European Journal of Molecular & Clinical Medicine
ISSN 2515-8260 Volume 07, Issue 09, 2020

SELFISH NODE AVOIDANCE USING ADAPTIVE TRUST COMPUTATION MODEL IN WSN

[1]Dr. N.SATHEESH KUMAR, [2]V.KAVITHA, [3]T.MENAKA, [4]DR.V. MANONMANI
[1]Professor, PBR Visvodaya Institute of Technology and Science, AP
[2]Associate Professor, Kings Engineering College, Chennai, TN
[3]Research Scholar, SRM Institute of Science and Technology, Chennai, TN
[4]Principal, Jaganath Institute of Technology, Chennai

Abstract

Providing a safer communication in the network improves the network credibility since WSN is often deployed over hostile environments. Isolating the selfish nodes from the routing path is mandate to build a strong network. The node might become irresponsible due to their low energy level, high congestion rate, etc. Categorizing the selfish nodes and normal nodes makes the network more reliable while routing the data packets. Therefore an adaptive trust computation model is proposed here. By computing trust values with control messages and energy levels for the nodes are identified. This removes the selfish nodes from the system and the routes are constructed with the avoidance of irresponsible nodes. Here adaptive trust computation model is proposed with two level node selections. Simulation results are analyzed for determining the efficiency of the proposed scheme.

Keywords: Trust computation, Energy computation, Irresponsible node avoidance, Wireless Sensor Networks.

1. Introduction

Selecting the forwarder node is essential and considered to be a main task in multi-hop communication since the source and sink node might locate at farther distance. Large scale WSN comprises of numerous sensor hubs and the sensed data packets needs to be delivered through several hops. Protection of hubs or nodes is a significant challenge and the routing attacks have the ability to isolate the actively participating sensor nodes from its Base Station (BS). Node misbehavior to be simply described as some malignant nodes will play in process of path creation and maintenance and refuses to forward the sensed info or injects false info with the original data [1]. Number of mechanisms had been proposed in identifying the subsequent forwarder node; among the most common approach is the cluster-based routing protocol [2, 3] here the cluster head is elected for data aggregation process from the nodes surrounded it. Attack classification and overview of WSN was provided in [4], here various security measurement techniques were discussed. Detection of security anomaly towards security measurement plays a major role. Multiple factor is more effective for the process of node selection decision compared to single factor consideration. Trust management models have been recently suggested as an effective security mechanism for WSN [5].

2. Related Works

Several mechanisms have been proposed to send the data in a secured and efficient manner. Also trust based solutions nave been proved to be more effective in facing and handling selfish nodes. Trust and Energy aware Routing Protocol (TERP) was presented to isolate the misbehaviour and faulty nodes from the routing [6]. Here residual energy encompasses trust and hop_count are taken for designing the network. This multi-facet routing plan makes the network secure and reliable. Node Reputation based Energy Aware Routing (NREAR) scheme [7] had proposed for improving safety

measures and offers an efficient communication. NREAR consists of two phases such as node behavior monitoring phase done through optimistic and pessimistic behaviors of nodes and node's energy value monitoring phase. Later through the selected optimistic nodes the info gets passed towards the sink.

Adaptive Trust based Routing Protocol (ATRP) was proposed in [8] here three types of trust is calculated like direct, indirect and witness trust in order to avoid the malicious nodes from the routing path. Moreover trustworthiness for the nodes is evaluated using pairwise comparisons makes the network highly secured however increases the computational cost. The wireless network applications are compromised as false data results due to the presence of some falsify nodes [9]. These nodes can be taken away from the network by evaluating trust model for the network. Trust evaluation is necessary to make the network distorted free. Therefore the network can function without the involvement of false data reports.

