AN EFFICIENT TRUSTED ROUTE WITH IDENTITY BASED NEIGHBOUR FEEDBACK LINKED CLUSTERING MODEL FOR SECURE DATA TRANSMISSION

ASWADHATI.SIRISHA[1], K.SANTHI SRI[2]

[1]Research scholar, Department of Information Technology &Computer Applications, School of Computing and Informatics ,Vignan's Foundation for Science, Technology & Research (Deemed to be University), Vadlamudi, Guntur, Andhra Pradesh, India and Department of IT, Vignan's Institute of Information Technology (Autonomous), Vishakapatnam, Andhra Pradesh.
[2]Department of Information Technology& Computer Applications, School of Computing and Informatics,Vignan's Foundation for Science, Technology & Research (Deemed to be University), Vadlamudi, Guntur, Andhra Pradesh, India.

E-mail: [1]aswadhati.sirisha@gmail.com [2]kss_it@vignan.ac.in

ABSTRACT

Maintaining network security is essential for keeping data safe. It is the responsibility of system administrators to ensure that the functionality, usability, and security of a network are all adequately addressed. Access control, virus and anti-virus software, and other security measures can all be used to keep a computer network safe. Identifying malevolent sensor devices and eliminating the data they collect is crucial for mission-critical applications. Networks cannot directly use normal authentication and cryptography systems due to the limited resources of sensor devices. Consequently, to lessen the effect of malevolent sensors by efficient routing, an energy-efficient approach is required. The rapid growth in demand for network services and infrastructure in the last several decades has led to the global proliferation of static networks. The speed of the network's deployment is heavily dependent on the routing protocol chosen. The creation of a feasible and secure routing protocol is a must to meet the deployment needs while also satisfying the service level. Using hierarchical routing protocols based on Cluster Heads (CH) in combination with trust management strategies can be a useful option for creating a secure and reliable network where each node has complete trust in the next hop on its forwarding path. Using trust management concepts to develop a safe and attack-resistant protocol for routing in networks is as strong as ever. In this research, an efficient Trusted Route with Identity based Neighbour Feedback Linked Clustering (TR-INFLC) model is proposed for selecting the trusted route with linked clustering for secure data transmission. The proposed model when contrasted with the existing models, proposed model exhibits best performance.

Keywords: *Network Security, Trust Factor, Neighbour Feedback, Routing, Linked Clustering, Data Security.*

1. INTRODUCTION

Wireless Sensor Networks (WSNs) are a type of self-organizing network that may collaborate on real-time monitoring and collect multiple ecological or object information inside its monitoring area [1]. The acquired data is processed by WSNs, and the WSN is ultimately responsible for delivering the info. It is possible to categorise the wireless sensor nodes based on their large number, their small size and their poor communication and computation powers as well as their limited and irreparable power supply [2]. The largest difficulty for WSNs is how to meet Quality of Service (QoS) requirements, such as delay and fault tolerance, while also increasing network throughput due to limited resources including bandwidth, data storage capacity, and node energy. The fundamental goal of WSN research is to develop new networking technologies and interconnected global processing technologies that can swiftly extract meaningful, reliable, and timely information for users in highly dynamic situations with self-organizing capacities [3]. The WSN structure is shown in Figure 1.

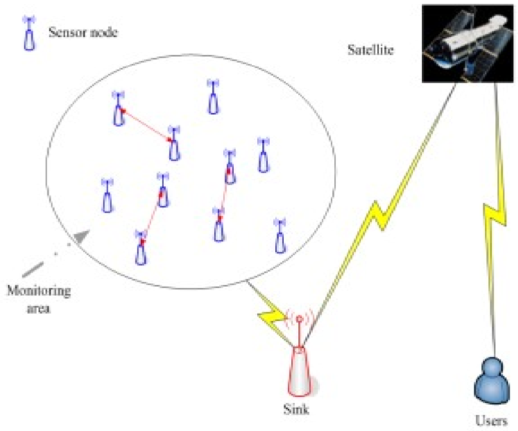


Fig 1: WSN Structure

There are a number of security-related solutions for WSNs, including authentication, key exchange, and safe routing, as well as security methods for specific attacks. There is some level of protection provided by these processes, but they cannot eradicate most of the security threats [4]. An IDS could be a solution to a variety of WSN security threats. A second line of defence for intrusion detection, a IDS can only identify attacks but has no ability to prevent or respond to them. In the event of an attack, the IDSs notify the controller so that they can take action. IDS based on anomalies identify intrusions by comparing traffic patterns and resource usage. False positive and false negative alarm rates are higher in anomaly-based IDSs, despite their capacity to detect well-known and novel assaults [5]. Some IDSs can only be used in certain situations or with specified protocols [6]. Route anomalies are detected by employing a proactive routing system, which is used by security analyzers. Because it is implemented on each node, detecting routing intrusions requires cooperation from all nodes. The use of reactive routing protocols is also found in some intrusion detection systems [7].

