INTERNATIONAL RESEARCH JOURNAL ON ADVANCED SCIENCE HUB
e-ISSN : 2582 - 4376
Open Access
RSP SCIENCE HUB
(The Hub of Research Ideas)
Available online at www.rspsciencehub.com

Special Issue of Second International Conference on Advancements in Research and Development (ICARD 2021)

A Trust Calculation Algorithm for Communicating Nodes in Wireless Sensor Networks

Jeelani[1], Kishan Pal Singh[2], Aasim Zafar[3],
[1]Department of Computer Application, IET, Mangalayatan University, Aligarh, India
[2]Department of Mechanical Engineering, IET, Mangalayatan University, Aligarh, India
[3]Department of Computer Science, Aligarh Muslim University, Aligarh, India
jeelani.0018@gmail.com,kishan.singh@mangalayatan.edu.in

Abstract

In various areas of the communication system, work based on Wireless Sensor Network (WSN) is being used these days. It is observed that trust-based model for WSN as a controlled secure, confidential and robustness with a consistent communication troubleshoots a lot of problems in delivering. This makes a node in WSN, that is, ready to deal with and act on attacks caused by additional nodes in different communication networks. This is a highly challenging task due to the lack of a trust resource and the dynamics that this network institute brings. In this paper, we propose Trust Calculation Algorithm for communicating nodes in WSN. Trust calculation algorithm provide the trust-based routing table for every node. It serves as an important role in the communication process for nodes from clusters, nodes from nodes and clusters from clusters in WSN.

Keywords: Wireless Sensor Networks (WSNs), Security, Trust calculation, Algorithm

1. Introduction

A Wireless Sensor Networks (WSNs) is a group of different tiny and autonomous sensor nodes. They gather of spatially distributed and committed sensors for observing and sensing the physical situations of the situation and establishing the organized evidence at an essential location. WSNs evaluate natural situations like temperature, sound, contamination levels, stickiness, humidity and wind, and so on. "Wireless sensor nodes have limited consumption power and less memory deployed in the environment to detect the measures and report back to the cluster head or base station. Because of the remote idea of the nodes, they are possible for different attacks". In this way, building up the trust structure which tends to the security, privacy, authentication, Strength, verification, and permission in the wireless sensor network is significant. Here, trust is the degree of declaration or assurance that an individual can take on someone else or an object. In a wireless network, the equivalent or grade of certainty that a node may take on another node is called trust. In this article, we present the characteristics of trust and also present the trust matrices in Wireless Sensor Network. Further, trust calculation has important parameter in WSN as packet delivery ratio, average throughput, and residual energy on the basis of algorithm. Researchers have also considered the Trust model with the help of its elements like security element, mobility element and reliability element. Furthermore, present the Trust calculation model with showing the sensor nodes and also direct trust

and indirect trust. In this trust model shows the direct, indirect trust and calculate the total trust with update trust value for Wireless Sensor Networks. Sensor nodes corelate with direct and indirect trust in the network. The most important thing in this article shows the how to calculate total trust with the help of trust algorithm. This algorithm main motive to calculate trust in the network due to some sub-trust for securing the network communication.

In WSN, the trust can be characterized as, "the joined attributes model for giving the security, dependability, protection concerning the versatility is called trust". Setting up the trust and evaluating the trust in WSN empowers the node to have stable, challenging communications based on their trust values with additional nodes or organisations. The issue of secure routing is solved by the trust value of the node in the enterprise, which offers a solid route for the package and the option of a protected mobility model.

For sensor nodes conveyed in abandoned and military environments, the trust value is important. The trust value evaluation is a prerequisite for the nodes in the network to have faith in transmission. Trust in network is more trouble when it is bigger. Fewer connections might be smarter to make one more dependent on its network and consequently more dependable. The trust is the level or level of sureness or conviction that a node can have on extra node. Trust the board in WSNs is utilized in evaluating the nature of the detected information, security to access control, verification, vulnerability, and malicious node identification. Trust advancement in the network has been recommended as an acceptable security technique for asset saved wireless sensor networks. Building up the trust commendable system for the wireless network makes the security more grounded, dependable, and more productive. Therefore, trust is a very useful for WSN.

