International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

Comprehensive Trust based Routing Protocol to Mitigate Black-hole attack in Wireless Sensor Networks

B.Sandhya Rani
Department of Computer Science & Engineering
UCE (A) - Osmania University, Hyderabad
Telangana, India.
sandhya.cse.nalgonda@gmail.com

Kattula Shyamala
Department of Computer Science & Engineering
UCE (A) - Osmania University, Hyderabad
Telangana, India.
prkshyamala@gmail.com

Abstract— Wireless Sensor Network (WSN) is a collection of sensor nodes, that sense environmental data and send it to the administrator for further processing. Sensor nodes are wireless devices with limited battery and are vulnerable to security attacks such as black hole attack, gray hole attack, sink hole attack etc. Researchers have proposed many security mechanisms to mitigate security attacks. Trust based approaches have gained tremendous interest among researchers to embed security in WSNs. A Trust Based Secure Routing Protocol to mitigate black hole attack is presented in this paper. The protocol computes comprehensive trust value for each node and routes the packets only through the nodes with trust value > 0.5. The results of the proposed protocol are compared with TBSEER [10] protocol. The results show an improvement in Packet Delivery Ratio (PDR), throughput, End to End (EED), routing overhead and energy consumption.

Keywords-– Black-hole attack, Comprehensive Trust, Secure EELB-AOMDV, Indirect trust, Trust based protocol

I. Introduction

The WSNs are extensively employed in the military, traffic control, environmental monitoring, and medical field. In addition, the nodes can also be deployed in hostile environment, making the network vulnerable to various attacks. Due to the lack of administration control, the sensors are free to join and leave the network to launch internal and external attacks; making the routing process a complex task. Security attacks such as black hole, gray hole, selective forwarding, and sink-hole attacks can launch DoS attack, packet drop, resource wastage and bandwidth wastage [1].

Black hole attack is a DoS attack [2], in which a malicious node advertises itself possessing a shortest path to the destination by sending RREP packet to the source as a response to RREQ packet during route discovery. The attacker node intercepts the source packets and drops them all to launch DoS attack. Many security mechanism are proposed to mitigate black hole attack such as cryptography, overhearing or promiscuous mode, sequence based threshold, acknowledgement based, cross checking based, cross layer, clustering, hybrid schemes, IDS and trust based schemes [3]. The cross layer collaboration leads to collision in the presence of heavy load, acknowledgement based scheme and cross checking based schemes leads to high routing overhead, sequence based schemes require to maintain sequence numbers in the routing table and leads to high storage capability. Cryptography and authentication-based schemes require complex calculations, storage and high energy consumption. Therefore, trust-based schemes can be considered to solve the issues. In a trust model, each node is allowed to evaluate the trustworthiness of its neighbor to mitigate the attacks. The communication in the trust model depends on the mutual trust between the nodes. Trust is calculated to identify the relationship among two entities to provide reliability, integrity and behavior of a node to improve node cooperation, ease of implementation, integrity, and flexibility. The cooperation of trustworthy nodes increases the packet delivery of the nodes in the network. Moreover, trust-based security mechanism is easily implementable, adaptable and integrated into sensor nodes as it doesn't require any extra hardware and software configuration and also doesn't affect the energy consumption of the nodes.

Trust Value (TV) is computed based on the past behavior and interactions of the participating nodes. Trust computation is classified as Direct, Indirect or Recommended Trust and Comprehensive Trust [4]. The direct trust of participating nodes (connected nodes) is computed by considering packet forwarding ratio or packet drop ratio or packet integrity of the nodes. In a wireless network, direct communication with the nodes is not always possible. To compute the TV of a node, which is not in direct communication, a node has to depend on indirect trust. An evaluator node (a node which calculates TV) in computing indirect TV depends on the trust-worthy node to compute the TV of another node which is not directly connected to it. A comprehensive trust is obtained by considering both direct and indirect TVs. Malicious node

Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

detection can be done during route discovery and data transmission phase. Source identifies the malicious behavior of other nodes by exchanging RREQ and RREP packets during route establishment phase. If a node's behavior is suspicious it is marked as malicious and is avoided in establishing a path. In data transmission phase, all the nodes enter into promiscuous mode to monitor the neighboring node's packet forwarding or dropping behavior to identify malicious node.

