INDIAN JOURNAL OF SCIENCE AND TECHNOLOGY

RESEARCH ARTICLE

Ensuring Secure Routing in Wireless Sensor Network Using Active Trust

G Amudha[1]*

1 Associate Professor, Computer Science and Business Systems, R.M.D Engineering College, Chennai, 601206, India

OPEN ACCESS

Received: 11.03.2021

Accepted: 23.11.2021

Published: 06.12.2021

Citation: Amudha G (2021) Ensuring Secure Routing in Wireless Sensor Network Using Active Trust. Indian Journal of Science and Technology 14(41): 3107-3113. https://doi.org/10.17485/IJST/v14i41.424

* **Corresponding author**.

gav.csbs@rmd.ac.in

Funding: None

Competing Interests: None

Published By Indian Society for Education and Environment (iSee)

ISSN
Print: 0974-6846
Electronic: 0974-5645

Abstract

Objective: Main objective is to provide a secure router for transferring the valuable data being sensed. One of the major security threats in WSN is the Black hole attack, due to which incoming and outgoing traffic is silently discarded without informing the source that the data did not reach its intended recipient. Overcoming the Black hole attack in WSN is a current research topic. So, the proposed method of trust based secure routing will overcome the black hole attack. **Method:** The method implemented is integrated as Active Trust to the existing AODV routing protocol to avoid the Black hole attack in WSN. ActiveTrust can relevantly maintain the data route success quality and capacity against black hole attacks and can optimize network lifetime. **Findings:** Packet delivery ratio and Throughput are measured considering the attack and applying the method implemented. It is noticed that packet delivery ratio is less when there is an attack, and it gets increased when the attack is been rectified by Active trust method. **Novelty:** Trust based secure routing when compared with existing protocol AODV the attack is reduced and the throughput gets increased by reducing the packet loss. Our approach is efficient in terms of throughput and PDR. As trust factor is so important factor while compared to other factors like Node identity, Node Address etc., our proposed system is efficient. Because node identity can also be spoofed and node address can also be modified by an intruder, but the trust calculation based on the activity of the node cannot be modified by any attacker, because it involves the neighbour node to calculate the trust.

Keywords: Black hole attack; AODV; Trust; Secure routing

1 INTRODUCTION

A Wireless Sensor Network (WSN) has a wide range of applications [(1)], slowly becoming an integral part of life. (Wireless network can be physical or environmental conditions to monitor the sensor to be spatially distributed autonomous devices. The sensor network consists of multiple detection stations called sensor node, which is small, lightweight & portable.) The main task of WSN is to sense and collect data from a certain domain, process, and transmit into the sink. WSN application and communication are mainly tailored to provide high energy efficiency. (WSNs are a single embedded

system that is very much interacted through various kinds of sensors, local information, and communication with their neighbours. WSN applications are the area, health care, and air pollution monitoring, environmental/earth sensing, forest fire detection, landslide detection, data logging, and so on. The sensor network architecture is more important to understand that Wireless sensor networks are very popular technology). However, the limited computing power, storage capacity, energy, and other restrictions of the nodes influence the development of WSNs[2]. When randomly deployed in complex environments, WSNs are especially vulnerable to routing attacks from malicious nodes. Therefore, it is essential to establish new methods that can optimize security issues and reduce energy consumption in WSN[3].

A Black hole attack is a type (DoS) attack; it is also called the packet dropped attack. In networking, the black hole is saliently dropped the data packet not giving any more information to the source that the data did not reach the destination.The black hole attack is frequently deployed to wireless networking. It drops the data and bluffs the previous node.

Trust-based route strategies face some challenging issues such as[4]. The core of a trust route lies in obtaining trust: however, the node of trust is more difficult, (and how it can be done is still unclear. Energy efficiency: WSNs very low in energy, the trust accession, and spreading have high energy-draining, which seriously affects the network's lifetime. Security: It is hard to locate the unwanted nodes, the security route is still a target for future challenges.

