RESEARCH ARTICLE OPEN ACCESS

Reduction of Energy Consumption in Wireless Sensor Network Using Data Aggregation Technique

Komal Shinde[1], Sangita Varpe[2], Rohini Shinare[3],Vishakha Varma[4] ,Prof.M.D.Ingle[5]

Abstract:

A wireless sensor network typically includes a huge number of low-powered, less-cost sensing devices called as sensors with restricted computational, memory and communication assets. In the data aggregation technique, the information of sensor nodes is merged at cluster head nodes and then transmitted that aggregated data to the base station. The sensor nodes consume energy during sensing, processing and transmission. In wireless sensor network power and energy resources are limited. If every node sends data to the base station, energy will be wasted and thus the network energy will be consume quickly. Existing work in the literature uses PCA (Principle Component Analysis) and CS(Compressed Sensing) strategies. The proposed algorithms are Iterative Case Filtering (ICF) is used to decrease the energy consumption in an energy efficient manner and SHA (Secure Hash Algorithm) for matching sender and receivers hash key. If both the hash keys are same then data will be sent and duplicated packets will be discarded to reduce network traffic.

Keywords **— Data Aggregation, Energy Consumption, Iterative Case Filtering, Secure Hash Algorithm, Wireless Sensor Network.**

I. INTRODUCTION

A wireless sensor network typically includes a huge number of low-powered, less-cost sensing devices called as sensors with restricted computational, memory and communication assets. Remote sensor network contains a few number of sensor nodes which are dispersed over different areas with the objective of monitoring their physical or environmental conditions, gathers the information and processes it. These sensing devices are comprised of basic controller, application particular sensors, transceiver and battery. Data aggregation approach includes gathering of data and making information accessible to the base station in energy profitable manner. In the data aggregation technique, the information of sensor nodes is merged at cluster head nodes and then transmitted that aggregated data to the base station. Data aggregation is utilized to decrease the transportation overhead because of finite amount of power in sensor nodes. Cluster head also called as aggregator performs data aggregation by gathering information from cluster members and then sends it to base station. Sensor nodes have limited computation power, battery, less storage capacity. Hence there is a need to save such assets and amount of data to be transmitted over network. This can be possible by utilizing the effective procedure called data aggregation . For giving security with

data aggregation, concept of Secure Hash Algorithm (SHA) can be utilized. Iterative Case Filtering (ICF) algorithms can be utilized for the same purpose. It reduces network traffic by discarding duplicated packets and reduces energy consumption. It utilizes a single iterative method and gives solution for the issues, data aggregation and secure data transmission. The dependability of every sensor is evaluated by taking into account the distance of sensor readings from given weights. Sensor readings are fundamentally varied from such estimate. So the sensors are considered as low dependability furthermore in the aggregation process, their readings are assigned with a lower weight in the present round of iteration. Secure Hash Algorithm (SHA) provides security to data transmission. If we send data from sender to receiver first it checks whether hash keys of sender and receiver are same then and only then data will be send. If duplicate data will send from sender to receiver then also data will be discarded at receiver side.

II. RELATED WORK

In this paper [1], author proposed clustering approaches, principal component analysis (PCA) and compressed sensing (CS) strategies. It Reduces power consumption, energy consumption and boost scalability of the network. When transmitted data is analysed computational effort & signalling required to find eigenvectors basis is not rewarded with a reduction in the energy consumption.

Author introduced [2] an optimal routing and data aggregation technique for wireless sensor networks. The objective is to increase the network lifetime by jointly optimizing data aggregation and routing. Multiple sink nodes and for nodes with sleeping mode are not used.

In this paper [3] author proposed IPC3 and OPC3 models to optimize amount of energy use for data transmission. Recovering schemes are slow in the event of an upstream node failure .

Energy-efficient and Secure Pattern-based Data Aggregation protocol (ESPDA) is energy and bandwidth effective because cluster-heads prevent the transmission of redundant data from sensor nodes. It increases the energy and bandwidth efficiency the protocol minimizes the number of packets transmitted [4]. Results are generated only for small networks.

In this paper [5], author introduces a new attack which is known as sophisticated collusion attack in contrast to existing IF algorithms. Advancement is contributed over the existing

Iterative filtering algorithm by giving initial approximation of trust, which makes existing algorithm more factual, robust and faster converging. Limitation of the approach is it does not detect and protect compromised aggregators. Author tried to implement approach in a deployed sensor network.

