SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V10I11P104

Volume 10 Issue 11, 33-44, November 2023

Original Article

Localized Distributed Secure Fast Neural Routing for QoS Maximization in WSN with IoT Using Machine Learning

N. Babu[1], Tamilarasi Suresh[2]

[1,2]*Department of Computer Science and Engineering, St. Peter's Institute of Higher Education and Research, Tamilnadu, India.*

[1]*Corresponding Author : babuskpt@gmail.com*

Received: 12 September 2023 Revised: 23 October 2023 Accepted: 12 November 2023 Published: 30 November 2023

Abstract *- Several routing algorithms in the literature promote secure communication between nodes of Wireless Sensor Networks (WSN). Most approaches perform route selection according to behaviour, frequency of transmission, throughput, latency, and other factors of any route. However, the deficiency of transmission details challenges the routing protocol and leads to poor security performance. By considering this, an efficient Localized Distributed Secure Fast Neural Routing (LDSFNR) is presented in this paper. The method focused on performing route selection according to the partial route trust, which is computed in a distributed way with a localized structure. Even though the nodes can choose their forwarder, the protocol is restricted for the Sensor Nodes (SN) and does not provide any freedom for Internet of Things (IoT) devices. With this result, the SNs involved in transmissions keep track of transmission traces in both ways. Using the traces, the intermediate node would measure the trust value of the partial route up to k hops. To calculate the trust value, the intermediate node would train the Neural Network (NN) with the available traces. The neurons are designed to measure the Partial Trust Score (PTS) for the k hop, which is calculated based on behaviour, transmission rate, retransmission rate, latency, etc. The model initially finds the set of routes to attain the target node and computes the Complete Trust Score (CTS) for various routes in the fast neural testing. Based on the result of neural testing, an optimal way is selected and transmitted. The intermediate node applies localized fast neural routing, identifying a secure route and forwarding the data packet according to the traces. The proposed model enhances the secure routing performance in WSN with higher Quality of Service (QoS) performance.*

Keywords *- WSN, IoT Devices, Secure routing, QoS maximization, LDSFNR.*

1. Introduction

Recent trends in data communication are highly reliant on sensor networks, as most services are accessed through various devices enabled with wireless communication. This challenges the service providers and network administrators in securely handling data transmission. Different security protocols to secure data transmission are named in the literature. For example, the throughput-based approach would be concerned with the throughput achieved by any route to measure the trust indirectly.

If the throughput is poor on the specific route, then it would indirectly conclude the trust of the route. Similarly, transmission latency is a key in specific approaches which conclude a high latency route as having malicious nodes. On the other side, by maintaining the number of traces of transmission, the behaviour of various nodes in the route can be measured. By measuring the trust of any route according to the behaviour, the security in routing can be achieved moderately. All these methods have specific achievements in secure routing, but points about secure transmission are still missing. In real-world networks, maintaining the traces and history of various nodes at one point, particularly at the source node, is not feasible. So, measuring the trust of the entire route at a starting point is impossible and would introduce higher overload. This also increases the network overhead due to sharing transmission details.

Also, this would leak all of the transmission details with the adversaries present in the network. With this result, measuring the trust of the route only up to a specific number of hops is necessary. By measuring the trust of routes in a short span, the efficiency of route selection can be improved. As the SNs have limited storage, they can store the transmission traces that come through them, and by using them, they can analyze the trust of the short-span route. Most routing protocols are dynamic in route selection, and the nodes can choose their next hop. The intermediate nodes can

perform trust measurement and perform route selection. By doing so, routing and data security can be improved. Machine Learning (ML) algorithms have many applications and can be used in problems. It has a variety of algorithms, including support vector machine, decision tree, Genetic Algorithm (GA), NN, and so on. Among them, the NN is the most effective one, which would produce rapid results on any classification problem.

The partial route trust can be computed efficiently by training the Fast NN (FNN) with the transmission traces maintained in distributed nodes. It would support the secure transmission of data packets. With this consideration, an efficient LDSFNR is presented in this article. The model is designed to measure trust in two ways. One is at the source, which computes the CTS to perform route selection, whereas the second case is at the intermediate k th node, which measures PTS. The method would perform routing by combining the measures and supporting secure transmission. The steps are estimated using the FNN, trained with the number of transmission traces available and would return the set of CTS and PTS values. With the use of such deals, route selection can be performed.

1.1. Research Gap

The challenging task of ensuring secure communication and high-quality service for IoT devices remains unresolved despite numerous routing algorithms designed for WSNs. While multiple established methodologies prioritize behaviour, transmission frequency, throughput, and latency when determining the optimal route, they frequently neglect to account for transmission intricacies thoroughly. The lack of comprehensive transmission information presents a formidable challenge for routing protocols and leads to less-than-ideal security performance.

The novelty of this work is that it introduces the novel LDSFNR protocol for WSNs. Unlike traditional routing algorithms, LDSFNR focuses on partial route trust computed in a distributed, localized manner, restricting the freedom to SNs while incorporating trace-based mechanisms. SNs track transmission details, and a trained NN assesses the PTS for each hop based on behaviour, transmission rate, retransmission rate, and latency. CTS is derived through fast neural testing, enabling optimal route selection. Intermediate nodes employ localized FNN, enhancing WSN security and QoS.

1.2. Problem Statement

This research aims to resolve the limitations of current routing algorithms that hinder secure communication in WSNs, specifically when IoT devices are present. Traditional methodologies might fail to consider critical transmission intricacies, thereby introducing susceptibilities into the network. Developing a routing protocol encompassing behaviour, transmission frequency, throughput, and latency and a mechanism for assessing and verifying the reliability of partial routes presents a formidable challenge. Furthermore, the current protocols may fail to adequately incorporate IoT devices into the secure routing procedure, compromising the network's QoS and overall security. The LDSFNR proposal presents a distributed and localized method for calculating partial route trust to mitigate these concerns.

