SEER: SECURED ENERGY EFFICIENT ROUTING ALGORITHMS FOR ATTACKS IN WIRELESS SENSOR NETWORKS

[1] DR.N.GAYATRI, [2] D. CHAITHANYA, [3] CH V RAGHAVENDRAN, [4] DR. PARVATHI MALEPATI, [5] K. SHYAM SUNDER REDDY, [6] DR. M. KIRAN KUMAR, *DR. P.NARESH

[1]Assistant Professor, Computer Science and Engineering, Kakatiya Institute of Technology and Science, Warangal.
[2]Assistant Professor, Department of CSE, CVR College of Engineering, Hyderabad, India.
[3] Professor, Department of Information Technology, Aditya College of Engineering & Technology, Surampalem
[4] Assistant Professor, Department of English & Foreign Languages, Madanapalle Institute of Technology & Science, Madanapalle
[5]Department of CSE, Maturi Venkata Subba Rao (MVSR) Engineering College, Hyderabad
[6]Asst. Prof, Department of CSE, GITAM *(Deemed to be University)*, Hyderabad.
*Assistant Professor, Dept of Computer Science and Engineering, Dayananda Sagar University, Bangalore

ABSTRACT

The main focus in WSN (Wireless Sensor Networks) is to perform an energy efficient routing for path finding from source to destination in communication channel. The existing studies performed well, but suffering from security aspects in terms of various attacks on networks. In this paper we focused more on how to handle various network attacks along with proper network routing. WSN deals with sensors hence involvement of energy consumption factors to be updated and can also be depends on topologies using for WSN. Node behavior is the major challenge which causes congestion in communication. We proposed secured energy efficient routing (SEER) algorithm to brief the mentioned problems. This method constructs an adaptive trust based secured model for network attacks such as black hole, sinkhole, hello flood and selective forwarding. The SEER algorithm uses various trust values to probe the attacks. Penalty mechanism can be used for identifying bad nodes in and around routing. By using multi hop routes predicted wormhole problems in network communication. Finally, the comparative study shows that our results are better than the others in saving of energy, detecting bad node behavior and prohibiting other network attacks.

Keywords: *WSN, Network Attacks, Secure Routing, Iot, Trust Based Model, Penalty Mechanism, Cluster Head.*

1.INTRODUCTION

Wireless Sensor networks comprised of huge amount of nodes acts as primary routing sources based on gathered information from surrounding environments. These actives nodes also take care of various attacks form the different areas. Nodes performs an energy efficient routing that saves energy consumption and look into the overall performance of the network. The prominent of WSN increased with the emerging of IoT technologies. It is proved that the combination of WSN with IoT has given outstanding results in major domains. Calculation of adaptive results with nodes such as energy, power consumption, memory access with respect to the environments. WSN give better results but suffers when they are with different topologies and heavy communication increases burden on the system. Routing is the major job which yields an efficient performance of the medium. These are vulnerability in handling various network attacks from unauthorized sources. When nodes are malicious the entire WSN can be damaged and will give fabricated outputs.

Security is the major aspect of any network, many researchers worked and given excellent solutions but still it is an open issue and challenge for them. In spite of many existed studies, they could not handle black hole, sinkhole, hello flood and selective forwarding attacks properly which causes still insecure. To protect network against these routing attacks we focused on to develop a secured trust model called Secured Energy Efficient Routing (SEER) algorithm. We aimed to give solution for the mentioned issues with the SEER algorithm.

The main contributions of our work is:

- Improving the trust value of the system for better accuracy and detecting the malicious nodes with respect to the penalty mechanism and constraints of time factors.
- To calculate trust value based on information gathered by the nodes from the surrounding environments and reduces the repeated communication for indirect trust value with the help of Sink value.
- To monitor the system with cluster heads to give safe routing to the nodes to avoid wormhole attacks.
- SEER model can be constructed to improve the performance and handling networks attacks.

The paper is organized as, section II briefs about various existing works related to secure routing. SEER is explained in section III. The routing protocols explained in in section IV. Finally, section V gives results part followed by the comparative study and conclusion mentioned.

2.RELATED WORK

Internet of Things became popular for the wireless sensor network in achieving goals of various networks and smart cities etc. Cloud of Things is the source of IoT in computing environments. IoT became major part of establishing smart cities due to its affordability and availability in less cost easy to usage and setup. IoT can be supporting for various real time applications domains such as transportation, medicine, engineering geological factors, environmental observation and security. In WSN communication sensor nodes pay a vital role in gathering information from various sources to give best routing path to the medium to travel. IoT hardware and software is a challenging factor in WSN structuring and constructing. Sensor can strongly resist the assaults from various network attacks while communication. In such cases conventional routing algorithms not justified the throughput hence we required a special monitoring algorithm for secured routing. Running WSN with limited sources is another challenging issue in this case. Designing a trusted secured model is required to face all these issues.

A secure hybrid routing protocol (SHRP), which is built on the ideas of geography and layering, is suggested in reference [2]. Two steps make up the entire SHRP procedure: clustering and choosing a cluster head, and safe routing.

