International Journal of Applied Engineering & Technology

SECURE AND ENERGY EFFICIENT ROUTE EVALUATION USING TRUST VALUE IN WIRELESS SENSOR NETWORK

J. Joselin[1] and S. Indumathi[2]
[1]Assistant Professor, Department of Computer Applications, Sri Krishna Arts and Science College, Coimbatore
[2]Assistant Professor, Department of Software Systems, Sri Krishna Arts and Science College, Coimbatore

ABSTRACT
Routing in wireless sensor networks (WSN) basically focuses on delivery of packets to destination or base station. But security is the major issues in the routing mechanism. Security may be spoiled during the transmission by several attack and freeze the activity of whole network. So trust based mechanisms are the best solution to provide the sufficient security of routing. This paper introduced a new routing mechanism-by considering trust value of each node and its node energy which evaluates the total path trust value of the entire network and produces reliable node and route to transmit packets to the desired base station. Simulation result proves the efficiency of the proposed routing mechanism based on the metrics such as packet delivery ratio, network throughput ratio, transmission delay and energy depletion ratio.

Keywords: throughput ratio, packet delivery ratio and trust value ,threshold,Energy ,delay

1. INTRODUCTION
Wireless Sensor Network is one of the emergent concepts in the field of communication. A lot of recent technology exists in this field, but nowadays most of the researchers are using this method to recognize smart computing along with preserving energy[1]. Wireless sensor network encompasses scattered autonomous sensor nodes. It is used to recognize environmental and physical circumstances such as sound, temperature, vibration, motion and pressure to supportively permit their information over the network to a core place or sink where the information has been perceived and examined. A sink node provides communication between remote users and the sensor network[2].

Routing is the stimulating concept which discriminates the wireless sensor network from the mobile and other networks.The main task of the network layer is to provide the routing between source and base station[3]. Suppose a node is very close to a sink node which reduces traffic and more energy consumption so these problems are overcome by using energy aware routing protocols .

Trust is always defined by trustworthiness, convenience, obtainability, risk, quality of services and other concepts. Trust value may reflect the data and behaviour of node. In general trust design consists of three components: data trust, behaviour trust and historical trust. Trust model concepts can be used for data aggregation with minimal scalability and additionally reduce energy consumption.

2. LITERATURE REVIEW
Energy-aware and trust-based routing protocol for wireless sensor networks using adaptive genetic algorithm called TAGA[11]. It is used to identify common routing attack and especially related to trust attacks and data is transferred with limited energy consumption. Also it is used to select cluster head and finally to apply crossover probability and mutation probability to provide secure routing for the head of the clusters. an Energy-Aware Trust algorithm based on the AODV protocol and Multi-path Routing approach (EATMR) to enhance the security in WSNs[7]. It comprises of 2 sections; open-source Development Model Algorithm (ODMA) and multipath route. AODV protocols are measured for trust awareness for energy here number of parameters are used such as distance, energy, trust and hop count. In this situation node trust is calculated using direct and indirect trust and multi valued function.

Trust based secure routing is used to avoid the black hole attack. This trust method is integrated with AODC that removes the Black hole attack in WSN[8]. A new concept called ActiveTrust can monitor quality of route and

capacity from the intruder attack and can improve the network lifetime. It maintain packet delivery ratio and throughput. It is computed when the packet delivery ratio very less can identify black hole attack is existing. With Novelty: Active trust protocol is compared with existing protocol attack is reduced and throughput is increased by reducing the packet loss our proposed method is efficient which deals the node identity and address of nodes etc., spoofing method is used for node identity and address of node to be changed that can be done by the advisory node. but trust-based calculation, activity and address of node cannot be changed by the intruders that trust is calculated by neighbour nodes. Energy efficient and proficient secure Model[9]. It is verified an encryption and decryption activities using java, AES, DES, triple DES and RC4. Blowfish algorithm here encryption and decryption is done by using mathematical expressions or equations then experimental results is shown by using Blowfish Algorithm that is more proficient energy than private key cryptography algorithms. And this research work is to identify and eliminate the back hole attack that shows the secure transmission among the sensor nodes and trust value is used to detect the black hole attack. [10].