1.1 Some Characteristics of Trust in WSNs

Some important characteristics given as follows.

- **Innovative:** It might increment else decrement through period dependent on fruitful and ineffective collaborations.
- **Intransitive:** If node *i* trusts node *j*, node *j*confides in node *k*. it isn't vital that node *i* trusts node *k*.
- **Asymmetric:** Two or more nodes do not have same trust key.
- **Trust is associated with risk:** If there is no danger involved, there is no motive to believe.
- **Auto catalysis:** There is nodes interactions references about further nodes.
- **Unqualified:** Node *i* does not rely on node *j* for any action, but it will rely on the specification.
- **Supportive:** The nodes organized in environments are supportive to each other by replacing data.

This paper organized in Section 2 present the related works which have done by other researchers, Section 3 proposed the element-based trust model for trust estimation and also define the figures and table related to this model. In Section 4 proposed the algorithm who calculate the trust and show the experimental work and finally conclude the paper in Section 5.

2. Literature Review

N. Aher[1], has introduced new approach for improving reliability of routing and data accumulation in Wireless Sensor Network. In WSN, trust is a significant issue in Wireless Sensor Network which resolves the problem of secure routing scheme, privacy, access control, and reliable communication. Data accumulation is method for eliminating redundancy and to minimize the number of packet broadcast. The ultimate objective of data accumulation stands to gather and accumulated data in a well-organized manner then that lifetime of the network increases by dropping the number of packets to be sent to the base station which reductions the communication costs and energy consumption. In this article, author has aggregation algorithm with two approaches have used over here, tree-based and cluster-based approaches. S. S. Babuet et al[2] have proposed a trust calculation dependent on highlights of node and neighbouring node's references for WSN. This presentation recognized the attacker and greedy nodes competently than the estimation mean-based strategies, and allowed genuine nodes in directing, accordingly killing malicious or narrow-minded nodes. The trust evaluation strategy was flexible and energy efficient, separating the responsible nodes and enabling them to commit to routing, while marking other nodes as malicious or egotistical.E.Thenmozhi and S. Audithan[3], have