II. Literature Survey

Light Weight Trust Based Routing Protocol (LTB-AODV) proposed in [5] addresses black hole and gray hole attacks. Every node computes the TV of neighbor node based on direct trust and indirect trust. In direct trust, node i computes TV based as a ratio of number of forwarded packets to the number of packets to be forwarded. In Indirect trust, the node i computes the TV based on the trust of neighboring nodes of i on node j .

$$Ti(j)=\alpha *Ti\ (self)(j) + \beta*Ti\ (neighbor)(j)$$

$$\text{Where } \alpha+\beta=1$$

The results are compared with AOMDV protocol using NS2 simulator in the presence of 3,5 and 7 malicious nodes exhibiting packet dropping behavior. PDR of the protocol is improved by 10%, 20% and 30% with 3,5 and 7 malicious nodes respectively. The EED of the LTB-AODV is increased by 1 ms compared to AOMDV protocol. Routing frequency of the protocol is reduced compared to AOMDV protocol.

Trust and Energy Aware Routing Protocol (TERP) [6] considers trust, residual energy, and hop count of the neighboring nodes as a metric. Direct trust, indirect trust, and the expected positive behavior are used to compute TV. The direct trust is calculated as packet-forwarding ratio and the recommendations made by other nodes make up indirect trust. The expected likelihood of the positive behaviors is calculated as the Beta probability density function to check the expected future forwarding behavior of the node. During route discovery, nodes with less residual and malicious behavior are eliminated and an alternative route is found to route the packets.

FDTM - IoT based RPL (FDTM-RPL) [7] is a fuzzy based trust model. TV is calculated based on the Quality of Service (QoS), Quality of Peer to Peer Communication (QPC) and Contextual Information (CI). QPC is calculated based on the direct communication of nodes, historical QPC and indirect QPC. Network throughput, availability, percentage of successful interactions and average EED are considered as metrics to evaluate QoS. Stability of the links, mobility of nodes is considered in computing CI. Final TV is calculated by combining QoS, QPC and CI. Five trust levels are introduced in the protocol. If the TV is less-than 0.5 a node is considered as a malicious node and is isolated from the network. The simulation is carried out in COOJA and the results show that the protocol improved packet loss ratio, EED and average number of parent changes compared to Minimum Rank with Hysteresis Objective Function (MRHOF) and Objective Function Zero (OFO) protocols.

Adaptive Trust-based Routing Protocol (ATRP) in [8] computes overall trust based on direct, indirect and witness trust. The Q-learning technique updates the TV in ATRP. The source receives the Indirect TV from the direct nodes to compute Total Trust. Witness Trust (WT) gives the confidence that the assessed node has in its immediate and indirect neighbors. The simulation is run for ten rounds with each round representing 100 s in MATLAB. The simulation results are compared with TERP and DTLSR [9] protocols. The results show an improvement in PDR, latency, throughput, and energy consumption with increase in number of nodes.

Trust Based Secure and Energy Efficient Routing protocol (TBSEER) in [10] computes direct TV as adaptive penalty coefficient and volatility factor with space and time constraints and sends it to the neighboring node by attaching the TV in the data packet itself. The indirect TV of ITij is calculated as:

$$IT_{ij} = 1/q\ \ \Sigma^{q}_{u€Bk}\ (DT^{t}_{iu} * DT^{t}_{uj})$$

Where q is the number of public trusted nodes.

The protocol also computes Energy TV of node j (Ej) as

$$Ej = REj/E0$$

Where REj is the residual energy of node j.

