ISSN:0975-9646

Secure Data Aggregation forEnhancingQoS in H-WSN

Ms. **Shubhangi Gaikwad**
Department of computer engineering of JSCOE
Handewadi Road, Hadapsar,
Pune-411028, India

Prof. **S. V. Todkari** (IEEE Member)
Department of information technology of JSCOE
Handewadi Road, Hadapsar,
Pune-411028, India

***Abstract*—The cost of energy is needed for performing the operation over node is equivalent to the forwarding the single bit of data over a network. At the time of forwarding data in sensor network, data transportation decreases the network lifetime. So, there is requirement of decrease the energy utilization and enhance the network lifetime. When communication is going on with anyone of the cluster member, that time cluster head comes often in communication because cluster head is the aggregator node of the cluster. So, there is more energy utilization as compared with other members in the cluster. Previous system has strategy to select cluster head randomly because of that it utilizes more energy. To solve the problem, we proposed system represents a technique in that effective cluster head is chosen based on the distance from the base station and remaining energy. When we choose effective cluster head, it utilizes minimum energy of sensor network and helps to increase the network lifetime of the sensor network. Responsibility of aggregation of data is over the head of the cluster from all its cluster members. Initially before data aggregation, verification of data is performed by cluster head and if data is not valid then data is discarded. Verified data only gets aggregated at the cluster head. Encryption of data is accomplished by using Homomorphic encryption technique and encrypted data is forwarded to the cluster head and data decryption is accomplished by only base station to provide end to end security. An ID based signature method is implemented to give hop by hop authentication. In this paper, we proposed a technique to recover the lost data because of the buffer overflow . In this system ,cluster head provide cache memory for data loss recovery. At the end, experimental outcomes are demonstrates on the basis of parameters such as time and energy utilization over jung simulator that our system is better as compared to the previous system.**

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

I. INTRODUCTION

In recent years, Wireless sensor networks (WSNs) are becomes popular in different areas of life. WSN has number of application areas such as observation of the environment, specifically, temperature, humidity and tectonic activities and number other ecological, law enforcement and military surveillance to securely forward their data by the network to a main location. WSNs are commonly implemented areas like in public or commonly untrusted and even unfriendly scenarios that prompt different security problems. These include the processes such as key administration, security, access control, authentication and DoS resistance etc.

The sensor network has some problems such as changing or energizing the node batteries due to dense and ad-hoc operation in critical environment as well as because of unobserved nature of WSNs. There is a significant question is emerges, how to enhance the network lifetime of the sensor networks. It is additionally critical problem such as enhance network lifetime by decreasing energy utilization of node in WSNs. Experimental outcomes are shows that the data transfer is very costly on the basis of energy consumption (EC) but on the other hand data processing consumes significantly low energy. Furthermore, a practical methodology requires to enhance the WSN lifetime and to reduce the sensor energy consumption at the time of data transfer. There is another one problem of security of information at the time of forwarding information from source to destination in the wireless sensor network.

Sensor nodes with forced resources are subject to number of attacks, therefore the data encryption is important in WSNs. If data is transmitted without encryption then the attackers will analyze the data and includes false data in the network. In hop- by- hop encrypted data aggregation (EDAs),which is a mediator aggregator having keys of all regarding sensor nodes decrypts got encrypted values, complete all the decrypted values and encrypts the result for forwarding to a base station (BS). This technique needs that mediator aggregators store keys for decryption in that a caught aggregator would reveal these confidential information.

In this paper, fundamentally concentrate on the three difficulties which is generally address in the wireless sensor networks. To begin with is enhancing the network lifetime of the sensor network through minimizing the energy utilization in the network. Second is to give the security while the information transmission from sender to recipient node or from sender to base station. Third is information loss recovery, when forwarding the information to cluster head information is lost due to storage capacity limitation of cluster head. For enhancing the system lifetime presented the strategy in which cluster head is chosen on the premise of energy, number of neighbors and separation to the base station. By choosing the cluster head through determining these three parameters diminishes the energy value needed to the sensor node. Homomorphic encryption is utilized for giving the security to the information.