focused on a distributed self-organizing trust based clustering framework for secure ad hoc networks. In WSN, improve security is very significant to measure the honesty of nodes deprived of conditional on central authorities. Researchers have use trust-based mechanism for reduce the compromised malicious nodes which is in cluster heads. Here, also experiment with network simulator-2 shown some parameters like quality of service, end-to-end delay and residual energy for performance of the trust-based mechanism. S. He and H. Zhao [4], have proposed field-based trust and possible routing protocol for Wireless Sensor Networks (WSNs). In this article, zeroed in on three principle segments including trust esteem, leftover energy and distance are thought of, and the node that is the ideal arrangement of cluster head choice role is the cluster head. WSNs can be crudely separated into two types: flat routing and hierarchical routing. Here, researchers have simulation with MATLAB for all the parameters which were given there. A. Miglani et al[5] have proposed a trust-based routing algorithm with energy-efficient routing in LEACH for wireless sensor networks. In WSN, secure routing is a very important concern in here. Here authors have improved in Low Energy-efficient Adaptive Clustering Hierarchy LEACH protocol with its functioning and performance. The simulation results demonstrated that for better performance, network lifetime, and energy consumption. [6]for WSN, a trust-based routing scheme in sensor networks has been suggested.If a high level of strength in node variety built on packet trust necessity with lifetime reflection. The protocol permits messages to be routed via malicious and defective devices with the range of trusted neighbours. Further, the network lifetime can also be extended by selecting those with their detecting functions covered by some current nodes. Jeelani et al [7] have discussed about various types of attacks and trust-based approaches to tackle these selective attacks on the wireless sensor network, including Sybil, Wormhole, Black-hole, Gray-hole, Hello flood, and Distributed Denial of Service attacks. The authors also presented direct and indirect trust and calculation of trust in your current article. X. Li et al [8] have proposed A trust step of node dependent on mindful routing protocol for WSN. To rise the energy adequacy of sensor nodes and affirm the rightness of numbers transmission dependent on an energy-aware protocol. In this article, the researchers have demonstrated highlights for network lifetime, packet loss rate, energy utilization is related with convention SIP, EAR to demonstrate the unwavering quality of TDAR. TDAR can allow minor end to end delay, recover the consistency of information transmission in networks, and spread the network lifetime intriguingly. W. Gong et al [9] have introduced a Trust-Based Routing for Misbehaviour Finding in Ad Hoc Networks. Each node assessed its individual trust route requirements about neighbours total checking neighbours' examples of traffic flow in the network. The researchers additionally incorporated the trust model into Dynamic Source Routing (DSR) and Ad-hoc On-Demand Distance Vector (AODV) that are the best particular steering conventions in MANET. Simulation results and parameters did with network simulator-2 (NS-2). N. Kumar et al [10] have proposed have proposed trust mindful routing protocol with assistance of energy productive algorithm for Wireless Sensor Network. This protocol includes of a 'trust metric and furthermore an exchange determination calculation'. The trust mindful measurement identified to the malicious nodes based on upkeep truthfulness, energy utilization and credit genuineness. S. Rajaram et al [11] caried out the study, a focused on indirect trust based mechanism in WSN. Researchers have created a model for trust calculation based on indirect, direct trust and calculate total trust for WSN. These trust-based approaches have widely used for counter internal attacks in the WSN. Basically, trust model consists routing protocols which is based on shortest route and search the trusty route between by compared the value of trust calculation. Afreen et al. [12] evaluated the performance of the following routing protocols. Ad hoc on demand routing protocol, dynamic routing protocol and dynamic MANET on demand routing protocol for ZigBee. ZigBee is the short wireless communication network. Simulation with QualNet (7.4) simulator and evaluate the network throughput, average n2n delay and jitter for the better performance. DSR performed better than AODV and DYMO routing protocols in the network. Daniel, A. D. and Roslin, S. E., [13-16] have proposed in WSN, developed a

trust-based data aggregation protocol that uses data validation and integrity verification. In WSN, validation of data and credibility is very important.Based on its trust features, the trust-based data aggregation protocol finds the valid data in the tree generated and evaluated for each node, and sensed data is encrypted with the help of a symmetric key. In this study, propped the technique improved the data correctness shown these comparison graphs. Dalal, K. [14] have compared the performance of routing protocols in WSN. Evaluated the performance of OLSR, DSR, DYMO and ZRP routing protocols with the simulation in QualNet. Compared the performance with parameters are average throughput, end-to-end delay, average jitter and total packet received. The DYMO gave the better results against OLSR, DSR and ZRP. Kumar et al. [15] in this survey, researchers have presented the various models and possible applied tries to trust and reputation models. These also used for the security purpose in wireless sensor network, in which found this study various attacks defined there. Most of the approaches used in this study as static environment. Wireless sensor networks have wide range of application, here described some for the better performance. Jeelani et al. [16] analyzed the distributed trust-based model in this study with the help of trust-based approaches for detection the malicious nodes with trusty nodes and attacks. The author also includes the direct and indirect trust in this article and found the result.

3. Element Based Trust Model

Trust Based Model depends on some attributes which as security element, mobility element and reliability element for nodes in fig. 1. In a trust-based architecture, a node's security model involves the use of a protected course discovery technique as well as encryption in guiding. The faith evaluation in this protection model is clear after using additional encryption methodology from the safe course discovering scheme. In any case trust estimation of a node popular secure model is nothing. In WSN, a mobility model to node popular the trust-based structure includes utilization of a made sure about mobility model for the node. They made sure about the mobility model also the base energy utilization throughout the mobility guarantees the from top to bottom trust an incentive with in mobility model to the node. Something else, a trust estimation to the node common the mobility model as nothing. A trust an incentive in the consistency of a node stands grow before it utilizes to data combination of packets through a smaller amount energy utilization. In this model, the reliability element uses in trust aimed at reliable communication in the wireless network location.

