A Novel Trust Based Routing Protocol For Wireless Sensor Networks

Vignesh Ramamoorthy H, Dr. R. Gunavathi

Abstract— Wireless Sensor Networks (WSNs) are used in most of the common places where the other technology fails due to natural and other calamities. WSN plays a major supportive factor in all areas such as industrial, agricultural, medical and so on. Therefore, WSN are prone to security attacks like blackhole, wormhole and other security breaches due to its wide range of support. These attacks focus in collapsing the network through draining the energy, sending fake data and other type of attacks. The proposed protocol focused in avoiding blackhole attack through identifying a greater number of reliable routes quickly. In addition, the proposed protocol obtains nodal trust, which improves the security of the network. The experimental results show the performance of the proposed protocol is better than the other previous approaches and studies. Thus, the proposed trust-based routing protocol successfully improves security and lifetime of the network.

Index Terms— blackhole, network, protocol, security, sensor, warmhole, WSN.

1 Introduction

Wireless Sensor Network (WSN) is used in agriculture, industrial, medical and so on for its easy and promising deployment behavior in any type of environment. WSN [1, 2] consists of small devices and very less battery power for its processing. The tiny sensor nodes consist of the microprocessor, minimum battery power and a small RAM [3]. The major part of WSN is to collect the data from the environment where deployed and forwards the collected data to the base station (BS). The collected data reaches the BS through direct relay or through multi-hop communication. Identifying the route to forwarding the data is a tedious process in WSN [3, 5]. Some of the security features are not reliable and there is a need for new techniques to avoid security attacks. Finally, the data center collects the data from BS for analysis and for other research [4, 6]. As WSN is an ad hoc based network where the network can be easily attacked by varieties of attack like, node capture, node cloning, and denial of service (DoS) attack and so on. Enormous researches were processed and in processing of improving the security of WSN. The attacker compromises the sensor node and forwards the fake messages from it, eavesdrop the receiving messages and utilize the unwanted resources to drain the energy soon. One of the general and dangerous security attacks in WSN is blackhole attack. The main objective of this attack is to compromise the sensor node to forwards fake messages and to receive the messages from the other nodes by showing this node as a shortest path node to reach BS. The affected sensor node absorbs the collected data form the other nodes and it forwards the fake data to the BS. So that the BS does not find any difference in the routine process of the network [4]. The source node forwards Route Request (RREQ) to all other nodes to receive the best route to forward the collected data to reach BS. Best route comprises highest sequence number, shortest path and less hop count [6]. The malicious node after receiving the RREQ from the source node it forwards the Route Reply (RREP) stating that it holds best sequence number and least hop count than the other nodes. The source node first checks for highest sequence number. When two or more nodes holds highest sequence number then it checks for least hop count. Finally, after receiving the RREP from malicious node it forwards the data to the malicious node. This process continued with all other nodes of the network to receive data from the nodes. Identifying the malicious node and recovering it is a tiresome process. The malicious node will remain unchanged as a forwarding node still it drains its energy through this the attack can identified. In addition, through checking the hop counts may identify the malicious node. The Figure. 1 depicts the flow of blackhole attack in WSN [4,5]. The next section, literature survey details about previous studies on blackhole attack in WSN. Section III proposed a Novel Trust Based Routing Protocol (NTBRP), an effective protocol to secure the network from blackhole attack. The performance of proposed work is details in Section IV and Section V concludes the paper.

- *Vignesh Ramamoorthy H is currently pursuing part time Ph.D program in Computer Science at Sree Saraswathi Thyagaraja College, Pollachi, India, and also working as an Assistant Professor, Dept. of Information Technology, Sri Krishan Arts and Science College, Coimbatore, India, PH-09791770735. E-mail: hvigneshram@gmail.com*
- *Dr.R.Gunavathi is currently working as a Head, PG Department of Computer Applications, Sree Saraswathi Thyagaraja College, Pollachi, India. E-mail: gunaganesh2001@gmail.com*