The node i calculates the comprehensive TV of node j as sum of direct TV, indirect TV and Energy. The node i calculates the comprehensive TV of node j as sum of direct TV, indirect TV and Energy. The results show an improvement of 62.5%, 30.77%, 18.1% in detecting black hole, forwarding and selective forwarding attacks respectively compared to TSSRM and TESRP protocols in the presence of 5% of malicious nodes in the network. The results also show an improvement of 47.83% and 18.31% in average EED.

Authors in [11] have proposed MC_TQR protocol to identify malicious nodes in mission critical networks. The protocol computes the TV of a node by considering packet forwarding ratio, expected transmission count and EED. A node with TV ranging between 0.9 - 1.0 is considered as trusted node and used for packet transmission. The performance of the protocol is compared with AOMDV, AOTDV, and TQR protocols. The results show that the protocol outperforms other protocols in terms of PDR, EED, and throughput.

III. Comprehensive trust based EELB-AOMDV Protocol

To further improve the energy consumption and EED of Secure EELB-AOMDV protocol [12], "Comprehensive Trust Based Secure EELB-AOMDV Routing Protocol (CTB Secure EELB-AOMDV)" is proposed. The protocol identifies and maintains multiple paths during route discovery process and can detect malicious nodes to provide reliability of mission-critical data. The protocol uses direct trust, indirect trust, queue occupancy ratio and residual energy of a node as a metrics to calculate comprehensive trust of a node. The protocol uses the metrics proposed in TBSEER [10] and also considers queue occupancy ratio to compute comprehensive TV. The flowchart for comprehensive trust calculation is presented in Figure 1.

Based on the TV, a node is marked as malicious or legitimate node during route discovery phase and packet transmission phase. During route discovery process, source broadcasts false RREQ packets with unavailable destination id in the network to setup a trap for malicious node. The legitimate nodes ignore RREQ packets; whereas the malicious nodes uni-casts RREP packets to the source claiming to have a shortest distance to reach destination. The source upon receiving RREP packets, marks the nodes as malicious node and isolates them from the network to mitigate black hole attack. During the packet transmission phase, the nodes with comprehensive TV greater than 0.5 [13] are considered for forwarding the packets.

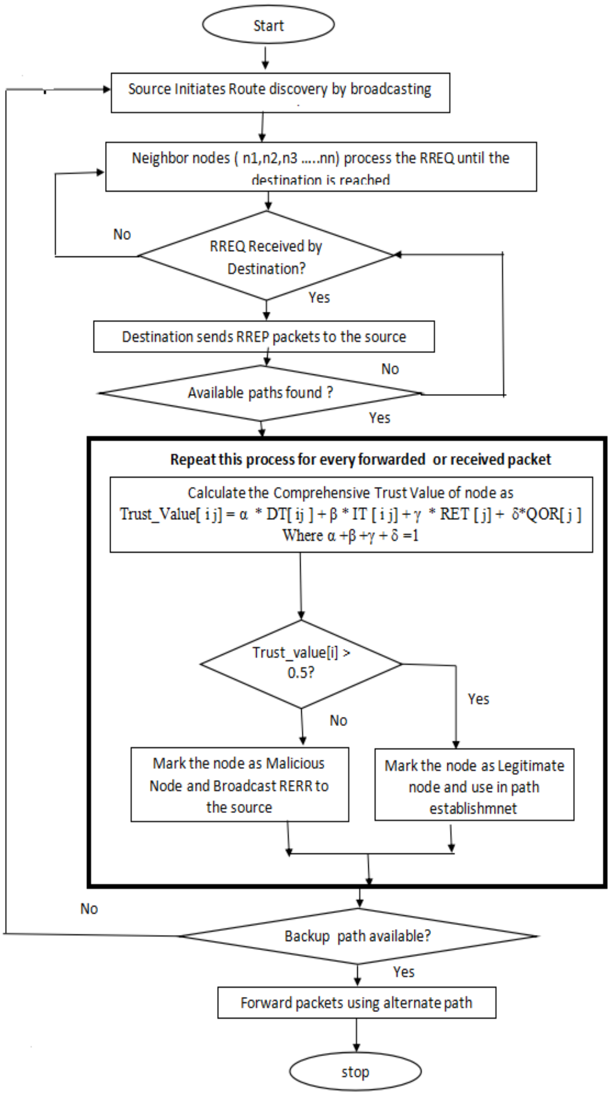
Start
Source Initiates Route discovery by broadcasting
Neighbor nodes (n1,n2,n3 …..nn) process the RREQ until the destination is reached
No
RREQ Received by Destination?
Yes
Destination sends RREP packets to the source
No
Available paths found ?
Yes
Repeat this process for every forwarded or received packet
Calculate the Comprehensive Trust Value of node as
Trust_Value[i j] = α * DT[ij] + β * IT [i j] + γ * RET [j] + δ*QOR[j]
Where α +β +γ + δ =1
Trust_value[i] > 0.5?
Yes
No
Mark the node as Malicious Node and Broadcast RERR to the source
Mark the node as Legitimate node and use in path establishmnet
No
Backup path available?
Yes
Forward packets using alternate path
stop