Information is forwarded in the encoded manner to the base station, base station decode the information subsequent to accepting the information. Likewise the procedure of information aggregation is accomplished in which cluster head aggregate the information which is gathered by the cluster nodes. For data loss recovery we are provide cache memory at cluster head. At the end, the outcome is contrasted for the network lifetime, energy utilization and for previous and proposed system.

This paper concentrates over related work in section II,system implementation details, problem definitions, algorithms, mathematical model in section III. Section IV demonstrates the expected outcome of a system and at the end conclusions and future workgiven in section V.

II. Literature Survey

This section describes the various works accomplished by the researchers for the data aggregation, enhancing network lifetime of the sensor nodes.

Kyung-Ah Shim [1] proposed a SDA technique, Sen-SDA, which depends on the grouping of suitable cryptographic primitives in heterogeneous cluster WSNs. To diminish the aggregate length of ciphertexts and to fulfill end-to-end protection, they expect an additional substance HE technique, so only a BS can decrypt encrypted data gathered by the CHs got from member nodes for each gathering of cluster. To provide hop-by-hop authentication, they use a coordinating free identity based signature (IBS) strategy, thus the BS and the CHs can observe the authenticity of all the transmitted encrypted data. To improve efficiency of various signatures verifications, they need a signature strategy in which various signatures from different endorsers on different messages can be checked quickly.

D. Boneh and M. Franklin [2] propose a totally practical identity based encryption method. This method has chosen cipher text security in the random oracle model receiving a variety of the computational Diffie-Hellman problem. This system relies on bilinear maps between clusters. The Weil consolidation on elliptic curve is an example of such an guide. They give a precise definition to secure identity based encryption plans and provide a couple of utilizations for such structures.

C. Castelluccia, E. Mykletun, and G. Tsudik[3] focus on productive, information transmission conversing security in WSNs. More specially, they combine unassuming encrypted techniques with essential aggregation frameworks to perform greatly productive gathering of encrypted data. To assess the sensibility of proposed procedures, they assess them moreover, display to a great ensuring outcomes which clearly show measurable information transmission ability protection and little overhead starting from both encrypted and aggregation operations.

C.-M. Chen, Y.-H.Lin, Y.-C.Lin, and H.-M. Sun [4] introduce a concept called as Recoverable Concealed Data Aggregation (RCDA). In RCDA, a base station can recover each detecting data created by all sensors regardless of the possibility that these data have been aggregated by cluster heads or aggregators. With these individual data, two functionalities are provided. In the first place, the base station can affirm the uprightness and authenticity of all detecting data. Second, the base station can play out any aggregation limits on them. By then, they propose two RCDA methods named RCDA-HOMO and RCDA-HETE for homogeneous and heterogeneous WSN independently. They display that the proposed methods are secure under these attack model in the security examination.

J. Domingo-Ferrer [5] represents one such PH which can be exhibited secure against known-cleartext attacks, the length of the ciphertext space is much greater than the cleartext space. A couple of applications to designation of sensitive handling and data and to e-betting are immediately illustrated.

J. Girao, D. Westhoff, and M. Schneider [6] introduce an approach that 1) covers identified data end-to-end by 2) up 'til now providing beneficial and versatile in-network data aggregation. The aggregating mediatory nodes are not important to work at the distinguished plaintext data. They implement a particular class of encrypted changes and discuss frameworks for enlisting the aggregate capacities "average" and "movement detection." They exhibit that the technique is feasible for the class of "going down" routing protocols. They consider the danger of contaminated sensor nodes by proposing a key pre-distribution algorithm that confines an attackers expansion and show up how key pre-distribution and a key-ID sensitive "going down" routing protocol grows the quality and trustworthiness nature of the related spine.

E. Mykletun, J. Girao, and D. Westhoff [7] reconsider the congruity of additively homomorphic public key encryption counts for certain classes of wireless sensor networks. Finally, they provide recommendations for picking the most suitable public key arrangements for different topologies and wireless sensor network circumstances.

