Journal of Computer Science 8 (6): 899-907, 2012
ISSN 1549-3636

Fuzzy Based Secure Data Aggregation Technique in Wireless Sensor Networks

[1]HevinRajesh, D. and [2]B. Paramasivan
[1]Department of Information Technology,
St. Xavier's Catholic College of Engineering, Tamil Nadu, India
[2]Department of Computer Science and Engineering,
National Engineering College, Kovilpatti, Tamil Nadu, India

Abstract: Problem statement: Secure data aggregation is a challenging task in wireless sensor network due to the facts like more complexity, greater overhead in the case of cryptographic techniques. These issues need to be overcome using efficient technique. **Approach:** We propose a fuzzy based secure data aggregation technique which was having 3 phases. In its first phase, it performs clustering and cluster head election process. In the second phase, within each clusters, power consumed, distance and trust values were calculated for each member. In the third phase, based on these parameters, fuzzy logic technique was used to select the secure and non-faulty node members for data aggregation. Finally, the aggregated data from the cluster heads was transmitted to the sink. **Results:** By simulation results we show that our technique had improved throughput and packet delivery ratio with reduced packet drop and less energy consumption. **Conclusion:** The proposed technique efficiently checks for malicious nodes based on the system parameters and maintains a secure aggregation process in the network.

Key words: Secure data aggregation, wireless sensor networks, energy consumption, fuzzy logic, clustering, tree-structured routing, adhoc system

INTRODUCTION

Wireless sensor networks: One of the up coming technologies is the wireless sensor network and now it has attained much consideration from the field of research. A sensor network consists of numerous small devices which are inexpensive and organize itself into an adhoc system. The wireless sensor network monitors the physical environment to collect the data and transfers it to the other sink nodes in the network. Usually, in the sensor nodes the range of radio transmission varies in the orders of the magnitude that is lesser than geological coverage of the network. Hence hop by hop technique is used in transmitting the information to the sink. The energy consumed in the sensor network can be decreased by reducing the total data transmission (Bhoopathy and Parvathi, 2012; Elangovan and Perinbam, 2012).

The wireless sensor network comprises of large amount of electromechanical devices which are smaller and possess the ability to sense, compute and communicate with each other. Such devices are used in gathering sensory data like that of temperature measurement in a geological area under extension (Bhoopathy and Parvathi, 2012). Based on the variety of application of the wireless sensor networks many research have been carried out in this field. Restricted power, memory and computational power are the characteristics of the nodes. The sensor nodes are susceptible to breakdown mainly because of intrinsic unsteadiness and sensor's energy constraints (Al-Azawi *et al*., 2012).

WSN is vulnerable to various problems related to security. In order to overcome the security related problems of the wireless sensor network, several works are done but are scattered in different papers. WSN gives way to several threats and limitation due to its characteristics such as tree-structured routing, data aggregation, tolerable failures, in-network filtering and computation and phased transmission periods. In the sensor network, maximum of the attacks in the network layer belong to one of the class, given as follows:

- Spoofed, altered, or replayed routing information
- Selective forwarding
- Sinkhole attacks

Corresponding Author: HevinRajesh, D., Department of Information Technology, St. Xavier's Catholic College of Engineering, Tamil Nadu, India

- Sybil attacks
- Wormholes
- HELLO flood attacks
- Acknowledgement spoofing

Data aggregation: In order to conserve energy and minimize the contention of the medium access layer in the wireless sensor networks, data aggregation is considered to be the most fundamental technique in distributed data processing. In the sensor networks, for routing in wireless, data aggregation is considered as an important pattern. Merging all the information from various sources, routing it and removing the redundant part, reducing the transmission number and conserving energy is the main scheme followed in data aggregation. Using the process of in-network data aggregation, the redundancy in the data that is gathered from other sensors can be prevented. Application specific information can be extracted by using this process in raw data. Sustaining high incidence is important for the network to preserve energy for a long lifetime (Bhoopathy and Parvathi, 2012).