Figure 1: Comprehensive Trust Calculation flowchart

The comprehensive Trust (CT) of a node j from i, represented as CT[ij] is computed as a weighted trust of Direct Trust (DT[ij]), Indirect Trust (IT[ij]), Residual Energy Trust (RET[j]) and Queue Occupancy Ratio (QOR[j]) as shown below :

$$CT[ij]= (\alpha * DT\ [ij]\ + \beta * IT\ [ij]\ + \ \gamma * RET\ [j]\ + \delta * QOR[j]) \qquad (1)$$

Where $\alpha + \beta + \gamma + \delta = 1$

DT[ij] is computed based on number of forwarded and received packets. TV of a node is increased by 0.15 upon forwarding and 0.05 upon receiving packets as shown below.

$$DT[ij]= 0.15 * Fwd\_pkts[j]+ 0.05 * Recv\_pkts[j] \qquad (2)$$

IT of node j from node i, represented as IT[ij] is computed based on the recommendations of the trusted neighbouring node as follows:

$$ITij = 1/n\ \Sigma^{n}_{u\in Bk}\ (DT^{t}_{iu} * DT^{t}_{uj}) \qquad (3)$$

where n is the number of public trusted nodes

RET of a node is computed as a ratio of difference between Initial Energy (IE[j]) and Energy Consumption(EC[j]) and IE[j] of a node as shown below:

$$RET[j]= (IE[j]- EC[j]) / IE[j] \qquad (4)$$

EC is computed based on the energy required to transmit and receive packets represented as TXenergy and RXenergy as shown below:

$$EC[j]=TXenergy * Transmittedpackets[j] + RXenergy * Receivedpackets[j]$$

where Transmittedpackets[j] is number of transmitted packets and Receivedpackets[j] is number of received packets by node j.

QOR[j] is computed based on the Queue Length (Qlength[j]) and Queue Size (Qsize).

$$QOR[j]= w * (Qlength[j] / Qsize) \qquad (5)$$

where Qlength[j] is the number of packets in the Queue of node j and Qsize is the total size of the Queue and w is the weighting factor between 0 and 1.

The Qlength of a malicious node is considered as 0, because in the black hole attack the malicious node drops all the packets and the Qlength of the legitimate node considered to be greater than 1. An example is presented below to better understand the protocol with 5 nodes in a network as shown in Figure 2. Recv represents the received packets, Fwd represents forwarded packets and QL represents the Queue length of a node and Qsize is considered as 5.