Author proposed [6] a reputation algorithm which is based on correlation model and used in web based rating system to solve the ranking problem that can be generated by the influence of spammer attack. Author represents user's reputation by using correlation coefficient and iterative method to find the similarity between users rating vector and objects weighted average rating vector. Proposed algorithm is more efficient and robust but still the exactness of algorithm can be improved.

Author introduced [7] an "Iterative Trust and Reputation Management Scheme" (ITRM) which is a strong system to estimate the reputation of the service provider and level of trust on the raters. Author proposes the central command that gathers reports and generates the provider's reputation based on the obtained ratings from consumers. Outcome of the comparison of proposed scheme and existing reputation controlling schemes shows that proposed scheme is more efficient and powerful to detect malicious ratings and to compute reputation of provider in less time in the existence of attack.

Author proposed a framework [8], called RFSN, in which each sensor node maintains the reputation for each other node in a network, based on which the trustworthiness is calculated. The framework also considers the limitations of the sensor nodes. Within RSFN, a beta reputation system is established which uses Bayesian formulation to estimate the trustworthiness of sensor nodes. RFSN gives the approach to detect all misdeed resulted from malicious and faulty sensors in a network. It also integrates various solutions of security.

III. Problem Definition

Energy is the most important aspect in wireless sensor network. The existing system has a problem of energy depletion at particular node which generates cuts in the network that results in decreased network lifetime. The main problem with previous system is that they are randomly selecting aggregator in each cluster. The main role of aggregator is to communicate with each member of cluster and perform the aggregation of all the data. So it is obvious that more energy is consumed at that node. Hence to overcome this problem we are electing aggregator node based on maximum energy from each cluster. Because of this low power performance of aggregator occurs in network. Most of the time duplicated data send from sender to receiver due to which network congestion/traffic occurs. This paper introduced Iterative Case Filtering (ICF) Algorithm to avoid such network traffic by discarding duplicated packets. While transmitting data, data is less secure so proposed system uses Secure Hash Algorithm (SHA) for matching senders and receivers hash keys. If both hash keys are same then and only then data will be send.

IV. Work Of Existing System

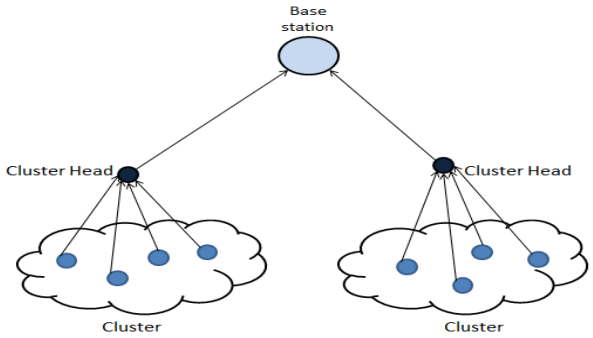

Fig.1. Existing System Architecture

In existing system, cluster head selection is done randomly due to which energy will be wasted and thus the network energy will be consume quickly. If duplicated packets reach to receiver from sender it simply accept packet without checking duplication due to which network congestion/traffic occurs. Existing system does not deal with security mechanism which is responsible to sending false data from sender to receiver.

V. Work Of Proposed System

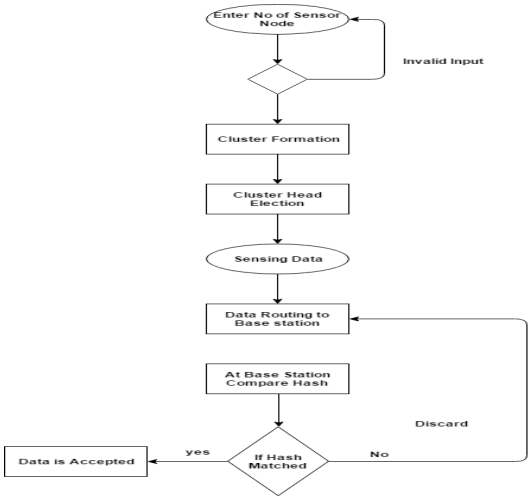

Fig.2. Proposed System Architecture

The nodes of network are partitioned into disjoint groups, and every group has a head which is known as an aggregator or cluster head. Information are intermittently gathered and aggregated by the cluster head. In the proposed system we accept the reality that the aggregator node can be compromised in the same way as that of cluster members. Compromised aggregator may send false aggregated values to the base station. Hence we expect a technique in propose work that can detect duplicated data as well as on aggregator with the help of Iterative filtering algorithm. This also includes a Secure Hash Algorithm (SHA) for matching hash keys of sender and receiver. With the introduction of this, it is expected to increase the security and energy efficiency of the WSN.

