International Journal of Engineering Sciences Paradigms and Researches (IJESPR)
(Vol. 20, Issue 01) and (Publishing Month: May 2015)
(An Indexed, Referred and Impact Factor Journal)
ISSN (Online): 2319-6564
www.ijesonline.com

Implementation of Fuzzy Based Secure Routing in WSN

Keshav Kumar[1] and Poonam[2]

[1]M.Tech. Scholar, ECE Deptt., OM Institute of Technology and Management, Hisar
keshav12412@gmail.com

[2]Assistant Prof., ECE Deptt., OM Institute of Technology and Management, Hisar

Abstract

The paper attempts to modify the existing technique of routing in WSN. In the existing work the node is selected only on the basis of the trust value of the node. This concept increases the security but the network lifetime may get decreased as the energy of the selected may be low and selection of the node may dead the node and resultant the dead network. The proposed work selects the node on the basis of the trust as well as the energy and number of neighbor. The node with high energy and high trust value is favorable to be selected but the node may not find the neighbor to transmit the data that's why the neighbor of neighbor is also necessary for the selection of the node.

Keywords: *WSN, Security, Trust, Routing, End to end delay.*

I. Introduction

Wireless Sensor Networks (WSN) offer efficient solutions in a great variety of application domains such as military fields, healthcare, homeland security, industry control, intelligent green aircrafts and smart roads. Security plays a vital role in all of them and foremost for military and surveillance cases. It can be interpreted in a list of security requirements, which include node verification, user authorization, data confidentiality, data integrity and freshness, privacy, secure localization and trusted resource allocation[1].A Wireless Sensor Network (WSN) consists of many wireless sensors to cooperatively monitor physical or environment conditions, such as temperature, humidity, light intensity, sound, vibration, pressure, motion etc. But currently they often have certain probabilities of failure, as well as high restrictions of computing, memory and energy capabilities. So, in WSNs, a new security system is being applied, called trust management system [2].

To protect the network from the above-mentioned attacks, a secure routing protocol (SRP), which addresses the limitation of sensor networks, must be used to secure the communication channel between nodes; since routing in WSNs is a cooperative process whereby route information is relayed between nodes. As there is no guarantee that all nodes in the discovered route will behave as expected to fulfill the promises made, some malicious or selfish nodes might exist [3].

II. Attacks on WSN

Security is one of the major aspects of any communication system. Traditional WSNs are affected by various types of attacks. Wireless sensor networks are energy constraint networks, having limited energy and power resources. This makes them exposed enough to attack by attacker deploying on nodes more resources than any individual node or base station, which is not difficult job for the attacker. A typical sensor network may be consisting of potentially hundreds of nodes which may use broadcast or multicast transmission. The broadcast transmission nature of the medium is the reason why wireless sensor networks are susceptible to security attacks. Denial of Service attack eradicates a network's range to satisfy its expected function [4].

Basically, attacks on WSNs can be classified into one or more of the following categories ([5]):

1) **Outsider vs. Insider attack**: in an outsider attack, a malicious node harms the WSN without being part of it. In contrast, in an insider attack the malicious node harms the WSN as (authorized) participant of the WSN.

2) **Physical vs. Remote attack:** in a physical attack an adversary physically accesses the sensor node that should be harmed by tampering or destroying the sensor's hardware. In contrast, a remote attack is implemented from a (large)

distance, e.g. by emitting a high-energy signal to interrupt the communication.

3) **Passive vs. Active attack:** in a passive attack an adversary just eavesdrops or monitors the communication within the WSN. In contrast, in an active attack the adversary directly influences the communication in the WSN by modifying, fabricating or suppressing data packets.

4) **Laptop-class vs. Mote-class attack:** a mote-class attack is an attack against a WSN that is implemented from a mote, i.e. the attacking device is of same type of hardware as the sensor nodes that should be attacked.

In contrast, in a laptop-class attack, the adversary utilizes a device which is superior to the sensor nodes that should be attacked in terms of computational power and transmission power.