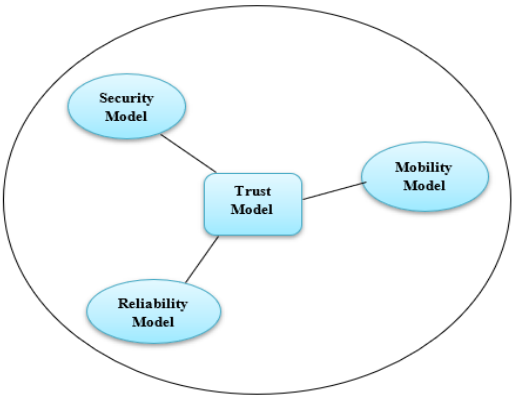

Fig. 1: Element based trust Model

3.1 Trust calculation model

In Wireless Sensor Networks, trust is very useful for communication. When we communicate one node to more nodes than the attacker node attack to communicating node. Trust calculation models have direct, indirect trust, and calculate overall trust with updated trust value, shown in fig. 2 [11].

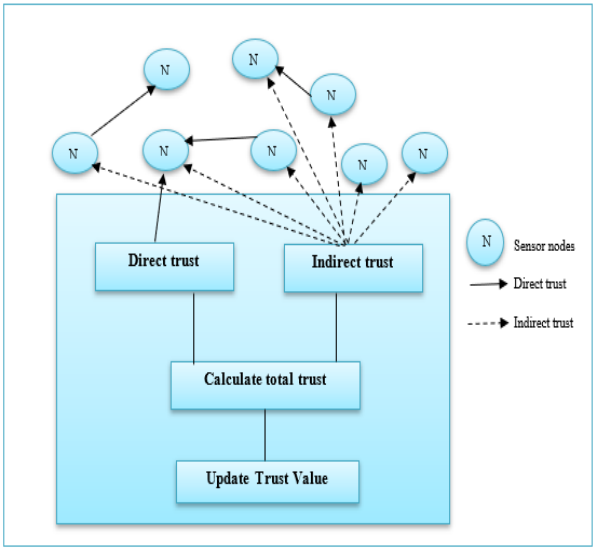

Fig. 2: Trust calculation model

Direct Trust: A Direct trust is dependent on the node's own perception in indiscriminate mode. A node can communicate with other node directly in the wireless network and gets all traffic inside its radio reach despite the fact that it isn't routed to it. Every node in the network notices neighbours

utilizing a trust system that consumes battery power. Sensor nodes depends on the battery as power consumption, if sensor nodes have power then it communicates or survive in the network.

Indirect Trust: An Indirect trust depends on the other node or recommender for communication in the wireless network. Indirect trust communicates to node to another node via any recommender nodes in the wireless network. In this Trust model shows the indirect trust how to communicate with deployed sensor nodes and these are in distributed way in the network. Indirect sensor nodes also have battery or power consumption for communication in wireless network.

Trust calculation: Calculation trust of sensor nodes resolved constructed on direct trust, indirect trust and sensor node. Trust will be revived after a time span and is connected with all trust which is resolved subject to the legitimate data of individual node without seeing some network components, for instance, node flexibility, trust spoil as time goes on, and some malevolent attacks [7].

$Trust\ calculation = W_1\ T_{ini} + W_2\ T_s + W_3\ T_{mob} + W_4\ T_r$

where, T_{ini} = initial trust, T_s = secure trust model, T_{mob}= mobility trust model, T_{rel} = reliability trust, W_1, W_2, W_3 *and* W_4 are the weight related to direct trust, reliability trust in addition indirect trust correspondingly for example $W_1 + W_2 + W_3 + W_4 = 1$, and each weight varies from 0 to l dependent on subject node and object node are one hops neighbor or multi-hops neighbor.