To do cluster planning, SHRP first employs a clustering technique. Then suitable cluster heads are chosen based on the nodes' mobility, remaining energy, and centre location. Lastly, safe routing technology employs symmetrical and asymmetric cryptography to safeguard packet security during transmission and defend against man-in-the-middle, impersonation, replay, and eavesdropping attacks. At least three nodes with GPS are required for each cluster. It leads more power consumption in implementation of protocol.

In [3] the authors proposed a strong routing algorithm for secure routing called HCBS (Hybrid Cryptography Based Secure) data transmission technique. In HCS authors used ECC (Elliptistic Curve Cryptography) for key and data encryption exchanges along with MAC concepts. In [4], authors introduced Extended Elliptic Key Cryptosystem (ECCSRA) for safe routing to improve the confidentiality in the communication. The combination of ECCSRA and ECC with 512 bit Beta and Gamma technique, they restricted malicious users using Elliptistic curve algorithm in discrete decoding data when with unknown secrete key. Additionally, ECCSRA successfully generates secret keys using beta and gamma functions, enhancing the security of network communication. A secure end-to-end routing system with a unique group key pre-distribution technique is suggested in reference [5].

The protocol may establish keys and offer authentication simultaneously. It can also offer authentication to launch routing paths and path keys. The protocol employs route keys to prevent intermediate sensors from encrypting or decrypting data, safeguarding data in routing and shortening the period needed for middle sensors to development data. In particular[5], employs a single end-to-end route key rather than numerous couples of public keys to recurrently execute encoding and decoding on each connection. The protocol also performs well in terms of accuracy, the recentness of authentication responses, the recentness of communication keys, the recentness of group keys' forward and backward secrecy. These approaches stated above do not take internal assaults into account. As a result, a trust-based security system is suggested to handle various internal assaults.

Effective clustering algorithms were used by Kesavan et al. [1] to provide a active inputting strategy for safeguarding the message system while validating the nodes as they were moving. We can create dynamic keys by using mentioned method in [1] for secured routing in network communication. The used keys can not be used again and again by intruders to fabricate the network by the unauthorized persons. Trusted nodes only can perform reliable communication in these situations. The word trusted is became crucial in all the areas even it was originated from social science. The LEACH protocol's extension was discussed in [2], and according to Heinzelman et al.'s [3] proposal, it is self-organizing and adaptable in terms of cluster formation.

To trick trustworthy nodes into sending data to them, several hostile nodes might pose as destination nodes. In [3], authors used TSSRM i.e Trust Sensing Based Secure Routing Mechanism against malicious nodes with nominal characteristics and capabilities. In order to create the routing measures for choosing the better trusted path, with semiring method in TSSRM to detect optimized paths by taking direct, indirect trust value carefully along with the energy trust, incentive factor and Quality of Servicing indexing. In large-scale WSNs, TSSRM may, however, result in significant network latency and information overload. In order to decrease network latency, reference [3] suggests a cluster based secure routing algorithm called secured quality of service (QoS) aware energy efficient routing protocol (SEER).

The SEER's trust model generates the trust score using authentication technologies and a key-based security system. First, the trust model uses the straight trust score and secondary trust score to determine the total trust score. Second, SQEER chooses cluster heads for cluster built safe routing based on the QoS index and trust value. Lastly, the ending path is chosen based on the path reliability, energy, and hops, which successfully implements routing security. The key security method, however, is a part of the SQEER implementation, which further raises the computational cost for nodes. Reference [12] suggests a security plan for self-centered nodes in WSNs to lessen the strain on nodes. The three different sorts of nodes in this approach are cluster head (CH), inspector node (IN), and member node (MN). The IN is banned and the MN in its area will be told to cease sending data to the CH if it detects any issues while listening to the CH's broadcast. However, MN has the option to reject IN's choice if it determines that IN was the target of a deliberate accusation grounded on its personal standing system. In order to ascertain whether the status is normal for IN, CH will also direct a random check appeal to IN at the same time. In order to conserve energy, CH also abstains from IN's election.

This work suggests an energy conserving safe solution to protect WSMs against wormhole attack. Energy consumption is one of the performance metrics in the current secure techniques that has received the least research. Therefore, in order to guarantee that the network will last a long time, energy performance is the key priority in this effort. Sensors often run on batteries and have a finite amount of energy. Because they are placed in a hostile environment and dispersed or installed at random, it is difficult to change their batteries on a regular basis. The detecting technique must not require a lot of computation to operate in order to achieve low energy usage. High calculations, such encryption, will quickly deplete the battery in the sensors. Due to the enormous number of sensors in the field, the suggested solution must also reduce the additional expenses associated with the implementation of the sensors. It will thus be expensive to use extra hardware, such as the Geographic Positioning System (GPS), guard nodes, synchronised clocks, or any other additional equipment. A overview of a few current detection techniques is provided in the section that follows.

Table 1. Summary Of Comparative Studies Of Trusted Model.