Secure data aggregation: Problems related to security in data aggregation are as follows (Ozdemirand Xiao, 2009):

- Data Confidentiality: The transferred data which are very sensitive towards the passive attacks are safeguarded by maintaining the data confidentiality. Data confidentiality is the most basic issue related to security. In unreceptive environment such as wireless channel which are very susceptible to eavesdropping, data confidentiality is very important. Cryptography techniques can maintain confidentiality but the complex encryption and decryption process involved such as modular multiplications which includes several public key based cryptosystems consumes power at high rate
- Data Integrity: The extensive alteration of the ultimate aggregated value by the compromised source node or the aggregator node can be eliminated by maintaining data integrity. The shortage of high cost tampering resistant hardware makes the sensor nodes get compromised in a effortless way. In case the sensor node possesses tampering-resistant hardware, it will be unreliable. Modification, forging and discarding of messages can be performed by the compromised node

Secure data aggregation can be carried out in two ways which are as follows:

- Hop-by-Hop encrypted data aggregation

End-to-End encrypted data aggregation (Ozdemir and Xiao, 2009).

Problem statement and proposed solution: Examining the existing methods related to protected data aggregation, the following issues are noted:

- High communication overhead
- High complexity
- Higher overhead whenever cryptographic technique is used
- Consumes more bandwidth
- No discussion about minimizing the energy consumed

No discussion about collective resolution for integrity and authentication.

In this proposal, we propose to design a fuzzy based secure data aggregation algorithm. This algorithm consists of 3 phases.

In phase1, the sensor nodes are grouped into various clusters and each cluster has one elected cluster head. The cluster head initially estimates the distance between each member and itself, by exchanging topology discovery packets.

In phase2, the cluster head collects the data from its members. Along with data, the each member attaches its current power level. Then the cluster head determines the trust level of each node by estimating the correctness of data. It can be estimated with the help of spatio and temporal changes (i.e.,) difference in two consecutive values and difference in readings of neighbor sensors.

In phase 3, Fuzzy logic is applied to select the best nodes for aggregation. The parameters trust level, power level and distance to the cluster head of each node are taken as input and fuzzy rules are formed. After applying the rules, the output will be the treated as the best node or Normal node or Worst node. The cluster head will try to aggregate the packets of the best node and normal node, rejecting the worst node. Finally, the aggregated data from all the cluster heads will be sent to the sink.

Since the fuzzy decision rule is based on trust and power level of the node, our approach is power efficient and secured. Moreover it does not involve any complex cryptographic operations, resulting in less overhead.

Related work: Almamani and Almashakbeh (2010) have proposed a power-efficient, secure routing protocol is proposed to help managing the resources in WSN networks. The proposed protocol is a hybrid of two major categories of protocols in WSNs, namely tree-based and cluster-based protocols. The proposed

protocol is combined with a Fuzzy Logic inference system to aid in the selection of the best route based on a combination of three factors: the path length, the available power and the node reputation resulted from the Intrusion Detection System (IDS).

Feng *et al*. (2011) have proposed a node behavioral strategies banding belief theory of trust evaluation algorithm that integrates the approach of nodes behavioral strategies and modified evidence theory. They employed a fuzzy set method temporarily to form the basic input vector of evidence. They compute the evidence difference among the indirect and direct trust values, which link the revised D-S evidence combination rule to finally synthesize integrated trust value of nodes.

Moon and Cho (2009) have proposed the intrusion detection scheme using fuzzy logic for detecting and defending sinkhole attacks in directed diffusion based sensor networks. In that study, they showed the vulnerability of the directed diffusion routing protocol to sinkhole attacks.

Senthilkumar and Chandrasekar (2010) have proposed secure routing technique in wireless sensor networks. They utilized a multile paths and multiple base stations to tolerate against the individual base station attacks or compromise attacks. Their mechanism offers pair-wise keys to each pair of neighboring sensor nodes. This provides a secure protection.

Perez-Toro *et al*. (2010) have proposed a robust data aggregation protocol (RDAS) which uses a reputation based approach to identify and isolate malicious nodes in a sensor network. Their scheme tolerates unreliable ratings to detect nodes that report faulty data. They used hierarchical clustering arrangement of nodes, where a cluster head uses the rating to prevent erroneous data from affecting the aggregation result.