A. Shamir [8] introduce a new sort of cryptographic arrangement, which enables any pair of customers to convey securely and to check each other's imprints without exchanging private or public keys, without keeping key indexes and without using the organizations of an outsider. The arrangement acknowledges the nearness of trusted key generation, whose sole configuration is to provide each customer a customized smart card when he first joins the framework. The information introduced in this card enables the customer to sign and encode the messages he sends and to interpret and check the messages he gets in a completely free way, despite of the identity of the other party. Already issued cards don't should be redesigned when new customers join the framework, and the diverse focuses don't have to encourage their activities or even to keep a client list. The focuses can be shut after all the cards are issued, and the system can continue working in a completely decentralized manner for an uncertain period.

III. Existing System

This section describes the previous system utilized for secure forwarding the data.

Working of the previous system is as follows:

1.Create 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 andEncrypt with the public key of base stationat 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 describes the system overview in which proposed algorithm and mathematical model of the proposed system is also present.

A. System Overview

System architecture of the proposed is displayed in figure 1that is separated in differentstepsand steps are illustrated below.

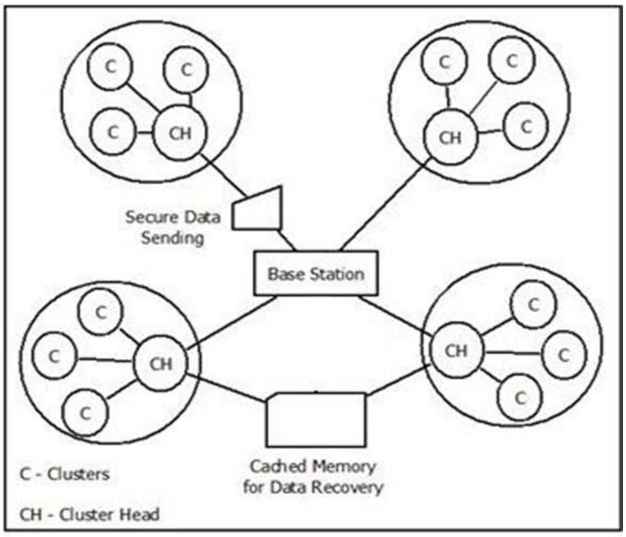

Fig. 1.Proposed System Architecture

- *Network Generation*

At start network is generated where vertices/nodes are associated with the edges.

- *Clustering Process*

After the network generation, the clustering procedure is executed in that nodes are separated in numerous clusters.

- *Cluster Head Selection*

After creating the group of clusters, from every group of clusters, the cluster head is chosenbased on energy and distance from base station and neighbor nodes parameters.

- *Key generation and distribution*

Base station can accomplish key generation and distribution to every node. Route generations performed from every node to the base station.

- *Data Encryption*

At every node data is generated and encrypted through the EC-ElGamal+.

- *Hash value evaluation*

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

- *Data Collection*

After assessing, the hash value at every node, every node forwards data to its cluster head. Cluster head have some limited capacity to store the data if the cluster head storage is overflowed then the data is dropped at cluster head. The cluster head aggregates all the data and verify the valid data.

- *Cached Data*

In system, to avoid the data loss at cluster head due to the limitation of storage capacity we are maintaining a cache storage that can store the data dropped in the process of data forwarding between cluster members and cluster head.

- *Data verification*
  By batch verification technique, verify the data by using hash value and timestamp. In this we are first verify cached data and then data that are stored in cluster head storage.
- *Data aggregation*

At the end, process of data aggregation is accomplished after verifying the valid data by the cluster head and data forwarded to the base station.

- *Data Decryption*

Base station collects the data from every cluster head and decrypts the data by the appropriate key.

B. Algorithm

Algorithm 1: Proposed Algorithm

Step 1: Generate a network graph as Graph g(v,e) where; V are vertices/nodes and E are edges.

Step 2: Implement clustering algorithm over the number of nodes and separate 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 every node via Base Station.

Step 5: Perform the route generations from every node to the base station.

Step 6: Create the data at every node and encrypt the data with the public key of base station.

Step 7: Compute the hash value of the encrypted data and Record the timestamp.

