RESOURCEFUL DECENTRALIZED INTELLECTUAL ROUTING PROTOCOL FOR WIRELESS SENSOR NETWORKS

Dr. C. Sharanya[1], Abhinav Singhal[2], S.Balaji[3], Dr. Prakash Chandra Behera[4], Gaurav D Saxena[5], Dr. Chinmaya Dash[6]

[1]Assistant Professor, Department of Electronics and Communication Engineering, Vels Institute of Science, Technology and Advanced Studies, Chennai-600117, Tamilnadu India.

[2]Assistant Professor, School of Sciences, Christ (Deemed to be University) Delhi NCR, Ghaziabad-201003, Uttar Pradesh, India.

[3]Assistant professor, Department of Computer Science and Engineering, Akshaya College of Engineering and Technology, Kinathukaduvu, Coimbatore -642108

[4]Assistant Professor, Department of Sciences, St.Claret College, Bangalore, India

[5]PG Student, Department of Computer Science, Kamla Nehru Mahavidyalaya, Nagpur, Maharastra-440024, India

[6]Assistant Professor, Department of Computer Science, St.Claret College, Bangalore, India

Sharanya0608@gmail.com1,ism.abhinav@gmail.com2,bbaallaajjii@gmail.com3,prakash@claretcollege.edu.in4,gauravsaxena711@gmail.com5, Chinmaya@claretcollege.edu.in6

Abstract— Wireless sensor network (WSN) have wide applications due to sensor nodes ease of deployment. But wireless sensor network are also highly vulnerable to attacks due to the nature of the wireless media and restricted resource. Sensor nodes are resource constraint devices and are thus vulnerable to a variety of attacks, which can compromise the security of an entire wireless sensor network. A generic wireless sensor network model has been created in network simulator and necessary changes have been done in the code library to simulate the attacks. Sensor measures like throughput, packets dropped, end to end delay have been recorded and the analysis has been carried out to understand the impact of these attacks. A trust sensing based secure routing mechanism with the lightweight properties and the ability to resist many common attacks simultaneously is developed in an effort to address the serious effects of typical network attacks on data transmission that are brought on by the limited energy and the poor deployment environment of wireless sensor networks. At the same time, the security route selection algorithm is also optimized by taking the trust degree and Quality of Service metrics into account. The performance analysis and simulation results show that trust sensing based secure routing mechanism can improve the security and effectiveness of wireless sensor network.

Keywords—Wireless sensor network, Network Stimulator, Network Algorithm.

I. INTRODUCTION

A WSN is a self configuring network of small sensor nodes communicating among themselves using radio signals. WSN provides a bridge between the real physical and virtual worlds. Ubiquitous sensor based devices have been playing a vital role in the evolution of the IOT. The energy issue of sensor terminals poses significant challenges to the widespread use of IOT. Algorithms are usually directed against soft malicious or selfish behavior attacks. It mainly

Submitted: 21/10/2022 **Accepted**: 24/11/2022

relies on encryption algorithms and authentication mechanisms. Routing Protocol based trust are not suitable for the multi hop distributed and energy constrained WSN. Wireless sensor networks are an important type of network for sensing the environment and collecting information. In order to sense environmental parameters, a large number of sensor nodes, such as sink nodes and sensor nodes, are deployed in distributed areas. These nodes form a multihop adhoc network system and execute assigned tasks according to the application requirements. WSN have been deployed in homes, buildings, forests, mountains, etc. The sensor network topology describes the wireless communications among the various sensor nodes in WSN and is the basis for the design of various network communication protocols and routing protocols, which play a vital role in network properties such as network lifetime, energy consumption, reliability and data latency. Black hole attack, one of the riskiest security attacks in WSNs. Here, the black hole attacker serves as the node that is closest to the target node in order to draw traffic. The attacker gathers all the data packets sent by the other nodes and discards them all without sending them to their intended destinations..

In the beginning, a node multicasts the Route Request (RREQ) packet whenever it wishes to deliver data packets to other nodes in the network. The neighbor node will determine whether it is the target node or not when it gets the RREQ packet. A Routing Response (RREP) packet is sent to the source node if the sending node is itself the target node. If not, it keeps sending the RREQ packet to identify the intended node. The source node will deliver the data packet right away after receiving the RREP packets.

. All nodes are often given equal roles or functionalities in flat-based routing. But nodes in a network that uses hierarchical based routing will have various functions. When routing data in a network, location-based routing makes use of the positions of sensor nodes. When specific system variables may be changed to adjust the system to the present network and energy conditions, the routing protocol is said to be adaptive. According to how they operate, these protocols can also be divided into multi-path, query, negotiation, and QoS-based routing strategies.