Wireless sensor network security is currently a big topic. An important technology problem must be solved in order to identify diverse network threats [8]. Wireless sensor networks security research can be classified into passive and active protection. Studies on active protection for wireless sensor networks are scarce in comparison to the progress made in passive defence studies. As a result, wireless sensor networks cannot be adequately protected by passive defence, which only responds to attacks after they have occurred [9]. Active defensive solutions must be studied urgently so that harmful intrusions can be detected before attacks take place. When it comes to protecting wireless sensor networks, intrusion detection will play a key role in the process [10].

Devices that are both affordable and energy efficient have been developed in response to the fast development of WSN [11]. With the use of sensors—which consist of digital logic and sensing devices—nodes in a WSN are able to communicate wirelessly. Nuclear power plants, petrochemical facilities, and disaster response centers are just a few of the many places you could find sensor networks in use. Each node in a WSN gathers data packets from its neighbours and sends them securely to the network's sink node. This allows us to present the user with the external environment while also ensuring that the found information is presented in an easily comprehensible manner. In data-intensive applications, every network must be able to recognize data packets [12]. By merging numerous data packets into one, data aggregation reduces data traffic and thereby energy consumption. In order to make the system last longer in general, many apps have been developed [13]. The most challenging aspect of implementing wireless infrastructure is dealing with its self-organization and variable communication. In a wireless sensor network, Sensor Nodes (SNs) that use multi-hop forwarding to transmit the detected data [14]. Because of multi-hop, in order to provide data to the sink node, each sensor node depends on its neighbours. Data integrity is at risk, leading to security vulnerabilities, the moment an attacker gains access to one of the cooperating nodes [15]. To prove secure data transfer, this study's routing strategy for WSN centers on a nominal routing trust factor that incorporates feedback from neighbors.

2. LITERATURE SURVEY

An intrusion detection system for wireless sensor networks was created by Zhou et al.[2] using the immunity idea as its foundation. By installing an intrusion detection subsystem on every sensor node, the system mimics the biological immune system's cloning and denial selection processes. Testing shows that the system has a false alarm rate of 90% when it comes to jamming attacks. Artificial collaborative stimulation has the potential to reduce false alarm rates; however, it lacks supervision, and manual collaborative stimulation is sometimes troublesome for WSNs. A hazard theory-based intrusion detection system for wireless sensor networks was proposed by Veerabadrappa et al. [3]. It was designed with the dispersed mechanism in mind. An intrusion detection system in its entirety is unnecessary on any one node. In order to identify intrusions, the central node maintains a library of antibodies and receptors, whereas the general node only detects threats. The method relies on statistically significant deviations from data link and network layer attributes to determine local node risk perception information. However, it fails to take into account the connection between a diverse network and multiple features, leading to insufficient risk data.

Ghosal et al. [5] constructed an intrusion detection model for wireless sensor networks based on risk theory. Model components include the dendritic cell (DC) algorithm and the theory of risk. The model is made up of the following parts: environment, decision, parameter library, rule library, operation library, and intrusion detection management. Environment monitoring, intrusion detection, decision subsystem, and detection model are the four main components that make up a module. According to the results of the experiments, the model uses very little energy while having a high detection rate. Even though this methodology routinely determines the MCAV index of antigens, it does so within a specific time frame. Although the signal and parameter settings are complex, there is a way to improve the real-time performance of intrusion detection.

Vishnu et al. [6] proposed a model for intrusion detection and prevention that relies on the differentiation of DC cells and operates in real-time. The model encompasses a number of domains, including the mathematical growth of DC cell models, the abstraction of DC cell information fusion processes, and the definition of the meaning and function of external signals in wireless sensor networks. Conducting a performance analysis, which takes into account factors like complexity, scalability, and resilience, is the last stage. Equally convoluted are the signals and parameters that comprise this model. Alghamdi et al.[8] used the differential evolution constraint multi-objective optimization problem as a foundation for their approach to the method used by intrusion detection systems in wireless sensor networks. Through the application of constraint processing and multi objective optimization techniques, the program aims to maximize non-self space coverage while simultaneously decreasing detector overlap. Black holes in non-self space are subsequently diminished via differential development. Research examines the algorithm's performance by mimicking a network. No factoring in of communication, processing, or energy consumption expenses is done.