Algorithm	**Methodology**	**Energy consumption**	**Cost of Network**	**Scope**	**Resistant for attacks**	**Ref**
TESRP	Trust, energy and hope number	Y	Medium	Moderate	N	10
SHRP	Cryptosystem uses symmetric & asymmetric	Y	More	Moderate	N	11
ECCSRA	Elliptic cryptography	N	More	Moderate	N	12
Trufix	Trust based model	Y	Medium	Wide	Y	13
HCBS	Mixed cryptography	N	More	Moderate	N	14
ESRT	Hop count	Y	Medium	Moderate	Y	15
TSRRM	Trusted model	Y	Medium	Moderate	Y	16
SQEER	Trusted model with key	Y	Medium	Moderate	Y	17

3.SEER MODEL

Nodes use trust values to determine malicious nodes, as described in references. The key to securing routing is understanding how to increase the trust value of legitimate nodes and fast decrease the trust value of malevolent nodes. In order to swiftly identify malicious nodes and quickly eliminate malicious nodes, this study employs the adaptive penalty coefficient to rapidly diminish the trust value of bad nodes.

Sensor nodes in SEER are typically separated into five components, as indicated in Figure 1, a processing, sensor, a wireless communication, a solar collector, and a battery modules. Similar to the components in a standard sensor network, it has a processing, sensor and wireless communication modules [5]. In contrast to conventional sensor nodes, it has a separate solar collector, battery module, and power controller. An energy consumption node model and the solar collector module's job is to convert solar energy into electrical energy through the photovoltaic or chemical effect. The system's power supply module is represented by the battery. It has a finite capacity and stores the electrical energy obtained from solar collectors. The solar collector charge the battery when not fully charged. Even though the solar collector continues to gather electrical energy, it cannot recharge the battery after it is fully charged. The mechanism for controlling electrical energy is called a power controller. In order to change the energy consumption of the wireless sensor and maximise the utilisation of scarce electrical energy, it modifies the transmission frequency of the wireless communication module based on the amount of battery life left, sun exposure time, intensity of sunlight, and day and night relationships.

A "trusted model" in the context of Wireless Sensor Networks (WSNs) often denotes a framework or method that guarantees the security and dependability of the network and its constituent parts. To avoid and reduce different security concerns and to guarantee the integrity of the data that sensor nodes gather and send, WSNs must be trusted.

The process of developing a trusted model for WSNs calls for a combination of operational, software, and hardware security measures. When developing and implementing security measures for WSNs, it is crucial to take the unique application and threat landscape into account because the demands may change depending on the deployment. Keeping up with new security risks and best practises is also essential to preserving the credibility of WSNs over time.

The nodes can establish trust connection between nodes based the behavior of individual nodes with the value of trust level. This value may be stated as:

$$DT_{ij}^{t}=\gamma * HT_{ij}^{t}+ (1\text{-}\gamma)*(R_j+S_j)^{t} \quad \text{---Eq(1).}$$

where HT^{t}_{ij} is the direct trust rating node i as determined by the node j afterwards volatility. The function of HT^{t}_{ij} is to further restrict the contribution of former trust values to the trust model. Before being identified as a rogue node, Node j could enjoy a high degree of trust.

To increase the trust value of js by reducing volatilization affect prior to the trust value. Whci can be dela with the following equation 2.

$$HT_{ij}^{t} = \lambda(DT_{ij}^{t-1} + HT_{ij}^{t-1}) \quad \text{----Eq (2).}$$

where λ determines how much the previous trust value affects the present direct trust value. The historical trust value's impact on the straight trust value increases with the value of.

$$R_j = \frac{\theta * receive\_message_j \text{-} rejection_j}{message_j}$$

$$S_j = \frac{\theta * send\_message_j \text{-} un\_send_j}{message_j}$$

--- Eq (3).

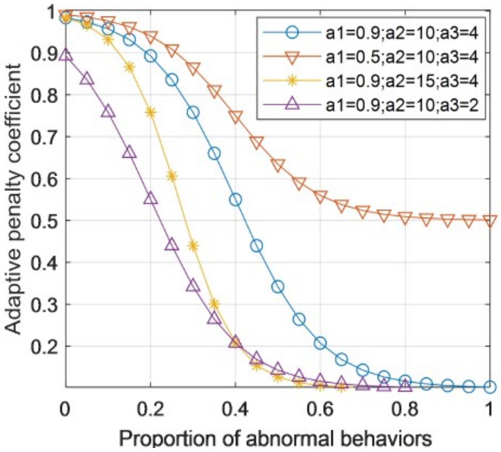


Figure 1. Adaptive Penalty Coefficient For Various Conditions.

TRUSTED VALUES

Indirect trust value demands a lot of energy for communication and could lead to information lack. This is so that node i can obtain direct trust value of node j from its publicly trusted neighbour node u before calculating the indirect trust node value of j.

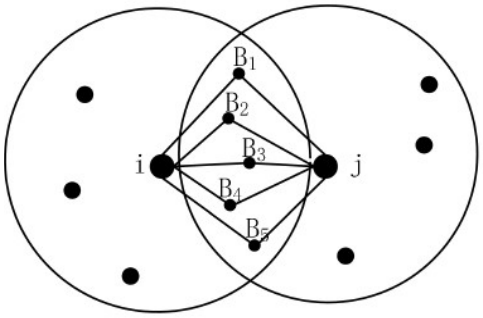


Figure 2. Neighbor Nodes In The Trusted System.