A routing protocol created for wireless sensor networks is called Stable Ad-Hoc On-Demand Distance Vector (AODV). This protocol supports both uncast and multicast routing and creates routes to destinations as needed. As a result of the usage of preconfigured keys or the knowledge that no hostile invader nodes exist, AODV is intended for use in networks where the nodes may trust one another. In order to increase scalability and performance, AODV has been created to limit the spread of control traffic and eliminate overhead on data traffic. Based on the node's direct and indirect trust, the node's trust is calculated. Based on the number of packets that are forwarded, received, and dropped, the direct trust is evaluated. The feedback is sent to the source node by the source node. A trustworthy route is used to transport data packets to their destination. The data packet is sent to the node's higher node if it is unable to locate the trusted next hop node. The top node then chooses a different node for transmission. If the data packet is received by the sink, the sink notifies the source node of the feedback.

II. LITERATURE SURVEY

Gururaj and Swathi. [1] The topic of sensor node assaults was covered. Wireless sensor networks have become increasingly important in recent years due to their cost-effectiveness, resilience to node and communication failure, ability to withstand harsh environmental conditions, mobility, and usability. Sensors are one of the many emerging trends in the field of networks. WSNs have several uses, including in the management of home applications, environmental monitoring, military, and battlefield awareness.

Real-time information processing and collection are performed by WSNs. These networks typically operate in dangerous and distant environments. As a result, they are susceptible to several security vulnerabilities that have a negative impact on performance. The sensor network's data needs to be secure from numerous threats. Attackers may use a variety of security risks, leaving the WSN system unstable and open to attack. Network layer attacks are thoroughly analyzed. Based on the vulnerability, kind of attacks, and security services, a comparison of attacks is made.

Yanli et al. [2] it is crucial to examine how to withstand attacks with a trust scheme because the trust issue in wireless sensor networks is becoming one of the key components of security schemes. These study categories numerous attacks types and defaces pertaining to trust models in WSNs. The creation of trust mechanisms should also be included, along with a brief summary of traditional trust methodology and an emphasis on the difficulties facing trust schemes in WSNs. By compiling the most recent trust techniques into two categories safe routing and secure data a comprehensive architecture is presented. An open field and future direction with trust mechanisms in WSNs is offered based on the analysis of attacks and the available research.

Danyang Qin et al. [3] presented a lightweight design and the simultaneous resistance to numerous common attacks. Trust level and QoS measurements are also used to optimize the security route selection process. The effectiveness and security of WSN can be increased thanks to TSSRM, according to performance study and simulation results. Since the WSN is a crucial component of contemporary communication networks and the trust sensing routing protocol for WSN is an efficient means of enhancing security, research into this protocol is crucial. In order to counteract common network assaults, this research provides a trust sensing-based secure routing technique. In comparison to the conventional trust method, it also increases the reliability of data transfer.

Deug Julia and Weisong Shi. [4] In order to protect multi hop routing in dynamic WSNs against malicious attackers, a comprehensive trust aware routing architecture for WSNs was discussed. A node can track the trustworthiness of its neighbors using trust management in TARF, which focuses on trustworthiness and energy efficiency. As a result, the node chooses a trustworthy route. By replaying routing information, the system successfully defends WSNs from serious threats. Through thorough modeling and actual testing with massive WSNs, the TARF's resilience and scalability are demonstrated. These disposable sensors can be networked in numerous applications that demand unattended operations and a large number of them.

These sensors have the capacity to communicate directly with an outside base station or among them. A greater number of sensors enable accurate detection over bigger geographic areas.

Maarouf et al. [5] trust-aware routing in wireless sensor networks is shown. Researchers have focused their attention on this issue because it is so important. The very confined nature of a WSN and its ease of exposure to unstable situations directly motivate the need to address this issue. In order to provide trust-aware routing, reputation-based solutions are used. This method, however, necessitates that a node constantly scan its surroundings for instances of inappropriate behavior. The disadvantage is that it is thought to be an expensive process for WSN nodes due to its limited resource availability. The implementation of a novel monitoring technique known as an efficient monitoring method in a reputation system has been presented as a trust-aware routing solution based on reputation systems (EMPIRE). EMPIRE is a probabilistic, distributed monitoring system that aims to cut down on monitoring tasks per node while yet having a high level of attack detection. To evaluate and investigate the effectiveness of our suggested technique, new assessment methodologies are presented. Reducing EMPIRE monitoring activity does not significantly affect system security performance, according to simulation results of the reputation system.

Marlon et al. [6] explored was the use of wireless sensor networks for system monitoring. They can be either active or passive systems. The implementation of an active hybrid monitor with minimal intrusion is discussed in this study. It is built on adding a monitor node to the sensor node, which can receive monitoring data supplied by a piece of software running in the sensor node through a standard interface. The monitor's impact on time, code, and energy consumption in the sensor nodes is assessed in relation to the magnitude of the data and the interface being utilized. Then, several serial peripheral interfaces and serial transmission interfaces, which are frequently found in sensor nodes, are assessed. The suggested hybrid monitor offers incredibly precise data regarding WSN behaviour that is seldom impacted by the measuring tool.