3.2 Trust matrices in WSNs

Here, we use some trust matrices for Wireless Sensor Network given in the below table 1[2]**.**

Table.1. Trust matrices

Trust Matrices	Explanation
Packet forwarding	Transmission of packets from one node to other network nodes
Packet or message accuracy	Nodes deployed in random way so packet accuracy will not 100% in the network
Communication Accuracy	When node work with tcp Protocol in network then communication will accurate
Accessibility	Accessibility based on behaviour of malicious activities
Protocol performance	Protocol performance provides a new way of understanding networks
Communication Coding	Coding is a method of protecting data and communications through the use of codes
Memory utilization	The wireless networks have a limited memory so memory utilization decrease performance for the related processes
Detection communication	Detection is a typical process from the modify of network monitoring and network traffic
Modify to address of packets	Network can modify the address of node with the help of routing protocol
Packet delivery ratio	PDR of the no. of packages obtained from the source node to the destination node
Energy consumption	Energy consumption can measure the energy on nodes in network which have consumes
Average throughput	The average throughput is determined by dividing the total consignment for the entire session by the total time.

3.3 Possible Trust Values

Here, trust values are given below table 2.

Table.2. Trust value estimation

Trust Stands	Tittle	Behaviour of Trust
1	Excessive Trust	Trust
1 to 0.75	High Trust	Trust
0.75 to 0.50	Middle Trust	Trust
0.50 to 0.25	Short Trust	Unsafe
0.25 to 0	weak Trust	Unsafe
0 to -0.25	Short Distrust	Threat
-0.25 to -0.50	Middle Distrust	Threat
-0.50 to -0.75	High Distrust	Threat
-0.75 to -1	Same Distrust	Threat

4. Algorithm for Trust Calculation of Node

Input: Node from source to destination with trust.

Output: Trust utility (value) calculation and communication (com).

a. $T_{ini} = (1+0) / (T_i+1)$ or P_r
b. If (T_{ini}= = com)
   Then permit for communication.
c. Else
   $T_s=A+E+R$
d. If (T_s = = com)
   Then permit for communication.
e. Else
   trust value calculates in secure trust model.
f. If (node = = ***fixed***)
   The assume trust value of node as 0.
g. Else
   trust value calculates in mobility trust model.
   $T_{mob} =M_{eva}+ E_{mob}$
h. If (T_{mob} = = com)
   Then permit for communication.
i. Else
   $T_{rel} = D_c + E_{dc}$;
j. If (T_{rel} = = com)
   Then permit for communication
k. Else
   Calculation of total trust for node.
   total trust = $W_1\ T_{ini} + W_2\ T_s + W_3\ T_{mob} + W_4\ T_{rel}$
   If (***total trust*** = = com)
   Then permit for communication with nodes.
l. Else
   Communication is not permitted.

4.1 Abbreviation List

Table.3. Abbreviation

Abbreviation	Definition
WSNs	Wireless Sensor Networks
T_{ini}	Initial Trust
T_s	Secure Trust
T_{mob}	Mobility Trust
T_{rel}	Reliability Trust
com	Communication
T_i	Total connections
P_r	Peer recommendations
A	Access control
E	Encoding packets
R	Routing
M_{eva}	Mobility evaluation
E_{mob}	Energy utilization via the mobility trust
D_c	Data combination
E_{dc}	Energy utilization throughout data combination
1	Successful condition
0	Unsuccessful condition

4.2 Experimental Results

In this section, to analyze the trust with the help of trust calculation algorithm, The NS-2 simulator was used. The primary trust cost of nodes are usual to 0.5 in all situations, indicating the initial common trust value. The collected results were calculated using. A network with 10 nodes that were randomly placed in a grid of 800 x 800 m2 was used for this purpose. Show the experimental results of our research article for trust with the help of trust calculation algorithm.

Table.4. Simulation parameters

Simulation Parameters	Values
Simulator version	NS-2.35
Routing Protocol	TAODV(Trust AODV)
Network channel	Channel/Wireless
Queue type	DropTail
Network interface type	Phy/Wireless
MAC layer protocol	Mac/802_11
Antenna model	Antenna/OmniAntenna
Number of nodes	10
Battery Type	Energy model
Initial energy	100 joules
Simulation Area	800m X 800m
Transport layer	UDP
Type of traffic	CBR
Packet size	500
Initial trust value	0.5
Random-way point	Mobility Model