To reduce the strain on nodes and avoid broadcasting a sizable quantity of necessary information across nodes, this study opts for a centralised computing mode. Since the Sink determines the indirect trust value of each node, each node just needs to attach the direct trust value to the neighbouring node in the data packet and deliver it to the sink. To properly determine the trust value of node j, node i must be informed of the direct trust value at which the third node u assesses node j. To get the indirect trust rating that node i uses to evaluate node j, apply the formula below:

$$IT_{ij}^{t} = \frac{1}{q}\sum_{u \in B_h}^{q}(DT_{iu}^{t} * DT_{uj}^{t})$$

---Eq (4).

A node with a high trust rating but low remaining energy may experience a circumstance in the network that causes it to collapse early and change the structure and energy use of the whole network. Therefore, this study accounts for the node's remaining energy while computing the node's trust value in order to reduce network overhead and balance node energy usage.

When a node's residual energy exceeds or is equal to the threshold, it is said to be capable of participating in the information transmission process; otherwise, no matter how high their trust value, they are not.

The three elements that make up the total trust value are direct trust value, indirect trust value, and energy trust value. It reveals the reliability of the nodes. As the trust level rises, so does the nodes' aggregate trust value. Node j will be flagged as malicious and removed from the network if node i finds that its comprehensive trust value is less than the CTth, prohibiting it from taking part in any network operations. As a result, the graph below illustrates the overall trust value from node i to node j:

$$CT_{ij}^{t} = \eta_1 * DT_{ij}^{t} + \eta_2 * IT_{ij}^{t} + \eta_3 * E_j$$

---Eq (5).

4.DESIGN FOR SECURE ROUTING

We would want to make a few assumptions about the fundamental network model before delving into the architecture of safe routing, including:

Step-1: In order to gather information about the environment, sensor nodes are randomly placed across the network.
Step-2: Each sensor node is static and has the same beginning energy, processing power, and storage capacity.

Step-3: The Sink has infinite resources and is immobile.

Step-4: The Sink is aware of each node's unique identification (ID) and location after node deployment.

Each cluster in the network is composed of three different types of nodes: member nodes (MNs), cluster heads (CHs), and inspector nodes (INs). The network has clusters of varying sizes. Data transport between and within clusters is handled by CHs. Without security measures, hostile nodes' CHs will harm the network more than those made by member nodes.

Therefore, CHs must be embraced by nodes with strong energy and trust values. The found data is supplied by MNs to the CHs, who then multi-hop transmit the data packets to the Sink. In addition to the direct trust value for the neighbour nodes and their energy, the found data is also delivered by MNs to the CHs. Based on the received direct trust value and residual energy, the Sink assesses the nodes' total trust value. The modified complete trust values are then transmitted to the nodes. As a result, while collecting the trust value of third party nodes for neighbours, the conventional trust model avoids the problems of slow connection times, high energy consumption, and information congestion. In order to determine which nodes in the cluster are being used as malicious nodes in wormhole attacks, IN is responsible for tracking changes in the signal strength of the cluster's nodes. Because of its close proximity and high trust value, the equivalent CH chooses IN.

Each node broadcasts its first neighbour ID that has the greatest comprehensive trust value. After receiving the messages, the neighbouring node checks to see whether their IDs match.

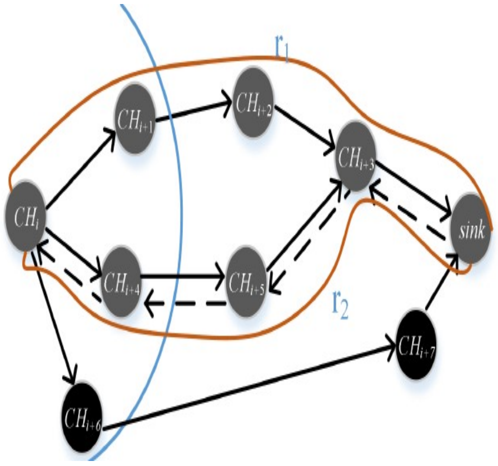


Figure 3. Safe Distance Path Routing.

The basis and primary emphasis of the trust model are the computation and updating of the trust value. In contrast to other trust-based safe routing protocols, the Sink of this protocol manages the indirect trust value rather than gathering several direct trust values from neighbour nodes. As a result, this protocol minimises communication overhead and reduces node congestion when updating trust values.

The following sections detail specific update procedures.

The first step involves MNs keeping an eye on the typical and unusual behaviours of the neighbour nodes and determining the direct trust levels of the neighbours using formula (1).

Step 2: The network starts to transition into the stable communication stage, similar to LEACH, once CHs, INs, and routes have been established.

Step 3: MNs attach the direct trust values of the evaluated neighbour nodes and their remaining energy to the data packet when they enter the last time slot of the stable phase.

In step 4, MNs transmit packets to their CHs, and CHs forward those packets over a series of hops to the Sink. The Sink then uses the direct trust value to generate the indirect trust value and the complete trust value.

Step 5: The Sink multicasts the estimated comprehensive trust value to each CH, and the CHs then transmit it on to the MNs in order for the node to update the neighbours' total trust value.

However, as they are evaluating adjacent nodes in step 3, malicious nodes may send some detrimental evaluations to the Sink.