Mashboob Abdul Karim et al. [7] addressed the growing use of wireless sensor networks in security-sensitive applications. They are vulnerable to several security threats due to their inherent resource limitations, and a black hole attack is one sort of assault that has a significant impact on data collection. The most significant advancement of active trust is that it eliminates black holes by actively creating a number of detection pathways to swiftly identify and establish nodal trust, hence enhancing the security of the data route. More significantly, the active trust scheme provides for the development and distribution of detection routes and is capable of making full use of the energy in non-hotspot areas to build as many detection routes as are required to meet the necessary security and energy efficiency. Energy Because of its modest complexity, it can be simply implemented in real-world WSNs.

Mohammad and Gadadhar. [8] The use of compressive sensing to reduce resource consumption and reduce battery and bandwidth utilization was discussed as a result of the knowledge of the energy that could be harvested. It also emphasizes ways to counteract aggression and bad behavior. The suggested neighborhood compressive sensing paradigm compresses local sparse data, including updates to the routing table, advertisements, and trust information. Because the leader node handles the bulk of the computations, it minimizes resource use. Because compressive sensing minimizes the quantity of data being transmitted across the network, it results in a decrease in resource consumption. A set of sparse data can be compressed and sent to the leader node in the area of ad-hoc networks. In order to recover the actual data, the leader node projects it, which lowers the quantity of data being transmitted throughout the network. The local nodes only make use of leader node ads. Because incorrect ads are not taken into account, the suggested model shields networks from several attacks.

Xiaoyong et al. [9] a trust mechanism was discussed as one of the most important needs for any wireless sensor network. The large overhead and low dependability of the present trust systems created for WSNs, however, prevent them from meeting these needs. This work develops a compact and reliable trust framework for WSNs that use clustering methods. First, an energy-efficient lightweight trust decision-making method based on the identities of the nodes in clustered WSNs is suggested. This scheme is appropriate for such WSNs since it promotes energy conservation. As a result of cluster members' feedback being cancelled (CMs). More significantly, a dependability enhanced trust assessing approach is proposed for collaborations between CHs, taking into account the significant amounts of data forwarding and communication responsibilities that CHs undertake. While using this method, flawed, selfish, and malevolent CHs can efficiently cut networking utilization. This solution overcomes the drawbacks of conventional weighing approaches for trust factors, which allocate weights in an arbitrary manner. According to theory and simulation studies, LDTS requires less memory and communication overhead than the standard trust systems for WSNs now in use.

Zheng Liu et al. [10] The energy balanced backpressure routing algorithm for lossless networks and the improved energy balanced backpressure routing algorithm for time-varying wireless networks with loss links were studied. Both the energy balanced backpressure routing method and the enhanced energy balanced backpressure routing algorithm are distributed, queuing stable, and don't need to know the details of the energy harvesting statistics to work. The simulation results demonstrate that our proposed algorithms can outperform existing schemes in terms of energy balance by a wide margin. Energy balance among nodes is an issue posed by energy harvesting technologies, despite the fact that they supply nodes with a lot of extra energy. Node with slower energy replenishment cycles likely to exhaust their energy sooner.

III. PROPOSED SYSTEM METHODOLOGY

This architecture as shown in Figure 1 illustrates the overall process of a safe routing system based on trust sensing for wireless sensor networks. Based on the node's direct and indirect trust, the node's trust is calculated. Based on the number of packets that are forwarded, received, and dropped, the direct trust is evaluated. The neighbors of a node estimate the indirect trust of that node, and this estimation is based on the node's forwarding behavior. The feedback is sent to the source node by the source node. A trustworthy route is used to transport data packets to their destination. The data packet is sent to the node's higher node if it is unable to locate the trusted next hop node. The top node then chooses a different node for transmission. The sink transmits the feedback to the source node if the data packet reaches it.

When a node receives a data packet, Stable AODV routing chooses one node from a list of candidates closer to the sink whose trust is greater than the predetermined threshold as the next hop. The upper node will recalculate the unselected node set and choose the node with the largest trust as the next hop if the node cannot discover any such suitable next hop nodes. Likewise, if the node cannot find any such suitable next hop, it sends a feedback failure to its upper node is shown in below figure 1. Due to the communication, processing, and delay limitations of wireless sensor networks (WSNs), conventional security measures cannot be applied. Wireless sensor networks are subject to a variety of security risks. Recently, models of trust management have been proposed as an efficient security measure for WSNs. The modeling and management of trust have been extensively studied