The following are advantages and disadvantages of various Routing Algorithms

Routing Protocols	Advantages	Disadvantages
Energy-Aware Trust multi path algorithm (EATMR) [7]	• By applying trust which gives more security • Energy of the node is maintained	• Sink node can be placed only in the specific locations . if any deviation is occurred then it doesn't give efficient outcome
Trust based secure routing Algorithm [8]	• It helps to eliminate black hole attack	• Some other attacks could not be predicted while transferring data • It doesn't give much importance for energy
Energy efficient and proficient secure Model [9]	• More security is provided for node through mathematical expression and trust value • Identify malicious node related to black hole attack	• While transferring data it consumes more time to check the security of the node
A Trust-Aware Secure Routing Protocol (TSRP) [10]	• Energy consumption is reduced and eliminate routing attack	• bad mounting attack is possible
adaptive genetic algorithm[11]	• It provides secure routing to the cluster heads	• Node security not considered • overhead is increased
A cluster based secure routing algorithm, Quality of Service (QoS) aware Energy Efficient Routing algorithm [12]	• It is used for providing security and energy of node which produce high quality data transmission	• The trust is calculated based on the previous experience of node.this lacking leads wrong data transmission and also reduces the speed of transmission
Trust history based protocols[14]	• Security is fixed based on the old trust vale so data transmission speed is increased	• Node configuration issues is occurred it never takes the updated trust value which affects the entire network

Table 2: Comparision of Routing Algorithm

3. SECURE ROUTE SELECTION

Recent applications lead to the development of micro sensors in wireless. The Wireless sensor network is a set of dynamically distributed sensor nodes to receive environmental parameters from various sources[15]. The sources pass their data through the network to a base location called sink. The wireless sensor network sink collects the

data from the various sources and passes it to the users through the internet by any Private Virtual Network. A sensor may be two types, homogeneous and heterogeneous types of sensor nodes. A sensor has a huge and diversified field of application from agriculture to home appliances control. Each sensor has unique characteristics and features; few sensors have reactors (react to events). The backlog of the sensor application is limited energy backup, and less bandwidth for communication but depending on the application the problem may vary other than, low energy back is an issue.

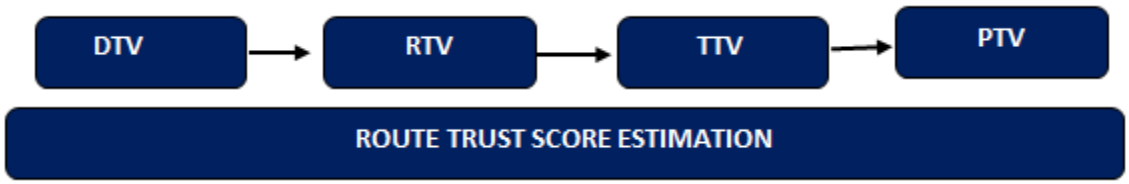

Figure 3: Trust Evaluation

The Trust Evaluation component is used to determine the level of trust. Trust is an assurance or association between two adjacent nodes[22]. In this paper, a new routing mechanism-based trust value of each node and it also evaluates the total path trust value in the figure 3.

There are two types of trust value prediction. They are, direct trust value and indirect trust value. This paper work uses both types of trust prediction. Direct Trust value(DTV_{xy}) is direct observation obtained by the trustor about trustee and Reference Trust value (RTV_{xy}) can be extracted from recommendations. The following are secure route selection elements such as DTV, RTV, TTV and PTV. The responsibility of this work is used to find the trustworthy secure route between source and sink. Therefore calculating various trust values.

Direct Trust Value (DTV)

The Direct Trust Value (DTV) is calculated for each node in the network. The Direct Trust Value is responsible for computing the direct trust score of each node. Direct Observation obtained by the trustor about the trustee[12]. It is considered as trustable and simple. At the same time, it is used to eliminate the bad mounting attack.

Reference Trust Value (RTV)

When a starting node cannot directly perceive the communication behaviour of ending nodes. Reference trust can be recognized. Indirect trust values can be obtained depending on the neighbor nodes comportment[26]. In Reference Trust Values, the evaluating node may get other types of trust experience provided by some other node. It gets reference trust values about a node from different adjacent nodes.

Total Trust Values (TTV)

Total trust value is calculated by appending both direct trust value and indirect trust values[23].The total trust rate (TTV) is calculated by summation of direct trust value and reference trust value.

Path Trust Values (PTV)

The overall sum of Total trust value is known as path trust values. The route has been selected based on the total trust value of the nodes from source (s) to destination (d) for transmitting the packets.

4. PERFORMANCE EVALUATION AND METRICS

The performance of the proposed method is evaluated by using Simulator. The following parameters are used to estimate the performance of proposed method such ,Energy consumption, Throughput ratio, End to End Delay

Network Throughput

When the number of nodes is between 100 and 250, each routing protocol of the network throughput is relatively large. Under the identical number of nodes, the network throughput of the routing protocol in this paper proposes the largest, which is because of the route protocol of this paper choose the trust node to accomplish the data forwarding when constructing the routing.