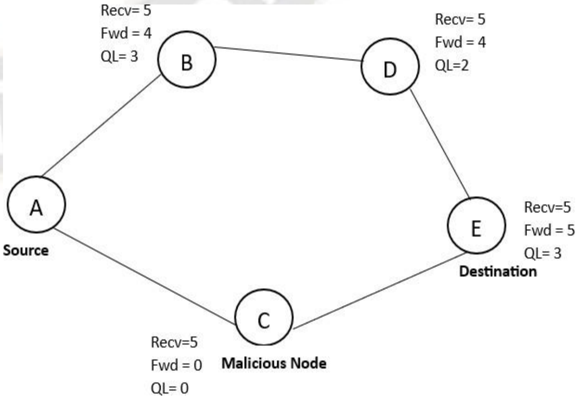

Figure 2: Comprehensive Trust Calculation Example

Let $\alpha = 0.5$, $\beta = 0.3$, $\gamma = 0.1$and$\delta = 0.1$, Qsize = 5, IE = 10J, TXenergy = 0.5J, RXenergy = 0.3J

TABLE I: COMPREHENSIVE TRUST COMPUTATION

Link	Recv	Fwd	QL	DT	IT	EC	RE	QOR	CT
AB	5	4	3	0.85	0	3.5	0.65	0.3	0.52
AC	5	0	0	0.25	0	1.5	0.85	0	0.21
BD	5	4	2	0.85	0	3.5	0.65	0.2	0.51
DE or CE	5	5	3	1	0	4	0.6	0.3	0.59

The values of DT, EC, RE, QOR and CT in Table I are computed using the formulas (1) to (5), presented above. The IT of all the nodes is considered as 0, because the nodes in the link column are directly connected to each other. The IT of a node is computed based on the recommendations of trusted nodes.

IT[AD], connected as A-B-D, computed as:
$IT[AD] = 1/n * (DT[AB]*DT[BD])$
$= 1/n * 0.85*0.85$
$= 0.7225/1$
$=0.7225$

n is considered as 1, as the number of public trusted nodes in the path is 1

IT[AE] connected as A-B-D-E is computed as:
$IT[AE] = 1/n *(DT[AB]*DT[BD]*DT[DE])$
$= 1/n * (0.85*0.85*1)$
$= 0.7225/2$
$= 0.36125$

n is considered as 2, as the number of public trusted nodes in the path are 2

IT[AE] connected as A-C-E is computed as:
$IT[AE] = 1/n *(DT[AC]*DT[CE])$
$= 1/n * (0.25*1)$
$= 0.25/1$
$= 0.25$

n is considered as 1, as the number of public trusted nodes in the path are 1

CT of the links is calculated as:
$CT[AB]= (\alpha * DT [AB] + \beta * IT [AB] + \gamma * RE[B] + \delta * QOR[B])$
$= 0.5 * 0.85 + 0.3 * 0 + 0.1 * 0.65 + 0.1 * 0.3$
$= 0.52$

$CT[AC]= (\alpha * DT [AC] + \beta * IT [AC] + \gamma * RE[C] + \delta * QOR[C])$
$= 0.5 * 0.25 + 0.3 * 0 + 0.1 * 0.85 + 0.1 * 0$
$= 0.21$

$CT[BD]=(\alpha * DT [BD] + \beta * IT [BD] + \gamma * RE[D] + \delta * QOR[D])$
$= 0.5 * 0.85 + 0.3 * 0 + 0.1 * 0.65 + 0.1 * 0.2$
$= 0.51$

$CT[DE] = (\alpha * DT [DE] + \beta * IT [DE] + \gamma * RE[E] + \delta * QOR[E])$
$= 0.5 * 1 + 0.3 * 0 + 0.1 * 0.6 + 0.1 * 0.3$
$= 0.59$

$CT[CE]= (\alpha * DT [CE] + \beta * IT [CE] + \gamma * RE[E] + \delta *QOR[E])$
$=0.5 * 1+ 0.3 * 0 + 0.1 * 0.6 + 0.1 * 0.3$
$= 0.5+0+0.06+0.03$
$=0.59$

If the CT is less than threshold (0.5), the node is considered as malicious node. In Table I, CT[AC] is 0.21 which is less than the threshold, therefore node C is considered as malicious node and is isolated from the network to mitigate black hole attack.