The total trust value of nodes is a measure of how secure they are. As long as the overall trust rating is below the threshold, the nodes are malevolent. Fig. 4 shows how several harmful attacks altered the hostile nodes' total trust scores. The security of SEER, TSSRM, and TESRP is evaluated over 100 rounds with a total of 5% of hostile nodes in WSNs. Then, these malicious nodes launch attacks utilising, successively, black holes, selective forwarding, sinkholes, and hello floods.

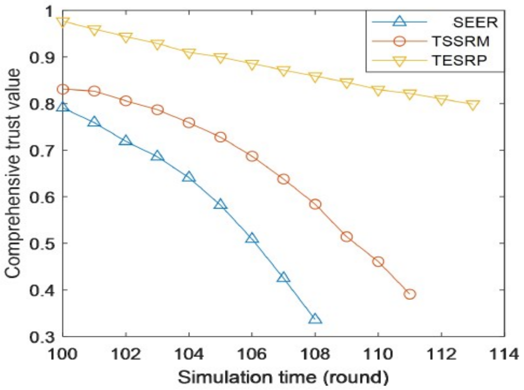


Figure 4. Bad Nodes Trust Values In Black Hole Attack.

While the system is still running, the comprehensive trust values of SEER, TSSRM, and TESRP decrease when the network reaches its 100th cycle and 6% of hostile nodes launch black hole assaults. It only takes 8 rounds to engage in conflict with and remove hostile nodes from the network, as seen in Fig. 4, and SEER's comprehensive trust value decreases the fastest. This proves that the most effective security system is SEER's. TSSRM and TESRP are outperformed by SEER against a black hole assault by 32.5% and 67.5 percent, respectively.

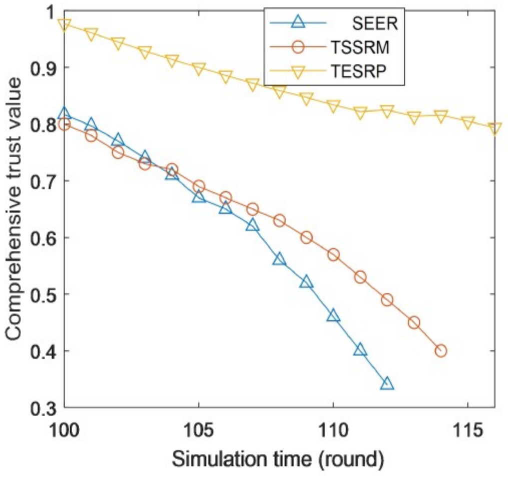


Figure 5. Hostile Nodes From Selective Forwarding Attacks.

Black hole attack is easier to detect than selective forwarding attack. because it may be difficult to identify selective forwarding attacks when they sporadically reject important packets. Fig. 5 illustrates how three security methods can stop hostile nodes from launching selective forwarding attacks. According to Fig. 5, SEER must fight against the selective forwarding attacks for 13 cycles before the network blocks it. When compared to TSSRM and TESRP, SEER's performance against selective forwarding attacks improved by 15.38% and 30.77%, respectively.

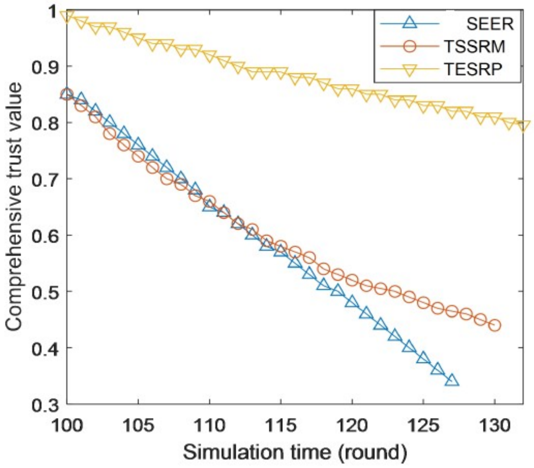


Figure 6. Malicious Nodes With Sinkhole Attack.

The underlying premise of sinkhole attacks is that hostile nodes alert the network to the fact that the control packet contains information on the arrival of the first hop. As a result, they receive a number of packets from neighbouring nodes that they subsequently decide to reject. In order to lessen the harm caused by this attack on the network and hasten other users' ability to identify malicious nodes, the SEER introduces an adaptive penalty coefficient that makes the more instances of malicious behaviour, the stronger the penalty effect, and quickly reduces the trust value of malicious nodes. Figure 6 shows that SEER must repel sinkhole attacks for 28 cycles in order to be removed from the network. In comparison to TSSRM and TESRP, SEER performs better against a selective forwarding assault by 13.11 and 121.52%, respectively.

The hello flood attack is then used to gauge the efficacy of three trust-based security solutions. Figure 6 demonstrates that security is at its maximum level when SEER is resisting when hostile nodes' comprehensive trust value falls below the threshold the quickest. Comparing SEER to TSSRM and TESRP, the efficacy of SEER against attacks from hello floods has increased by 15% and 65%, respectively.