Trust aware secure mechanisms provide an alternative way to counter such attacks. However, most of trust aware schemes lacks robust trust model design, therefore Weight based Probabilistic Trust Evaluation (WPTE) scheme for WSN was proposed [10]. Here, a Beta probability distribution mechanism is applied for deriving the node's trustworthiness. Trust management mechanism [11] was proposed for clustered WSNs to keep watching the nodes behavior and to evaluate their trust values. Identification labels are generated for the nodes by using a hash algorithm that can able to distinguish external attackers from normal nodes. Many trust models have been developed recently like fuzzy logic based trust evaluation, entropy trust model, D-S support trust models, and also Game Theory trust models [12, 13]. Information theoretic system [14] was used to measure the trust values quantitatively and to construct the efficient trust model with various trust conclusion factors in regarding the trust management scheme. These factors are combined together to determine the trust association ambiguity from various angles. Renewing a node's trust for next decision-making costs more energy is a drawback of this mechanism also the factors used here has no defined weight measures.

A light-weight trust model [15] was proposed for reducing communication failures and for easy data aggregation. Through the node interactions (successful or unsuccessful interactions) the direct trust factor is computed and data comparisons are made for similarity checks. To compute the total trust value communication ability, node lifespan and data consistency are all taken that increases the computational cost.

3. Proposed work

Adaptive Trust Computation Model (ATCM) is proposed here with two level node selection processes. Isolating the selfish nodes from the routing path is mandate to build a strong network. The node might become irresponsible due to their low energy level, high congestion rate, etc. Categorizing the selfish nodes and normal nodes makes the network more reliable while routing the data packets. Therefore by computing energy values the trustable nodes are identified from the selfish nodes and the routes are constructed with the avoidance of irresponsible nodes.

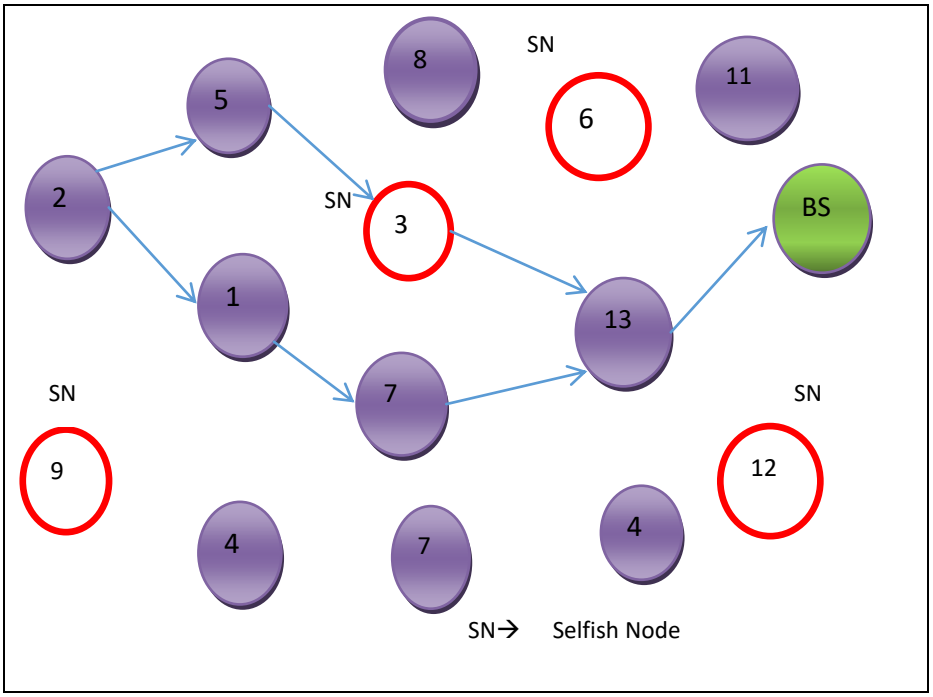

Figure 1: Example Scenario of ATCM

Figure 1 shows the example scenario of ATCM mechanism. The nodes present in the network need to communicate each other. The control (request) messages are broadcasted from the source node '2' in the network towards the base station 'BS'. The relay nodes {5, 3 13} and {1, 7, 13} are the available transmission path that accept RQ messages and send back route reply messages among each other. The trust value and energy level is calculated for the replied nodes for the detection of selfish nodes.

a. Trust Computation Unit

The normal nodes sometimes do not respond properly to other nodes in the network since there is low energy for the node, it might drop the packet sent by the sender node. Therefore the node becomes irresponsible or dead when those nodes are in continuous communication or respond to other nodes.