The PTS is computed utilizing neural networks, considering many factors such as latency, transmission rate, retransmission rate, and behaviour. The primary objective of this research is to optimize the reliability of specific routes to improve the security capabilities of WSNs, thereby resulting in an enhanced QoS. The difficulty lies in developing a protocol that effectively manages the routing process while considering the distinct attributes of SNs and IoT devices. CTS and PTS values are measured according to various constraints like behaviour, transmission rate, retransmission rate, etc. The workings of the research model were explained in detail in the coming sections.

2. Related Works

2.1. Background

To improve QoS and security, this section investigates various models and methodologies associated with the secure routing of WSNs. Significant research has been applied to secure communication within WSNs, mainly when IoT devices are present. This chapter examines various methodologies, such as optimization techniques, blockchain-based protocols, trust-oriented models, and secure routing algorithms. Considering energy efficiency, dependability, trustworthiness, and encryption mechanisms, each approach attempts to tackle the challenges associated with safe and efficient data transmission in WSNs.

A Blockchain (BC) secure routing protocol model in WSN was developed in [1], where the model was safe. Moreover, the protocol developed for BC Security of IoT was to present authentication among the Cluster Heads (CH), mobile Base Stations (BS), and the Member Node (MN) for WSN. The protocol made its network's required keys at all the sensor levels for the various conditions evaluated, migration and BS mobile nodes. Reliable, Secure, and Energy Efficient (EE) WSN routing was discussed in [2].

Recently, increased attention has been directed towards addressing the difficulties in routing to ensure the EE, security, and reliability of networks. Studies have delved into analyzing EE, safety, and reliability routing models. The work [3] employed a trust-oriented approach to identify data and collaborative trust. Collaborative trust was assessed through indirect and direct trust mechanisms, while data trust was calculated using node energy and received signal strength. The evaluation of network efficiency involved analyzing performance parameters like throughput, routing load, and other relevant factors.

In the research [4], an innovative, secure routing model was developed through optimal path selection and encoding. The initial phase involved optimal link-states multipath routing, wherein specific transmission paths or nodes were selected. To achieve optimal path selection for both source and destination, the Crossover Mutated Marriage in Honey Bee (CM-MH) model was formulated and introduced in this study. In the "Ant Colony Optimization (ACO)-based QoS aware Energy Balancing Secure Routing (QEBSR) Algorithm for WSNs" [5], the article introduced the QEBSR algorithm tailored for WSNs.

The proposed algorithm included improved heuristics for calculating the transmission delay and the trust factors associated with nodes along the routing paths. In [6], a novel routing metric known as HRMS was introduced. This metric incorporates the cryptographic security features known as Improved Advance Encryption Standards Methodology (IAESM) for ensuring data security during communications. The suggested hybrid logic amalgamates various advanced communication logic to enhance both the transfer and reception schemes, surpassing the performance of classical WSN routing protocols. The study [7] developed a taxonomy to classify current hierarchical routing protocols for WSNs. The research involved an examination of the performance and functionality of these established hierarchical protocols for routing. A comparative analysis was also conducted to underscore notable technological distinctions among existing routing protocols.

The study also presented a performance evaluation focusing on selected LEACH-based routing protocols. The research Trusts-Based Secured and EE Routing (TBSEER) for WSNs in [8] aimed to address pertinent issues in WSNs. TBSEER introduced a comprehensive trust calculation method, incorporating adaptive indirect, direct, and energy trust values. This approach was designed to provide resistance against various attacks. The protocol included an adaptive penalty approach and volatilization factor to facilitate the swift identification of malignant nodes. Notably, nodes just needed to compute the value of direct trust, while the value of indirect trust was attained from the sink, thereby minimizing energy consumption associated with iterative calculations. In [9], a Lightweight Trust Management Scheme (LTMS) was introduced, utilizing binomial distribution to enhance defence against internal attacks.

Simultaneously, the study incorporated the distance, energy, security, and environment domains to develop the Multidimensional Secured Clustered Routing (MSCR) methodology within hierarchical WSN. The MSCR scheme utilized dynamic dimension weights to optimize performance in these domains. In [10], the trust-aware secured routing protocol was introduced to safeguard against several attacks. Initially, all nodes computed their neighbour's trust values, considering factors such as indirect and direct trust values, residual energy, and volatilization factor. This approach aimed to provide defence against various attacks. Secondly, for any source node requiring data transmission, the routing request packet was forwarded to neighbours in a multipath setting, persisting till it reached the BS at the endpoint. The study in [11] introduced an energy-efficient, low-complexity data security model for WSN using an encryption mechanism based on a linearly complex voice inspired by the GSM model.

This model facilitated energy-efficient and secure routing, achieving optimal performances in the face of dynamically changing network conditions and varying counts of malicious nodes. The research also proposed a novel mathematical model designed to enhance the total possible combinations of shift registers, thereby reinforcing the security of the data encryption mechanism - a unique contribution not previously explored in this context. Particle-Water Wave Optimizer for secured routing was presented in [12], which designs the P-WWO model by combining Water Wave Optimization (WWO) with Particle Swam Optimization (PSO). The work in [13] introduced a secured routing approach for WSNs based on trust computations. The algorithm analyzed the security attack status within WSN. Drawing upon the specific features of WSN, the study proposed a safety trust evaluation mechanism tailored for WSN. In [14], an Energy-Efficient-based Secure Routing Protocol (EESRP) was introduced, incorporating elements of optimization algorithms, trust, and critical management.

