network lifetime of the sensor network. The head of the cluster is responsible to aggregate the data from all its cluster members. Before aggregation, cluster head verifies the data and discards the invalid data. Only verified data gets aggregated at the cluster head. Homomorphic encryption scheme is used which encrypt the data and send the encrypted data to the cluster head and only base station can decrypt it to give end to end confidentiality. To provide hop by hop authentication an ID based signature scheme is used. In this paper we introduced the method which recovered the lost data, for this base station checks for the lost data and run the cache based recovery system to recover the data. Finally the result are compared on the basis of distinct parameters like packet drop ratio and energy consumption on jung simulator which shows how our system outperforms the existing one.

Keywords : Wireless Sensor Networks, Sensor Nodes, Cluster Head, Base Station, Cache Based System, Hop by hop authentication.

I. INTRODUCTION

Wireless sensor networks (WSNs) are becoming progressively popular in numerous circles of life. Application areas include monitoring of the environment such as temperature, humidity and seismic activity as well as numerous other ecological, law enforcement and military settings to carefully pass their information through the network to a primary location. In the meantime, WSNs are regularly conveyed in public or generally untrusted and even unfriendly situations, which prompt various security issues. These incorporate the usual topics, e.g., key administration, security, access control, authentication and DoS resistance, among others.

The sensor network faces the issue in changing or energizes the node batteries because of dense and ad-hoc operation in dangerous environment and due to

unattended nature of WSNs. The critical question arise is how to increase the network lifetime of the sensor networks. Increasing the lifetime of the system through reducing the energy is an challenging issue in WSNs. Exploratory estimations have demonstrated that for the most part information transmission is extremely costly regarding in terms of energy consumption (EC), while information processing consumes appreciably less. Consequently, a practical approach to increase the WSN lifetime is to decrease the sensor energy consumption in data transmissions. Second problem face in the wireless sensor network is the security of data while sending the data from source to destination.

When sensor nodes with constrained resources can be subject to numerous types of attacks, the information encryptions are essential in WSNs. If encryption plan is not utilized, attackers can examine and introduce false information into the system. In hop- by- hop encoded information aggregation (EDAs), which is an intermediate aggregator possessing keys of all related sensor nodes decodes received encoded values, totals all the decoded values, and encodes the outcome for broadcasting to a base station (BS). This methodology requires that inter mediate aggregators store keys for decryption in which a captured aggregator would uncover these secret data.

In this paper, basically focus on the three challenges which is mostly face in the wireless sensor networks. First is increasing the network lifetime of the sensor network by minimizing the energy consumption in the network. Second is to provide the security while the data transmission from sender to receiver node or from sender to base station. Third is data loss recovery, while sending the data to the base station or cluster head data is loss, hence there is need to recover the data. For increasing the network lifetime introduced the method in which cluster head is selected on the basis of energy, number of neighbors and distance to the base station. By selecting the cluster head by considering these three parameters decreases the energy value required to the sensor node homomorphic encryption is used for providing the security to the data. Data is send in the encrypted format to the base station, base station decrypt the data after receiving the data. Also the process of data aggregation is done in which cluster head aggregate the data which is collected by the cluster nodes. Base station checks for the lost data and run the cache based recovery system to recover the data.Finally the result is compared for the network lifetime, energy consumption and pack drop ratio for existing and proposed system.

This paper focus on related work in section II, system implementation details, problem definitions, algorithms, mathematical model in section III. Section IV shows the expected result of a system and at last conclusions and future work provided in section V.

II. LITERATURE SURVEY

This section discussed about the different work done by the researchers for the data aggregation, increasing network lifetime of the sensor nodes.

In [1], propose a SDA plan, Sen-SDA, which is based on the grouping of suitable cryptographic primitives in heterogeneous cluster WSNs. To decrease the aggregate length of ciphertexts and to accomplish end-to-end privacy, they assume an added substance HE method, so just a BS can decode encoded information collected by the CHs received from member nodes for every group of cluster. To give hop-by-hop validation, they utilize a matching free identity based signature (IBS) method, so the BS and the CHs can check the legitimacy of all the transmitted encoded information. To enhance productivity of numerous signature verifications, they require a signature plan in which numerous signatures from various endorsers on various messages can be checked rapidly.

In [2], propose a completely practical identity based encoded technique. This technique has selected ciphertext security in the random oracle model accepting a variation of the computational Diffie-Hellman issue. This framework depends on bilinear maps among clusters. The Weil combination on elliptic curve is a sample of such a guide. They provide an exact definition for secure identity based encryption conspires and give a few applications for such frameworks.

In [3], concentrate on efficient, data transmission conversing security in WSNs. All the more particularly, they mix modest encoded procedures with basic aggregation systems to accomplish extremely efficient collection of encoded information. To evaluate the reasonableness of proposed strategies, theyevaluate them furthermore, exhibit extremely promising results which plainly exhibit calculable data transfer capacity conservation and small overhead originating from both encoded and aggregation operations.