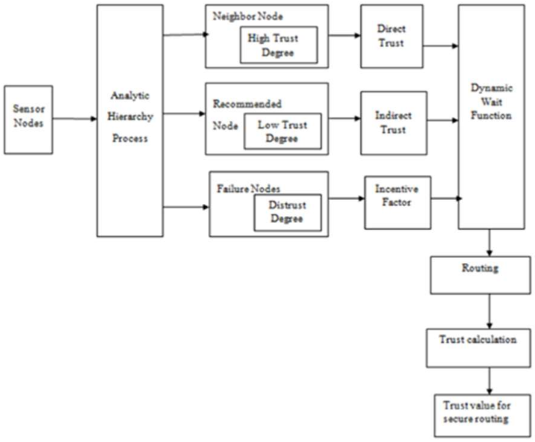


Fig.1: Trust based Routing Mechanism in WSN

. They are safe routing, secure data aggregation, secure localization, and secure node selection. They also include the detection of harmful attacks. In addition, several harmful assaults on trust models are categorized, and it is determined whether or not the current trust models can withstand these attacks. Last but not least, based on all the research and comparisons, mention a few trust best practices that are crucial for creating a strong trust model for WSNs..

Sensor Nodes in Wireless Sensor Networks

Sensor nodes make up wireless sensor networks, and they all use wireless to communicate with one another. Any particular node uses a sensor to gather information from its surroundings and transmits it to another node, which then transmits it to a third node and so on until it reaches the gateway node. The gateway node serves as the conduit between the nodes and the server, which stores and subsequently processes all of the information gathered from each node. Sensor nodes that can sense or modify physical parameters to interact with their surroundings, these nodes must cooperate in order to do their responsibilities because, in most cases, a single node is unable to do so. They use wireless communication to make this cooperation possible. A sensor is a tiny device with short-range communications, low-power compute, low-power signal processing, and micro sensor technology. Typically, sensor nodes consist of five fundamental parts such as the sensor unit, memory, transceiver, power supply and microcontroller [11-26].

Analytical Hierarchy Process in WSN

Energy-constrained nodes make up wireless sensor networks. Due to this restriction, energy-conscious protocols are very necessary in order to create an effective network. The next hop relay node selection uses the analytical hierarchy process (AHP) and takes into account the distance to the target location, remaining battery capacity, and queue size of potential sensor nodes within the local communication range. In comparison to the original geographical routing strategy, which just took into account distance to the destination location, simulation results demonstrate that this scheme can extend the network lifetime farther. Since the buffer capacity is taken into account, the suggested approach can also lower the packet loss rate and link failure rate.

Routing Protocol and Sensor Nodes

Routing in wireless sensor networks differs in a number of ways from traditional routing in fixed networks. No infrastructure exists, wireless connections are unstable, sensor nodes could malfunction, and routing methods must adhere to tight energy-saving guidelines. In general, many routing methods were created for wireless networks. The secure routing protocol and packet encryption used for routing are part of the node's security model in the trust framework[2-16]. When a security model employs a secure routing protocol and encryption, there is a high value placed on that model's ability to be trusted. If not, the node's trust value in the security model is 0. The trust framework's node mobility model makes use of a node-specific secured mobility model.

Trust based Routing by using Stable AODV

Figure 2 describes in Stable AODV, to strengthen network security and shield the nodes from vulnerabilities, a paradigm for managing trust vectors that assesses a node's trustworthiness. Based on their past behavior, a node's trust value is determined. Weighted forwarding ratio, similarity, and time ageing are some of the variables taken into account while determining a node's trust value. The weights given to the packets according to their significance range from 0 to 1[16-28]. Using Pearson Correlation, the similarity between two nodes is determined. For calculating the node's trust value, the weighted average of these variables is used. The route that yields the highest trust rating in the trust vector is the most reliable one from node I to node k. In a trust vector, the maximal product value of all directed edges along a path can be used to calculate the most reliable path. The path created using this method yields a path with trusted nodes as well as fewer hops.

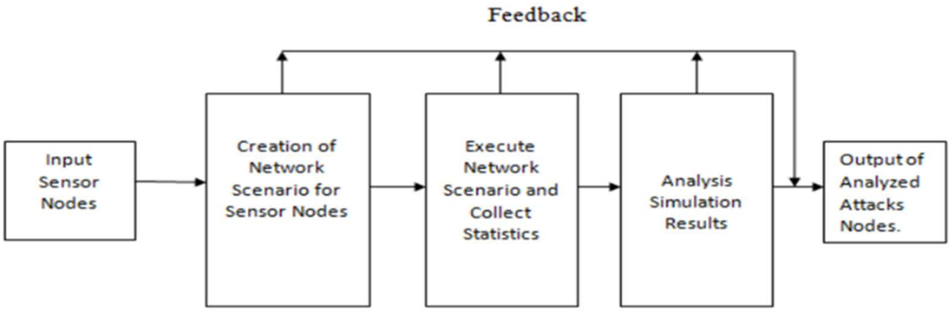

Feedback
Input Sensor Nodes
Creation of Network Scenario for Sensor Nodes
Execute Network Scenario and Collect Statistics
Analysis Simulation Results
Output of Analyzed Attacks Nodes.