2 LITERATURE REVIEW

The trust-based AODV (Ad hoc On-Demand Distance Vector) routing protocol by the exclusion of a black hole attack is suggested by[5]. The black hole attack is an ordinary security issue in the mobile ad hoc network (MANET) routing protocol. The routing table is inserted into the trust value. The route was established according to the routing table and the rest of the part is similar to the traditional AODV routing protocol. The trust value and threshold value are depending upon the black hole node is identified.

Bambi defines as (Black hole Attack Mitigation with Multiple Base station in WSN) techniques by[6] has suggests to effectively mitigate the adverse effects of black hole attacks on WSNs. An adversary captures the network and create some nodes to drop the packets which leads to Black hole attack.As multiple base stations are deployed in the network, copies of data packets are routed to these base stations and the solution is highly effective and requires very little message exchanges in the network, thus saving the energy. The Bambi identified all the black hole attack in the network. This attack technique completed more than 99% packet delivery success rate and prove that project can identify 100% of the black hole nodes.

Clean and efficient methods by[7] to discover and identify the silent failures, i.e. data packets are silently dropped inside the network without giving any responses. This method uses edge routers to raise alarms whenever end to end connectivity is interrupt at active measurement. In this tier-I ISP network successfully discover and confine the black holes and authors focus on the silent faults from the interactive b/w MPLS and IP layers of backbone networks. The real failure data get from a tier-1 network's IPFM and MPFM systems, then troubleshooting failures are demonstrated effectively using both systems at network operators.

In[8] to resist smart black-hole attacks empowered timers and baiting message consists of two phases: Baiting and Nonneighbor Reply. In Baiting phase each node has a bait-timer, the value of the timer is set randomly to B seconds, and each time the timer reaches B it creates and broadcasts a bait request with a randomly generated fake id. Depending on the natural behavior of a black-hole node when it receives any route request it responds with a reply claiming that it has the best path even if it does not exist.

To design a multipath routing protocol that detects and avoids the path containing black-hole. Our paper[9] proposes a way to defense the black-hole and gray-hole attacks with the help of intelligence in MANET.

In[10], a trust-based drone energy-saving data acquisition scheme which uses the quadratic optimization method of the drone path was proposed to find routing paths. Moreover, trust inference and evolve mechanisms are also utilized to identify the trust degree of the sensor node. Therefore, it can effectively find an optimized data collection trajectory and better balance the energy consumption of the network.

In[11], the beta and direct trust model is used for secure communication in WSNs to reduce energy consumption. However, large overlapping areas of communication range among the cluster heads often lead to too many cluster heads, which wastes energy accordingly. In addition, the defendable attacks were not specified in BRDT.

In[12], a secure routing protocol based on the trust levels of nodes called Grade Trust was proposed to defend against black-hole attacks. The packet delivery ratio is improved in Grade Trust, but only a black-hole attack can be defended against.

Therefore, to defend against other kinds of attacks, a clustering-based secure routing protocol was proposed in[13]. First, cluster heads are selected by the energy-efficient clustering algorithm. Next, a trusted hardware module is adopted to encrypt the data during the operation of the network, which can effectively defend against many kinds of attacks such as data confidence and data integrity, and compare node attacks. However, the cluster head nodes need to have permanent energy supply equipment,

which leads to high requirements for the WSN layout.

In [14], a trust-based energy-preserving multihop routing protocol which is a hybrid of encryption and a trust management-based protocol was proposed. However, it does not calculate the indirect trust value, so some errors will occur when calculating the trust values of neighbor nodes.

Therefore, based on semiring theory a trust sensing secure routing mechanic was proposed in [15]. It considers the direct trust calculation of nodes, indirect trust calculation of nodes, incentive factor, energy trust, and quality-of-service metrics to optimize secure routing paths. High computing power for the nodes is needed in [16]. Hence, to reduce the computational complexity of the nodes, a lightweight and quickly deployable trust–based secure routing protocol (TBSRP), which can detect and isolate the misbehaving nodes, was proposed in [17].