IV. EXPERIMENTAL SETUP

The simulation is carried out in NS2 simulator with 50 nodes spread across 1000m X 1000m area with 2 to 10 malicious nodes. The packet size considered as 512 bytes, transmission range 250 m, initial battery 100 J, and simulation time 10 to 50 sec as shown in Table II.

TABLE II: SIMULATION PARAMETERS

Parameter	Value
Area	1000 m X 1000 m
Transmission Range	250m
Simulation Time	50 Sec
Nodes	50
Malicious Nodes	2 to 10
Packet Size	512 bytes
Initial Battery	100 J
TXPower	31.32e-3
RXPower	35.28e-3
Idle Power	712e-6
sleep Power	144e-9

V. RESULTS AND DISCUSSION

The results are compared with TBSEER [10] protocol, in which the sink node calculates comprehensive trust by considering direct trust, indirect trust and residual energy of the node. The protocol assumes sink node to have unlimited energy. The problem with TBSEER [10] protocol is that, the protocol requires lot of computations to be carried out at sink node and exchange of TVs among nodes incurs extra delay. The results are computed to check the PDR, EED, throughput, routing overhead, and energy consumption parameters with increase in simulation time.

The results in Table III,show an improvement of 4.86% in PDR and 6.66% in throughput with increase in simulation time. An improvement in PDR and throughput is achieved with the use of multiple paths simultaneously.

TABLE III. PDR AND THROUGHPUT COMPARISON OF COMPREHENSIVE TRUST BASED EELB-AOMDV AND TBSEER [10] PROTOCOL

Simulation Time (Sec)	**PDR**			**Throughput (KBPS)**		
	TBSEER [10]	***CTB Secure EELB-AOMDV***	***Percentage Increase (%)***	***TBSEER [10]***	***CTB Secure EELB-AOMDV***	***Percentage Increase (%)***
10	80.2	84.1	4.86	330	352	6.66
20	81.0	83.8	3.45	333	353	6.0
30	82.5	85.5	3.63	332	350	5.42
40	83.7	86.1	2.86	340	361	6.17
50	84.1	86.5	2.85	347	366	5.47

TABLE IV. EED AND ROUTING OVERHEAD COMPARISON OF CTB SECURE EELB- AOMDV AND TBSEER [10] PROTOCOL

Simulation Time(Sec)	**EED (msec)**			**Routing Overhead**		
	TBSEER [10]	***CTB Secure EELB-AOMDV***	***Percentage reduction (%)***	***TBSEER [10]***	***CTB Secure EELB-AOMDV***	***Percentage reduction (%)***
10	28.2	20.5	27.3	7.23	3.13	56.71
20	29.6	21.1	28.7	7.3	3.56	51.23
30	29.1	21.2	27.14	6.63	3.92	40.91
40	30.8	23.0	25.3	8.26	4.77	42.25
50	30.9	24.1	22.0	14.01	7.74	44.75

The results in Table IV show an improvement of 28.7% in EED by considering the queue length as a metric to avoid delays in queue and routing through the malicious nodes. The routing overhead is reduced upto 56.71% because the protocol finds multiple paths during the initial route discovery, reducing the process of re-initiating the route discovery upon link failure.

TABLE V. AVERAGE RESIDUAL ENERGY COMPARISON OF COMPREHENSIVE TRUST BASED EELB-AOMDV AND TBSEER [10] PROTOCOL

Simulation Time (msec)	**Average Residual Energy(J)**		
	TBSEER [10]	***CTB Secure EELB-AOMDV***	***Percentage Increase (%)***
10	93.35	99.91	7.03
20	93.9	99.84	6.33
30	94.44	99.77	5.64
40	94.61	99.56	5.24
50	94.78	99.34	4.81

Average residual energy of the protocol is increased by at most 7.03% with simulation time as 10 sec in Table V. The average residual energy of the protocol is improved because of the multiple paths, nodes are busy in transmission and dissipate less energy during idle states.