MATERIALS AND METHODS

Fuzzy based secure data aggregation technique:

Phase1: Clustering: In the wireless network, the nodes select the clusterhead based on the connectivity of the nodes. The nodes in the network, which possess higher connectivity when compared with its 2 hop neighbors, are initially selected as clusterhead. These clusterheads then broadcast an advertisement message to all its surrounding nodes. The advertisement message includes the cluster-head ID and location information of the cluster head. The non cluster head nodes first record all the information from cluster heads within their communication range.

Each non-cluster head node chooses one of the strongest Received Signal Strength (RSS) of the advertisement as its cluster head and transmits a member message back to the chosen cluster head. The information about the node's capability of being a cooperative node, i.e., its current energy status is added into the message. The message also includes information related to consistency value, consistent sensing count and inconsistent sensing count of the node.

If an advertisement message signal is obtained at a clusterhead from another clusterhead y, which has the RSS value greater than a threshold then clusterhead y will be considered as the neighbor clusterhead and the ID of y is stored.

Phase 2:

Distance estimation:

In wireless communications,

If the communication distance d < distance threshold d_0,

then free Space channel model is used.

Else

multi-path fading model is used (Jun *et al*., 2010).

Hence, for transferring k-bit message over a distance d, the energy consumed is determined by the radio model using Eq. 1:

$$\begin{aligned} E_T &= E_{Tx}(k,d) = E_{Tx-elec}(k) + E_{Tx-amp}(k,d) \\ &= \begin{cases} kE_{elec} + k\varepsilon_{fs}d^2, (d < d_0) \\ kE_{elec} + k\varepsilon_{mp}d^4, (d \geq d_0) \end{cases} \end{aligned} \quad (1)$$

where, E_{elec} is the transmitter circuitry dissipation per bit.

The receiving cost is computed using Eq. 2:

$$E_R = E_{Rx}(k) = E_{Rx-elec}(k) = kE_{elec} \quad (2)$$

Reducing the network energy cost in WSN to increase the lifetime is shown in our mathematical model using Eq. 3:

$$\text{Min}(E_{total}) \quad (3)$$

$$E_{total} = E_T + E_R + E_I + E_S \quad (4)$$

Where:

E_{total} = Total energy cost in the network
E_T = The transmission cost
E_R = The receiving cost
E_I = The energy cost while being in idle state
E_s = The energy cost while sensing

Generally, in sensor nodes the cost for transmitting the data is a variable whereas the idle cost and cost for receiving and sensing the data are non varying. Hence the total cost of the network is calculated based on the transmission cost. Therefore the new equation for the total energy cost of Eq. 4 is given by Eq. 5:

$$\text{Min}\left(E_T\right) \tag{5}$$

In the wireless model, based on the cost of transmission Eq. 5 can be given as Eq. 6:

$$\begin{aligned}&\text{Min}\left(E_{Tx}(k,d)\right) = E_{Tx-elec}(k) + E_{Tx-amp}(k,d)\\ &= \begin{cases} kE_{elec} + k\varepsilon_{fs}d^2, (d < d_0) \\ kE_{elec} + k\varepsilon_{amp}d^4, (d \geq d_0) \end{cases}\end{aligned} \tag{6}$$

Where:
k = The number of bit forwarding on the distance d
E_{elec} = The transmitter circuitry dissipation per bit
ε = The transmit amplifier dissipation per bit

The critical effect of d on the energy cost of the network is shown in Eq. 6. Hence the system model can be given as Eq. 7:

$$\text{Min}\ (d^n) \tag{7}$$

where, n is set to 2 or 4.

In the wireless sensor networks, between the nodes the communication distance is lower and the mode of communication is a two way process. We have set the n value to 2 and hence Eq. 7 can be given as Min(d^2).

d_{NoCH} is used to represent the distance between a node and a cluster head. Hence our Eq. 8 is further reduced to:

$$\text{Min}\left(d^2_{NtoCH}\right) \tag{8}$$

Trust evaluation: To test the consistency of the sensor nodes, its trust values are determined.