The protocol extends the route establishment process in ad hoc on-demand distance vector (AODV) routing [18] to select a reliable and effective path that includes all trusted nodes. The salient features of AODV include on-demand route finding, reduced control packet overhead, providing the latest routing information, broadcasting or unicasting routes at the same time, low storage cost, high scalability, and short connection analyzed [19]. In all the above mentioned techniques the amount of storage and time taken to compute the attack are very high compared to the proposed system,

3 PROPOSED WORK

The Active Trust method for WSN to avoids black holes by keeping track of their number and obtains a trust model. The method improves the data route security. ActiveTrust can relevantly maintain the data route success quality and capacity against black hole attacks and can optimize network lifetime.

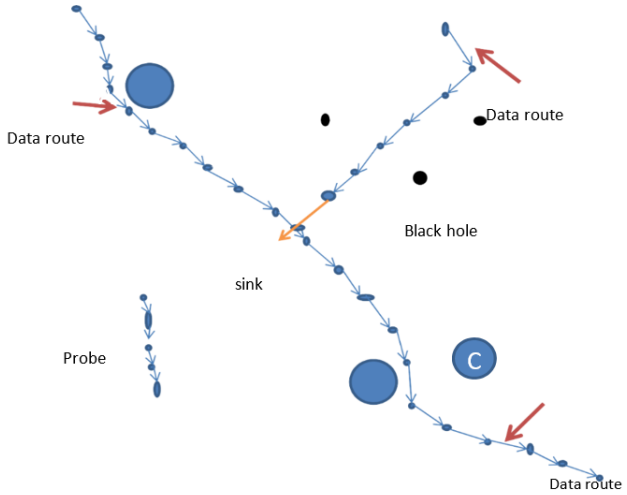

Fig 1. Illustration of the Activetrust

ActiveTrust methods have two routing protocols are, 1)Active detection routing protocol: A detection route has absent of data packets, the goal to satisfy the contender to launch a router attacker, then the black hole attack can be complex recognizer to mark the attack. The active detection routing guides the data route to select the node with a high-level trust to keep away from the black hole attack. 2)Data routing protocol: The data routing is the process of nodal data routing to the sink. The route will select a node with high trust to avoid the black hole attack and improves the success radio of reaching the destination.The idea of data routing is any node receives a data packet, it selects the 1 node from the set of the node with trust is greater than the threshold. The upper node recalculates the unselected and selected node to check if the node cannot find the next step of the hop node it sends a feedback failure report to the upper node.

In this work, Active Trust computation is implemented using the subjective logic method. Subjective logic [20] is involving unpredictability and untrustworthy sources in situations for model and analysis type of probabilistic logic. Subjective logic uses constant unpredictability and trust parameter alternative of using discrete trust values. Subjective opinions about state variables that can take values from the mark condition value can be an idea of as a proposition that can be true or false.Figure 2, The

subjective logic tubules are (b,d,u,a)where,

b = belief mass,

d =disbelief mass,

u =uncertainty,

a = base rate.

$\boxtimes_x$= (b,d,u,a), let x be the trust value of the binary domain.

b,d,u,a ε [0,1], whereb+d+u=1;

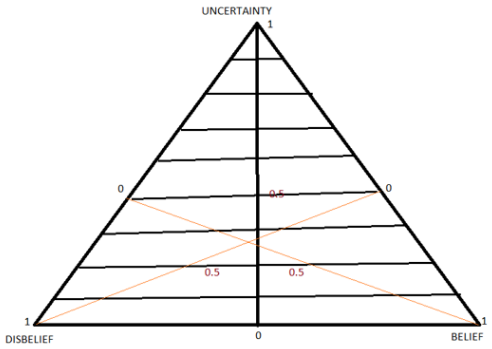

Fig 2. Opinion Triangle

The capacity of subjective logic in the presence of uncertainty, and modelling trust networks, combined with the power of Bayesian networks for modelling structures, creates a combination that calls a Subjective Network. A probabilistic logic for uncertain probabilities becomes subjective network logic. It distinguishes between certain and uncertain conclusions it is possible to make clear analysis throughput on preserved uncertainty is an advantage.