III. Security and Trust

The emerging importance of sensor networks could be hindered by their inherent security problems. This technology is tightly associated to the physical world. Thus, the nodes are as accessible as the event they monitor. The wireless channel used in the communications can also be accessed by anyone. Also, the nodes are highly constrained in terms of computational power, memory, communication bandwidth and battery power. Consequently, any malicious adversary could launch a certain set of attacks that could render the network partially or totally useless. In order to solve the security problems present in WSN, a set of security primitives that could improve the robustness and the reliability of the network should be included[6].

Trust management can help improving the security of WSN. For example, for the routing process, sensor nodes might need to know which other nodes to trust for forwarding a packet. For sensing purposes a node might need to trust other neighbouring nodes for checking anomalous measurements. Other examples of trust in sensor networks include data disclosure decisions and key exchange. However, as sensor nodes are usually constrained devices, the trust management systems must be lightweight enough to provide a good performance without hindering the functionality of the system. Moreover, due to the distributed nature of those networks, trust management systems for them are susceptible to attacks.

Figure 1: Basic Security Requirements in WSN

Security and trust are two tightly interdependent concepts and because of this interdependence, these terms are used interchangeably when defining a secure system [7].

However, security is different from trust and the key difference is that, it is more complex and the overhead is high.

IV. Trust Management

Any trust management system has to be specially designed and prepared for reacting against the particular issues, such as autonomy, decentralization, and initialization that can be found in WSN environments. Although there are some existing architectures for WSN that partially solve these problems, it is still possible to point out the neglected aspects that can be considered crucial for creating a satisfactory trust system. It should be necessary to deduce different trust values for every distinct behavior of the nodes. Sensor nodes should also be aware of the trust history of their neighborhood. The consistence in the trust readings is also significant. Note that all the important decisions taken by the nodes, such as node exclusion, should be notified to the base station for logging, monitoring and maintenance purposes. As a final matter, one of the biggest constraints regarding trust management for sensor networks is the overhead that the existence of this system may impose over the constrained elements of the network.

The multi-valued trust level routing protocol, called MTR (Multi-valued Trust level Routing). This routing protocol can find malicious nodes and improve the ability of resisting malicious sensor nodes attack. MTR mainly considers sensor's trust and level of topology. The trust is based on the QoS characteristic such as packet forward, data rate, power consumption, reliability, etc. The level in topology is based on the sensor's topology position in the whole net. According to the trust and topology level, it can compute probability value, and select a suitable sensor to transmit message [2].

A. Computing Trust and CRS

The basic idea of MTR is to evaluate trust value of sensor nodes and select a suitable node as next hop. Sensor nodes monitor their neighborhood to obtain first-hand information and second-hand information about their neighboring nodes. By first-hand information, direct trust value can be achieved, and by second-hand information, recommend trust value can be achieved. Combined with direct trust value and recommend trust value, integrated trust value can be calculated [2].

i. Calculation of Direct Trust Value

For any two nodes *Ni* and *Nj* $(i, j \in 1 \ldots . n$, *n* is the number of nodes), $S_{i\to j}$ (*i* is the ID of sponsor node, *j* is the ID of target node) is the number of the success interaction between node N_i and N_j, $C_{i\to j}$ (*i* is the Id of sponsor node, *j* is the Id of target node) is the number of the cooperation between node N_i and N_j. Direct trust value for the node *Ni* to node *Nj* can be computing as follows:

$$T_{direct(i\to j)} = W_{old} \times T_{olddirect} \times T_{newdirect} \quad (1)$$

$$T_{newdirect(i\to j)} = S_{i\to j}/C_{i\to j} \quad (2)$$

Where W_{old} and W_{new} denote as the weights of the old trust value and the new trust value, $W_{old} + W_{new} = 1$. The nodes adjust the weights of the old trust and the new trust based on its own standards and circumstances. For $\partial = W_{oldesdirect}/W_{newdirect} : if \partial$ is big the system will be more rely on $T_{olddierct}$ and $T_{newdierct}$, in this case the interference capability of transient disturbance will become strong. If ∂ is small, the system will be less rely on $T_{olddierct}$ than $T_{newdierct}$, in this case the response time of detecting malicious node will become short.