The node trust value is computed during the data transmission to its neighbor node. Trust value of the node falls between (0, 1). The reference trust value is set as 0.7 and the node trust value 'NT' falls below the reference is considered to be the selfish or irresponsible nodes and remove from the routing process. The differentiation between the dropped packets (P_d) and forwarded packets (P_f) gives the node trust value and it is measured using the equation 1.

$$NT_{n2}^{n1} = \frac{P_f}{P_f + P_d} \tag{1}$$

Algorithm: Trust computation

```
Procedure NodeTrust();
    Pkts_SENT ← 0
    Pkts_FWD ← 0
Loop(n1);
    If Pkts_SENT(n1) == True;
    Pkts_SENT ← Pkts_SENT+1;
```

```
    If Pkts_FWD(n1) == True;
    Pkts_FWD ← Pkts_FWD+1;
NodeTrust(n1)=Pkts_FWD/Pkts_SENT;
Goto loop;
Do compute for all nn;
Close;
```

The presence of selfish or irresponsible nodes in the route threatens the node cooperation and degrades the network performance and influences the routing control, battery, average end-to-end delay, etc.

b. Energy Computation Unit

Every node in the network will have a certain amount of energy. If the node is being active for a longer time or it has already involved in more number of transmissions more data then there is the possibility of energy lost for the particular node. If again that particular node involves in data routing, the node might die due to energy loss and this causes data disruption during routing over the path. Therefore, if node has minimum energy level then it can be avoided from the routing process before it involves. The nodal energy values are computed and the nodes that fall under the threshold value is considered as selfish nodes in the system. Here the total energy value is set as 10J and the threshold energy level is set as '3J'. The rate at which energy is consumed in the network by individual sensor nodes is defined by the energy model.

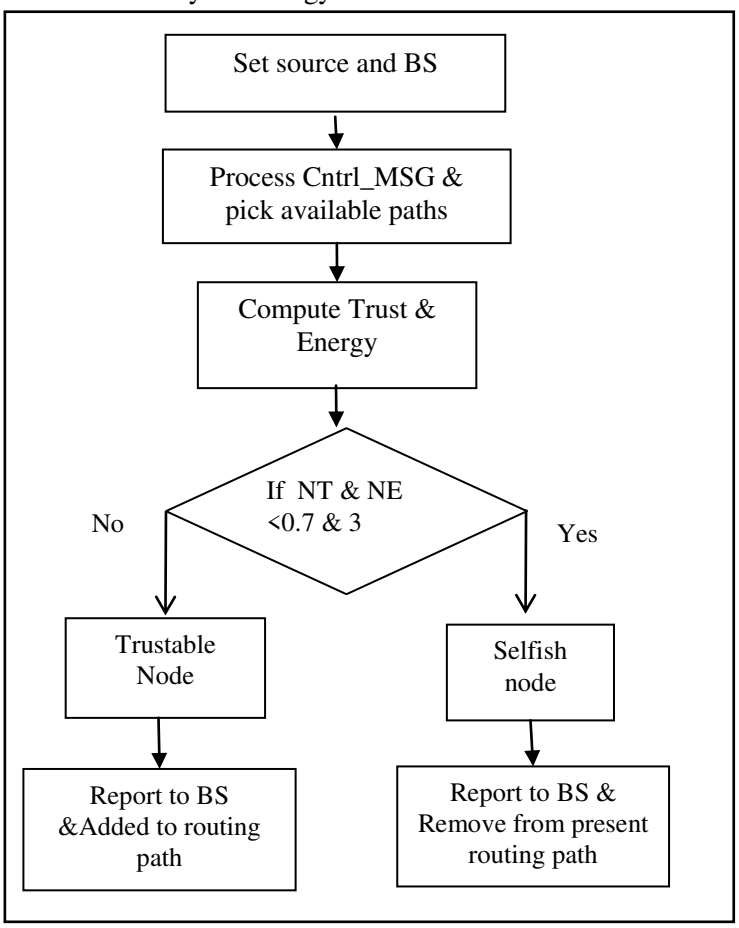

Figure 2: Flowchart of ATCM

The basic nodal energy consumption is calculated using equation 2.