Spatio values: The calculation based on the spatio readings considers the average of the difference between the distances of the nodes in the cluster. Then the obtained value is compared with the threshold value.

For instance, the cluster possess 5 sensor nodes i.e., s1, s2, s3, s4 and s5. Then the distance between the consecutive nodes is calculated as d1, d2, d3, d4 and d5. The average of the values is calculated, η_1 and compared with threshold value, δ_1 of the cluster.

Temporal values: For the calculation based on the temporal process, each sensor node compares its present reading with the previous reading and an average of the readings of all the sensors is determined. The average value is then compared with the threshold value.

For instance, the cluster possesses 5 sensor nodes i.e., s1, s2, s3, s4 and s5 and the difference between the consecutive readings of every node is r1, r2, r3, r4 and r5. Then the average value η_2 of the readings is compared with its threshold value, δ_2 of the cluster.

If $\eta_1 > \delta_1$ and $\eta_2 > \delta_2$, then the nodes are inconsistent.

If $\eta_1 < \delta_1$ and $\eta_2 < \delta_2$, then the nodes are consistent.

Two counters called consistent sensing counter and inconsistent sensing counter are maintained, for the values of η_1 and η_2.

Consistency factor: It indicates the reliability of the sensor node. The sensor nodes can be classified as malicious or compromised node based on the consistency factor. Thus it helps in maintaining the network data away from that of the malicious nodes. This factor is estimated using the formula:

$$CV_i = \frac{CC_{Si} - IC_{Si}}{CC_{Si} + IC_{Si}} \text{ where } -1 \leq C_i \leq 1$$

Where:
CV_i = The consistency value of node i ($1 \leq i \leq k$)
CC_{Si} = The consistent sensing count of node i
IC_{Si} = The inconsistent sensing count of node i

Sensing communication factor: It maintains the information related to the communication ratio.

The selfishness and the regularity of the sensor nodes is indicated by this factor:

$$SR_i = \frac{SS_i - SF_i}{SS_i + SF_i}$$

Where:
SR_i = The sensing communication value of node i where $1 \leq i \leq k$
SS_i = The sensing success count of node i
SF_i = The sensing failure count of node i

Battery factor: It indicates the remaining lifetime of the sensor node in the network. The collapse of the biased battery can be eliminated by working out according to the selected battery factor. This in turn minimizes the further procedures required to process the power managing strategies.

B_i is the battery value of node i where $1 \leq i \leq k$

The Combined Trust Value (CTV) of the node i is calculated as follows:

$$CTV_i = \frac{W_1 B_i + W_2 SR_i + W_3 CV_i}{\sum_{i=1}^{3} W_i} \text{ where } 0 \leq W_i \leq 1$$

where, W_i is the weight which represents the importance of a particular factor from 0 (unimportant) to +1 (most important).

Power estimation: The battery value represents the power in the nodes. Each sensor node broadcasts quantification value of its own B_i:

$$B_i : -1 \leq B_i \leq 1$$

Phase 3: The cluster head now evaluates the status of the node in order to select the nodes for data aggregation. For this purpose, fuzzy logic is used.

Fuzzy logic: The problems involving QoS can be settled by the pro-active technique provided by the fuzzy logic. The working of a very dynamic nonlinear scheme such as a WSN, not in need of the system mathematical model can be handled efficiently by fuzzy logic (Basaran *et al*., 2010). Applications like control systems, decision making, pattern recognition and system modeling make use of the fuzzy if-then rules. Three stages are involved in the fuzzy rule based inference algorithm.

- Fuzzy matching: the degree to the input fundamental steps and condition of the fuzzy logic are determined
- Inference: on the basis of the degree of match, the conclusion of the rule is determined
- Combination: the result obtained by every fuzzy rules are merged together into a single overall result (Feng *et al*., 2011)

Rule definition: A fuzzy set A in X is characterized by a membership function which are easily implemented by fuzzy conditional statements. In the case of fuzzy statement if the antecedent is true to some degree of membership then the consequent is also true to that same degree.