Fig.2: Detailed Architecture for Attacks Analysis in WSN

MODULE DESRIPTION

Analyses a few common network attacks in WSN. Provides support for the security claims of WSN by extracting sensor node characters. Two basic attacks namely black hole attack and DoS by hello flooding attack. (1)Analysis of network attacks in WSN (2) Routing process in WSN (3)Trust calculation process in WSN.

Analysis of Network Attacks in WSN

Analyses numerous common network threats in WSN and draws conclusions from them to validate the security claims of WSN. One of the risky security attacks in WSNs is the black hole attack. In this case, the black hole attacker poses as the target node or acts as the closest path to the destination node to draw traffic. The attacker gathers all the data packets sent by the other nodes and discards them all without sending them to their intended destinations. Initially, a node multicasts the route request packet when it needs to send a data packet to another node in the network.

When a neighbor node receives an RREQ packet, it determines whether or not it is the target node first. A routing response (RREP) packet is sent to the source node if the sending node is itself the target node. If not, it keeps sending the RREQ packet to identify the intended node. The source node will deliver the data packet right away after receiving the RREP packets.

A single black hole attack or a group of black holes working together can both be used to achieve black hole attack. In a single black hole attack, the malicious node responds to the RREQ packet delivered by the source node and believes it is the fastest way to get there. Malicious nodes work together in a cooperate black hole attack to entice the average person into their manufactured routing information.

Routing Process in WSN

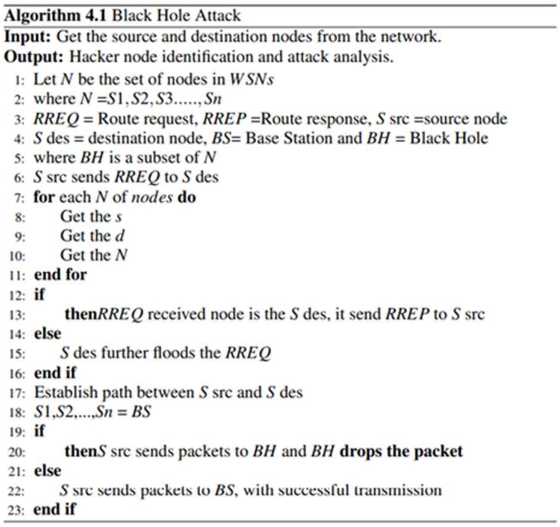
In order to decrease the network's routing overhead, a novel routing algorithm is implemented. AHP is a method for making decisions that breaks down factors that are always relevant to decision-making into objectives, criteria, and schemes before performing qualitative and quantitative analysis.

Trust Calculation in WSN

The trust model between two nodes serves as the foundation for the trust calculation model of the entire multi hop route. It also includes the direct trust degree, indirect trust degree, and incentive factor to evaluate the secure route of data transmission. The behavior and energy are utilized to evaluate the nodes' trustworthiness in detail.

BLACK HOLE ATTACK

Broadcasting is a typical networking element used in WSN to address security or any other problem. A rogue node will absorb all network traffic directed at it during a black hole attack and then reject every packet.

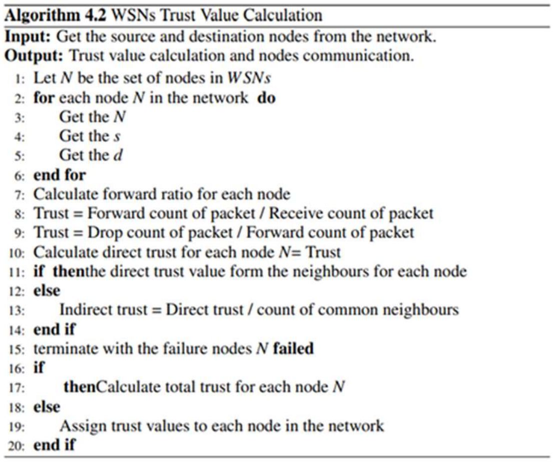


```
Algorithm 4.1 Black Hole Attack
Input: Get the source and destination nodes from the network.
Output: Hacker node identification and attack analysis.
Let N be the set of nodes in WSNs
where N =S1,S2,S3.....,Sn
RREQ = Route request, RREP =Route response, S src =source node
S des = destination node, BS= Base Station and BH = Black Hole
where BH is a subset of N
S src sends RREQ to S des
for each N of nodes do
    Get the s
    Get the d
    Get the N
end for
if
     thenRREQ received node is the S des, it send RREP to S src
else
    S des further floods the RREQ
end if
Establish path between S src and S des
S1,S2,...,Sn = BS
if
     thenS src sends packets to BH and BH drops the packet
else
    S src sends packets to BS, with successful transmission
end if
```

WSNS TRUST VALUE CALCULATION

Based on prior interactions and referrals from nearby nodes in networks, a node's trust value is determined. Indirect trust value of the node is the name given to this assessment of trust value. Additionally known as the node's initial trust value, the indirect trust value is a node's value. The node begins communication if the node's initial trust value is sufficient for it. Unless such occurs, the calculation of the direct value trust is used.

