Available online at www.sciencedirect.com

SciVerse ScienceDirect

ELSEVIER

Procedia Engineering 38 (2012) 3331 – 3336

Procedia Engineering

www.elsevier.com/locate/procedia

International Conference on Modeling Optimization and Computing

Fuzzy logic based performance optimization with data aggregation in wireless sensor networks

D. Hevin Rajesh[a] , Dr. B. Paramasivan[b, a*]

[a]*Department of Information Technology, St. Xavier's Catholic College of Engineering, Chunkankadai, 629003, India*
[b]*Department of Computer Science & Engineering, National Engineering College, Kovilpatti, 628503, India*

Abstract

Wireless sensor networks are characterized by multi hop wireless lossy links and resource constrained nodes. Energy efficiency is a major concern in such networks. Due to their constraints in computation, memory, and power resources, the performance optimization is a challenging task in these networks. In this paper, fuzzy based secure data aggregation technique is used to select the secure and non-faulty node members for data aggregation. The aggregated data from the cluster heads is transmitted to the sink. This technique efficiently checks for malicious nodes based on the system parameters and maintains a secure aggregation process in the network. By simulation results, we show that our technique has improved throughput and packet delivery ratio with reduced packet drop and less energy consumption based on rate.

Keywords: Wireless sensor networks, Data aggregation, Fuzzy logic

1. Introduction

A wireless sensor network is a collection of sensors interconnected by wireless communication channels. Each sensor node is a small device that can collect data from its surrounding area, carry out simple computations, and communicate with other sensors or with the controlling authorities of the network. Long distance communications are achieved in a multi hop fashion. Such networks have been

* Corresponding author. Tel.: +91-936-021-2753; fax: +91-465-223-3982.
E-mail address: hevin@sxcce.edu.in.

1877-7058 © 2012 Published by Elsevier Ltd.
doi:10.1016/j.proeng.2012.06.385

realized due to recent advances in micro electromechanical systems and are expected to be widely used for applications such as environment monitoring, intrusion detection, and earthquake warning [1]. Potential applications for WSNs-apart from military are the detection of fire in huge forest areas, the monitoring of wild animals. Movement patterns, the incremental shift of ice and snow in alpine mountains, or even the control of the ground humidity in vineyards. Further applications for wireless sensor networks are envisioned in the biomedical sector. Even monitoring the health status of cattle stocks on farms may be supported by a WSN [2]. 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 [3].

1.1. Data aggregation

In many of these applications, the data to be collected are "state-based," that is, they consist of measurements of ambient surroundings. Significant redundancies often exist in such data due to spatial-temporal correlations. These local redundancies can be removed prior to sending the oversized raw data to the sink and draining the limited sensor energy store. This process, referred to as "data aggregation" or "data fusion," is quite attractive, as it is often infeasible or costly to replenish the batteries of the deployed sensors [4]. Data aggregation is an important primitive that aims to combine and summarize data packets from several sensor nodes so that communication bandwidth and energy consumption are reduced [5]. In terms of security, data aggregation is risky. A sensor node that is compromised by an adversary can either illegally disclose the data it collects from other nodes or report arbitrary values as its aggregation results. Therefore, an adversary can compromise both the confidentiality and the integrity of the data of a large portion of the wireless sensor network by capturing a number of data aggregators that are positioned close to the base station [6].

2. Problem statement and proposed solutions

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, and no discussion about minimizing the energy consumed. 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.

2.1. Related works

Iman Almomani et al. 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) [7].

Tae Kyung Kim and Hee Suk Seo have suggested a trust model using fuzzy logic in sensor network. Trust is an aggregation of consensus given a set of past interaction among sensors. They applied their suggested model to sensor networks in order to show how trust mechanisms are involved in communicating algorithm to choose the proper path from source to destination [8].

Soo Young Moon and Tae Ho Cho have proposed the intrusion detection scheme using fuzzy logic for detecting and defending sinkhole attacks in directed diffusion based sensor networks. In that paper, they showed the vulnerability of the directed diffusion routing protocol to sinkhole attacks [9].

Bryan Parno et al. have designed, implemented, and evaluated a new secure routing protocol for sensor networks. Their protocol is efficient yet highly resilient to active attacks [10].

Junbeom Hur et al. have proposed a secure data aggregation scheme based on trust evaluation model which can identify trustworthiness of sensor nodes. This model suggests a defensible approach against insider attacks incipiently beyond standard authentication mechanisms and conventional key management schemes [11].