Step 8: Send the individual data to the cluster head from every cluster member in all the clusters. If storage capacity of cluster head is exceed the limit then store the data in cache memory.

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.

Description: Proposed algorithm illustrates the flow of thesystem. Initially, network is generated including sensor nodes, further clustering algorithm applied and number of nodes is separated in number of clusters.Cluster head is chosen based on parameters, key distribution is executed at every node by the base station.Route is created from every node to the base station. Data encryption is accomplished through the EC-ElGamal+ algorithm with the private key. Hash value is assessed of the encrypted data and timestamp is recorded. Cluster member forwards the data to the cluster head in all clusters and overflow data is stored in cache memory. Data verification is done on the basis of hash value; if it is verified then only accepted otherwise rejected. After that aggregate all the data and forward to the base station. Base station decrypts the data with the appropriate keys.

C. Mathematical Model

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

1. Deploy nodes

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

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

3. Select the Cluster Heads in Each Clusters
H = {H1, H2,....,Hn}
Where H is a set of all cluster heads.

4. Generate the the keys for authentication
G = {G1, G2,....,Gn}
Where G is a set of all Keys.

5. Generate the the signature for verification
SK = {SK1, SK2,....,SKn}
Where SK is a set of all signature.

6. 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.

7. 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.

8. 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:

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

D. Experimental Setup

System builds on Java framework (version jdk 8) over Windows platform. For development, the Netbeans (version 8.1) tool is utilized. The network is created utilizing Jung tool with sensor nodes. System doesn't require any particular hardware to run any standard machine is able to run the application.

V. Result And Discussion

A. DataSet

This system doesn’t need a dataset.

B. Results

Figure 2 demonstrates the comparison graph for energy consumption of existing and proposed system. In the existing system energy consumption is more as compare with the proposed system on the basis of round vs energy consumed.

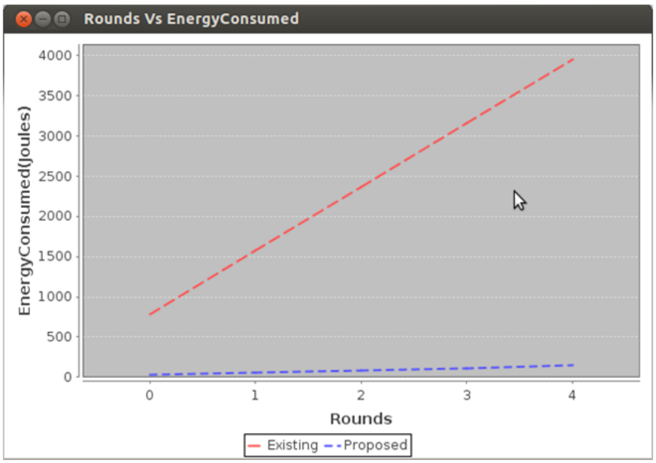

Fig2. Round Vs Energy Consumed Comparison Graph

Figure3 demonstrates the comparison graph for time of existing and proposed system. The existing system requires more timeas compared with the proposed system.

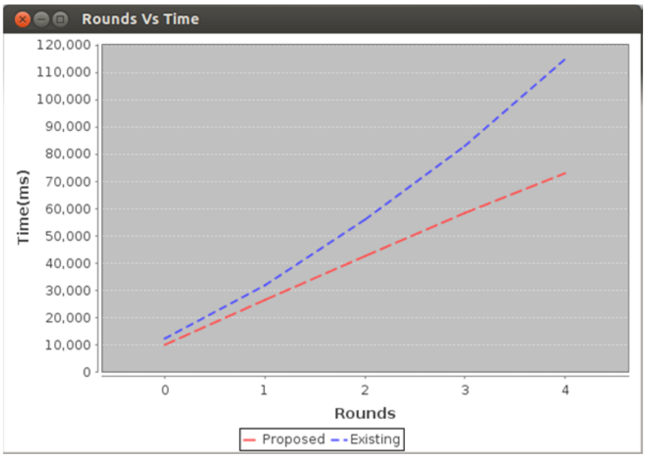

Fig3. Rounds Vs Time Comparison Graph

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 less 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.

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.