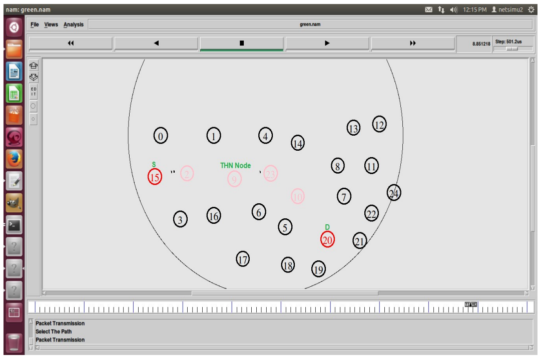
In order to find criteria for intrusion detection, Vijayalakshmi et al. [11] adopted an innovative evolutionary approach. Managing and extracting rules from different sets is done by looking at how far apart laws are in the same set and in separate sets. Automated threat recognition for wireless sensor networks was presented by Manisha et al. [13] in their enhanced hybrid intrusion detection system. In order to lower the power consumption of the sensor nodes, AHIDS employs a clustered design and an improved LEACH algorithm. An AHIDS anomaly and misuse detector is a multi-layer perceptron neural network with fuzzy rules.

Mehto et al. [14] presented a WSN-NSA intrusion detection model for wireless sensor networks using an upgraded V-detector method, due to the benefits of the negative selection algorithm (NSA) in the classification domain. Reduce detection characteristics in the V-detector technique with principal component analysis by optimizing detectors and altering detector generation algorithms. An intrusion detection model was developed by Anamika et al. [15] using fuzzy association rules and matching metrics. This model has the capability to evaluate new samples against multiple rule sets. For ease of use, samples are labeled with the class that corresponds to the best-matching rule set. According to Lin et al. [16], WSNs exhibit a distinct set of anomalies that can develop in a cluster of nearby nodes all at once and last for a long time. In order to make decisions, a distributed segment-based recursive kernel estimate can monitor a global probability density and compare its changes every two time intervals.

New methods for segmenting data have been developed by Fang et al [18]. The spatial predictability of a set of contiguous data segments can be used to identify those who are performing abnormally by leveraging their predictive capability to identify a group of random variables. The realism of existing intrusion detection system datasets can be evaluated using a fuzzy logic approach, according to Rachedi et al. [19]. They created an artificially realistic next-generation intrusion detection system collection based on the proposed metric results to aid in future intrusion detection system design.

3. PROPOSED MODEL

There is a trust-based routing technique that takes into account the activities of a prospective router and their validation status when making a routing decision. A trust-based routing protocol is another name for this sort of protocol [18]. A metric known as the Trusted Node Factor quantifies this viewpoint. The necessary route from the origin to the destination can be determined using trust metrics. Secure data transfer, protection of network resources from improper use, and maintenance of network performance are all achieved through the use of routing based on trust of node and neighbor feedback [20]. Secure data routing protocols protect not just the data but also its value, the safety information it contains, and the transfer of data between parties. Traditional trust-based routing algorithms, on the other hand, have a lot of serious flaws [21]. The trust-based systems address the dangers that are inherently present in wireless networks, but they also introduce new risks that require further attention. In order to solve the issues that were discussed, a trust-based neighbour feedback linked node clustering model is provided in this manuscript. The trusted nodes are only involved in the routing process. The trusted node routing process is shown in Figure 2.



Packet Transmission
Select The Path
Packet Transmission

Fig 2: Trusted Node based Routing

Components developed for wired networks cannot be adequately mapped to wireless networks due to the wide variety of mobility nodes [23]. This structure for QoS in WSN is composed of several layers, like the network and application layers, with a focus on the network layer. When a session begins, the network layer's routing protocol must be able to meet QoS criteria and address portability concerns. A routing protocol's job is to find the most secure way to send data packets to a destination when many paths exist. It is expected that the performance of a routing protocol remains unchanged when only defined pathways are utilized. Only access points with positive feedback are included in the suggested paradigm, and every node takes neighbour input into consideration before trusting other nodes [24]. At first, the node will be authenticated by the neighboring node using the trust factor. If the node acts maliciously, it will lose its authorization and be removed from the routing process. After the neighbor node has successfully authenticated, the next step is for the Trusted Head Node (THN) to authenticate. The THQ is in charge of monitoring the actions of all the nodes while data is being transmitted. Our system's routing algorithm considers not only the other quality requirements for path selection, but also the trust measure's features. An efficient Trusted Route with Identity based Neighbour Feedback Linked Clustering model is proposed for selecting the trusted route with linked clustering for secure data transmission. The proposed model is explained in the algorithm clearly.