ii. Calculation of Recommend Trust Value

Beside direct trust value, recommend trust value is another important basic value. In this system, recommend trust value can get from its neighborhood, and it can be computing as follows [3]:

$$T_{recommend(i->j)} = \frac{1}{n} \times \sum_{k=1}^{m} T_{direct(i\to k)} \times T_{direct(k\to j)}$$

Where *m* is the number of neighborhood of sensor *i*.

iii. Calculation of Integrated Trust Value

Based on direct trust value and recommend trust value, now get integrated trust value as follows:

$$T_{integrated(i->j)} = W_{direct} T_{direct(i\to j)} + W_{recommend} \times T_{recommend(i\to j)}$$

Where W_{direct} and $W_{recomend}$ donate as the weights of the direct trust and the indirect respectively, and . $W_{direct} + W_{recommend} = 1$The nodes adjust the weights of the direct trust and the indirect trust based on its own standards and circumstances.

iv. Calculation of CRS

Coefficient of Routing Select (CRS) is the ability of a node send message to BS. When sensor node needs to send value can get from the integrated trust value and the TL value of its neighborhood. The formula is given as following:

$$CRS_{i\to j} = \frac{1}{C^{i.TL - j.TL}} \times T_{integrate(i\to j)}$$

Where *C* is a constant and the value of *C* based on its own standards and circumstances, 0<*C*<1, *i.TL* refers to the topology level of sensor node *Ni*, *j.TL* refers to the topology level of sensor node *Nj*.

If the value of $T_{integrate\ (s1\to s2)}$and $T_{integrate\ (s1\to s2)}$is the same, and *s2.TL* is smaller than *s3.TL*, then $CRS_{(s1\to s2)}$is bigger than $CRS_{(s1\to s3)}$On the other hand, if the TL value of sensor node *s2* and sensor node *s3* is the same, and $T_{(s1\to s2)}$is bigger than $T_{(s1\to s3)}$s1 then $CRS_{(s1\to s2)}$ is bigger than$CRS_{(s1\to s3)}$.

V. Proposed Work

In the existing work the node is selected only on the basis of the trust value of the node. This concept increases the security but the network lifetime may get decreased as the energy of the selected may be low and selection of the node may dead the node and resultant the dead network. The proposed work selects the node on the basis of the trust as well as the energy and number of neighbor. The node with high energy and high trust value is favorable to be selected but the node may not find the neighbor to transmit the data that's why the neighbor of neighbor is also necessary for the selection of the node. The proposed system uses the fuzzy to select the node. The trust value updating method is similar to the existing technique.

The proposed technique along with the fuzzy can be easily understood by the following algorithm:

1. Select the source node S and destination node D.
2. Each node is initiated with trust value say T and energy level say E.
3. Present node=Source node
4. While present node ~=D
5. Select neighbor of present node
6. If neighbor of present node already visited then select the neighbor of destination node
7. Calculate the number of neighbor, trust vale and energy level for selected node
8. Apply fuzzy
   Selection=Fuzzy (trust, number of neighbor, energy level)
9. If the selection >0.5
10. The update the present node
11. Update the trust value and energy level
12. End if

VI. Results

The proposed algorithm is implemented using the MATLAB. The MATLAB doesn't contain any toolbox for the WSN. The m file coding is done to design the WSN. The comparison is done the different size networks by using the parameters average time consume, energy left and the throughput.

1. Throughput: Throughput or network throughput is the average rate of successful message delivery over a communication channel. This data may be delivered over a physical or logical link, or pass through a certain network node. The throughput is usually measured in bits per second (bit/s or bps), and sometimes in data packets per second or data packets per time slot.
Throughput = (Packet Size/(stopTime-startTime))*(8/1000)

2. End-to-end Delay: The average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.
∑ (arrive time – send time) / ∑ Number of connections.