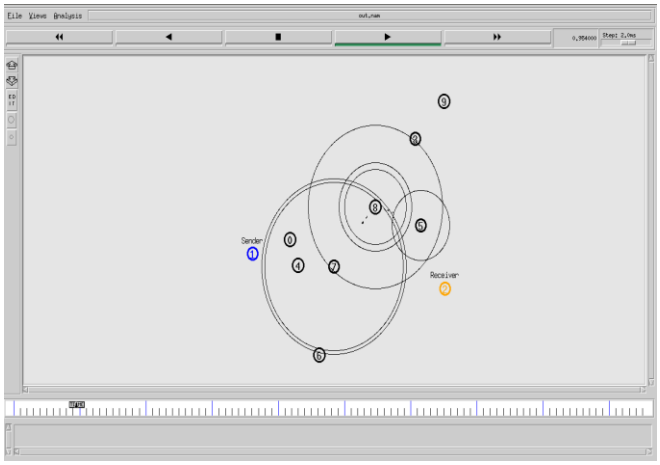

Fig.3. Simulation screenshot

In this simulation, deployed ten nodes with random waypoint, node 1 as a sender and node 2 as receiver. These are communication to each other with the help of neighboring nodes and create the routing table for trust calculation in the network. Every node maintains the trust routing table for the trust foundation which has based on threshold values in the wireless network. Routing table maintain the neighbor details and activities all node maintains each table see fig. 4.

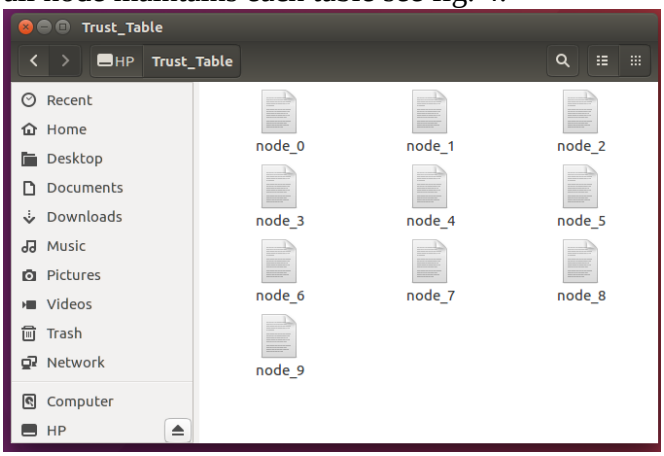

Fig.4. Trust table for node 0-9

In this figure, researchers shown the trust table folder which has get from run the simulation. In this experiment, using the trust-based routing as TAODV which modified and use the UDP agent with CBR traffic in this scenario. In addition, node 0 to node 9 these are maintaining the routing table with threshold values.

Table 5: Trust routing table

Node ID	
Energy	
Neighbor ID	Trust Value

The method for sending this communication is that the node increases its sequence number as a single unit and stores it in the sequence number field. The destination-related data is then imported into the current fields. It also stores the source address field's ID and records the time when a message is created in a related field. For all nodes in the network, the trust-based routing table keeps track of their node ID, energy label neighbor ID, and most significant trust value.

Conclusions

Wireless Sensor Network (WSN) becoming more popular in the current time due to its wide range of applications. This work presented trust among nodes with the help of a trust calculation algorithm for communicating nodes in WSN. We have used the trust calculation to tackle malicious attacks in a real-time environment. This trust model can sense the malicious node with the help of a trust calculation algorithm. Further, provide the trust-based routing table which is used to find the trusty nodes in the network. On the basis of this article, we can create a more secure trust model with routing protocols for the Wireless Sensor Network in the future.

References

[1]. C. N. Aher, "Trust Calculation for Improving Reliability of Routing and Data Aggregation in WSN," *Int. Jourrnal Electron. Eng.*, pp. 386–392, 2019.

[2]. S. S. Babu, A. Raha, and M. K. Naskar, "Trust Evaluation Based on Node's Characteristics and Neighbouring Nodes' Recommendations for WSN," *Wirel. Sens. Netw.*, vol. 06, no. 08, pp. 157–172, 2014, doi: 10.4236/wsn.2014.68016.