The deployment of node locations was initially computed with their respective values of trust. The secure transmission of packets was ensured by employing a combination of Elliptic Curve Cryptography (ECC) and Digital Signature Algorithm (DSA). The protocol further integrated trust, key, location, and energy parameters, utilizing PSO and the Harmony Search (HS) approach to determine the safest, most efficient, and shortest paths. A Multilevel EE Clustering protocol with Secure Routing (MEECSR) was presented in [15], which used probabilistic random walking and energy balancing to prevent difficulties in WSN. A Review on Secured and EE Routing was submitted in [16], which presented a brief review of various secure and EE routing protocols in WSNs, outlining their underlying principle and operations.

A P-SMO algorithm was presented in [17], which integrated PSO and Spider Monkey Optimization (SMO) algorithms to define optimal routes effectively. A low-energy secure routing protocol was presented in [18], which worked based on the multi-objective ACO algorithm. In [19], a routing scheme focused on lightweight security and privacy awareness was introduced. This scheme incorporated several cryptographic techniques, including ECC, symmetric encryption, scalar blinding, and a modified Diffie-Hellman key exchange protocol. These elements collectively formed

an additive perturbation, contributing to data integrity while ensuring effective authentication for confidentiality during routing. In [20], a practical trust-based reliable communication strategy was introduced to mitigate the impact of selfish nodes. The proposed scheme, TASRP, adopted a hybrid trust model and utilized trust scores, residual energy levels, and path lengths as factors in a multifactor routing approach.

The goal of TASRP was to establish safe routing paths within trusted nodes while minimizing energy utilization. The multifactor process involved selecting trusted nodes for data forwarding, contributing to shorter routing paths and reducing overall energy consumption. In [21], the multi-objectives optimization issue for WSN was defined, and an algorithm named Lightweight Secured Routing (LSR) was introduced to address this optimization challenge in WSNs specifically. The LSR algorithm incorporated various components, including ACO, an adaptive security approach utilizing indirect and direct trust computations, a hybrid deployment approach using uniform and 2-D Gaussian distributions, an adaptive QoS framework, and an adaptive connectivity approach employing a suitable communication radius. Together, these elements aimed to solve the complex issues. In [22], an Intelligent Clustering approach for Intelligent Transportation Systems (ITS), called ICITS, was introduced.

This approach involved the selection of CHs through a hybrid optimization method known as GA-BAT, which integrated the strengths of GA and BAT Algorithm (BA). The framework was specifically designed for application in road transport within military areas, where strict demands for security and reliability existed, especially in collecting data from deployed SNs. In [23], an Energy-Efficient Data Aggregation Mechanism (EEDAM) secured by BC was introduced. This mechanism employed a data aggregation approach at the cluster level to conserve energy. Additionally, edge computing was utilized to deliver on-demand trusted services to the IoT with minimal delay. Blockchain technology was integrated within a cloud server to validate the edge and ensure the provision of secure services to the IoT. In [24], a hierarchical trust management model tailored for Software-Defined WSNs (SDWSNs), referred to as TSW, was implemented to identify potential threats within the network.

TSW aimed to foster cooperation among nodes and aid decision-making in the forwarding phase. This trust management scheme assessed the trust of participating nodes and facilitated the identification of malignant behaviours at different levels of the model's architecture. In [25], BC was implemented on BSs and CHs for register nodes utilizing their credentials and addressing diverse security problems. An ML model, Histograms Gradient Boost (HGB), was also deployed on BSs to categorize nodes as legitimate or abnormal. If a node was recognized as strange, its registration was cancelled from the networks; for legitimate nodes, data was saved in the Interplanetary Files Systems (IPFS). IPFS stored information in segments, generating a hash for each segment in the Blockchain. Furthermore, Verifiable Byzantine Fault Tolerances (VBFT) were utilized rather than Proof of Works (PoW) for transaction and consensus validation. The proposed system underwent extensive simulations using the WSN dataset, denoted as WSN-DS.

2.2. Research Analysis Summary

The literature review discovers a wide array of secure routing protocols designed for WSNs, each providing distinct advancements in the domain. In [1, 23, 25], it is described how models based on blockchain technology implement secure authentication mechanisms and data integrity verification. Trust-oriented methodologies, which have been examined in references [3, 4, 8, 9, 10], prioritize the assessment of data and collaborative trust via diverse trust mechanisms.

This ultimately improves the dependability of routing determinations. Innovative routing models, including those referenced in [5, 6, 14, 15], ensure the security and efficiency of data transmission through the implementation of encryption methods, advanced optimization algorithms, and energy-efficient approaches. The utilization of machine learning models, such as HGB in [25], and the integration of intelligent clustering in [22] respectively, demonstrate the incorporation of recent advances to improve security [26]. Furthermore, the review emphasizes the criticality of confronting the obstacles presented by malevolent nodes, as supported by references [8, 11, 13, 20]. From trust-aware routing and optimization algorithms to blockchain-based authentication, the background research examines secure routing strategies for WSNs.

These methodologies combined to maintain the goal of establishing a resilient and secure communication structure for WSNs, which is critical for the effective incorporation of IoT devices and guarantees an exceptional quality of service. The above-analyzed approaches suffer from achieving higher performances in secure routing and other QoS metrics.

3. Proposed LDSFNR Model

The LDSFNR routing protocol starts with discovering the routes available according to the geographic topology of the network. With the ways available, the source node computes CTS according to the behaviour, transmission rate, retransmission rate and latency values using the transmission trace available.

According to the CTS score, an optimal, more secure route has been identified, and data packets are transmitted through the route selection. By receiving the data packet, the intermediate kth hop computes the PTS for the route given.