Table 1: Parameter Analysis of Existing For 20 Nodes

Run	Delay	Energy left	Through put
1.	1.0115	108.5000	0.9886
2	3.0353	106.5000	0.3295
3	4.0491	101	0.2470
4.	2.0620	95	0.4850
5.	2.0316	122	0.4922

Table 2: Parameter Analysis of Proposed For 20Nodes

Run	Delay	Energy left	Throughput
1.	0.1917	107.5000	5.2176
2.	0.1618	106.5000	6.1793
3	0.1559	102	6.4124
4	0.1732	94	5.7735
5	0.1430	122	6.9928

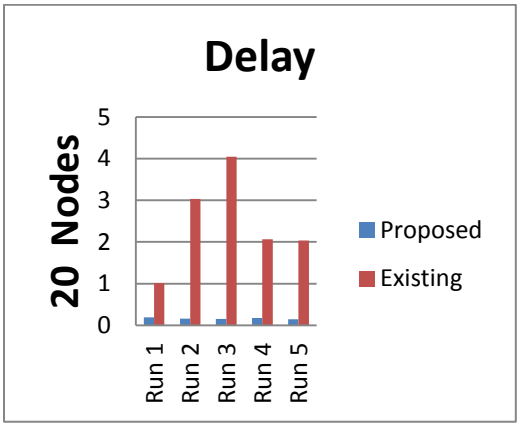

Figure 2: Comparison of Delay between Existing and Proposed For 20 Nodes

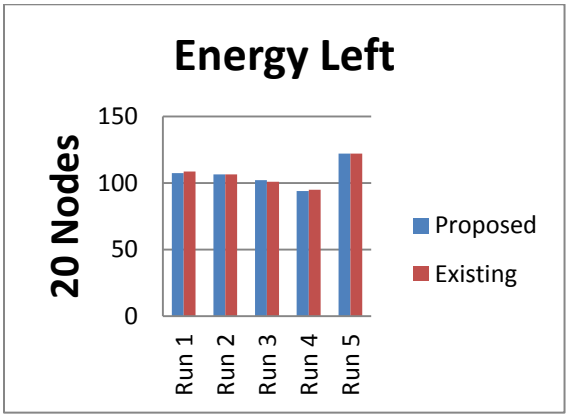

Figure 3: Comparison Of energy Left Between exiting and Proposed For 20 Nodes

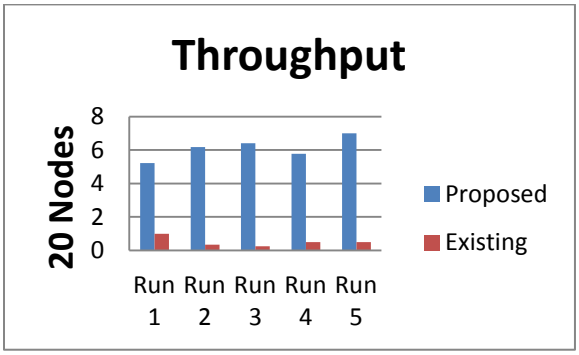

Figure 4: Comparison Of Throughput Between Exiting And Proposed For 20 Nodes

Table 3: Parameter Analysis of Existing Algorithm for 50 Nodes

Run	Delay	Energy left	Throughput
1.	3.04889	258.5000	0.3280
2	3.0444	231.5000	0.3285
3	2.0292	312	0.4928
4	3.0444	285.5000	0.3285
5	3.0491	268.5000	0.3280

Table 4: Parameter Analysis of Proposed Algorithm for 50 Nodes

Run	Delay	Energy left	Throughput
1.	0.0986	259	10.1447
2.	0.0997	231.5000	10.0297
3.	0.0997	311	10.0319
4.	0.0981	285.5000	10.1917
5	0.02212	268.5000	4.5208