In [4], present an idea termed as Recoverable Concealed Data Aggregation (RCDA). In RCDA, a base station can recoup every sensing information produced by all sensors even if these information have been aggregated by cluster heads or aggregators. With these individual information, two functionalities are given. To begin with, the base station can confirm the uprightness and authenticity of all sensing information. Second, the base station can perform any aggregation capacities on them. At that point, they propose two RCDA plans named RCDA-HOMO and RCDA-HETE for homogeneous and heterogeneous WSN separately. They exhibit that the proposed plans are secure under these attack model in the security investigation.

In [5], present one such PH which can be demonstrated secure against known-cleartext attacks, the length of the ciphertext space is much bigger than the cleartext space. A few applications to designation of sensitive processing and information and to e-betting are quickly outlined.

In [6], present a methodology that 1) covers detected information end-to-end by 2) as yet giving productive and adaptable in-network information aggregation. The aggregating intermediate nodes are not necessary to work on the detected plaintext information. They apply a specific class of encoded changes and talk about systems for registering the total functions "average" and "movement detection." They demonstrate that the methodology is achievable for the class of "going down" routing protocols. They consider the risk of defiled sensor nodes by proposing a key pre-distribution algorithm that limits an attacker's addition and appear how key pred-istribution and a key-ID delicate "going down" routing convention expands the strength and dependability quality of the associated backbone.

In [7], re-examine the pertinence of additively homomorphic public key encryption calculations for certain classes of remote sensor networks. At last, they give suggestions for choosing the most appropriate public key plans for various topologies and remote sensor system situations.

In [8], present a novel type of cryptographic plan, which empowers any pair of clients to communicate safely and to check one another's marks without trading private or public keys, without keeping key indexes, and without utilizing the administrations of a third party. The plan accept the presence of trusted key generation focuses, whose sole design is to give every client a customized smart card when he first joins the system. The data installed in this card empowers the client to sign and encode the messages he sends and to decode and check the messages he gets in an absolutely independent manner, notwithstanding of the character of the other party. Beforehand issued cards do not need to be upgraded when new clients join the system, and the different centers don't need to facilitate their exercises or even to keep a user list. The centers can be closed after all

the cards are issued, and the network can keep on working in a totally decentralized way for an indefinite period.

III. EXISTING SYSTEM

In this section discussed the existing system used for sending the data securely.

The working of the existing system are as follows:

1. Generate a network graph as Graph g (v,e) where; V are vertices/nodes and E are edges.
2. On the number of nodes perform the clustering and divide the nodes in to number of clusters and Select the cluster head randomly.
3. Perform the key distribution and route generations at each node through Base Station.
4. Generate the data and Encrypt with the public key of base station at each node.
5. Calculate the hash value of the encrypted data and Record the timestamp.
6. Send the individual data to the cluster head from each cluster member in all the clusters.
7. Collect all data at the cluster head and verify the data by its hash value and accept the verified data or discard if not verified.
8. Aggregate all the data and send this data to the base station.
9. Base station accepts the data from each cluster head.
10. Base station verifies the data and decrypts the data with appropriate key.

IV. PROPOSED SYSTEM

This section studied the system overview in detail in which proposed algorithm, and mathematical model of the proposed system is also presented.

A. System Overview

The propose system architecture is shown in figure 1 which is divided into various steps which are describes below.

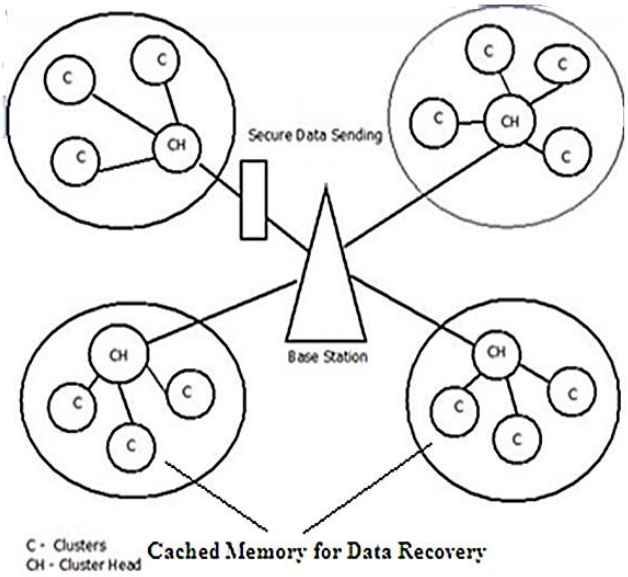

Figure 1. Proposed System Architecture

- Network Generation

Initially network is created where vertices/nodes are connected with the edges.