Trust network analysis using subjective logic (TNA-SL)[10] provides a simple notation for expressing transitive trust relationships and defines a method for simplifying complex trust networks, Trust measures are expressed as trust subjective logic is used to calculate between random reunion in the network. Trust values are components of an absolute structure(T;$\leq$), P is the set of principals and the trustspace is a partial function T: (P $\boxtimes$ T), P be the set of nodes in the network. Let $\varphi^{v}{}_{r}$= (x; y) be aroute(r) where x; y are the numbers of lucky and unlucky packet transmissions individually, the opinion corresponds to φ be$\boxtimes(\varphi)$= (b; d; u) where

$$b = x = (x + y + r) \tag{1}$$

$$d = y = (x + y + r) \tag{2}$$

$$u = r = (x + y + r) \tag{3}$$

where r $\geq$1 is a parameter behavior of the rate of loss of unpredictability, which can be used to adjust the use of uncertainty.

The transitivity and fusion operators are modeled with a combination of subjective trust networks. Let [A;B] express the someone trust edge from A to B, and let [B, X] express the trust edge from B to X. As expressed on subjective trust node are $([A;B] : [B,X] \diamond [A;C] : [C,X])$

As shown in Figure 3. The source A, B, and C specify that consecutive order in which the trust edges and advices are formed. Then, given set of trust edges with index A, the origin trust A receives advice from B and C, and is able to gain trust in variable X. By expressing each trust edge and belief edge as an opinion, it is possible for A to derive belief in X.

The advantage of subjective logic is, it is real-world situations can be modelled and analyzed more realistically, it allows decision-makers to be better informed about uncertainties specific situations, and future outcomes, it is directly compatible with traditional mathematical frameworks and handling ignorance and uncertainty.

4 RESULT AND ANALYSIS

As shown in Figure 4. The Packet to Delivery ratio can analyze by introducing an attacker to any of the nodes. The transmission remains constant throughout the packet delivery ratio is very high and the absence of an attacker gets Normal transmissions

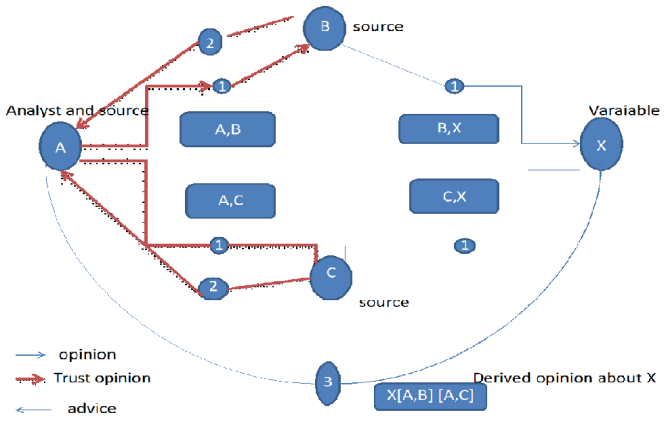

Fig 3. Subjective trust network

of packets.The number of packets sends the results to the number of packets received the performance very high. While in the packet delivery ratio has comedown to very low values to get a clear notice about the presence of an attacker. The attacker takes over the sent packets results from the source leading to the low delivery of packets to the destination.

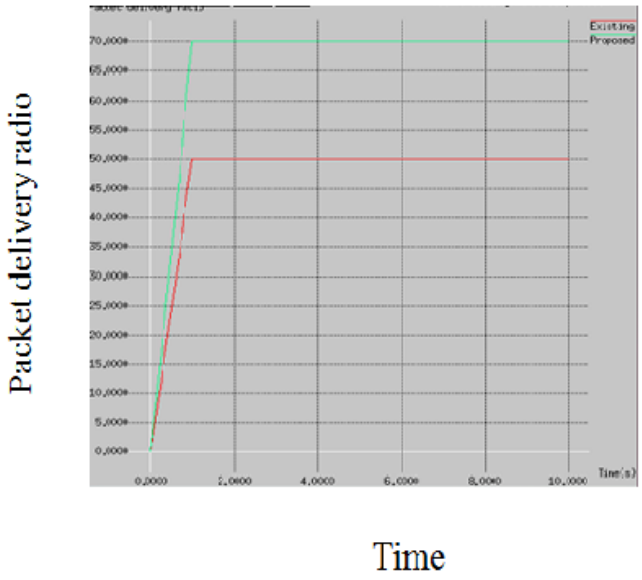

Fig 4. Packet delivery radio graph

As show in Figure 5 The midpoint in every part of the absence then the attacker is very high; the large part of packets sending from the source will reach the planned destination without any packet loss.