System is divided into number of steps which are described as follows:

• Generation of Network: Generation of sensor nodes network is performed here. And the nodes are connected through the edges.

• Cluster Formation: Numbers of clusters are formed by dividing the sensor nodes into different groups.

• Selection of Cluster Head/ Aggregator: Aggregator is selected from each cluster. Aggregator selection is done by using parameter like highest remaining energy of the nodes. This step is performed twice, after initial formation of clusters and for selection of new aggregator on detecting attack on old aggregator.

• Iterative Case Filtering: The new ICF algorithm is used for discarding duplicated packets. This iteratively checks the readings and assigns weights to the node.

• Matching hash keys: Hash keys are generated at sender and receiver side. Hash keys are checked while transmission of data .If sender and receiver's hash keys are same then and only then data will be send.

VI. Mathematical Model

- Set Theory:

Let, S be a system, S= { N, C, CH, B, CN, A}, where,

1. Deploy Sensor nodes.N= { N1, N2, ..., Nn }, N is set of all deployed sensor nodes.

2. Cluster formation. C= { C1, C2, ..., Cn }, C is a set of all clusters.

3. Select the Cluster Heads that is aggregator for Each Clusters. CH= { CH1, CH2, ..., CHn }, CH is a set of all cluster heads.

4. Create Base Station. B= { B1, B2, ..., Bn }, B is a set of all base stations.

- Mathematical Model Of ICF Algorithm:

Input: X, n, m.

Output: The reputation vector r

l ← 0;

w(0) ← 1;

repeat

Compute r (l+1);

$$\mathbf{r}^{(l+1)} = \frac{X \cdot \mathbf{w}^{(l)}}{\sum_{i=1}^{n} w_i^{(l)}}$$

Compute d;

$$d_i = \frac{1}{m} \left\| \mathbf{x}_i - \mathbf{r}^{(l+1)} \right\|_2^2$$

Compute w(l+1);

$$w_i^{(l+1)} = g(d_i),\ (1 \le i \le n).$$

l ← l + 1;

l ← l + 1;

until reputation has converged;

parameter

X:- a block of readings is represented by a matrix

n:- no of sensor node

m: m-dimensional readings reported by sensor node

d:- d which is the distance between the sensor readings

and the reputation vector

w:- weight vector

w(0) = 1 :- The iterative procedure starts with giving equal credibility to all sensors, i.e., with an initial value w(0)

- Mathematical model for proposed system For Energy Calculation :

Etx (k; d) = Eelec * K+ ∈amp * k * d n ERx(k) = Eelec * k

d: Distance for neighbouring sensor node. ∈amp: Energy required for the transmitter amplifier.

Eelec: Energy consumed for driving the transmitter or receiver circuitry.

VII. Algorithm

- Algorithm 1 Pseudo code of propose system is

1. Input: V = Set of all nodes
2. Initialize energy to each node of V
3. Calculate energy of each node N
4. Calculate distance to the neighbouring node and to the base station
5. Compare energy and distance of all nodes
6. Select maximum energy and minimum distance node

7. Output: CH = node whose having maximum energy and minimum distance to base station

VIII. ANALYSIS AND RESULT

- Energy Graph

  Figure 3 shows the comparison graph for energy consumption ratio of existing and expected system. We expect that the energy consumed by the propose system will be less as compared to existing system.