[3]. E. Thenmozhi and S. Audithan, "Trust based cluster and secure routing scheme for wireless sensor network," *2nd Int. Conf. Curr. Trends Eng. Technol. ICCTET 2014*, pp. 489–494, 2014, doi: 10.1109/ICCTET.2014.6966345.

[4]. S. He and H. Zhao, "Trust and potential field-based routing protocol for wireless sensor networks," *2015 IEEE Int. Conf. Signal Process. Commun. Comput. ICSPCC 2015*, 2015, doi: 10.1109/ICSPCC.2015.7338813.

[5]. A. Miglani, T. Bhatia, and S. Goel, "TRUST based energy efficient routing in LEACH for wireless sensor network," *Glob. Conf. Commun. Technol. GCCT 2015*, no. Gcct, pp. 361–365, 2015, doi: 10.1109/GCCT.2015.7342684.

[6]. K. S. Hung, K. S. Lui, and Y. K. Kwok, "A trust-based geographical routing scheme in sensor networks," *IEEE Wirel. Commun. Netw. Conf. WCNC*, pp. 3123–3127, 2007, doi: 10.1109/WCNC.2007.577.

[7]. Jeelani, M. Rana, S. Kumar, and A. Zafar, "Trust Based Approaches to Counter Selective Attacks on Wireless Sensor Networks," *Int. J. Comput. Sci. Mob. Comput.*, vol. 7, no. 12, pp. 291–303, 2018.

[8]. X. Li, J. Li, C. Sun, B. Liu, and X. Hao, "A trust degree of node based on aware routing protocol for wireless sensor network," *CSAE*

2012 - Proceedings, 2012 IEEE Int. Conf. Comput. Sci. Autom. Eng., vol. 2, no. 1, pp. 98–101, 2012, doi: 10.1109/CSAE.2012.6272736.

[9].W. Gong, Z. You, D. Chen, X. Zhao, M. Gu, and K. Y. Lam, "Trust based routing for misbehavior detection in Ad hoc networks," *J. Networks*, vol. 5, no. 5, pp. 551–558, 2010, doi: 10.4304/jnw.5.5.551-558.

[10].N. Kumar, Y. Singh, and P. K. Singh, "An energy efficient trust aware opportunistic routing protocol for wireless sensor network," *Int. J. Inf. Syst. Model. Des.*, vol. 8, no. 2, pp. 30–44, 2017, doi: 10.4018/IJISMD.2017040102.

[11].S. Rajaram, A. B. Karuppiah, and K. V. Kumar, "Secure Routing Path Using Trust Values for Wireless Sensor Networks," Int. J. Cryptogr. Inf. Secur., vol. 4, no. 2, pp. 27–36, 2014, doi: 10.5121/ijcis.2014.4203.

[12].G. Afreen, C. E. Mohan, C. H. Pooja and F. T. Pooja, "Wireless Network Simulation and Analysis using Qualnet", IEEE 2nd International Conference on Communication and Electronics Systems (ICCES), pp. 251-255, 2017.

[13].A. D. Daniel and S. E. Roslin, "Data validation and integrity verification for trust-based data aggregation protocol in WSN", Microprocessors and Microsystems 80, 2021.

[14].S. Pahal, and K. Dalal, "Performance Evaluation of Routing Protocols in WSN using QualNet 5.3", International Journal of Recent Trends in Engineering & Research (IJRTER), (2016), Vol. 02, Issue 06, pp. 223-231.

[15].G. E. P. Kumar, I. Titus, and S. I. Thekkekara, "A Comprihensive Overview on Application of Trust and Reputation in Wireless Sensor Network", International Conference on Modling and Optimisation and Computing, Procedia Engineering 38, pp. 2903 – 2912, 2012.

[16].Jeelani, M. Rana, S. Kumar, and A. Zafar, "A Distributed Trust Based Approach for Wireless Sensor Networks", International Journal of Research and Analytical Reviews (IJRAR), Vol. 6, Issue 2, 2019, pp. 842-850.