ESRP to repel a wormhole attack. As seen in Fig. 6, the malicious nodes' total trust levels for TSSRM and TESRP are unaffected. The network's evaluation of the performance of malicious nodes still enjoying a very high degree of trust shows that the wormhole attack launched by malicious nodes cannot be halted by the defensive mechanisms of TSSRM and TESRP. But in just 8 rounds, SEER can thwart wormhole attempts from 2% of malicious nodes.

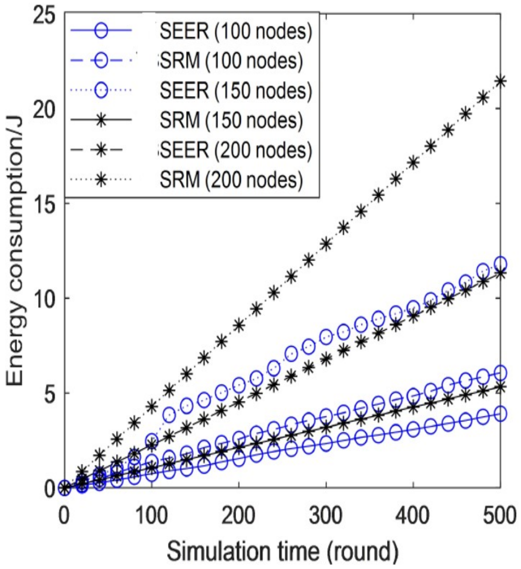
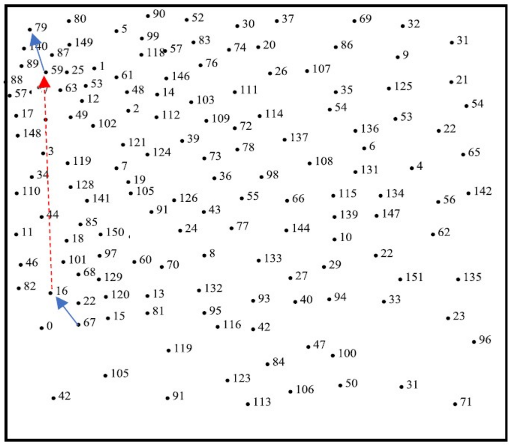


Figure 7. Calculating Indirect Trust Value For Energy Consumption.

The ability of SEER to survive sinkhole attacks is next put to the test using a variety of malicious node counts. The volatilization coefficient, adaptive penalty coefficient, S_j, R_j, and the volatilization factor all work together to quickly lower the trust level of malicious nodes. According to Fig. 5(c), the average identification speed of SEER is 14.63% and 27.62% faster than TSSRM and TESRP, respectively.

In the trust model, the indirect trust value of neighbours is determined by taking into account the direct trust value supplied by the third-party nodes. As a result, the trust model has resulted in a particular communication cost.

The communication energy used by the node to determine the indirect trust value in various situations is depicted in Fig. 7. The Sink distributes the load of the nodes and conserves nodes' energy since SEER utilises the Sink with infinite energy and strong functionalities to update and compute the indirect trust value. Additionally, as there are more nodes in a network, the more energy each node uses. The performance of SEER is still superior to TSSRM, though.



Because it has a shorter tunnel than the 50-node network size and a smaller neighbourhood list than the 150-node network size, the 100-node network size has the lowest values for energy and end to delay. Node-76 has neighbours that total 53,86,87,50,88,74,31,69,22,33,6, node-6 has neighbours that total 86,48,87,76,69,59,88,50,49,33,27,74,58,31,44, and node-39 has neighbours that total 40,4,57,77,64,21,26,25,61,43.

The 150-node network size has a greater value than the 100-nodes network size in energy and end to end delay because in is denser therefore, has a longer neighbourhood list were node-79 has {1, 57, 87, 140, 89, 53, 88, 63, 149, 80, 59, 25} neighbours, node-59 has {1, 57, 87, 140, 89, 53, 12, 149, 25, 88, 63, 61, 102, 17, 3, 2, 49, 79, 48, 148, 80, 5} neighbours, and node-16 has {67, 0, 101, 82, 81, 68, 97, 15, 22, 13, 120, 60, 46, 18,129} neighbours.

Additionally, the secured method shifts to a different channel for transmission once the malicious nodes are found, enabling the secured measure to transport the complete message through this different path. The packet delivery ratio, which is determined by the number of successfully delivered packets to their destinations, is likewise determined using this alternate route. A wireless sensor network is made up of sensors that can communicate wirelessly on their own, perceive the environment around them, and connect to the Internet using a base station. Since sensors are typically widely dispersed and must be inexpensive, their battery life, processing power, and memory capacity are constrained. Sensors are susceptible to numerous forms of attacks because of their limited capacity to perform standard security measures. Additionally, many of their applications, such as those used for forest re-detection and disaster assistance, are vulnerable to delays or packet corruption. Therefore, it is imperative to increase security. Different network levels are the targets of various assaults.

One kind is a wormhole assault, which harms the routing layer and is quickly deployable. In this study, an energy-saving secure method based on network connection is developed with the goal of detecting wormhole attacks. Using Network Simulator 3, the suggested method is tested against the ad hoc on-demand distance vector routing protocol. According to the findings, when the wormhole tunnel is four hops or longer, the detection accuracy is 100%. Additionally, because the approach is not dependent on any inserted hardware, such as synchronised clocks or a global positioning system, it incurs no additional expenditures, which makes it ideal for wireless sensor network situations.