- Clustering Process

After the network creation, the clustering process is performed in which nodes are divided into number of clusters.

- Cluster Head Selection

After generating the group of clusters, from each group of clusters, the cluster head is selected on the basis of energy, distance from base station and neighbor nodes parameters.

- Key generation and distribution

Key generation and distribution to each node is done by the base station generates the key and distributes the keys. Perform the route generations from each node to the base station.

- Data Encryption

At each node data is generated and encrypted by using the EC-ElGamal+.

- Hash value evaluation

After the data is encrypted, hash value is evaluated and recorded the timestamp.

- Data Collection

After evaluating the hash value at each node, each node sends data to its cluster head. Cluster head collect all the data and verify the valid data.

- Data aggregation

Finally the process of data aggregation is done after verifying the valid data by the cluster head. And send data to the base station.

- Data Decryption

Base station receives the data from each cluster head and decrypts the data by the appropriate key.

- Data Recovery

Base station checks for the lost data and run the cache based recovery system to recover the data.

B. Algorithm

Algorithm 1: Proposed Algorithm

Step 1.Create a network graph as Graph g(v,e) where; V are vertices/nodes and E are edges.
Step 2. Apply clustering algorithm on the number of nodes and divide the nodes in to number of clusters.
Step 3.On The basis of energy, number of neighbors and distance to the base station select the Efficient Cluster Head.
Step 4. Perform the key distribution at each node through Base Station.
Step 5.Perform the route generations from each node to the base station.
Step 6.Generate the data at each node and encrypt the data with the public key of base station.
Step 7.Calculate the hash value of the encrypted data and Record the timestamp.
Step 8.Send the individual data to the cluster head from each cluster member in all the clusters.
Step 9. Collect all data at the cluster head. Verify the data by its hash value and accept the verified data or discard if hash value is invalid.
Step 10.Aggregate all the data and send this data to the base station. Base station accepts the data from each cluster head.
Step 11.Base station verifies the data and decrypts the data with appropriate key.
Step 12.Base station checks for the lost data and run the cache based recovery system to recover the data.

Description: The propose algorithm describes the flow of a system. First network is created with sensor nodes, after that clustering algorithm implemented and number of nodes is divided into number of clusters, cluster head is selected on the basis of three parameters, key distribution is performed at each node through base station, route is generated from each node to the base station. Encrypt the data by using the EC-ElGamal+ algorithm with the private key. Hash value is evaluated of the encoded data and timestamp is recorded. Cluster member send the data to the cluster head in all clusters. Data is verified by its hash value, if it is verified then it is accepted otherwise rejected. After that aggregate all the data and send to the base station. Base station decrypts the data with the appropriate keys. Base station checks the lost data and run the cache based recovery system for data recovery.

C. Mathematical Model

System S is represented as S= { D, T, U, H, G, F, LD, DR}

1. Deploy nodes

D= {D1, D2, ..., Dn}
D is set of all deployed nodes.

2. Create Base Station

T= {T1, T2, ..., Tn}
Where, T is a set of all base stations.

3. Create clusters

U= {U1, U2, ...,Un}
Where, U is a set of all clusters.

4. Select the Cluster Heads in Each Clusters

H = {H1, H2,....,Hn}

Where H is a set of all cluster heads.

5. Generate the the keys for authentication

G = {G1, G2,....,Gn}

Where G is a set of all Keys.

6. Generate the the signature for verification

SK = {SK1, SK2,....,SKn}

Where SK is a set of all signature.

7. Data sending from cluster members to cluster Head and from here to base station

F={f1, f2, f3, ...fn}

Where, F is a set of all data files transmitted.

8. If the data is lost during operation recover the lost data.

LD = {LD1, LD2,.....,LDn}

LD is a set of all lost files which are manipulated.

9. Data recovery

DR= {DR1, DR2,....,DRn}

Where, DR is a set of all recovered files at base station.

Energy consumption is evaluated as:

$E_{TX}(l, d) = E_{TX\text{-}elec(l)} + E_{TX\text{-}amp(l,d)}$

$$= \begin{cases} E_{elec} * l + \epsilon_{fs} d^2 * l & d < d0 \\ E_{elec} * l + \varepsilon_{amp} d^4 * l & d \geq d0 \end{cases}$$

Where $d0 = \sqrt{\frac{\varepsilon_{fs}}{\varepsilon_{amp}}}$ and the energy consumption of receiving this message is:

$E_{RS}(l) = Eelec * l$

D. Experimental Setup

The system developed in Java framework (version jdk 8) on Windows platform. For development, the Netbeans (version 8.1) tool is used. The network is generated using Jung tool in which contain sensor nodes. The system doesn't need any specific hardware to run, any standard machine is capable of running the application.

V. RESULT AND DISCUSSION

E. DataSet

In this system dataset is not required.