The rule structure: If antecedent then consequent.

The rule: If variable1 and 2 are low and variable3 is high then output is benign else output is malignant.

The fuzzy Logic in decision making uses the following technique.

In this study, the fuzzy if-then rules consider the parameters: distance, power consumed and trust for evaluating the nodes. For the three inputs: distance, power consumed and trust, the resulting possibilities are Best Node (BN), Normal Node (NN) and Worst Node (WN). Here the inputs can take 2 values Less and High. Hence the total number of outputs in this case is $2^3 = 8$.

The selection criterion is such that a node should have lower distance and power consumption values but with high trust value.

The first parameter, distance D can be represented as a fuzzy set as:

Distance, D = FuzzySet[{BN, a}, {NN, b}, {WN, c}]

Where:

a = The membership grade for Best Node in Distance calculation
b = The membership grade for Normal node in Distance calculation
c = The membership grade for Worst node in Distance calculation

The second parameter, power consumed P can be represented as a fuzzy set as:

Power consumed, P = FuzzySet[{BN, e}, {NN, f}, {WN, g}]

Where:

e = The membership grade for Best Node in the calculation of power consumption
f = The membership grade for Normal node in the calculation of power consumption
g = The membership grade for Worst node in the calculation of power consumption

The third parameter, trust T can be represented as a fuzzy set as:

Trust, T = FuzzySet[{BN, u}, {NN, v}, {WN, w}]

Where:

u = The membership grade for Best Node in trust calculation
v = The membership grade for Normal node in trust calculation
w = The membership grade for Worst node in trust calculation

The final decision is made on the basis of the output of the intersection of the corresponding members of the fuzzy sets of the three parameters; distance, power consumed and trust value.

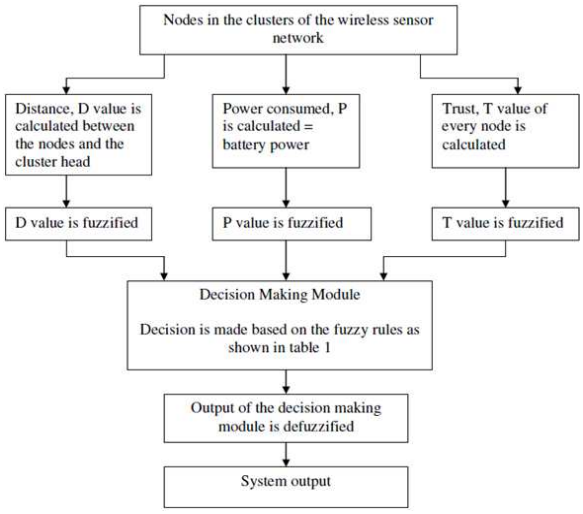

Fig. 1: Decision making using fuzzy logic

Table 1: Fuzzy rules

Distance, D	Power consumed, P	Trust, T	Result
Less	Less	High	Best
Less	High	High	Normal
High	Less	Less	Normal
Less	Less	Less	Normal
Less	High	Less	Worst
High	Less	Less	Worst
High	High	High	Worst
High	High	Low	Worst

The resultant of the system is the one with the high membership grade. Table 1 shows the conditions for decision making in fuzzy logic for inputs and its corresponding results. The Fig. 1 shows the block representation of the decision making in our fuzzy system.

Let distance, trust and power consumed be denoted by D, T and P:

If D and P are less and if T is high then node is a best node.
If D is less, P is high and T is high then node is a normal node.
If D is high, P is less and T is less then node is a normal node.
If D is less, P is less and T is less then node is a normal node.
If D is less, P is high and T is less then node is a worst node.
If D is high, P is less and T is less then node is a worst node.
If D is high, P is high and T is high then node is a worst node.
If D is high, P is high and T is less then node is a worst node.

The if-then rule simplifies this as the following.