Algorithm TR-INFLC

{

Step-1: Initially the nodes are registered in the network. The node will be allocated with the digital label for further identifications. The digital label will be a unique identity that is allocated to all the registered nodes in the network. The digital label allocation is performed as

$$DL(Node(i)) = \sum_{i \in N_i} \sum_{i=1} \frac{nodeaddr(i)}{Th} + gettime[N(i)]_N + ener(i)$$

$$DLneigh(i) = neighbour[Node(i)] - PDR(Node(i)) - ener(Node(i))$$

Step-2: The nodes which are registered with the network will be allotted with the digital label and the nodes trust factor is considered based on the nodes previous data transmission rate and load capabilities. The trust factor is calculated that is used to make the node involve in routing process or remove the node from routing process. The trust factor is calculated as

$$TL = PDR(Node(i)) + \sum_{i=1}^{N} DL(Node(i)) + TI + eneglevel[Node(i)] + Th$$

$$Trfactor(Node(i)) = \sum_{i=0} \max(TL) + DL * \frac{Th}{count(DL)}$$

Step-3: After calculating the trust factor of the nodes, the Trusted Head Node (THN) is selected from the trusted nodes which has high trust factor. The THN node is selected as

$$THN(Node(i)) = \sum_{i=1} \max(Trfactor(Node(i)) + \frac{[(N_2 - N_1) + (M_2 - M_1)]}{\max(ener(Node(i))}$$

Step-4: Every node neighbour feedback is considered and the neighbour feedback based routing is performed. The neighbour feedback helps in identification of the nodes behaviours and its transmission capabilities. The node neighbour feedback is considered as

$$Nf(Node(i+1)) = \sum_{i=1}^{M} PR(Node(i+1)) - PR(Node(i)) + \frac{availener(Node(i))}{allocener(Node(i))} + load(Node(i+1)) - load(Node(i))$$

Step-5: Based on the neighbour feedback, the neighbour feedback node clustering will be performed for linking the nodes that are normal in nature based on the feedback analyzed by THN node. The Neighbour Feedback Linked Clustering is performed as

$$LC(Nf(i)) = \frac{Nf}{\max(Trfactor(Node(i)))} + \max(PDR(Node(i))) + \frac{\max(Nf(Node(i)))}{count(Nf)}$$

Step-6: The optimal route is identified based on the neighbour feedback linked clustering model with considering trusted nodes. The routing table is updated based on the trusted nodes in the linked cluster and the process is performed as

$$Troute(LC(i)) = \sum_{i=1} \max(LC(Node(i+1))) - \min(LC(Node(i))) + \frac{setlink(Trfactor(Node(i+1)), Trfactor(Node(i)))}{count(DL)}$$

}

4. RESULTS

Due to the fact that it is concerned with the transmission of data to base stations, routing is one of the most critical processes in WSNs. Attacks directed at the routing protocol have the potential to quickly and severely hinder the operation of WSNs. The majority of routing attacks originate from compromised nodes, which means that traditional security techniques such as cryptography and authentication are insufficient to defend against them on their own. Recently, a trust mechanism has been implemented in an effort to strengthen collaboration among nodes and increase network safety. The trust mechanism in routing decides whether to exclude or include nodes in the routing operation based on an estimated trust value.

Among the many uses for trust management are routing, data aggregation, intrusion detection, and security access control. The model encompasses more than simply trust; it also includes reputation management, which is an integral aspect of any trust management system. Its primary function is to oversee the administration of trusts. Data collection for trust-related decisions, assessing trust-related criteria in neighbor relationships, and monitoring and re-evaluating existing relationships are all part of this process.