$$NE_{n1} = E_{tx} + E_{proc} + E_{amp} + E_{rx} \quad (2)$$

Here

E_{tx} denotes transmitting energy

E_{proc} represents energy spent for data processing

E_{amp} represents energy spent for amplification process

E_{rx} denotes energy spent for data reception.

Figure 2 represents the flow chart of the proposed work and it explains how the proposed mechanism ATCM works in step by step process.

4. Results and Discussions

Network simulator tool is used to simulate the proposed ATCM and existing ATRP protocols. The data channel model used for the purpose of communication between the nodes is data Constant Bit Rate (CBR) traffic model. CSMA/CA channel is used to send and receive the data; the channel type is wireless medium. The parameters such as Packet Delivery Rate, Loss Rate, Node trust ratio and Energy leftover are taken for the evaluation of the proposed model. The MAC type value of 802.11 is used and the data rate is 11Mbps. The nodes can communicate with one another is up to 250m range.

Packet Delivery Rate

Packet Delivery Rate (PDR) is defined as the rate of sum of packets that delivered successfully with respect to the sum of packets sent. It is obtained from the equation 3 given below. Here n denotes the total number of nodes in the networks.

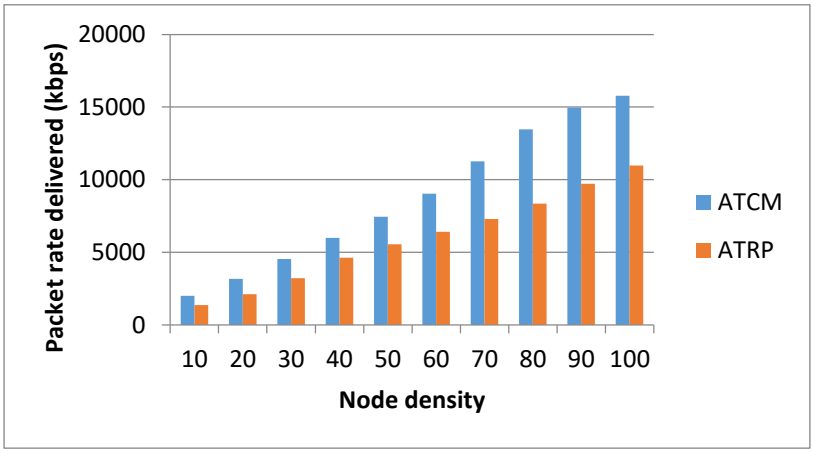

Figure 3: Delivery rates of packets

$$PDR = \frac{\sum_0^n PktRcv(n)}{\sum_0^n PktRcv(n) + \sum_0^n PktLost(n)} \quad (3)$$

The delivered rates of packets at the receiver end are shown in the figure 3 for both the proposed ATCM scheme and existing ATRP scheme. Proposed model has high delivery rates of packets compared to the conventional which directly reflects in better network performance.