Defuzzification of the fuzzified values can be carried out by several techniques such as centroid average method, max centre method, mean of maxima, smallest of maximum and largest of maximum. In our case, we defuzzify using the maximum method. After decision making on the basis defuzzification, the normal and the best nodes are selected by the clusterhead for data aggregation whereas the worst nodes are neglected by the cluster head.

Then the clusterhead transfers the aggregated data to the destination i.e., sink. Since the values of malicious and faulty sensors are not aggregated, secure data aggregation is ensured in the wireless sensor network.

RESULTS AND DISCUSSION

The performance of our Fuzzy Based Secure Data Aggregation (FBSDA) technique is evaluated through NS2 Network Simulator. A random network deployed in an area of 500×500 m is considered. Initially 30 sensor nodes are placed in square grid area by placing each sensor in a 50×50 grid cell. 4 phenomenon nodes which move across the grid (speed 5 m sec^{-1}) are deployed to trigger the events. 4 cluster heads are deployed in the grid region according to our protocol. The sink is assumed to be situated 100 meters away from the above specified area. In the simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. The simulated traffic is CBR with UDP source and sink. The number of sources is fixed as 4 around a phenomenon.

Table 2 summarizes the simulation parameters used.

Performance metrics: The performance of FBSDA technique is compared with the Power-Efficient Secure Routing Protocol (PESRP) (Almamani and Almashakbeh, 2010). The performance is evaluated mainly, according to the following metrics.

- Average Packet Delivery Ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted
- Throughput: It is the number of packets received by the sink successfully
- Drop: It refers to the no. of valid packets dropped due to malicious nodes
- Energy: It is the average energy consumed for the data transmission

Table 2: Simulation parameters

No. of nodes	30
Area size	500×500
Mac	802.11
Routing protocol	DSDV
Simulation time	50 sec
Traffic Source	CBR
Packet Size	512 bytes
Rate	50-250 kb
Transmission range	150 m
No. of events	4
Speed of events	5 m sec^{-1}
Transmit power	0.395 w
Receiving power	0.660 w
Idle power	0.035 w
Initial energy	5.1 Joules
Misbehaving nodes	2
No. of clusters	4