TM is concerned with the monitoring of neighbouring nodes during transmissions, the detection of misbehaviour, the estimation of trust values based on the detection results/recommendations, and the propagation of trust value/recommendation. All of these concerns pertain to the context of routing. The proposed is implemented in TCL script and executed in NS2 simulator. The proposed Trusted Route with Identity based Neighbour Feedback Linked Clustering (TR-INFLC) model is compared with the existing Trust Based Secure and Energy Efficient Routing protocol (TBSEER) model. The evaluation parameters and the comparisons are clearly illustrated.

Figure 3 illustrates the trust value calculation accuracy levels of the proposed and existing models. Initially, a node's trust value is calculated based on previous interactions and suggestions from its network neighbours. The node's trust value is referred to as the node's indirect trust value that is based on its load capabilities also. The trust factor helps in detecting the normal and malicious behaviour of nodes.

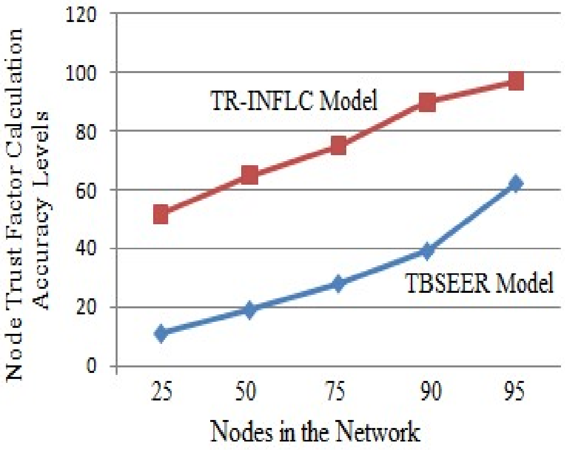


Fig 3: Node Trust Factor Calculation Accuracy Levels

In order for a node to gain the trust of its neighbours, it takes into account the positive feedback they have received from their neighbours. Every node in the network then undergoes authentication to prevent any nefarious activity. The neighbour node will initially authenticate the node. The Figure 4 represents the neighbour feedback consideration time levels of the proposed and existing models.

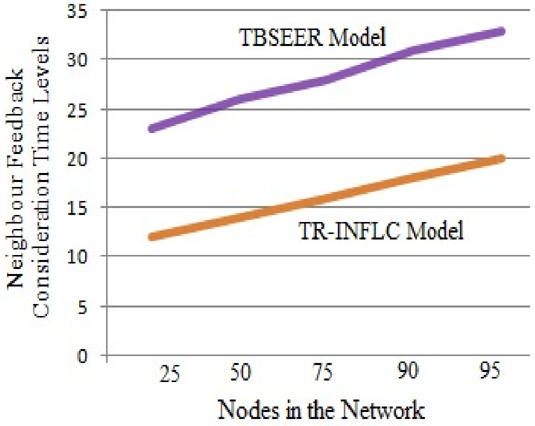


Fig 4: Neighbour Feedback Consideration Time Levels

The feedback gathered from the neighbour nodes is linked so that the trusted nodes can be organized to identify a secure route. The linked neighbour feedback helps in analysing the node performance levels. The linked neighbour feedback generation accuracy levels of the proposed and traditional models are shown in Figure 5.

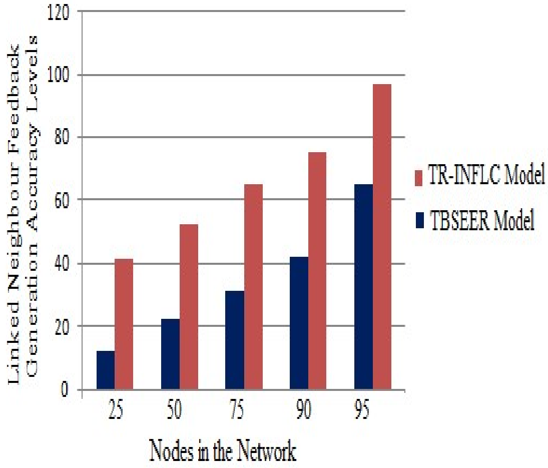


Fig 5: Linked Neighbour Feedback Generation Accuracy Levels

The nodes which are having positive feedback from the neighbours and the trusted nodes are considered in the routing process. On the other hand, in routing, the trust mechanism includes nodes depending on the trust estimation. When determining whether a node is malicious or helpful, the trust threshold is applied. The Figure 6 represents the trust route detection accuracy levels of the existing and proposed models.