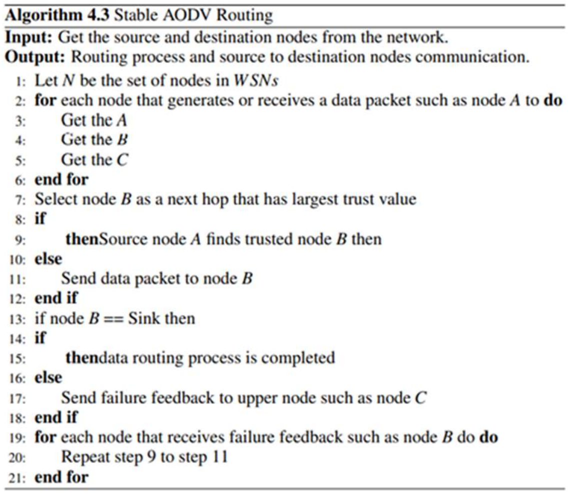
Similar to the trust framework, three models are used in the direct trust calculation. Three models for the node: the node's security model, node's mobility model, and node's reliability model. For each node model, the node assesses the trust value.



```
Algorithm 4.2 WSNs Trust Value Calculation
Input: Get the source and destination nodes from the network.
Output: Trust value calculation and nodes communication.
Let N be the set of nodes in WSNs
for each node N in the network do
    Get the N
    Get the s
    Get the d
end for
Calculate forward ratio for each node
Trust = Forward count of packet / Receive count of packet
Trust = Drop count of packet / Forward count of packet
Calculate direct trust for each node N= Trust
if thenthe direct trust value form the neighbours for each node
else
    Indirect trust = Direct trust / count of common neighbours
end if
terminate with the failure nodes N failed
if
    thenCalculate total trust for each node N
else
    Assign trust values to each node in the network
end if
```

STABLE AODV ROUTING

One of the most significant Stable AODV routing protocols is employed in the routing process of WSNs. A reactive protocol that seeks routes only when they are required is included in this method. For routing, it always exchanges control packets with nearby nodes[25]. Eliminate the route discovery phase by limiting neighbor distance and the number of identified routes in order to reduce control overheads and bandwidth usage and make Stable AODV useful for WSNs. Most control overheads are reduced as a result of this constraint. This approach reduces control overheads and stabilizes routes. The mobility model is one of the WSNs.



```
Algorithm 4.3 Stable AODV Routing
Input: Get the source and destination nodes from the network.
Output: Routing process and source to destination nodes communication.
1:  Let N be the set of nodes in WSNs
2:  for each node that generates or receives a data packet such as node A to do
3:      Get the A
4:      Get the B
5:      Get the C
6:  end for
7:  Select node B as a next hop that has largest trust value
8:  if
9:      thenSource node A finds trusted node B then
10: else
11:     Send data packet to node B
12: end if
13: if node B == Sink then
14: if
15:     thendata routing process is completed
16: else
17:     Send failure feedback to upper node such as node C
18: end if
19: for each node that receives failure feedback such as node B do do
20:     Repeat step 9 to step 11
21: end for
```

IV. IMPLEMENTATION AND RESULTS

STABLE AODV ROUTING MAINTENANCE IN WSN

Stable AODV routing requires that a node select a node from the list of candidates closer to the sink whose trust is higher than the predefined threshold as the next hop when it receives a data packet. If the node is unable to locate any such suitable next hop nodes, it will provide failure feedback to the higher node, which will then rediscover an alternative path by choosing the node with the most trust as the next hop. In a similar manner, if it is unable to locate any such suitable next hop, it sends a failure feedback to its upper node. In Figure 3, the Stable AODV routing technique used in this project work is explained. Figure 3 displays the results of the stable AODV routing.