As the packet delivery ratio is good, the throughput is also high when there is a huge number of nodes.The throughput hears the packet pass by the sender will not be successful in reaching the destination.

The throughput and packet delivery ratio is AODV protocol using a black hole attack by analyzing the measure an attacker on a particular node. Whatever, the attacker declares for a specific node, it is possible to get various parameters like throughput, packet delivery ratio, etc. can differ accordingly.

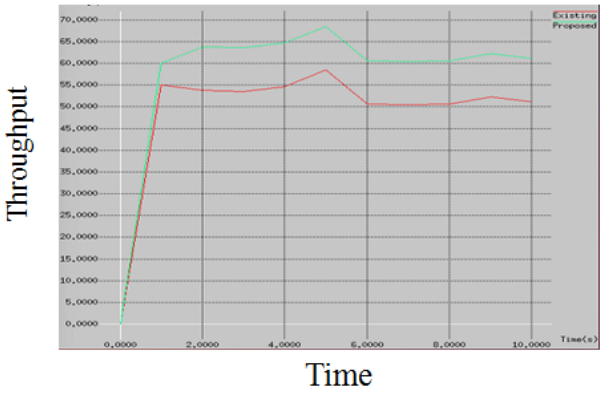

Fig 5. Throughput graph

5 CONCLUSION

The approach explained in this work is to detect and avoid the black hole attack in the WSN. The detection of these attacks has shown to improve the secure transmission of packets between the sensor nodes.The trust value is used to identify the black hole attack and it is barred from the route establishment process.The Active Trust plan can quickly discover the nodal trust and then avoid doubtful nodes to quickly achieves a 100% successful router probability. This scheme improves both energy efficiency and network security performance. Our proposed method after implemented in the network number of packets delivered ration gets improved by 5% for instance in case of existing AODV based routing method the PDR is in range of 50, our proposed method has got PDR as in range around 70. Similarly, throughput also gradually increasing compared to the existing algorithm. So active trust based algorithm is efficient when compared to the existing algorithms.