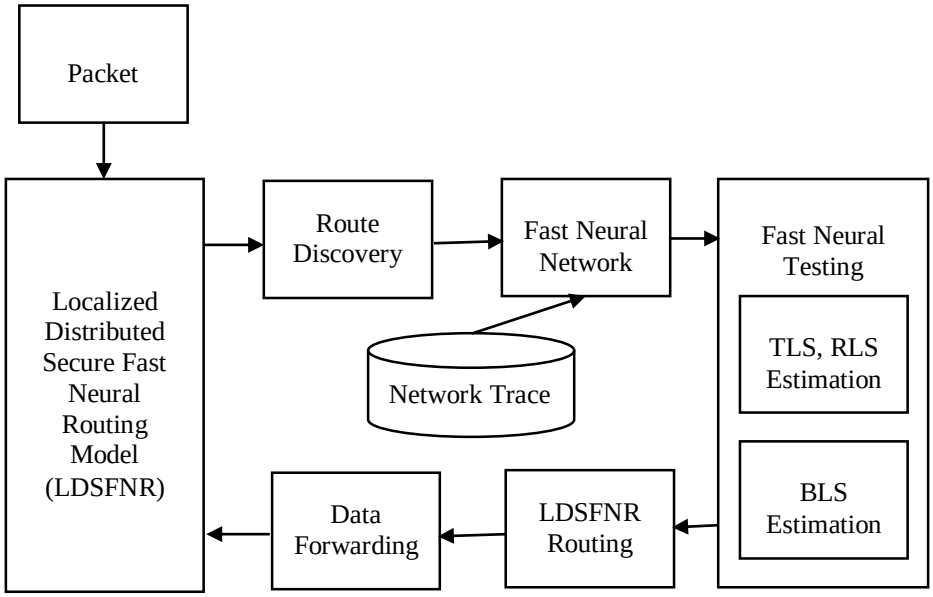

Fig. 1 LDSFNR routing protocol architecture

According to the value of PTS, the intermediate node detects the secure way and forwards the data packet. The CTS and PTS values are measured by training the traces with NN, and at the test phase, the network returns the value. The network has five layers, which replace the concerned PTS and CTS scores. Based on the importance of PTS, the intermediate node forwards the data packet. The workflow of the protocol is presented below. The working model of the LDSFNR routing protocol is represented in Figure 1, which details the workflow.

3.1. Route Discovery

The proposed LDSFNR routing protocol executes route discovery according to the broadcast nature. The model generates an LDSFNR route discovery message, which is added with the sequence number, source ID, and destination ID. The LDSFNR_RD message has been broadcast on the network.

By receiving the LDSFNR_RD message, the neighbours verify their route trace and neighbour trace. If they have the route, they generate an LDSFNR_RR message with the node ID added at the end of the route data. Otherwise, they add their ID at the end of the route sequence and multicast the packet to their neighbours. Similarly, the packets are flooded throughout the network, and the source node accepts the LDSFNR_RR messages.

The source node extracts the route sequence from the route reply received and adds it to the route trace. The route reply packet contains two pieces of information: the route sequence and the transmission table. The source node extracts the details of the transmission table and updates it with its own to support routing.

Algorithm
Input : Route Trace RTR, Node Trace NTR, Transmission Trace TTR, Packet P
Obtain : Route Trace RTR, Node Trace NTR, Transmission Trace TTR

Start
Read RTR, NTR, TTR, P.
Generate LDSFNR_RR = {SourceId, P.Destination}
Initialize Broadcast Timer.
Broadcast LDSFNR_RR.
While Timer Runs
Intermediate Node receives LDSFNR_RD.
If Route Available, then
Generate LDSFNR_RD= {Add Node id to route sequence, Add transmission table}
Send to the source node.
Else
Add node ID to route sequence.
Add transmission table to LDSFNR_RD packet.
Broadcast in the network.
End
Source receives LDSFNR_RR packet.
Extract route sequence and add to RTR.
Extract the transmission table and update it to transmission trace TTR.
End
Stop

The route discovery approach detects the route sets available to reach the destination and collects the transmission traces of different nodes to support efficient routing.

3.2. FNN Training

The LDSFNR routing approach trains the FNN according to the transmission trace collected at the route discovery phase and the transmission trace maintained by the individual. The method extracts various features of different nodes from the transmission trace, like transmission rate, retransmission rate, number of drops, number of delayed transmissions, exact forwarding, throughput, and latency. Such features extracted are converted into a feature vector. For each node in the network, the method generates a neuron and initializes it with the features mentioned above. The network has been designed with five layers, which contain three intermediate layers responsible for computing Transmission Legacy Score (TLS), Retransmission Legacy Score (RLS) and Behavior Legacy Score (BLS). The output layer neurons return three outputs of such legacy scores. The trained network has been used towards route selection.

3.3. FNN Training

The Fast Neural testing algorithm measures the trust value of any route given, either partially or entirely. The model detects the nodes available in the way for the given path R. For each sensor node or IoT device present in the routes, the model collects the transmission trace and converts it into a feature vector. The feature vector has been given as an input to the already trained NN. The intermediate layer neurons compute the TLS, RLS and BLS values. Such computed values are produced as a result of the output layer. The neurons compute TLS as follows:

$$\text{TLS} = \frac{Tr}{\left.\sum_{i=1}^{size(R)} R(i).Tr?R(i).NodeId!=NodeId \middle/ Size(R)\right.} \times \frac{DC}{TT} \quad (1)$$

Where Tr-Transmission Rate, DC-Drop Count, and TT-Total Transmission.

Similarly, the RLS is measured as follows:

$$\text{RLS} = \frac{RTr}{\left.\sum_{i=1}^{size(R)} R(i).RTr?R(i).NodeId!=NodeId \middle/ Size(R)\right.} \times \frac{DC}{TT} \quad (2)$$

Also, the BLS is measured as follows:

$$\text{BLS} = \frac{DC}{DT} \times \frac{EF}{Th} \times \frac{DC}{L} \quad (3)$$

Where EF is the number of Exact Forwarding, DT is the number of Delayed Transmissions, Th is Throughput, and L is Latency. The TLS, as mentioned above, RLS, and BLS values are measured for each node present in the route given. The method performs testing for n number of times by providing the feature vector of each hop present in the way. At each iteration, the network returns a set of TLS, RLS, and BLS values to select routes.