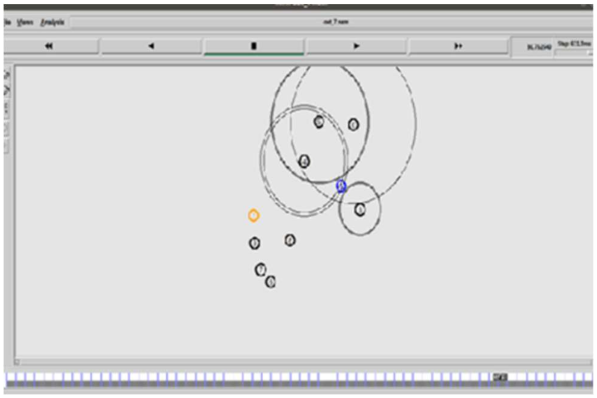


Fig.3: Stable AODV Routing Maintenance Process in WSN

TRUST EVALUATION IN WSN

Indirect trust value of the node is the term used to describe the evaluation of the trust value. Indirect trust value is another name for the node's initial trust value. The node begins communicating if its initial trust value is sufficient for that purpose. Otherwise, the direct value trust computation is used. The security model of the node, mobility model of the node, and dependability model of the node are the three models used in the direct trust calculation, much like in the trust framework. For each node model, the node assesses the trust value. The communication begins if the security model's trust value is sufficient. If not, it begins to assess the mobility model's trust value. The dependability model of the node is evaluated if the mobility model's value is insufficient for communication. If the node's reliability model is insufficient for communication, it will add its indirect and direct trust to determine the entire amount of trust. If the node's overall trust value is insufficient for trusted communication, the node will reject its request for communication.

Each node's energy levels are listed below. Each cluster's most energetic node has been identified by a green marker. With the exception of clusters 1 and 4, the ESRP chose the node in each cluster with the highest energy to serve as the CH. Although higher energy nodes were available, the Stable AODV chose lower energy nodes as the CH for clusters 1 and 4, which are highlighted in red. This is caused by the Stable AODV algorithm's shortcomings when used in a real-time setting.

V. RESULT AND ANALYSIS

The trust-based secure routing provided by each node and anomalous node behavior in the network are both brought about by the stable AODE routing mechanism in WSN. It is computed and compared how well the black hole nodes and trustable nodes deliver packets. It has been found that using black hole nodes significantly lowers the packet delivery ratio and has a negative impact on the successful packets posted ratio, successful packets received ratio, node-to-node delay, routing overhead, and throughput. Figure 4 illustrates the results of the simulation of the trust evolution sensor nodes.

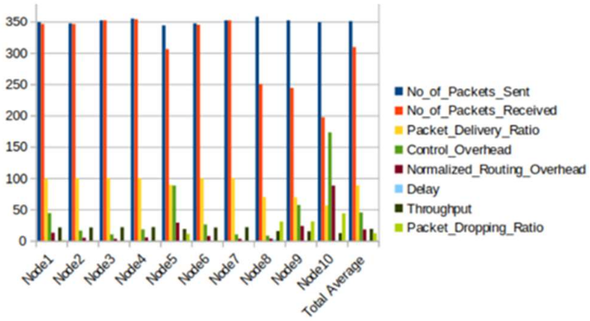


Fig.4: Trust based Performance Evolution in WSN

VI. CONCLUSION

According to the proposed system, a stable AODV-based safe routing technique based on trust sensing has been built. This routing method has advantageous qualities such a high chance of effective routing, security, and scalability. To locate the network's black hole nodes, a routing method is used. The trust evaluation algorithm is used to calculate the node trust values. The most effective routing path is chosen based on the categorized trust values. This system offers secure trust-aware routing that, before forwarding, finds the active nodes and creates backup routes as necessary. The plan increases the security of the data route while conserving energy. By utilizing Stable AODV routing algorithms, the power, energy, bandwidth, and trust sensing based secure routing in WSN can be improved. In this research, only the black hole assault has been addressed; in the future, work may address the wormhole attack and QoS attack. A strong attack will be recognized in the upcoming work using a highly flexible approach.

VII. REFERENCES

[1] Gururaj H L and Swathi B H. “A critical analysis on network layer attacks in wireless sensor network”. Journal of Engineering and Technology, vol. 05:pp. 2395–0072, 2018.

[2] Yanli Ya, Wanlei Zhou Li, and Ping Li. “Trust mechanisms in wireless sensor networks attack analysis and counter measures”. Journal of Network and Computer Applications, vol. 35:pp. 867–880, 2015.

[3] Danyang Qin, Songxiang Yang, Shuang Jia, Yan Zhang, Jingya, and Qun Ding. “Trust sensing based secure routing mechanism for wireless sensor network”. IEEE Access of Networking, vol. 10:pp. 438–448, 2017.

[4] Deug Julia and Weisong Shi. “Robust trust aware routing framework for wireless sensor networks”. IEEE International Conference, vol. 9:pp. 0302–9743, 2016.

[5] Maarouf, Ismat, Uthman Baroudi, and Abdurahim R. “Efficient monitoring approach for reputation system based trust aware routing in wireless sensor networks”. IEEE Transaction communications, vol. 42:pp. 846–858, 2016.

[6] Marlon, Jose N C, Campelo A, Rafael O, Juan V C, and Juan J S. “Active low intrusion hybrid monitor for wireless sensor networks”. Journal of Network and Computer, vol. 15:pp. 227–252, 2015.

[7] David, D. S., Anam, M., Kaliappan, C., Arun, S., Sharma, D. K. et al. (2022). Cloud Security Service for Identifying Unauthorized User Behaviour. CMC-Computers, Materials & Continua, 70(2), 2581–2600.