End-to-End Delay

The time taken by a packet to route through the network from a source to its destination is called Average End-to-end delay. By computing the mean of end-to-end delay of all successfully delivered messages, the average end-to-end delay can be obtained. Therefore, we can infer that, end–to-end delay partially depends on the packet delivery ratio. When the distance between source and destination escalates, the probability of packet drop rises. The average end-to-end delay comprises all possible delays in the network such as buffering route discovery latency, retransmission delays at the MAC, and propagation and transmission delay.

Energy Consumption

Battery power being utilized by each node for specific data transfer is considered to be energy consumption. By taking a difference of initial and final battery powers of each node, this can be calculated. In a sensor network with „n‟ nodes,

6.CONCLUSION

Now a days, in the real time environment most popular technique is wireless sensor network in order to competes the wide range of applications. Secure Route Selection Trust path trust assessment routing protocol (TPTAR) is used to find the attack in WSN. Detecting malicious node is a difficult process that can be achieved through proposed protocols. It is used to identify the reliable route and reliable node to transfer packets. With the help of reliable route, it can reduces the energy consumption. The main role of the trust method is it can assist in most of the applications such as aggregation of data, routing in secure manner and exchange the trusted key between the nodes.

REFERENCE

[1] Han, Y., Hu, H., & Guo, Y. (2022). Energy-Aware and Trust-Based Secure Routing Protocol for Wireless Sensor Networks Using Adaptive Genetic Algorithm. *IEEE Access*, *10*, 11538-11550.

[2] Kalidoss, T., Rajasekaran, L., Kanagasabai, K., Sannasi, G., & Kannan, A. (2020). QoS aware trust based routing algorithm for wireless sensor networks. *Wireless Personal Communications*, *110*(4), 1637-1658.

[3] Hu, H., Han, Y., Wang, H., Yao, M., & Wang, C. (2021). Trust-aware secure routing protocol for wireless sensor networks. *ETRI Journal*, *43*(4), 674-683.

[4] Jedidi, A. (2020). Trust History-based Routing Algorithm to Improve the Quality of Service in Wireless Sensor Network. In *Communication, Signal Processing & Information Technology* (pp. 47-56). De Gruyter.

[5] Keum, D., Lim, J., & Ko, Y. B. (2020). Trust based multipath qos routing protocol for mission-critical data transmission in tactical ad-hoc networks. *Sensors*, *20*(11), 3330.

[6] Saini, K., & Ahlawat, P. (2019). A trust-based secure hybrid framework for routing in WSN. In *Recent Findings in Intelligent Computing Techniques* (pp. 585-591). Springer, Singapore.

[7] Veerapaulraj, S., Karthikeyan, M., Sasipriya, S., & Shanthi, A. S. (2023). An Optimized Novel Trust-Based Security Mechanism Using Elephant Herd Optimization. Computer Systems Science & Engineering, 44(3).

[8] Mastan, M., Jose, G. J. A., & Al-Nuaimy, L. A. H. (2023). A Novel Wosrcnn-Based Trust Model With Secure Routing And Data Transmission In Wsn Using Clf_Avoa And Ascii-Dsaes. Journal Of Theoretical And Applied Information Technology, 101(16).

[9] Praneetha, G. S., Janagama, D., & Anjaneyulu, N. (2016). Cost Aware Secure Routing (CASER) Protocol Design for Wireless Sensor Networks.

[10] Fang, W, Zhang, C, Shi, Z, Zhao, Q & Shan, L 2016, ‘BTRES: Betabased Trust and Reputation Evaluation System for wireless sensor networks’, Journal of Network and Computer Applications, vol. 59, pp.88-94

[11] Jadidoleslamy, H, Aref, MR & Bahramgiri, H 2016, 'A fuzzy fully distributed trust management system in wireless sensor networks', AEU-International Journal of Electronics and Communications, vol.70, no.1, pp. 40-49.

[12] Y. Liu, M. Dong, K. Ota, and A. Liu, "ActiveTrust: secure and trustable routing in wireless sensor networks," *IEEE Transactions on Information Forensics and Security*, vol. 11, no. 9, pp. 2013–2027, 2016.

[13] J. Kaur, S. S. Gill, and B. S. Dhaliwal, "Secure trust based key management routing framework for wireless sensor networks," *Journal of Engineering*, vol. 2016, Article ID 2089714, 9 pages, 2016.

[14] P. Gong, T. M. Chen, and Q. Xu, "ETARP: an energy efficient trust-aware routing protocol for wireless sensor networks," *Journal of Sensors*, vol. 2015, Article ID 469793, 10 pages, 2015.

[15] R. W. Anwar, M. Bakhtiari, A. Zainal, A. H. Abdullah, and K. N. Qureshi, "Enhanced trust aware routing against wormhole attacks in wireless sensor networks," in *Proceedings of the International Conference on Smart Sensors and Application (ICSSA '15)*, pp. 56–59, Kuala Lumpur, Malaysia, May 2015