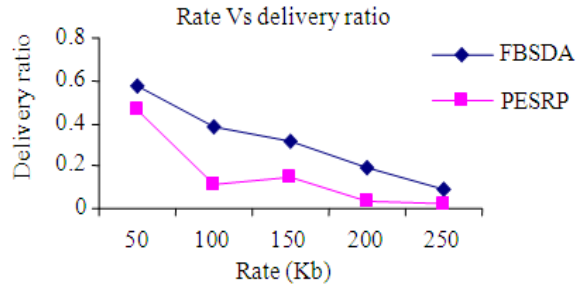

Fig. 2: Rate Vs delivery ratio

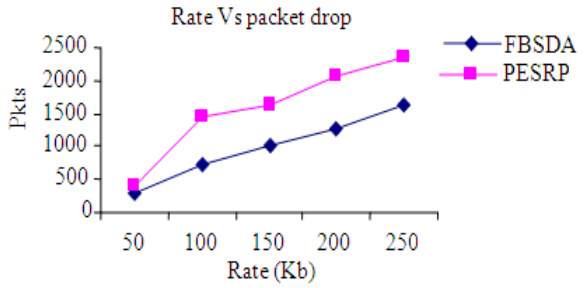

Fig. 3: Rate Vs drop

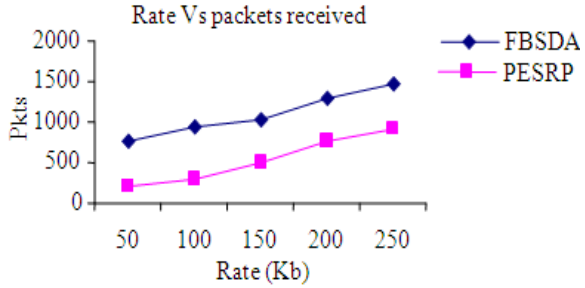

Fig. 4: Rate Vs received

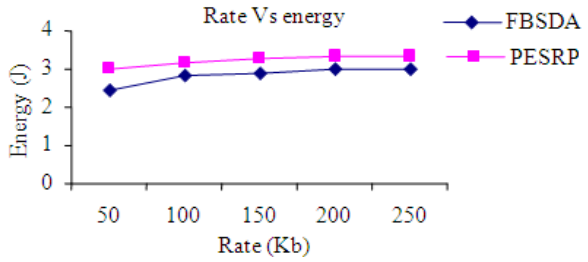

Fig. 5: Rate Vs energy

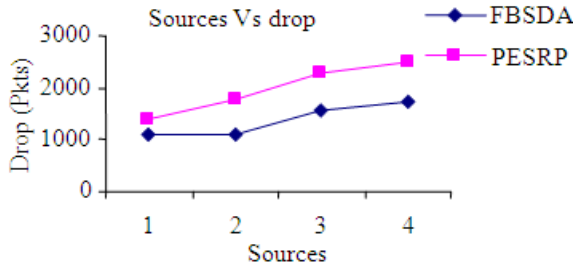

Fig. 6: Sources Vs delivery ratio

Based on rate: In our initial experiment, we vary the rate as 50, 100, 150, 200 and 250 Kb.

Figure 2 gives the packet delivery ratio when the rate is increased. It shows that our proposed FBSDA protocol achieves good delivery ratio when compared to PESRP.

Figure 3 gives the packet drop when the rate is increased. It shows that our proposed FBSDA has lower packet drop than the PESRP.

Figure 4 gives the packet received, when the rate is increased. It shows that our proposed FBSDA protocol has received more number of packets than the PESRP.

Figure 5 gives the energy consumption, when the rate is increased. It shows that our proposed FBSDA has less Energy consumption than PESRP.

Based on sources: In the second experiment, we vary the traffic flows as 1, 2, 3 and 4.

Figure 6 gives the packet delivery ratio when no. of sources is increased. It shows that our proposed FBSDA protocol achieves good delivery ratio when compared to PESRP.

Figure 7 gives the packet drop when no. of sources is increased. It shows that our proposed FBSDA has lower packet drop than the PESRP.

Figure 8 gives the Packet Received, when no. of sources is increased. It shows that our proposed FBSDA protocol has received more number of packets than the PESRP.

Figure 9 gives the energy consumption, when no. of sources is increased. It shows that our proposed FBSDA has less Energy consumption than PESRP