3.4. LDSFNR Routing

The LDSFNR routing algorithm executes route selection by computing trust measures in a localized distributed way. The source node performs route discovery and calculates CTS value by passing the features of nodes present in the route. The method uses a Fast Neural testing algorithm for each path to obtain TLS, RLS and BLS values. With the values obtained, the model calculates the CTS value initially to identify the most effective route in the network.

The packet with the k-hop value has been passed to the first neighbour of the route. Now, the intermediate node checks the hop count and measures the PTS value using the FNN. With the PTS value, the intermediate node will choose an optimal route to forward a data packet. This will be performed at various parts of the path till the packet reaches the destination.

As the nodes in the route maintain the transmission trace and train their network according to the traces collected at various transmissions, the intermediate node would choose the most secure path according to the local knowledge.

Algorithm
Given : Dp- Data packet, TT- Transmission Trace.
Obtain : Null

Initiate
Read Dp, TT.
Route Trace RT = Perform route discovery.
Identify node set Nset =

$$if\ TT(i).NodeId \nexists Nset\ then\ Nset \cup TT(i).NodeId \quad \begin{matrix} size(TT) \\ i=1 \end{matrix}$$

Initialize Feature Vector Set Fevs.
For each node, n
Generate Feature Vector Fv.
Fv = {TT(n).Tr, TT(n).RTr, TT(n).DC, TT(n).DT, TT(n).EF, TT(n).Th,TT(n).L}
Fevs = $\sum(fv \in Fevs) \cup Fv$
Perform Fast Neural Training.
End
Initialize k.
For each route, r
Node set Ns = $\sum Nodes \in r$
For each node, n
{TLS, RLS, BLS} = Perform FNN Testing
End

$$\text{Compute CTS} = \left(\frac{\left.\sum_{i=1}^{size(r)} Sum(r(i).RLS) \middle/ size(r)\right.}{\left.\sum_{i=1}^{size(r)} Sum(r(i).TLS) \middle/ size(r)\right.} \times \left.\sum_{i=1}^{size(r)} Sum(r(i).BLS) \middle/ size(r)\right.\right) \times \frac{1}{IoTC}$$

End
Route R = Choose a route with maximum CTS.
Forward data packet Dp with route R.
Intermediate node receives Dp and k.
Compute hop count Hp = Dist(source,Intermediate node)
If Hp == k then
Route R = Substring (R, k, node id)
For each node, n
{TLS,RLS,BLS} = Perform Fast Neural Testing (n,Fves(n))
End
Compute LTS = $\left(\frac{\sum_{i=1}^{size(r)} Sum(r(i).RLS) \Big/ size(r)}{\sum_{i=1}^{size(r)} Sum(r(i).TLS) \Big/ size(r)} \times \sum_{i=1}^{size(r)} Sum(r(i).BLS) \Big/ size(r)\right) \times \frac{1}{IoTC}$
Route R = Choose a route with maximum CTS.
Forward data packet Dp with route R.
End
Stop

The proposed LDFSNR routing algorithm discovers the routes available and calculates the values of CTS and LTS to execute secured routing to maximize the QoS of the network.

4. Results and Discussion

The LDFSNR routing model was implemented with a Network Simulator and experimented for its performances under different factors. The outcomes attained were compared with the results of other models.

Table 1. Evaluation details

Simulation Parameters	Values
Tool	Ns2
Number of sensor nodes	200
Number of IoT devices	15
Simulation time	10 Minutes

The simulation constraints used towards performance evaluation are presented in Table 1, and the varying count of nodes in the networks measures the performances. The performances of the model are measured in the following parameters.

Performance of Secure Routing: Secure routing defines the model's ability to route the data packets securely. It is evaluated based on the total threats identified in routing for the given number of transmissions.

$$SR = \frac{Number\ of\ threats\ identified}{Number\ of\ transmission\ performed} \times 100 \quad (4)$$

Throughput Performance: The throughput performance is the QoS metric, representing the performance of methods in transmitting the data. It is evaluated according to the total packets delivered on time for the given count of packets.

$$Throughput = \frac{Number\ of\ Bytes\ delivered}{Total\ Bytes\ transmitted} \times 100 \quad (5)$$

Energy Efficiency: The model's performance is computed for their EE. It has been measured according to average joules of energy spent on the number of transmissions. It has been calculated as follows:

$$EE = \frac{Sum\ of\ all\ joules\ spent}{Total\ no\ of\ transmissions} \times 100 \quad (6)$$

4.1. Test Case 1 (Different Number of k)

The method's performance in routing the data packets through a secure route has been measured with specific considerations such as the size of intermediate localized trust estimation. For example, if the path has 15 hops, and the selected k is 5, then the trust measurement will be performed at node number 5 and node number 10. In each case, the performance of the routing scheme is measured on each performance metric mentioned and presented in this part.

Table 2. Analysis of security performance vs Number of intermediate trust measurement

Secure Routing Performance % vs k			
Nodes	**10**	**20**	**30**
EESRP	71	68	61
MEECSR	75	71	67
LSR	77	74	71
LDFSNR	87	93	97

The performance of methods in secure routing according to the number of intermediate trust evaluations in the route is calculated and represented in Table 2. The results demonstrated that the proposed LDFSNR maintains the performance in all the test cases. By measuring trust at different intervals, the security performance is improved.