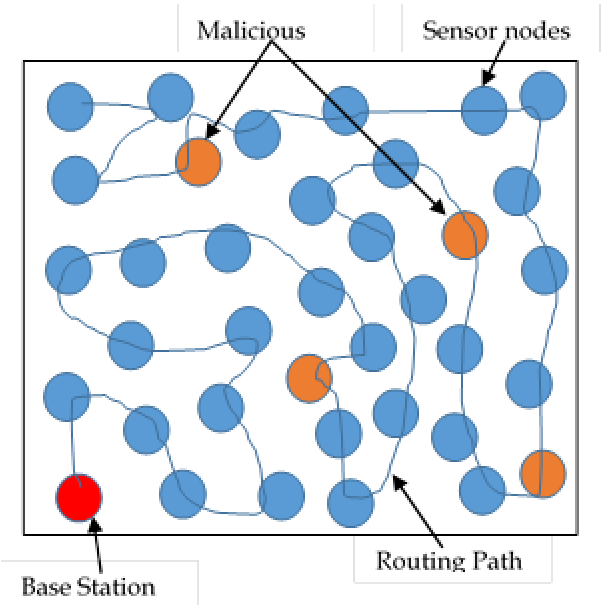

Figure 1: Blackhole attack in WSN.

2 Literature Survey

Kaur & Kumar [7] discussed about the mitigation of blackhole attack in WSN. In this paper, detect and defend method is used in identifying the blackhole attack. The attacker launches many DoS attacks to reduce the performance of the network. They proposed detect and defend method to identify the blackhole attack in WSN. The method performs better in identifying the blackholes in the network. The defending algorithm of the proposed model less performs with the network model where the energy efficiency schemes added together. Dubey et al [8] introduce the Warning Message Counter (WMC) method. This method identifies and blackhole attack with grayhole and sinkhole attack in WSN. This proposed method uses lightweight symmetric key cryptography to defend the network form the attacks. The performance of the proposed scheme achieves minimum false positive as well as less false negative in identifying the attacks. The pitfall of this proposed scheme is that it utilizes the same algorithm for identifying the all attacks where the energy constraints are not considered. Farooq et al propose the protective scheme against the blackhole attacks in WSN [9]. They proposed a scheme to consider the energy of sensor for better packet delivery ratio. Less delay time and high throughput also achieved through this scheme. The end- to-end delay is decreased and overall energy consumption and network traffic reduced using this scheme. Packet delivery ratio and energy constrains are compared with other schemes. The high detection rate is not considered and energy consumption model is not fit when the sensor nodes holds high energy level. Kalkha et al. [10] introduces the Hidden Markov Model (HMM) solution to identify blackhole attack in WSN. The HMM analyses the shortest path to detect the malicious node of the network. This approach works with the RREP received from the adversary node. This scheme checks the RREP and its own shortest path algorithm to identify its reliability. This scheme outperforms in identifying the malicious node and detains its level in resolving other issues like data integrity and aggregation and so on.

Upadhyay et al. [11] developed an authentication method for ad hoc network based on certificate based security services. This model proves its efficiency through reduced transmission time and energy consumption. Hashing algorithm and certification authority is developed and encrypted using private key of certification authority. The hash values were compared and communication is established when the two hash values remains unchanged.

A secure routing model WSN based on trust evaluation model is the scheme proposed by yang et al. [12]. Energy Optimized Secure Routing (EOSR) proposes distributed trust evaluation model to identify and isolate malicious nodes. Node's trust level, energy and path is considered by EOSR. The comprehensive path cost is introduced to identify the node trust value, energy and residual energy. Reliability and load balance are improved effectivity

3 Sections Novel Trust based Routing Protocol

The proposed routing protocol composed of a novel trust - based routing protocol shown in Figure 2.

3.1 AODV Protocol

This proposed protocol uses a multi-hop flat routing topology where all nodes assigned with equal energy, functionality and roles. Ad Hoc Distance Vector (AODV) routing protocol is used in this scheme to identify and defend the blackhole attack in WSN [13].

AODV is a reactive distance vector routing protocol. It uses the sequence number to identify the routes. An input of routing table contains the destination address, next node address, distance, hop counts, destination sequence number, time expiration for each entry of the table. When a node checks to find a route if it avails in routing table it follows the route or else it broadcasts a RREQ message to all of its neighbors. The RREQ messages creates temporary records in routing table for reverse route nodes to reach RREP. The temporary routing entries in routing table will remove after receiving RREP from its neighbors or after a certain period [14]. After receiving RREP the source node forwards the collected data to the neighbor node which is nearer to destination. The neighbor node also follows RREQ and RREP to reach its destination [13, 14].