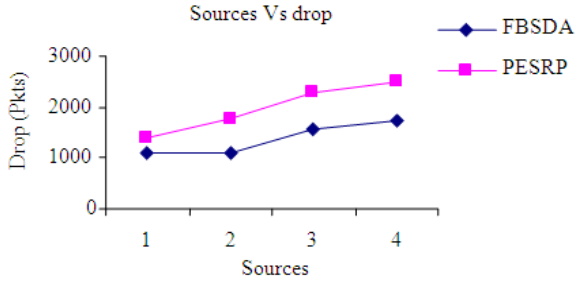

Fig. 7: Sources Vs drop

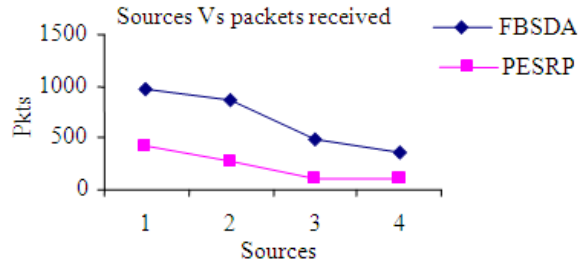

Fig. 8: Sources Vs received

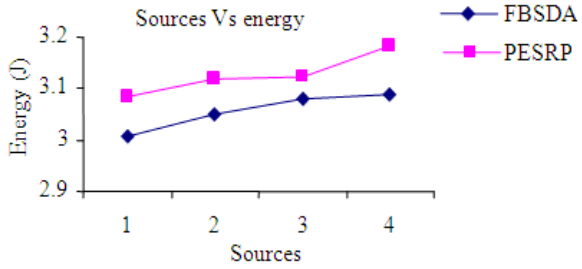

Fig. 9: Sources Vs energy

CONCLUSION

In this study we have developed a technique which performs secure data aggregation. Our technique consists of three phases. In the first phase, the network is divided into clusters. The sensor nodes with the higher signal strength are selected as clusterhead. In the second phase, the distance between the nodes and the clusterhead is calculated. Also the trust and the power consumed by the member nodes in each cluster are determined. These three parameters: distance, power consumed and the trust value of the sensor nodes are used to determine if the sensor node can be used for data aggregation. In the third phase, we use fuzzy logic to classify the sensor nodes into best node, normal node and worst node based on the selected parameters. After classification of the nodes, the best and the normal nodes are selected for data aggregation whereas the worst nodes are neglected by the clusterhead. Finally the aggregated data is transferred by each cluster head to the sink. Since the values of malicious and faulty sensors are not aggregated, secure data aggregation is ensured in the wireless sensor network. By simulation results we show that our technique has improved throughput and packet delivery ratio with reduced packet drop and less energy consumption.

REFERENCES

Almamani, I. and E. Almashakbeh, 2010. A power-efficient secure routing protocol for wireless sensor networks. WSEAS Trans. Comput., 9: 1042-1052.

Al-Azawi, S., S. Boussakta and A. Yakovlev, 2012. Image compression algorithms using intensity based adaptive quantization coding. Am. J. Eng. Applied Sci., 4: 504-512. DOI: 10.3844/ajeassp.2011.504.512

Bhoopathy, V. and R.M.S. Parvathi, 2012. Energy constrained secure hierarchical data aggregation in wireless sensor networks. Am. J. Applied Sci., 9: 858-864. DOI: 10.3844/ajassp.2012.858.864

Basaran, C., K.D. Kang and M.H. Suzer, 2010. Hop-by-hop congestion control and load balancing in wireless sensor networks. Proceedings of the 35th IEEE Conference on Local Computer Networks (LCN), Oct. 10-14, IEEE Xplore, Denver, CO., pp: 448-455. DOI: 10.1109/LCN.2010.5735758

Elangovan, G. and J.R. Perinbam, 2012. Wideband E-shaped microstrip antenna for wireless sensor networks. Am. J. Applied Sci., 89-92. DOI: 10.3844/ajassp.2012.89.92

Feng, R., X. Xu, X. Zhou and J. Wan, 2011. A trust evaluation algorithm for wireless sensor networks based on node behaviors and d-s evidence theory. Sensors, 11: 1345-1360. DOI: 10.3390/s110201345

Jun, W., Z. Xin, X. Junyuan and M. Zhengkun, 2010. A distance-based clustering routing protocol in wireless sensor networks. Proceedings of the 12th IEEE International Conference on Communication Technology (ICCT), Nov. 11-14, IEEE Xplore Press, Nanjing, pp: 648-651. DOI: 10.1109/ICCT.2010.5688947

Moon, S.Y. and T.H. Cho, 2009. Intrusion detection scheme against sinkhole attacks in directed diffusion based sensor networks. IJCSNS Int. J. Comput. Sci. Netw. Security, 9: 118-122.

Ozdemir, S. and Y. Xiao, 2009. Secure data aggregation in wireless sensor networks: A comprehensive overview. Comput. Netw., 53: 2022-2037. DOI: 10.1016/j.comnet.2009.02.023

Perez-Toro, C.R., R.K. Panta and S. Bagchi, 2010. RDAS: Reputation-based resilient data aggregation in sensor network. Proceddings of the 7th Annual IEEE Communications Society Conference on Sensor Mesh and Ad Hoc Communications and Networks (SECON). Jun. 21-25, IEEE Xplore Press, Boston, MA., pp: 1-9. DOI: 10.1109/SECON.2010.5508273

Senthilkumar, A. and C. Chandrasekar, 2010. Secure routing in wireless sensor networks. Int. J. Comput. Sci. Eng., 2: 645-655.