The key advantages of this approach are that, although relying on neighbouring knowledge to solve a problem, it uses less energy because it does not need testing all pathways that have been found. The chosen path is only tested if the sensor nodes on it and their one hop neighbours are in charge of doing the computations. Additionally, it makes little effort to increase the system's level of security while acquiring a negligible overhead in transmission capacity and not expanding the range of network traffic. Additionally, it does not require any additional technology, such as synchronised clocks or GPS. There is also no increase in the delay or energy usage because it is based on straightforward calculations. Additionally, the second-degree neighbours' nding intersection characteristic reduces false positives in sparse networks. Additionally, it has a 100% detection rate for tunnels with four hops or more because sensor A builds a one hop neighbourhood list and sensor B builds a two hop neighbourhood list, allowing sensor A and B to look for a three hop alternative path between them. Therefore, sensor A and B would not be able to look for this developed harmful path if the generated malicious tunnel had four hops. The two malevolent sensors might fake their neighbourhood list to trick the detection system, which is one of this approach's drawbacks. Additionally, if the tunnel is shorter than four hops, it is typically exceedingly uncommon to detect this assault.

6.CONCLUSION

In wireless sensor networks with constrained resources, it's critical to offer secure and energy-efficient routing techniques. This article proposes a novel secured energy efficient routing protocol (SEER) to address numerous prevalent network attacks. In order to the maximum degree possible, SEER aims to decrease network energy consumption while simultaneously strengthening network security. SEER presents a unique trust model that accounts for the adaptive punishment coefficient and volatilization component. It can distinguish malicious nodes more rapidly and attacks like black holes, selective forwarding, sinkholes, and hello floods more effectively. Additionally, the nodes actively prevent wormhole assaults by using a multi-path search process based on the trust concept to find a safe and energy-efficient route. The simulation results show that, when compared to the traditional trust-based strategies, SEER may reduce routing overhead and increase data transmission reliability.

REFERENCES

[1] B. Khalifa et.al, "Coverage Hole Repair in WSNs Using Cascaded Neighbor Intervention," IEEE Sensors Journal, vol. 17, no. 21, pp. 7209-7216.

[2] P. Naresh, P. Srinath, K. Akshit, M. S. S. Raju and P. VenkataTeja, "Decoding Network Anomalies using Supervised Machine Learning and Deep Learning Approaches," 2023 2nd International Conference on Automation, Computing and Renewable Systems (ICACRS), Pudukkottai, India, 2023, pp. 1598-1603, doi: 10.1109/ICACRS58579.2023.10404866.

[3] X. Yang et.al., "Hybrid MAC Protocol Design for Mobile Wireless Sensors Networks," in IEEE Sensors Letters, vol. 2, no. 2, pp. 1-4, June 2018.

[4] Hussan, M.I. & Reddy, G. & Anitha, P. & Kanagaraj, A. & Pannangi, Naresh. (2023). DDoS attack detection in IoT environment using optimized Elman recurrent neural networks based on chaotic bacterial colony optimization. Cluster Computing. 1-22. 10.1007/s10586-023-04187-4.

[5] Ravindra Changala “A Surveyl on Clustering Techniques to Improve Energy Efficient Routing in Wireless Sensor Networks” in International Journal of Applied Engineering Research ,10(58), pp.-1-5,2015.

[6] A. Tripathi et.al. , "Coverage and Connectivity in WSNs: A Survey, Research Issues and Challenges," in IEEE Access, vol. 6, 2018.

[7] P. Naresh, S. V. N. Pavan, A. R. Mohammed, N. Chanti and M. Tharun, "Comparative Study of Machine Learning Algorithms for Fake Review Detection with Emphasis on SVM," 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 2023, pp. 170-176, doi: 10.1109/ICSCSS57650.2023.10169190.

[8] Sarma H K, Kar A, Mall R, et al. "A Hierarchical and Role Based Secure Routing Protocol for Mobile Wireless Sensor Networks". Wireless Personal Communications, vol. 90, no. 3, pp. 1067-1103, Jun. 2016.

[9] Naresh, P., & Suguna, R. (2021). IPOC: An efficient approach for dynamic association rule generation using incremental data with updating supports. Indonesian Journal of Electrical Engineering and Computer Science, 24(2), 1084. https://doi.org/10.11591/ijeecs.v24.i2.pp1084-1090

[10] Selvi M, Thangaramya K, Ganapathy S, et al. "An Energy Aware Trust Based Secure Routing Algorithm for Effective Communication in Wireless Sensor Networks". Wireless Personal Communications, vol. 105, no. 4, pp. 1475-1490, Feb. 2019.

[11] Rajeshkumar G, Valluvan K R. "An Energy Aware Trust Based Intrusion Detection System with Adaptive Acknowledgement for Wireless Sensor Network". Wireless Personal Communications, vol. 94, no. 4, pp. 1993-2007, Ay. 2017.