[8] Jayachandran, A., and D. Stalin David. "Textures and Intensity Histogram Based Retinal Image Classification System Using Hybrid Colour Structure Descriptor." Biomedical and Pharmacology Journal, vol. 11, no. 1, 2018, p. 577+. Accessed 12 Feb. 2021.

[9] D. Stalin David, 2019, “Parasagittal Meningiomia Brain Tumor Classification System based on MRI Images and Multi Phase level set Formulation”, Biomedical and Pharmacology Journal, Vol.12, issue 2, pp.939-946.

[10] Thendral R., David D.S. (2022) An Enhanced Computer Vision Algorithm for Apple Fruit Yield Estimation in an Orchard. In: Raje R.R., Hussain F., Kannan R.J. (eds) Artificial Intelligence and Technologies. Lecture Notes in Electrical Engineering, vol 806. Springer, Singapore. https://doi.org/10.1007/978-981-16-6448-9_27

[11] D. S. David and A. Jeyachandran, "A comprehensive survey of security mechanisms in healthcare applications," 2016 International Conference on Communication and Electronics Systems (ICCES), Coimbatore, 2016, pp. 1-6, doi: 10.1109/CESYS.2016.7889823.

[12] Stalin David, D., Jayachandran, A. A new expert system based on hybrid colour and structure descriptor and machine learning algorithms for early glaucoma diagnosis. Multimed Tools Appl 79, 5213–5224 (2020). https://doi.org/10.1007/s11042-018-6265-1.

[13] D Stalin David, A Jayachandran, 2018,Robust Classification of Brain Tumor in MRI Images using Salient Structure Descriptor and RBF Kernel-SVM, TAGA Journal of Graphic Technology, Volume 14, Issue 64, pp.718-737.

[14] D Stalin David, 2016, Robust Middleware based Framework for the Classification of Cardiac Arrhythmia Diseases by Analyzing Big Data, International Journal on Recent Researches In Science, Engineering & Technology, 2018, Volume 4, Issue 9, pp.118-127.

[15] M. Rajdhev, D. Stalin David, "Internet of Things for Health Care", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 2 Issue 2, pp. 800-805, March-April 2017.

[16] P. Prasanth, D. Stalin David, "Defensing Online Key detection using Tick Points", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 2 Issue 2, pp. 758-765, March-April 2017.

[17] Sudalaimani, D. Stalin David, "Efficient Multicast Delivery for Data Redundancy Minimization over Wireless Data Centres", International Journal of Scientific Research in

Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 2 Issue 2, pp. 751-757, March-April 2017.

[18] R. Abish, D. Stalin David, "Detecting Packet Drop Attacks in Wireless Sensor Networks using Bloom Filter", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 2 Issue 2, pp. 730-735, March-April 2017.

[19] Vignesh, D. Stalin David, "Novel based Intelligent Parking System", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 2 Issue 2, pp. 724-729, March-April 2017.

[20] D Stalin David, 2020, 'Diagnosis of Alzheimer's Disease Using Principal Component Analysis and Support Vector Machine, International Journal of Pharmaceutical Research, Volume 12, Issue 2, PP.713-724.

[21] Jaswanth K S, Dr. D. Stalin David, "A Novel Based 3d Facial Expression Detection Using Recurrent Neural Network", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 6 Issue 2, pp. 48-53, March-April 2020.

[22] D Stalin David, 2020, 'An Intellectual Individual Performance Abnormality Discovery System in Civic Surroundings' International Journal of Innovative Technology and Exploring Engineering, Volume 9, Issue 5, PP.2196-2206.

[23] D Stalin David, 2020, 'Machine learning for the prelude diagnosis of dementia', International Journal of Pharmaceutical Research, Volume 13, Issue 3, PP.2329-2335.

[24] David, D.S. and Y. Justin, 2020.A Comprehensive Review on Partition of the Blood Vessel and Optic Disc in RetinalImages.Artech J. Eff. Res. Eng. Technol., 1: 110-117.

[25] D. Stalin David and A.A. Jose, 2020. Retinal image classification system for diagnosis of diabetic retinopathy using SDCMethods.Artech J. Eff. Res. Eng. Technol., 1: 87-93.

[26] D. Stalin David and T. Joseph George, 2020. Identity-based Sybil attack detection and localization.ArtechJ. Eff. Res. Eng. Technol., 1: 94-98.

[27] David, D.S. and L. Arun, 2020.Classification of brain tumor type and grade using MRI texture and shape in a machine learning scheme.Artech J. Eff. Res. Eng. Technol., 1: 57-63.

[28] David, D.S., 2020. Retinal image classification system for diagnosis of diabetic retinopathy using morphological edgedetection and feature extraction techniques.Artech J. Eff. Res.Eng. Technol., 1: 28-33.