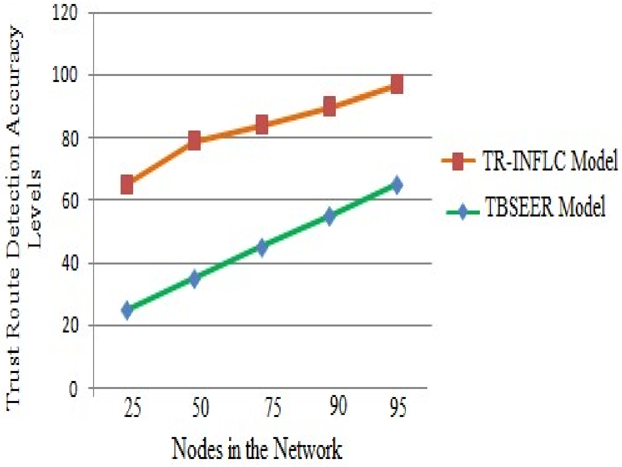


Fig 6: Trust Route Detection Accuracy Levels

Choosing a secured route involves a lot of trust in the nodes to avoid malicious actions. Each node maintains a list of neighbours and a trust value for each one. It is possible to integrate a level of trust that differs depending on the routing protocol in order to avoid a malicious node. THN node will monitor the node selection based on the trust of node and neighbour feedback to select the optimal route that securely transmits the data. The trusted route detection time levels of the proposed and traditional models.

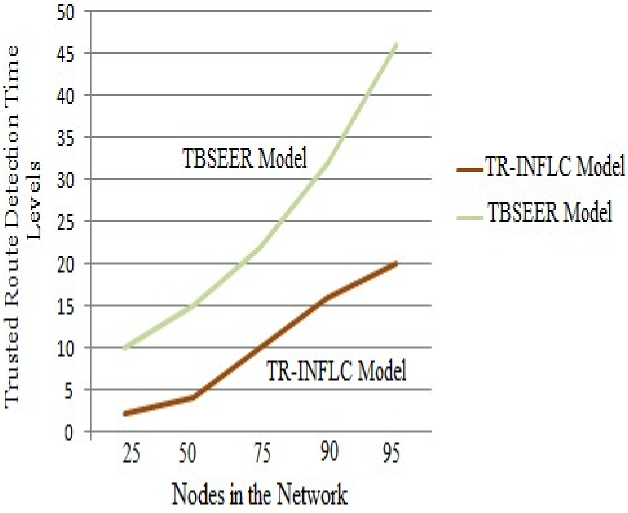


Fig 7: Trusted Route Detection Time Levels

The act of transferring data from one node to another is known as data transmission. Point-to-point digital data or channels are used for this transfer. One or more computational, network, communication, and electronic tools may be involved in the transfer of data. Point-to-point, point-to-multipoint, and multiple point-to multiple point device transmission and communication are all possible with this technology. The proposed model considers a trusted route for secure data transmission rate. The data transmission security levels are shown in Figure 8.

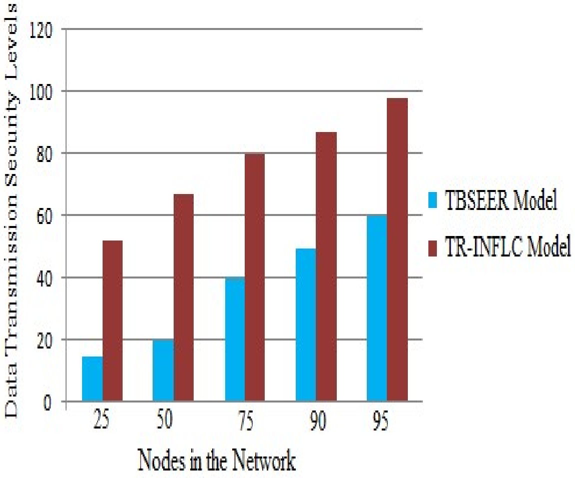


Fig 8: Data Transmission Security Levels

5. CONCLUSION

There are nodes that can move around in other networks in order to exchange data in WSNs. The loss of links generated by mobility makes it more difficult to go back and retrace one's path. In conjunction with a new routing strategy, more stable paths from the source to the destination node can be created by leveraging node velocity, position, and residuals. It has been proven through extensive simulations in a variety of operational settings and scenarios that the approaches presented are successful. Both the trust factor and the feedback from neighbours are taken into account while creating a safe data transfer path in the suggested method. There are numerous typical network vulnerabilities during data transmission hence this research presents a new trust-based secure and energy-efficient routing protocol. The primary goal is to increase network security while reducing attacks as only trusted nodes are involved. The proposed Trusted Route with Identity based Neighbour Feedback Linked Clustering method is able to discover the safest path in the network by analysing authorised and trusted nodes. The proposed model decreases latency because of its high packet delivery. When compared to standard models, the offered model has a low packet drop rate. In future, multi-level validation and trust parameter computation methods can be enhanced and more node parameters are considered for secured route detection.