[12] B. Narsimha, Ch V Raghavendran, Pannangi Rajyalakshmi, G Kasi Reddy, M. Bhargavi and P. Naresh (2022), Cyber Defense in the Age of Artificial Intelligence and Machine Learning for Financial Fraud Detection Application. IJEER 10(2), 87-92. DOI: 10.37391/IJEER.100206.

[13] Yang Q, Zhu X, Fu H, et al. "Survey of Security Technologies on Wireless Sensor Networks". Journal of Sensors, vol. 2015, pp. 1-9, Dec. 2015.

[14] Ravindra Changala, "Diminution of Deployment Issues in Secure Multicast System with Group Key Management" published in International Journal of Computer Application (IJCA), Impact Factor 2.52, ISSN No: 2250-1797, Volume 2, Issue 3, June 2012.

[15] M. I. Thariq Hussan, D. Saidulu, P. T. Anitha, A. Manikandan and P. Naresh (2022), Object Detection and Recognition in Real Time Using Deep Learning for Visually Impaired People. IJEER 10(2), 80-86. DOI: 10.37391/IJEER.100205.

[16] Bilgin B E, Baktir S. "A light-weight solution for blackhole attacks in wireless sensor networks". Turkish Journal of Electrical Engineering and Computer Sciences, vol. 27, no. 4, pp. 2557-2570, Sep. 2019.

[17] Naresh, P., & Suguna, R. (2021). Implementation of dynamic and fast mining algorithms on incremental datasets to discover qualitative rules. Applied Computer Science, 17(3), 82-91. https://doi.org/10.23743/acs-2021-23.

[18] Devanagavi G D, Nalini N, Biradar R C, et al. "Secured routing in wireless sensor networks using fault-free and trusted nodes". International Journal of Communication Systems, vol. 29, no. 1, pp. 170-193, Ay. 2016.

[19] Selvakumar K, Sairamesh L, Kannan A, et al. "An Intelligent Energy Aware Secured Algorithm for Routing in Wireless Sensor Networks". Wireless Personal Communications, vol. 96, no. 3, pp. 4781-4798, Ay. 2017.

[20] Tang J, Liu A, Zhang J, et al. "A Trust-Based Secure Routing Scheme Using the Traceback Approach for Energy-Harvesting Wireless Sensor Networks". Sensors, vol. 18, no. 3, pp. 751, Mar. 2018.

[21] Ravindra Changala, "Object Tracking in Wireless Sensor networks using Data mining Techniques", in IOSR Journal of Electrical and Electronics Engineering, 2015.

[22] H. Ayadi et.al. , "Network Lifetime Management in Wireless Sensor Networks," in IEEE Sensors Journal, vol. 18, no. 15, 2018.

[23] Nagesh, C., Chaganti, K.R. , Chaganti, S. , Khaleelullah, S., Naresh, P. and Hussan, M. 2023. Leveraging Machine Learning based Ensemble Time Series Prediction Model for Rainfall Using SVM, KNN and Advanced ARIMA+ E-GARCH. International Journal on Recent and Innovation Trends in Computing and Communication. 11, 7s (Jul. 2023), 353–358. DOI:https://doi.org/10.17762/ijritcc.v11i7s.7010.

[24] Sunder Reddy, K. S. ., Lakshmi, P. R. ., Kumar, D. M. ., Naresh, P. ., Gholap, Y. N. ., & Gupta, K. G. . (2024). A Method for Unsupervised Ensemble Clustering to Examine Student Behavioral Patterns. International Journal of Intelligent Systems

and Applications in Engineering, 12(16s), 417–429. Retrieved from https://ijisae.org/index.php/IJISAE/article/view/4854.

[25] P. Naresh, P. Srinath, K. Akshit, G. Chanakya, M. S. S. Raju and P. V. Teja, "Revealing Cyber Risks: Malicious URL Detection with Diverse Machine Learning Strategies," 2024 2nd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS), Erode, India, 2024, pp. 546-550, doi: 10.1109/ICSSAS64001.2024.10760533.

[26] K. R. Chaganti, P. V. Krishnamurty, A. H. Kumar, G. S. Gowd, C. Balakrishna and P. Naresh, "AI-Driven Forecasting Mechanism for Cardiovascular Diseases: A Hybrid Approach using MLP and K-NN Models," 2024 2nd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS), Erode, India, 2024, pp. 65-69, doi: 10.1109/ICSSAS64001.2024.10760656.

[27] C. Nagesh, B. Divyasree, K. Madhu, T. Allisha, S. Datta Koushlk and P. Naresh, "Enhancing E-Government through Sentiment Analysis: A Dual Approach Using Text and Facial Expression Recognition," 2024 International Conference on Science Technology Engineering and Management (ICSTEM), Coimbatore, India, 2024, pp. 1-6, doi: 10.1109/ICSTEM61137.2024.10560678.

[28] Balakrishna, C. ., Sapkal, A. ., Chowdary, B., Rajyalakshmi, P., Kumar, V. S. ., & Gupta, K. G. . (2023). Addressing the IoT Schemes for Securing the Modern Healthcare Systems with Block chain Neural Networks. International Journal on Recent and Innovation Trends in Computing and Communication, 11(7s), 347–352. https://doi.org/10.17762/ijritcc.v11i7s.7009.