ACKNOWLEDGMENT

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

References

1) Sun Z, Wei M, Zhang Z, Qu G. Secure Routing Protocol based on Multi-objective Ant-colony-optimization for wireless sensor networks. *Applied Soft Computing*. 2019;77:366–375. Available from: https://dx.doi.org/10.1016/j.asoc.2019.01.034. doi:10.1016/j.asoc.2019.01.034.
2) Selvi M, Thangaramya K, Ganapathy S, Kulothungan K, Nehemiah HK, Kannan A. An Energy Aware Trust Based Secure Routing Algorithm for Effective Communication in Wireless Sensor Networks. *Wireless Personal Communications*. 2019;105(4):1475–1490. Available from: https://dx.doi.org/10.1007/s11277-019-06155-x. doi:10.1007/s11277-019-06155-x.
3) Li T, Liu W, Wang T, Ming Z, Li X, Ma M. Trust data collections via vehicles joint with unmanned aerial vehicles in the smart Internet of Things. *Transactions on Emerging Telecommunications Technologies*. 2020. Available from: https://dx.doi.org/10.1002/ett.3956. doi:10.1002/ett.3956.
4) Sun HM, Chen CM, Hsiao YC. An efficient countermeasure to the selective forwarding attack in wireless sensor networks. *IEEE TENCON*. 2007;p. 1–1. doi:10.1109/TENCON.2007.4428866.
5) Bar RK, Mandal JK, Singh MM. QoS of MANet Through Trust based AODV Routing Protocol by Exclusion of Black Hole Attack. *Procedia Technology*. 2013;10:530–537. Available from: https://dx.doi.org/10.1016/j.protcy.2013.12.392.
6) Satyajayantmisra K, Bhattarai G, Xue. BAMBi: Blackhole Attacks Mitigation with Multiple Base Stations in Wireless Sensor Networks. *the IEEE International Conference on Communications (ICC)*. 2011;p. 1–5.
7) Kompella RR, Yates J, Greenberg AA, Snoeren AC. Detection and Localization of Network Black Holes. *IEEE INFOCOM 2007 - 26th IEEE International Conference on Computer Communications*. 2007;p. 2180–2188. doi:10.1109/INFCOM.2007.252.
8) Yasin A, Zant MA. Detecting and Isolating Black-Hole Attacks in MANET Using Timer Based Baited Technique. *Wireless Communications and Mobile Computing*. 2018;2018:1–10. Available from: https://dx.doi.org/10.1155/2018/9812135.
9) Panda N, Pattanayak BK. Defense Against Co-Operative Black-hole Attack and Gray-hole Attack in MANET. *International Journal of Engineering & Technology*. 2018;7(3.4):84–84. Available from: https://dx.doi.org/10.14419/ijet.v7i3.4.16752.
10) Jiang B, Huang G, Wang T, Gui J, Zhu X. Trust based energy efficient data collection with unmanned aerial vehicle in edge network. *Transactions on Emerging Telecommunications Technologies*. 2020;p. 3942–3942. Available from: https://dx.doi.org/10.1002/ett.3942.
11) Priayoheswari B, Kulothungan K, Kannan A. Beta Reputation and Direct Trust Model for Secure Communication in Wireless Sensor Networks. *Proceedings of the International Conference on Informatics and Analytics*. 2016;73:1–11. Available from: https://doi.org/10.1145/2980258.2980413.
12) Airehrour D, Gutierrez J, Ray SK. GradeTrust: A secure trust based routing protocol for MANETs. In: 2015 International Telecommunication Networks and Applications Conference (ITNAC). IEEE. 2015;p. 65–70. doi:10.1109/ATNAC.2015.7366790.
13) Wang T, Zhang G, Yang X, Vajdi A. A Trusted and Energy Efficient Approach for Cluster-Based Wireless Sensor Networks. *International Journal of Distributed Sensor Networks*. 2016;12(4):3815834–3815834. Available from: https://dx.doi.org/10.1155/2016/3815834. doi:10.1155/2016/3815834.

14) Raza S, Haider W, Durrani NM, Khan NK, Abbasi MA. Trust Based Energy Preserving Routing Protocol in Multi-hop WSN. In: Networked Systems;vol. 9466. Springer International Publishing. 2015;p. 518–523. doi:10.1007/978-3-319-26850-7_42.
15) Qin D, Yang S, Jia S, Zhang Y, Ma J, Ding Q. Research on Trust Sensing Based Secure Routing Mechanism for Wireless Sensor Network. *IEEE Access*. 2017;5:9599–9609. Available from: https://dx.doi.org/10.1109/access.2017.2706973.
16) Ahmed A, Bakar KA, Channa MI, Haseeb K. Countering Node Misbehavior Attacks using Trust Based Secure Routing Protocol. *TELKOMNIKA (Telecommunication Computing Electronics and Control)*. 2015;13(1):260–260. Available from: https://dx.doi.org/10.12928/telkomnika.v13i1.1181.
17) Perkins CE, Royer EM. Ad-hoc on-demand distance vector routing. In: Proceedings WMCSA'99. Second IEEE Workshop on Mobile Computing Systems and Applications. IEEE. 1999;p. 90–100.
18) Heinzelman WR, Chandrakasan AP, Balakrishnan H. Energy-efficient communication protocol for wireless microsensor networks. In: Proceedings of the 33rd Annual Hawaii International Conference on System Sciences. IEEE Comput. Soc. 2000;p. 3005–3014.
19) Muzammal SM, Murugesan RK, Jhanjhi NZ. A Comprehensive Review on Secure Routing in Internet of Things: Mitigation Methods and Trust-Based Approaches. *IEEE Internet of Things Journal*. 2021;8(6):4186–4210. Available from: https://dx.doi.org/10.1109/jiot.2020.3031162.
20) Audunjosang. Artificial Reasoning with Subjective Logic. *Appears in the Proceedings of the 2nd Australian Workshop on CommonsenseReasoning*. 1997. doi:10.1.1.614.5935.