3.2 Trust Based Routing

The proposed protocol provides a prevention from blackhole attack using AODV protocol in WSN. Prevention approach utilizes the shortest path between source and destination node. The AODV routing protocol suggests the process of finding a malicious node and path in route discovery phase. Through NTBRP using AODV protocol the nodal trust can be obtained quickly and effectively guiding data route with high trust to avoid blackholes.

3.3 Calculation of Trust

The proposed protocol provides a prevention from blackhole attack using AODV protocol in WSN. Prevention approach

Every node performs trust calculation to avoid blackhole attack. When the node N_{source} performs a detection route for node $N_{neighbor}$ at time t_i. The trust of node N_{source} to $N_{neighbor}$ is $\{\wedge^{N_{source}}_{N_{neighbor}}(t_1)$; otherwise $\{\vee^{N_{source}}_{N_{neighbor}}(t_1)$e;

Consider the node N_{source} has n interactions with $N_{neighbor}$ during the time t, the detection is as follows,

$$\left\{\bigwedge_{N_{neighbor}}^{N_{source}}(t_1)\Big|\bigvee_{N_{neighbor}}^{N_{source}}(t_1), \bigwedge_{N_{neighbor}}^{N_{source}}(t_2)\Big|\bigvee_{N_{neighbor}}^{N_{source}}(t_2), \ldots. \bigwedge_{N_{neighbor}}^{N_{source}}(t_w)\Big|\bigvee_{N_{neighbor}}^{N_{source}}(t_w)\right\}$$

$\wedge^{N_{source}}_{N_{neighbor}}(t_i)\Big|\vee^{N_{source}}_{N_{neighbor}}(t_i)$ refers the trust value of N_{source} to $N_{neighbor}$ at (t_i), when the data is dropped then $\vee^{N_{source}}_{N_{neighbor}}(t_i) < 0$; otherwise $\wedge^{N_{source}}_{N_{neighbor}}(t_i) > 0$.

The proposed trust based routing algorithm is defined in Table 1.

```
1: Initialize the Network, with N nodes where: N = 1,2,3 ., n
2: Initialize Route Discovery by Source Node $N_{source}$
3: $N_s$ sends RREQ Packets to Neighbor $N_{neighbor}$
4: $N_{neighbor}$ receives the RREQ Packets and forwards the RREP Packets to $N_{source}$
5: $N_{source}$ checks all $N_{neighbor}$ RREP Packets and choose $N_{neighbor}$ which holds highest sequence number
6: IF more than one $N_{neighbor}$ holds highest sequence number then
    Checks for $N_{neighbor}$ hop counts
    Select $N_{neighbor}$
7: IF $N_{neighbor}$ is sink then
    Data routing process completed
  Else
    Repeat step 2 to step 7
8: End process
```

3.4 Energy Consumption Model and Related Definitions

The energy consumption model for the proposed protocol is represented in Eq.1 and Eq.2.

Eq.1 represents the energy consumption for transmitting data packet and Eq.2 represents the energy consumption for receiving data packet.

E_{elec} represents the transmission circuit.

$\varepsilon_{fs}\ and\ \varepsilon_{amp}$ are the energy model for power amplification.

$$\begin{cases}E_{mem} = lE_{elec} + l\varepsilon_{fsd^2\ if\ d\leq}d_0 \\ E_{mem} = lE_{elec} + l\varepsilon_{amp}d^4\ if\ d > d_0\end{cases} \tag{1}$$

$$E_R(l) = lE_{elec} \tag{2}$$

The content of trust based routing protocol can be divided into 6 parts shown in Figure.2.

P_head	P_type	Src_ID	Max_rou_len	Ack_nei_node	P_ID

Figure 2: Structure of detection route packets.

- Packet head
- Packet type
- Source node ID
- Maximum route length
- Acknowledge from neighbour node
- Packet ID

The structure of feedback packet composed into 6 parts shown in Figure 3.

- Packet head

P_head	P_type	Src_ID	Dest_node	Detect_P_ID	P_ID

Figure 3: Structure of feedback packets of detection route.