CONFLICT OF INTERESTS

The authors declare that there is no conflict of interest in submission.

REFERENCES

[1]. Y. Swathi, S. Chitnis, “Game theory trust model with authentication and AES encryption (GTAAES) model for secure data aggregation in WSN”, International Journal of Advanced Sciences and Technology, vol.29, pp.2193–2207, 2020.

[2]. L. Zhou, Y. Shan, “Privacy-preserving, energy-saving data aggregation scheme in wireless sensor networks”, Journal of Inf. Process. Syst., vol.16, no.1, pp.83–95, 2020.

[3]. G.MN Veerabadrappa, P.M. Booma, “ESDAM - efficient and secure data aggregation against malicious nodes in Iot environment”, International Journal of Innovative Technology and Exploring Engineering (IJITEE), vol.9, no.2, pp.2278–3075, 2019.

[4]. Hassan A, Anter A and Kayed M, “A Robust Clustering Approach for Extending the Lifetime of Wireless Sensor Networks in an Optimized Manner with a Novel Fitness Function”, Sustainable Computing: Informatics and Systems, 2020

[5]. Ghosal A, Halder S and Das S. K, “Distributed on-demand clustering algorithm for lifetime optimization in wireless sensor networks”, Journal of Parallel and Distributed Computing, 2020.

[6]. Vishnu V. M and Manjunath P, “SeC-SDWSN: Secure cluster-based SDWSN environment for QoS guaranteed routing in three-tier architecture”, International Journal of Communication Systems, vol.32, no.14, 2020.

[7]. Vinitha A and Rukmini M. S. S, “Secure and energy aware multi-hop routing protocol in WSN using taylor-based hybrid optimization algorithm”, Journal of King Saud University-Computer and Information Sciences, 2019.

[8]. Alghamdi, Turki A, “Secure and energy efficient path optimization technique in wireless sensor networks using DH method”, IEEE Access, vol.6, pp.53576-53582, 2018.

[9]. L.Narayana,V., Lakshmi Patibandla, R.S.M., Pavani, V., Radhika, P. (2023). Optimized Nature-Inspired Computing Algorithms for Lung Disorder Detection. In: Raza, K. (eds) Nature-Inspired Intelligent Computing Techniques in Bioinformatics. Studies in Computational Intelligence, vol 1066. Springer, Singapore. https://doi.org/10.1007/978-981-19-6379-7_6.

[10]. Narayana, V.L., Sujatha, V., Sri, K.S., Pavani, V., Prasanna, T.V.N., Ranganarayana, K. (2023). Computer tomography image based interconnected antecedence clustering model using deep convolution neural network for prediction of covid-19. Traitement du Signal, Vol. 40, No. 4, pp. 1689-1696. https://doi.org/10.18280/ts.400437

[11]. Vijayalakshmi, K.; Ananda, P. Global evy flight of cuckoo search with particle swarm optimization for effective cluster head selection in wireless sensor network. Intell. Autom. Soft Comput. 2020, 26, 303–311.

[12]. V. Narayana L, S. Bhargavi, D. Srilakshmi, V. S. Annapurna and D. M. Akhila, "Enhancing Remote Sensing Object Detection with a Hybrid Densenet-LSTM Model," 2024 IEEE International Conference on Computing, Power and Communication Technologies (IC2PCT), Greater Noida, India, 2024, pp. 264-269, doi: 10.1109/IC2PCT60090.2024.10486394.

[13]. Manisha, R.; Sushil, K.; Amir, G. Ant Colony Optimization Based Quality of Service Aware Energy Balancing Secure Routing Algorithm for Wireless Sensor Networks. IEEE Trans. Eng. Manag. 2021, 68, 170–182.

[14]. Mehto, A.; Tapaswi, S.; Pattanaik, K.K. A review on rendezvous based data acquisition methods in wireless sensor networks with mobile sink. Wirel. Netw. 2020, 26, 2639–2663.