3. Proposed work

In order to select nodes for data aggregation, fuzzy logic based selection is used. The problems involving quality of service 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 [12]. Applications like control systems, decision making, pattern recognition and system modelling make use of the fuzzy if-then rules. Three stages are involved in the fuzzy rule based inference algorithm are fuzzy matching, inference and combination. Fuzzy matching is the degree to the input fundamental steps and conditions of the fuzzy logic are determined. Inference is on the basis of the degree of match, the conclusion of the rule is determined. Combination is the result obtained by every fuzzy rules are merged together into a single overall result [8].

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 fuzzy Logic in decision making uses the following technique. In this work, 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 two 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 is the membership grade for best node in distance calculation, b is the membership grade for normal node in distance calculation and c is 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 is the membership grade for best node in the calculation of power consumption, f is the membership grade for normal node in the calculation of power consumption and g is 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 is the membership grade for best node in trust calculation, v is the membership grade for normal node in trust calculation and w is 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. 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.

Table 1. Fuzzy rules

Serial No.	Distance, D	Power consumed, P	Trust, T	Result
1	Less	less	high	best
2	Less	high	high	normal
3	High	less	less	normal
4	Less	less	less	normal
5	Less	high	less	worst
6	High	less	less	worst
7	High	high	high	worst
8	High	high	low	worst

4. Performance metrics

The performance of fuzzy based secure data aggregation technique is evaluated through NS2 simulation. The performance of FBSDA technique is compared with the Power-Efficient Secure Routing Protocol (PESRP) [7]. The performance is evaluated mainly, according to the following metrics. Average packet delivery ratio is the ratio of the number of packets received successfully and the total number of packets transmitted. Throughput is the number of packets received successfully. Received refers the number of packets received by the receiver. Energy refers the total energy required to the packet transmission.

5. Results

In our experiment, we vary the rate as 50,100,150.200 and 250 Kb. Fig. 2. gives the packet delivery ratio when the rate is increased. It shows that our proposed FBSDA technique achieves good delivery ratio when compared to PESRP. Fig. 3. gives the packet drop when the rate is increased. It shows that our proposed FBSDA has lower packet drop than the PESRP. Fig. 4. gives the packet received, when the rate is increased. It shows that our proposed FBSDA technique has received more number of packets than the PESRP. Fig. 5. gives the energy consumption, when the rate is increased. It shows that our proposed FBSDA has less energy consumption than PESRP.