Figure 5: Comparison Of Delay Between Exiting And Proposed For 50 Nodes

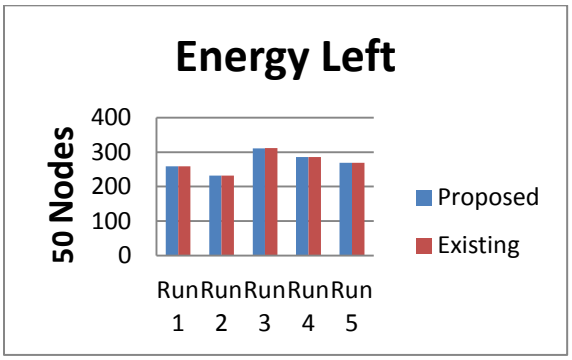

Figure 6: Comparison Of Energy Left Between Exiting And Proposed For 50 Nodes

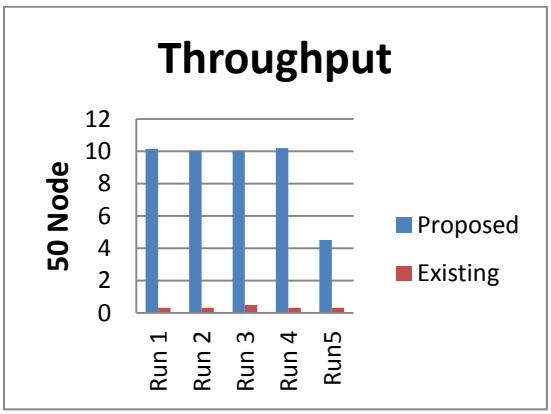

Figure 7: Comparison of Throughput Between Exiting And Proposed For 50 Nodes

The simulation results show that the proposed technique is better than the existing technique. The comparison is done by using the throughput, delay and the energy left. The delay gets decreased and the throughput gets increased. The energy left in the proposed algorithm is greater than the existing algorithm so the proposed algorithm is better than the existing algorithm.

Conclusion

The proposed system uses the fuzzy to select the node. The trust value updating method is similar to the existing technique. The simulation results show that the proposed technique is better than the existing technique. The comparison is done by using the throughput, delay and the energy left. The delay gets decreased and the throughput gets increased. The energy left in the proposed algorithm is greater than the existing algorithm so the proposed algorithm is better than the existing algorithm. In future, the proposed algorithm can be extended to use the neuro-fuzzy. The proposed algorithm can be compared with other existing algorithms. The proposed algorithm can be extended with meta-heuristic techniques.

References

[1] Trakadas, P., Maniatis, S., Karkazis, P., Zahariadis, T., Leligou, H. C., & Voliotis, S. (2009, March). A novel flexible trust management system for heterogeneous wireless sensor networks. In Autonomous Decentralized Systems, 2009. ISADS'09. International Symposium on (pp. 1-6). IEEE.

[2] Chen, Z., Zhang, R., Ju, L., & Wang, W. (2013, July). Multivalued trust routing based on topology level for wireless sensor networks. In Trust, Security and Privacy in Computing and Communications (TrustCom), 2013 12th IEEE International Conference on (pp. 1516-1521). IEEE.

[3] Momani, M., & Challa, S. (2010). Survey Of Trust Models In Different Network Domains. International Journal of Ad hoc, Sensor & Ubiquitous Computing, 1(3).

[4] Hiremani, V., & Madne, M. Secure Mechanism for Wireless Sensor Networks-A Review.

[5] Kellner, A., Alfandi, O., & Hogrefe, D. (2012). A survey on measures for secure routing in wireless sensor networks. International Journal of Sensor Networks and Data Communications, 1, 1-17.

[6] Kavitha, T., & Sridharan, D. (2010). Security vulnerabilities in wireless sensor networks: a survey. Journal of information Assurance and Security, 5(1), 31-44.

[7] Pirzada, A. A., & McDonald, C. (2004, January). Establishing trust in pure ad-hoc networks. In Proceedings of the 27th Australasian conference on Computer science-Volume 26 (pp. 47-54). Australian Computer Society, Inc.