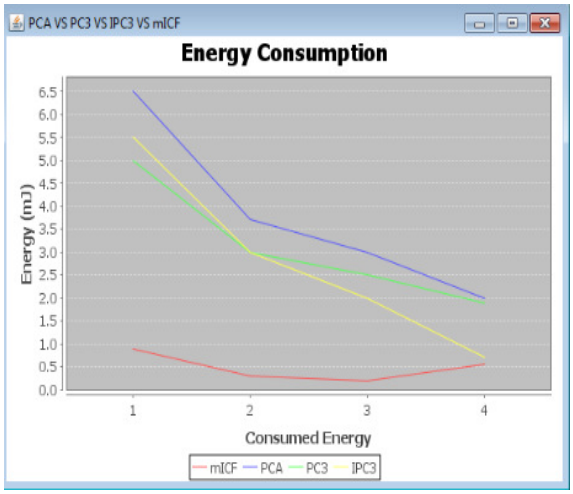

Fig. 3 Energy Comparison between Existing and Propose Algorithms

- Data Graph

  Figure 4 shows, comparison between mean number of average data of different algorithms. We expect that the mean number of average data send by the propose system will be less as compared to existing system.

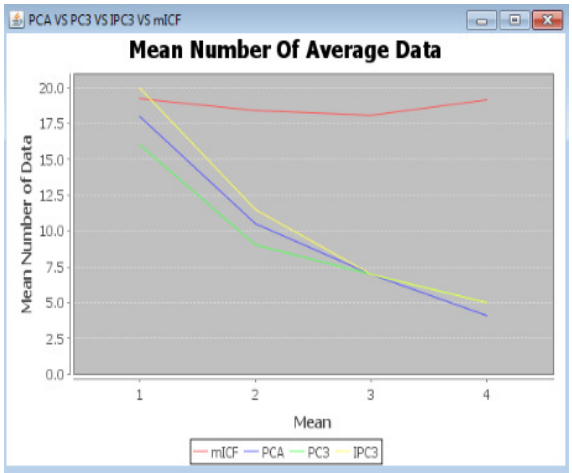

Fig. 3 Mean Number of Average Data Send between Existing and Propose Algorithms

IX. CONCLUSION

Iterative Case Filtering (ICF) algorithm is one of the powerful techniques for secure data aggregation which provides trust valuation for sensor nodes based on the data gathered from different sources. In proposed work, secure and robust data aggregation will perform. Also it will detect the duplicate packets send by sender and energy efficiency will improve by discarding duplicate packets. Secure Hash Algorithm (SHA) is used for matching hash keys of sender and receiver. If both keys are same then and only then data will be send. We expect that the propose system will be more robust against compromised aggregator node also it will reduce mean number of average data and energy consumption compared to the existing system. In future work, we will try this algorithm on real time system.

REFERENCES

[1] Antoni Morell, Alejandro Correa, Marc Barceló, and José López Vicario, "Data Aggregation and Principal Component Analysis in WSNs", IEEE transaction on wireless communication, VOL. 15, NO. 6, June 2016.

[2] C. Hua and T. P. Yum, "Optimal routing and data aggregation for maximizing lifetime of wireless sensor networks," IEEE Trans. Netw., vol. 16, no. 4, pp. 892–903, Aug. 2008.

[3] C. Anagnostopoulos and S. Hadjiefthymiades, "Advanced principal component-based compression schemes for wireless sensor networks," *ACM Trans. Sensor Netw.*, vol. 11, no. 1, pp. 7:1–7:34, Jul. 2014.

[4] H.cum, S. Ozdemir, P. Nuir*, D.Muthuavinashiappun, "ESPDA: Energy-efficient and secure pattern base data aggregation for wireless sensor networks," 0-7803-813 3-5/03/$17.0002 003IEEE .

[5] M. Rezvani, A.r. Ignjatovic, E. Bertino, and S. Jha, "Secure Data Aggregation Technique for Wireless Sensor Network in the Presence of Collusion Attacks ", IEEE transaction on dependable and secure computing, vol. 12, no. 1, january/february 2015.

[6] Y. Zhou, T. Lei, and T. Zhou, "A robust ranking algorithm to spamming," Europhys. Lett., vol. 94, p. 48002, 2011.

[7] E. Ayday, H. Lee, and F. Fekri, "An iterative algorithm for trust and reputation management," Proc. IEEE Int. Conf. Symp. Inf. Theory, vol. 3, 2009, pp. 20512055.

[8] S. Ganeriwal, L. K. Balzano, and M. B. Srivastava, "Reputation based framework for high integrity sensor networks,"ACM Trans. Sens. Netw., vol. 4, no. 3, pp. 15:1-15:37, Jun.2008.