F. Results

Figure 2 shows the comparison graph for package drop ratio of existing and proposed system. In the existing system package drop ratio is more as compare to the package drop ratio in the proposed system.

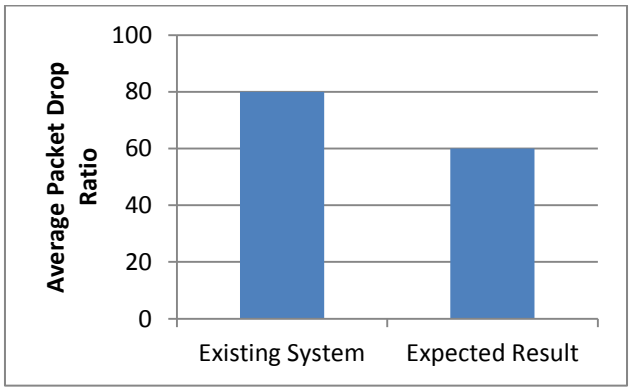

Figure 2. Average packet drop ratio graph comparison

Figure3 shows the comparison graph for energy consumption ratio of existing and proposed system. The existing system has high energy consumption ratio than the proposed system.

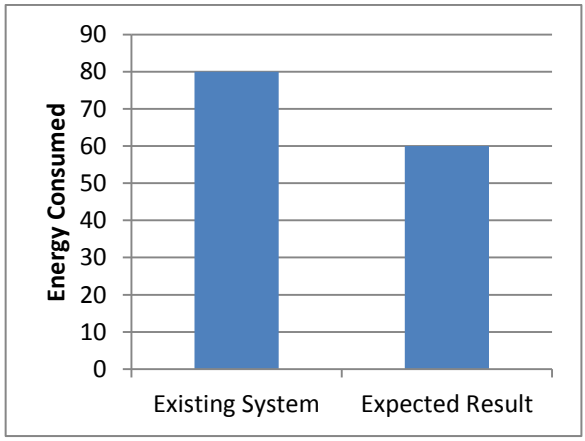

Figure 3. Energy Consumption Graph Comparison

VI. CONCLUSION

The proposed method helps to increases the network lifetime of the wireless sensor network also introduced the method by which cluster head is selected on the basis of three parameters, from which the network consumes its energy and increase the network lifetime of the wireless sensor network. The proposed system also introduced the method for recovery of the data loss at the time of broadcasting the data. Finally generate the results which conclude that the proposed system is increase the network lifetime of the system.

VII. REFERENCES

[1]. Kyung-Ah Shim, "A Secure Data Aggregation Scheme Based on Appropriate Cryptographic Primitives in Heterogeneous Wireless Sensor Networks", in IEEE transactions on parallel and distributed systems, vol. 26, NO.8, august 2015.

[2]. D. Boneh and M. Franklin, "Identity-based encryption from the Weil pairing," SIAM J. Comput., vol. 32, no. 3, pp. 586-615, 2003.

[3]. C. Castelluccia, E. Mykletun, and G. Tsudik, "Efficient aggregation of encrypted data in wireless sensor network, MobiQuitous '05," pp. 1-9, 2005.

[4]. C.-M. Chen, Y.-H.Lin, Y.-C.Lin, and H.-M. Sun, "RCDA: Recoverable concealed data aggregation for data integrity in wireless sensor networks," IEEE Trans. Parallel Distrib. Syst., vol. 23, no. 4, pp. 727-734, Apr. 2012.

[5]. J. Domingo-Ferrer, "A provably secure additive and multiplicative privacy homomorphism," in Proc. 5th Int. Conf. Inf. Security, 2002, pp. 471-483.

[6]. J. Girao, D. Westhoff, and M. Schneider, "CDA: Concealed data aggregation for reverse multicast traffic wireless sensor networks," in Proc. IEEE Int. Conf. Commun., 2005, pp. 3044-3049.

[7]. E. Mykletun, J. Girao, and D. Westhoff, "Public key based cryptoschemes for data concealment in wireless sensor networks," in Proc. IEEE Int. Conf. Commun., 2006, pp. 2288-2295.

[8]. A. Shamir, "Identity-based cryptosystems and signature schemes," in Proc. Int. Cryptol. Conf. Adv. Cryptol., 1984, pp. 47-53.

[9]. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks:Attacks and countermeasures," Ad Hoc Networks, vol. 1,pp. 293-315, 2003.

[10]. X. Liu, "Survey on clustering routing protocols in wireless sensornetworks," Sensors, vol. 12, pp. 11113-11153, 2012.

[11]. E. Mykletun, J. Girao, and D. Westhoff, "Public key based cryptoschemesfor data concealment in wireless sensor networks," inProc. IEEE Int. Conf. Commun., 2006, pp. 2288-2295.