Packet Loss Rate

Packet Loss Rate (PLR) is defined as the ratio of the packets lost to the total packets sent respectively. PLR is estimated using the equation 4.

$$PLR = \frac{\sum_0^n PktLost(n)}{\sum_0^n PktRcv(n) + \sum_0^n PktLost(n)} \quad (4)$$

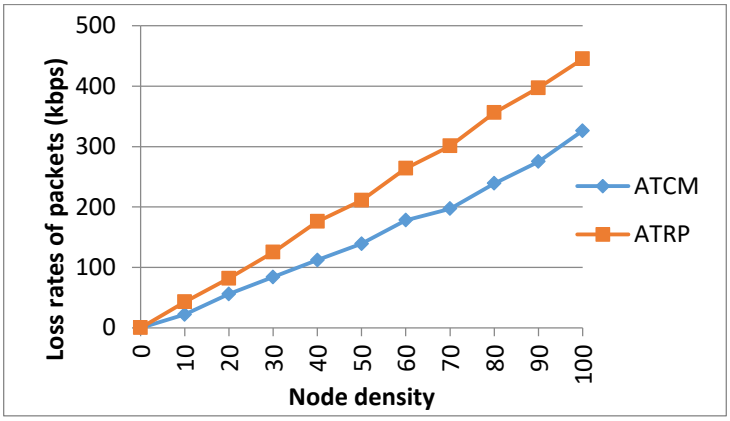

Figure 4: Packet Lost Rate

The lost rates of packets at the sink node or base station are shown in the figure 4 for both the proposed ATCM and existing ATRP scheme. ATCM model has low loss rates of packets when compared with the conventional ATRP scheme.

Node Trust Ratio

The node trust ratio is determined with respect to the node density present in the network. The average node trust ratio computed for the proposed scheme is 0.84 and for the conventional ATRP is 0.75.

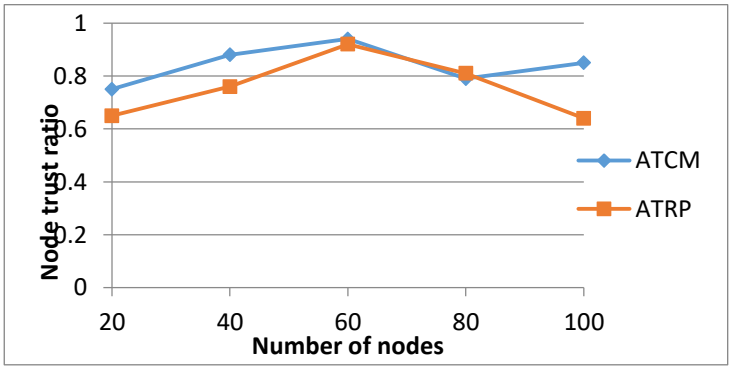

Figure 5: Node Trust Ratio

Therefore the proposed scheme has selected more number of trusted nodes during routing. Figure 5 shows the node trust ratio for both the ATCM and ATRP models.

Leftover Energy

The amount of energy level that remains in the node after each set of data transmission at the current instance of time is said to be energy leftover in the node. Figure 6 shows the analysis of energy leftover for both the proposed ATCM and conventional ATRP mechanism.

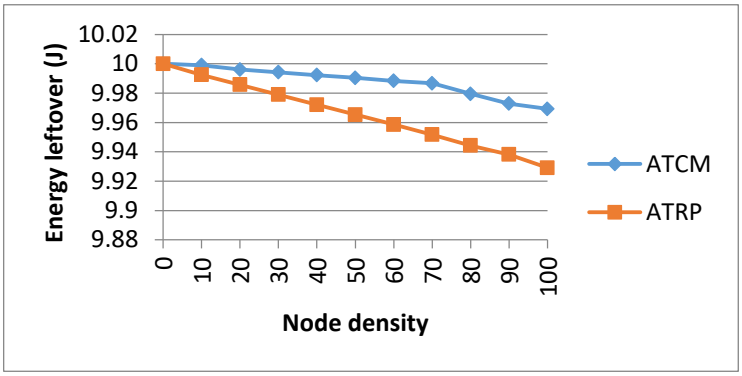

Figure 6: Leftover Energy

5. Conclusion

Removal of selfish nodes from the routing path and allowing only normal nodes makes the network more reliable while routing the data packets. Therefore by computing trust values with control messages and energy levels for the nodes are identified. This removes the selfish nodes from the system and the routes are constructed with the avoidance of irresponsible nodes. Here adaptive trust computation model is proposed with two level node selections. Simulation results are analyzed and the efficiency of the proposed scheme is proved to be better in terms of node trust ratio and packet rates delivered.