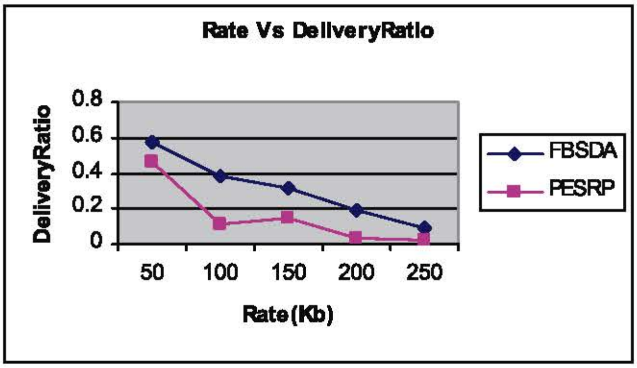

Fig. 2. Rate vs delivery ratio

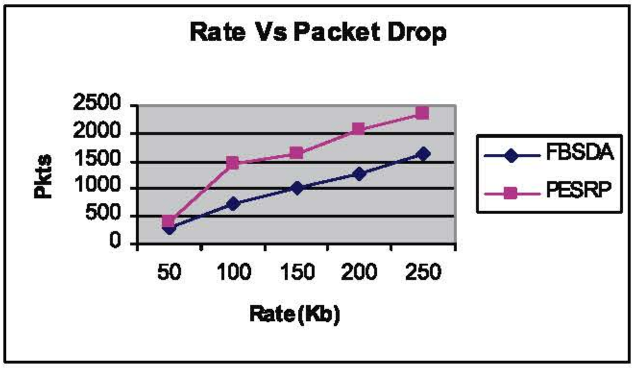

Fig. 3. Rate vs drop

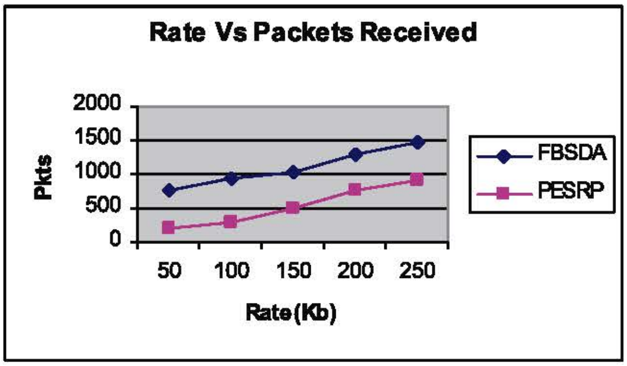

Fig.4. Rate vs received

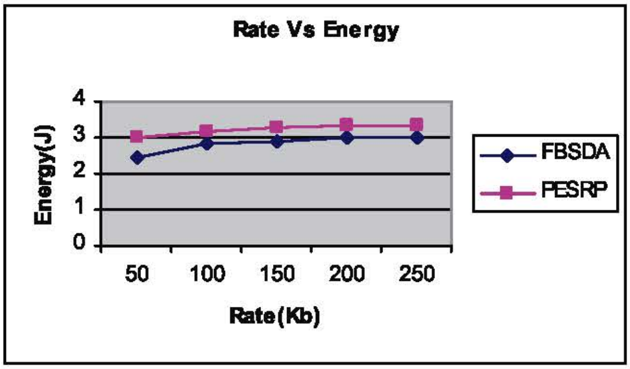

Fig. 5. Rate vs energy

6. Conclusion

In this paper, we have developed a technique which performs fuzzy based secure data aggregation. 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 cluster head. 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 based on rate.

References

[1] F. Zhao, L. Guibas. Wireless sensor networks: an information processing approach. *(Morgan Kaufmann Series in Networking)*. San Mateo, CA: Morgan Kaufmann; 2004.

[2] Dirk Westhoff, Joao Girao, Mithun Acharya. Concealed data aggregation for reverse multicast traffic in sensor networks: encryption, key distribution, and routing adaptation. *Ieee Transactions On Mobile Computing*; 2006, 5:1417-1431.

[3] John A. Clark, John Murdoch, John A. McDermid, Sevil Sen, Howard R. Chivers, Olwen Worthington. et al. Threat modelling for mobile ad hoc and sensor networks. *Annual Conference of ITA*. 2007, p. 25-27.

[4] Yuanzhu Peter Chen, Arthur L. Liestman, Jiangchuan Liu. A hierarchical energy-efficient framework for data aggregation in wireless sensor networks, *Ieee Transactions On Vehicular Technology*; 2006, 55:789-796.

[5] S. Ozdemir, Y. Xiao. Secure data aggregation in wireless sensor networks: a comprehensive overview. *Computer Networks*; 2009, 53:2022–2037.

[6] S. Ozdemir, Y. Xiao. Integrity protecting hierarchical concealed data aggregation for wireless sensor networks. *Computer Networks*; 2011, 55:1735–1746.

[7] Iman Almamani, Emad Almashakbeh. A power-efficient secure routing protocol for wireless sensor networks. *Wseas Transactions on Computers*; 2010, 9:1042-1052.

[8] Tae Kyung Kim, Hee Suk Seo. A trust model using fuzzy logic in wireless sensor network. *World Academy of Science, Engineering and Technology*; 2008, 42:63-66.

[9] Soo Young Moon, Tae Ho Cho. Intrusion detection scheme against sinkhole attacks in directed diffusion based sensor networks. *International Journal of Computer Science and Network Security*; 2009, 9:118-122.

[10] Bryan Parno, Mark Luk, Evan Gaustad, Adrian Perrig. Secure Sensor Network Routing: A Clean- Slate Approach. *In Proceedings of the 2nd Conference on Future Networking Technologies*; 2006.

[11] Junbeom Hur, Yoonho Lee, Seongmin Hong, Hyunsoo Yoon. Trust-based secure aggregation in wireless sensor networks. *3rd International conference on Computing, Communications and Control Technologies*; 2005, 3:1-6.

[12] Can Basaran, Kyoung-Don Kang, Mehmet H. Suzer. Hop-by-hop congestion control and load balancing in wireless sensor networks. *In Proceedings of the 35th Ieee Conference on Local Computer Networks*; 2010.