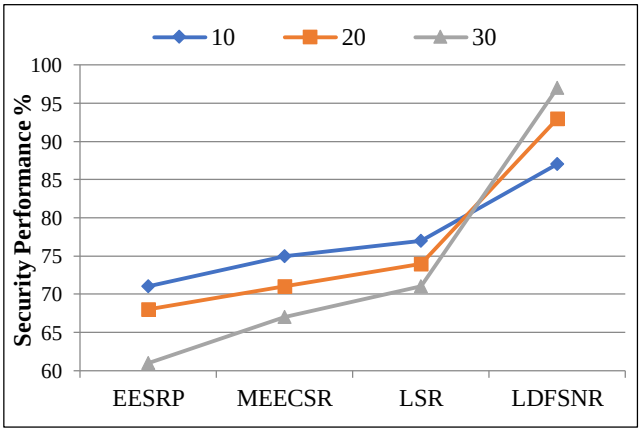

Fig. 2 Analysis of security performance vs k

The performance in secure routing provided by various methods was measured in the presence of the number of intermediate route selections and depicted in Figure 2. However, the LDFSNR achieves improved routing performances compared to other schemes.

The throughput result of different models in varying counts of intermediate trust measurements is conducted and presented in Table 3, where the proposed LDFSNR has obtained the best throughput performances in every test case considered.

Table 3. Analysis of throughput performance vs k

Throughput Performance vs k Intermediate Trust Analysis			
Nodes	**10**	**20**	**30**
EESRP	69	64	57
MEECSR	74	69	65
LSR	79	74	68
LDFSNR	87	92	97

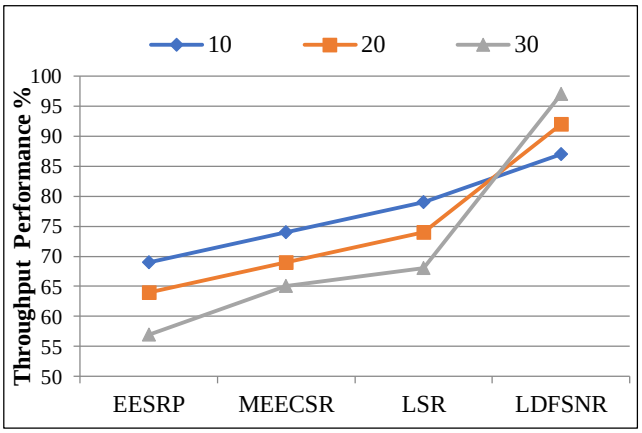

Fig. 3 Analysis of throughput performance vs k

The throughput performance of various schemes in the presence of different numbers of intermediate trust evaluations is measured and compared in Figure 3, where the LDFSNR model obtained higher throughput than other models.

4.2. Test Case 2 (Presence of Blackhole Threat)

The WSN is highly open to Blackhole attacks as they are involved in cooperative transmission. The presence of IoT devices encourages the Blackhole attack, which would divert the traffic towards specific nodes, which would learn the network behaviour.

This highly degrades the results of the entire network model. The proposed LDFSNR routing model performs security checks at different k intermediate nodes, which involve identifying the secure route to transmit the packet. This can be used in handling Blackhole attacks, and the method's performance is measured in the presence of Blackhole attacks and validated with other models.

To analyze the versions of the technique at this condition, the diverse nodes in the network are considered, and the performance is measured to compare with the performance of others. The performance of methods in secure routing according to the presence of a Blackhole attack in the network is calculated and compared.

The proposed LDFSNR model enhances the security performances compared to other approaches. As the proposed routing protocol measures the trust of the route at different intermediate levels, the secure routing performance is improved.

Table 4. Security performances vs Presence of Blackhole attack

Secure Routing Performance % vs (Presence of Blackhole Attack)			
Nodes	**50**	**100**	**200**
EESRP	71	74	79
MEECSR	75	79	83
LSR	77	81	85
LDFSNR	87	92	97

The security performance of various approaches in the presence of a Blackhole attack is measured and shown in Figure 4.

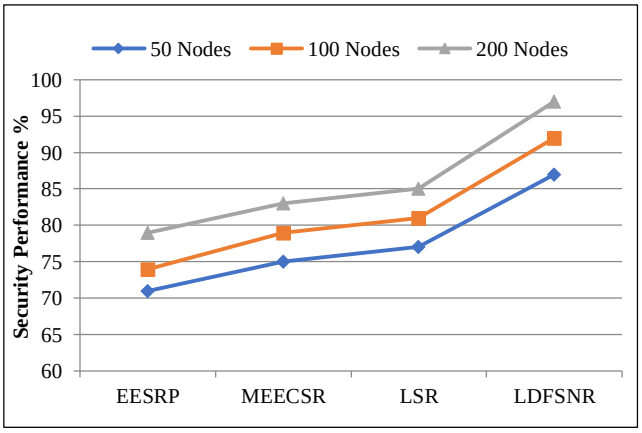

Fig. 4 Analysis of security performances vs Blackhole attack

Table 5. Throughput performance vs Blackhole attack

Throughput Performance vs Blackhole Attack			
Nodes	**50**	**100**	**200**
EESRP	69	74	79
MEECSR	74	79	85
LSR	79	84	88
LDFSNR	88	93	98

The throughput performance of different approaches in the presence of a Blackhole attack is considered and measured. The analysis result is presented in Table 5, where the proposed LDFSNR has obtained higher throughput in every test case considered. The throughput performance of various schemes in the presence of a Blackhole attack is measured and compared in Figure 5, where the LDFSNR model obtained higher throughput results than other models.