[15]. Anamika, S.; Siddhartha, C. Sensor Fusion for Distributed Detection of Mobile Intruders in Surveillance Wireless Sensor Networks. IEEE Sens. J. 2020, 20, 15224–15231.

[16]. Lin, C.; Han, D.; Deng, T. P2S: A Primary and Passer-by Scheduling Algorithm for On-demand Charging Architecture in Wireless Rechargeable Sensor Networks. IEEE Trans. Veh. Technol. 2017, 66, 8047–8058.

[17]. Lin, C.; Zhou, J.; Guo, C. TSCA: A Temporal-Spatial Real-Time Charging Scheduling Algorithm for On-Demand Architecture in Wireless Rechargeable Sensor Networks. IEEE Trans. Mob. Comput. 2018, 17, 211–224.

[18]. W. Fang, W. Zhang, W. Yang, Z. Li, W. Gao, and Y. Yang, ‘‘Trust management-based and energy efficient hierarchical routing protocol in wireless sensor networks,’’ Digit. Commun. Netw., vol. 7, no. 4, pp. 470–478, Nov. 2021, doi: 10.1016/j.dcan.2021.03.005.

[19]. A. Rachedi and A. Hasnaoui, ‘‘Advanced quality of services with security integration in wireless sensor networks,’’ Wireless Commun. Mobile Comput., vol. 15, no. 6, pp. 1106–1116, Apr. 2015.

[20]. G. D. Devanagavi, N. Nalini, and R. C. Biradar, ‘‘Secured routing in wireless sensor networks using fault-free and trusted nodes,’’ Int. J. Commun. Syst., vol. 29, no. 1, pp. 170–193, Jan. 2016.

[21]. K. Thangaramya, K. Kulothungan, S. I. Gandhi, and M. Selvi, ‘‘Intelligent fuzzy rule-based approach with outlier detection for secured routing in WSN,’’ Soft Comput., vol. 24, no. 21, pp. 16483–16497, Apr. 2020.

[22]. T. Yang, X. Xiangyang, L. Peng, L. Tonghui, and P. Leina, ‘‘A secure routing of wireless sensor networks based on trust evaluation model,’’ Proc. Comput. Sci., vol. 131, pp. 1156–1163, Oct. 2018.

[23]. Q. Shi, L. Qin, Y. Ding, B. Xie, J. Zheng, and L. Song, ‘‘Information-aware secure routing in wireless sensor networks,’’ Sensors, vol. 20, no. 1, p. 165, Dec. 2019.

[24]. N. Sun and Y. Lu, ‘‘A self-adaptive genetic algorithm with improved mutation mode based on measurement of population diversity,’’ Neural Comput. Appl., vol. 31, no. 5, pp. 1435–1443, May 2019.

[25]. J. Xu, L. Pei, and R.-Z. Zhu, ‘‘Application of a genetic algorithm with random crossover and dynamic mutation on the travelling salesman problem,’’ Proc. Comput. Sci., vol. 131, pp. 937–945, May 2018.

[26]. X. Guoxin, T. Xin, P. Wei, and R. Tao, ‘‘Clustering analysis based on chaos micro variation adaptive genetic algorithm for radio fuze jamming,’’ in Proc. 29th Chin. Control Decis. Conf. (CCDC), May 2017, pp. 616–620, doi: 10.1109/CCDC.2017.7978287.

[27]. H. Hu, Y. Han, M. Yao, and S. Xue, ‘‘Trust based secure and energy efficient routing protocol for wireless sensor networks,’’ IEEE Access, early access, Apr. 27, 2021, doi: 10.1109/ACCESS.2021.3075959.

[28]. C. Wang, X. Liu, and H. Hu, ‘‘Energy-efficient and load-balanced clustering routing

protocol for wireless sensor networks using a chaotic genetic algorithm,'' IEEE Access, vol. 8, pp. 158082–158096, 2020.

[29]. S. A. Sert, E. Onur, and A. Yazici, ''Security attacks and countermeasures in surveillance wireless sensor networks,'' in Proc. 9th Int. Conf. Appl. Inf. Commun. Technol. (AICT), Oct. 2015, pp. 201–205.

[30]. S. A. Sert, C. Fung, R. George, and A. Yazici, ''An efficient fuzzy path selection approach to mitigate selective forwarding attacks in wireless sensor networks,'' in Proc. IEEE Int. Conf. Fuzzy Syst. (FUZZ-IEEE), Jul. 2017, pp. 1–6.