- Packet type
- Source node ID
- Destination node
- Detection packet ID

4 Performance Analysis

The simulation platform used in this proposed protocol is NS3.25 [15, 16]. The parameters specified in this protocol is specified in Table I.

The network model in this work:

- All sensor nodes in network are fixed and homogeneous.
- Uniformly deployed and same initial energy.
- Fixed base station.
- Weight is symmetric
- Transmission weight is same in both direction

The performance of NTBRP is compared with previous studies ActiveTrust and EOSR. The simulation parameters used for this proposed protocol is, packet delivery ratio, network throughput and average energy consumption.

TABLE I

NETWORK PARAMETERS SPECIFIED FOR PROPOSED PROTOCOL

Parameters	Value
Network Space	100 X 100
Number of Nodes	100 (0 – 99)
BS	Node 0
TX Power	-5 dBm
Eelec	50nJ/bit
Initial Energy	1J
Packet length	6400 bits
Simulation Time	1000 sec
MAC type	MAC/802_11

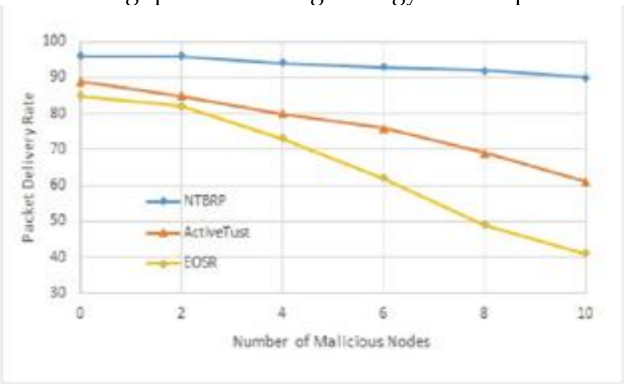

Figure 4: Packet Delivery Ratio

The Figure 4 shows packet delivery ratio between NTBRP, ActiveTrust and EOSR. NTBRP achieves high packet rate than the existing schemes.

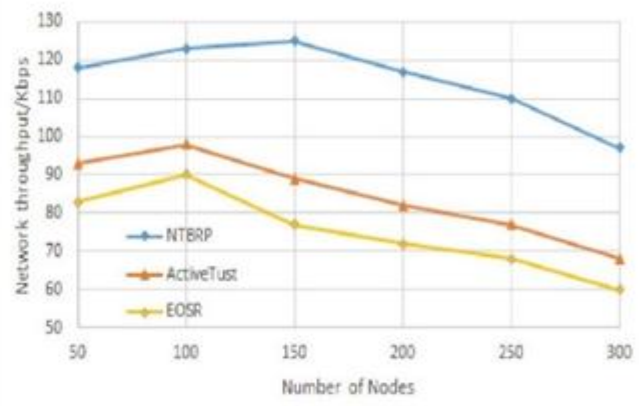

Figure 5: Network Throughput

The Figure 5 shows network throughput between NTBRP, ActiveTrust and EOSR. The proposed protocol NTBRP achieves higher throughput compared with the existing models.

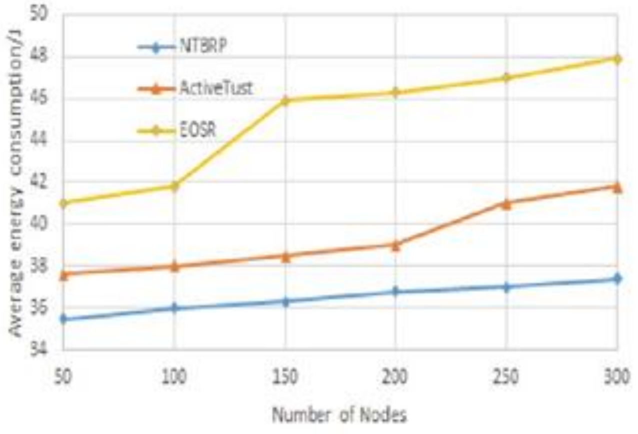

Figure 6: Average Energy Consumption

The Figure 6 displays average energy consumption between the proposed NTBRP and the existing schemes ActiveTrust and EOSR. The proposed protocol NTBRP consumes less energy compared to the previous studies.