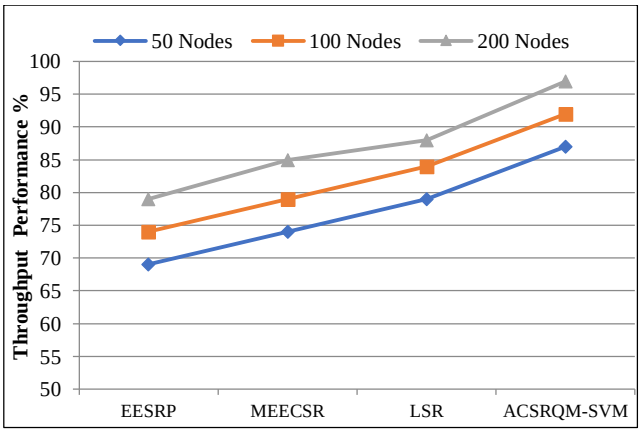

Fig. 5 Analysis of throughput performance vs Blackhole attack

4.3. Overall Performance Results

The proposed model's performance in secure routing was calculated using different numbers of nodes and compared in Table 6. The LDFSNR model enhances the security performances compared to other approaches.

Table 6. Analysis of security performances

Secure Routing Performances %			
Nodes	**50**	**100**	**200**
EESRP	71	75	81
MEECSR	75	78	85
LSR	79	82	89
LDFSNR	85	91	99

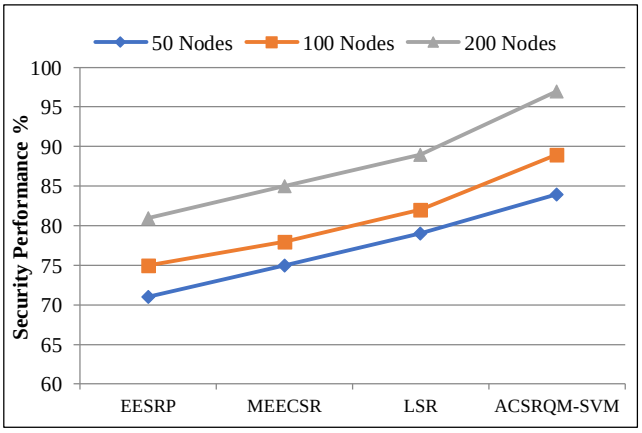

Fig. 6 Analysis of security performance

The proposed model's security result has been calculated and compared in Figure 6, where the LDFSNR model obtained higher security results than other models. The proposed model's performance in throughput achievement was measured in different numbers of nodes and compared in Table 7. The LDFSNR approach improves the throughput performances than other approaches. The performance of models in throughput achievement has been measured and compared in Figure 7, where the LDFSNR protocol achieves better throughput performances than the compared models.

Table 7. Analysis of throughput performances

Throughput Performances %			
Nodes	**50**	**100**	**200**
EESRP	64	69	74
MEECSR	71	74	79
LSR	75	79	87
LDFSNR	84	89	97

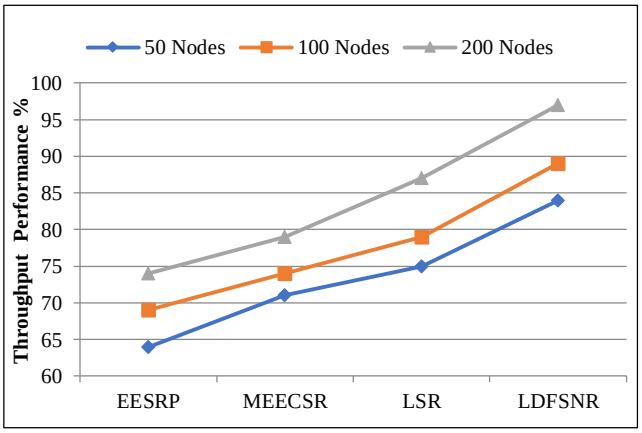

Fig. 7 Analysis of throughput performances

Table 8. Analysis of energy efficiency

Energy Efficiency %			
Nodes	**50**	**100**	**200**
EESRP	61	65	69
MEECSR	67	72	75
LSR	72	76	79
LDFSNR	83	87	94

The proposed model's performance in energy efficiency was calculated using different numbers of nodes and compared in Table 8. The proposed LDFSNR approach improves the energy efficiency performance compared to other techniques.

The proposed model's energy efficiency performance was calculated and compared in Figure 8, where the LDFSNR model achieves higher performance than different approaches.

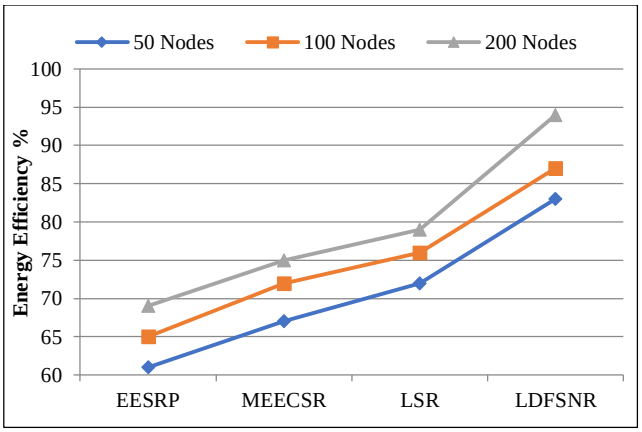

Fig. 8 Analysis of energy efficiency

4.4. Advantages of the LDSFNR Model

The proposed LDSFNR model exhibits notable advantages in EE, throughput, and secure routing compared to existing models like EESRP, MEECSR, and LSR. In test case 1, where different numbers of hops (k) are considered for trust estimation, the LDSFNR model demonstrates superior performance across various metrics.

The method's ability to measure trust at specific intermediate nodes contributes to efficient routing and enhances overall network performance. Moreover, in test case 2, which evaluates the model's performance in the presence of Blackhole threats, the LDSFNR model showcases robust security checks at different intermediate nodes (k).

This feature proves advantageous in handling Blackhole attacks, preventing traffic diversion towards malicious nodes and thereby maintaining the integrity of the network. The proposed model's effectiveness in securing data transmission in the face of potential threats, such as Blackhole attacks, positions it as a resilient solution for enhancing network security.