References

1. Kumar, A. S., & Logashanmugam, E. (2016). Secure Acknowledgement based Misbehavior Detection in WSN (S-ACK). Indian Journal of Science and Technology, 9(40), 96063.

2. Tyagi, S., & Kumar, N. (2013). A systematic review on clustering and routing techniques based upon LEACH protocol for wireless sensor networks. Journal of Network and Computer Applications, 36(2), 623-645.

3. Jadidoleslamy, H. (2013). An introduction to various basic concepts of clustering techniques on wireless sensor networks. International journal of Mobile Network Communications & Telematics (IJMNCT), 3(1), 1-17.

4. Xie, H., Yan, Z., Yao, Z., & Atiquzzaman, M. (2018). Data collection for security measurement in wireless sensor networks: a survey. IEEE Internet of Things Journal, 6(2), 2205-2224.

5. Han, G., Jiang, J., Shu, L., Niu, J., & Chao, H. C. (2014). Management and applications of trust in Wireless Sensor Networks: A survey. Journal of Computer and System Sciences, 80(3), 602-617.

6. Ahmed, A., Bakar, K. A., Channa, M. I., Haseeb, K., & Khan, A. W. (2015). TERP: A trust and energy aware routing protocol for wireless sensor network. IEEE Sensors Journal, 15(12), 6962-6972.

7. Thirunavukkarasu, V., Kumar, A. S., Josephine, D. J., & Arasu, T. P. (2020). Selection of Optimistic Nodes for Reputation Based Routing in Wireless Networks. In 2020 7th International Conference on Smart Structures and Systems (ICSSS) (pp. 1-5). IEEE.

8. Khalid, N. A., Bai, Q., & Al-Anbuky, A. (2019). Adaptive trust-based routing protocol for large scale WSNs. IEEE Access, 7, 143539-143549.

9. Kodali, R. K., & Soratkal, S. (2015). Trust model for WSN. In 2015 International Conference on Applied and Theoretical Computing and Communication Technology (iCATccT) (pp. 903-906). IEEE.

10. Ahmed, A., & Bhangwar, A. R. (2017). WPTE: Weight-Based Probabilistic Trust Evaluation Scheme for WSN. In 2017 5th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW) (pp. 108-113). IEEE.

11. Luo, W., Ma, W., & Gao, Q. (2016). A dynamic trust management system for wireless sensor networks. Security and Communication Networks, 9(7), 613-621.

12. Chen, Y., Weng, S., Guo, W., & Xiong, N. (2016). A game theory algorithm for intra-cluster data aggregation in a vehicular ad hoc network. Sensors, 16(2), 245.

13. Fan, Q., Xiong, N., Zeitouni, K., Wu, Q., Vasilakos, A., & Tian, Y. C. (2016). Game balanced multi-factor multicast routing in sensor grid networks. Information Sciences, 367, 550-572.

14. Xia, H., Jia, Z., & Sha, E. H. M. (2013). Research of trust model based on fuzzy theory in mobile ad hoc networks. IET information security, 8(2), 88-103.

15. Wang, N., & Pang, Y. (2014). An improved light-weight trust model in WSN. Computer Modeling & New Technologies, 18(4), 57-61.

16. Kumar A, Senthil & Logashanmugam,. (2017). Secured Optimal Routing Based on Trust and Energy Model in Wireless Sensor Networks. IIOAB Journal. 9. 3-13.

17. Dr.V.Thirunavukkarasu, Dr.A.Senthil kumar, K.T.JayaBharathi. (2020). Anonymous Secure Reputation Routing System For Selective Forwarding Attacks In Wireless Sensor Networks. International Journal of Advanced Science and Technology, *29*(7s), 2959-2967.

18. Kumar A, Senthil & Logashanmugam. (2016). Novel key management techniques in Three-Tier Wireless Sensor Networks. 9. 903-910.