VI. CONCLUSION

Comprehensive Trust Based EELB-AOMDV protocol is presented in this paper to improve the EED and energy consumption of the Secure EELB-AOMDV protocol presented in [ ]. The protocol computed indirect TV by considering Direct Trust, Indirect Trust, Residual energy and Queue Occupancy of the node. The results are compared with TBSERR [10] protocol by increasing the simulation time from 10 sec to 50 sec. The results show that the protocol out performs TBSEER [10] in terms of PDR, throughput, EED, routing overhead and energy consumption.

ACKNOWLEDGMENT

The research work is carried out in the department of Computer Science & Engineering, Osmania University, Hyderabad, Telangana State, India and is funded by Visvesvarayya Scheme, Ministry of Electronics and Information Technology.

REFERENCES

[1] S. Mohammadi, R . E. Atani, and H. Jadidoleslamy, “A Comparison of Routing Attacks on Wireless Sensor Networks,” organization, vol. 4, p. 21, 2011.

[2] S. Om and M. Talib, “Wireless Ad-hoc Network Under Blackhole Attack,” International Journal of Digital Information and Wireless Communications (IJDIWC), vol. 1, no. 3, pp. 591–596, 2011.

[3] Prasanna, Srinivasa, and Srinivasa Rao. "An overview of wireless sensor networks applications and security”, International Journal of Soft Computing and Engineering Vol. 2, no. 2, pp. 2231-2307, 2012.

[4] Z. Zhang, G. Xu, P. Zhang, and Y. Wang, “Personalized Recommendation Algorithm for Social Networks Based on Comprehensive Trust,” Applied Intelligence, Springer, vol. 47, no. 3, pp. 659–669, 2017.

[5] Marchang, Ningrinla, and Raja Datta. "Light-weight trust-based routing protocol for mobile ad hoc networks", IET information security, Vol. 6., no. 2 , pp. 77-83, 2012.

[6] Ahmed, K. A. Bakar, M. I. Channa, K. Haseeb, and A. W. Khan, “TERP: A Trust and Energy Aware Routing Protocol for Wireless Sensor Network,” IEEE Sensors Journal, vol. 15, no. 12, pp. 6962–6972, 2015.

[7] Pradeska, Nurrahmat, Warsun Najib, and Sri Suning Kusumawardani. "Performance analysis of objective function MRHOF and OF0 in routing protocol RPL IPV6 over low power wireless personal area networks (6LoWPAN).", 8th International Conference on Information Technology and Electrical Engineering (ICITEE), 2016.

[8] A. Khalid, Q. Bai, and A. Al-Anbuky, “Adaptive Trust-based Routing Protocol for Large Scale WSNs,” IEEE Access, vol. 7, pp. 539- 549, 2019.

[9] M. Demmer and K. Fall, “DTLSR: Delay Tolerant Routing for Developing Regions,” in Proceedings of Networked Systems Developing Regions, pp. 1–6., 2007.

[10] Ishmanov, Farruh, and Yousaf Bin Zikria. "Trust mechanisms to secure routing in wireless sensor networks: Current state of the research and open research issues.", Journal of Sensors 2017.

[11] H. Hu, Y. Han, M. Yao, and X. Song, “Trust Based Secure and Energy Efficient Routing Protocol for Wireless Sensor Networks,” IEEE Access, vol. 10, pp. 10585–10596, 2021.

[12] Rani, B. Sandhya, and Kattula Shyamala. "Secure EELB-AOMDV Protocol to Mitigate Blackhole Attack." 9th IEEE International Conference on Advanced Computing and Communication Systems (ICACCS). Vol. 1., 2023.