Thus, the simulation performance shows that the proposed protocol improves efficiency in identifying and defending blackhole attack in WSN.

5 CONCLUSION

This paper proposes a novel trust based routing protocol to identify blackhole attack in WSN. Identifying the malicious node is tedious process and it achieved through the proposed protocol. It detect the reliable routes of the network and follows same energy consumption model and trust route is calculated to defend the blackhole attack. The proposed protocol NTBRP achieves better performance than the existing schemes. Thus improves the performance of network lifetime.

REFERENCES

[1] Vignesh Ramamoorthy H & Dr.R.Gunavathi. (2019). “Survey on Discovery Practices of Black Hole Attack”, International Journal of Information and Computing Science (IJICS), 6 (5), pp. 486-492.

[2] Vignesh Ramamoorthy H, (2016). “A Review on Structural Health Monitoring in Wireless Sensor Networks”, International Journal for Research in Applied Science & Engineering Technology (IJRASET), 4(7), pp. 550-559.

[3] Biswas, S., Das, R., & Chatterjee, P. (2018). Energy-efficient connected target coverage in multi-hop wireless sensor networks. In Industry interactive innovations in science, engineering and technology (pp. 411-421). Springer, Singapore.

[4] Mahgoub, I., & Ilyas, M. (2018). Sensor network protocols. CRC press.

[5] Liu, Y., Dong, M., Ota, K., & Liu, A. (2016). ActiveTrust: Secure and trustable routing in wireless sensor networks. IEEE Transactions on Information Forensics and Security, 11(9), 2013-2027.

[6] Krishnakumar, A., & Anuratha, V. (2019). Energy-Efficient LEACH Protocol with Multipower Amplification for Wireless Sensor Networks. In Pervasive Computing: A Networking Perspective and Future Directions (pp. 103-110). Springer, Singapore.

[7] Kaur, T., & Kumar, R. (2018, August). Mitigation of Blackhole Attacks and Wormhole Attacks in Wireless Sensor Networks Using AODV Protocol. In 2018 IEEE International Conference on Smart Energy Grid Engineering (SEGE) (pp. 288-292). IEEE.

[8] Dubey, P., Veenadhar, S., & Gupta, S. (2019). Survey on Energy Efficient Clustering and Routing Protocols of Wireless Sensor Network.

[9] Farooq, M. U., Wang, X., Sajjad, M., & Qaisar, S. (2018). Development of Protective Scheme against Collaborative Black Hole Attacks in Mobile Ad hoc Networks. TIIS, 12(3), 1330-1347.

[10] Kalkha, H., Satori, H., & Satori, K. (2019). Preventing Black Hole Attack in Wireless Sensor Network Using HMM. Procedia computer science, 148, 552-561.

[11] Upadhyay, A., Khan, U., & Ahmad, M. (2019). WSN Existence Data Rate with High Quality using AODV-RSA Based Analysis. Available at SSRN 3351075.

[12] Yang, T., Xiangyang, X., Peng, L., Tonghui, L., & Leina, P. (2018). A secure routing of wireless sensor networks based on trust evaluation model. Procedia computer science, 131, 1156-1163.

[13] Anwar, M. N. B., Chowdhury, S., Haque, U. M., & Khan, S. S. (2018). Wildlife Monitoring using AODV Routing Protocol in Wireless Sensor Network. International Journal of Computer Networks and Communications Security, 6(1), 17-23.

[14] Bar, R. K., Mandal, J. K., Halder, T. K., & Mukhopadhyay, S. (2018, January). Extending Lifetime of a Network by Load Sharing in AODV Routing Protocol. In Annual Convention of the Computer Society of India (pp. 107-112). Springer, Singapore.

[15] Modieginyane, K. M., Malekian, R., & Letswamotse, B. B. (2019). Flexible network management and application service adaptability in software defined wireless sensor networks. Journal of Ambient Intelligence and Humanized Computing, 10(4), 1621-1630.

[16] Vignesh Ramamoorthy H & Dr.R.Gunavathi (2019, August). Improving the Lifetime of Wireless Sensor Network through Energy Proficient AODV Protocol. International Journal of Engineering and Advanced Technology (IJEAT), Vol. 8, no.6.