4.5. Limitations of the LDSFNR Model

While the LDSFNR model demonstrates notable strengths, it is essential to acknowledge potential limitations. While advantageous, the localized and distributed nature of the trust estimation mechanism may pose challenges in scenarios where dynamic network conditions or node mobility are prevalent.

Although practical, reliance on trace-based trust evaluation could introduce overhead regarding storage and computational requirements, particularly in large-scale networks. Additionally, restricting the protocol to SNs may limit its applicability in diverse network architectures where the active participation of IoT devices is crucial. The model's performance, especially in test case 2, must be further evaluated under varying network sizes to ensure scalability and robustness.

However, while the LDSFNR model exhibits notable advantages in EE, throughput, and security, addressing potential challenges related to dynamic network conditions, scalability, and broader device inclusion will be essential for its successful deployment in diverse WSN scenarios.

5. Conclusion

An efficient LDFSNR protocol is sketched in this article. The method involves discovering the routes and computing CTS measures in initial route selection with the help of FNN. The FNN is trained with a different number of nodes and layers.

The neurons are trained and designed to measure the CTS and LTS measures. The source node identifies the route with CTS, where intermediate k nodes are involved in route selection with LTS value. The proposed method improves the security performance and challenges different threats in the network. The LDFSNR protocol enhances security performance and maximizes the QoS performance.

Future research directions for the presented LDSFNR protocol include exploring its adaptability to dynamic network conditions, incorporating self-learning mechanisms for evolving threats, assessing scalability for more extensive networks, optimizing energy efficiency in resource-constrained nodes, and evaluating real-world applicability through simulations and practical deployments. These efforts aim to enhance the protocol's resilience, efficiency, and effectiveness in diverse WSN and IoT scenarios.

Acknowledgements

The authors thank the St. Peter's Institute of Higher Education and Research, Chennai, Tamilnadu, India, for their support and motivation throughout this research.

References

[1] Wassim Jerbi et al., "A Novel Blockchain Secure to Routing Protocol in WSN," *2021 IEEE 22nd International Conference on High Performance Switching and Routing (HPSR)*, pp. 1-6, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[2] Mallanagouda Biradar, and Basavaraj Mathapathi, "Secure, Reliable and Energy Efficient Routing in WSNs: A Systematic Literature Survey," 2021 *International Conferences on Advance in Electrical, Computing, Communications and Sustainable Technologies (ICAECT)*, pp. 1-13, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[3] Puja Rani, and Neetesh Kumar Gupta, "Composite Trusts for Secured Routing Strategy through Energy-Based Clustering in WSNs," *2021 International Conferences on Advance in Electrical, Computing, Communications and Sustainable Technologies (ICAECT)*, pp. 1-6, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] Majid Alotaibi, "Improved Blowfish Algorithms-Based Secure Routing Techniques in IoT-Based WSN," *IEEE Access*, vol. 9, pp. 159187-159197, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[5] M. Manisha Rathee et al., "Ant Colony Optimization Based Quality of Service Aware Energy Balancing Secure Routing Algorithm for Wireless Sensor Networks," *IEEE Transaction on Engineering Managements*, vol. 68, no. 1, pp. 170-182, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[6] C. Senthilkumar et al., "Experimental Analysis of Secure Routing Protocols Establishment over Wireless Sensors Networks," *2021 5th International Conferences on Trend in Electronic and Informatics (ICOEI)*, pp. 691-698, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[7] Muhammad K. Khan et al., "Hierarchical Routing Protocols for Wireless Sensor Networks: Functional and Performance Analysis," *Journal of Sensors*, vol. 2021, pp. 1-18, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[8] Huangshui Hu et al., "Trusts Based Secured and Energy Efficient Routing Protocols for Wireless Sensors Network," *IEEE Access*, vol. 10, pp. 10585-10596, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[9] Weidong Fang et al., "MSCR: Multidimensional Secure Clustered Routing Scheme in Hierarchical Wireless Sensors Network," *EURASIP Journal on Wireless Communication and Networking*, vol. 14, pp. 1-20, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[10] Huangshui Hu, "Trust-Aware Secured Routing Protocols for Wireless Sensors Network," *ETRI Journal*, vol. 43, no. 4, pp. 674-683, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[11] M. Saud Khan et al., "A Low-Complexity, Energy-Efficiency Data Secure Models for Wireless Sensors Networks Based on Linearly Complex Voices Encryption Mechanisms of GSM Technology," *International Journal of Distributed Sensor Networks*, vol. 17, no. 5, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[12] Pradeep Sadashiv Khot, and Udaykumar Naik, "Particle-Water Wave Optimizations for Secured Routing in Wireless Sensors Networks Using Cluster Heads Selections," *Wireless Personal Communication*, vol. 19, pp. 2405-2429, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] Qingzeng Xu, "Wireless Sensors Network Secured Routing Algorithms Based on Trust Values Computations," *International Journal of Internet Protocol Technology*, vol. 14, no. 1, pp. 10-15, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[14] S. Sudha Mercy, J.M. Mathana, and J.S. Leena Jasmine, "An Energy-Efficient Optimal Multi-Dimensional Locations, Keys and Trust Managements Based Secured Routing Protocols for Wireless Sensors Network," *KSII Transaction on Internet and Information System*, vol. 15, no. 10, pp. 3834-3857, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[15] L. Rajesh, and H.S. Mohan, "A Multilevel Efficient Energy Clustering Protocols with Secured Routing (MEECSR) in WSN," *International Journal of Applied Science and Engineering*, vol. 18, no. 2, pp. 1-6, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[16] T.G. Ganga, and R.A. Roseline, "A Review on Secured and Energy-Efficient Routing Protocol in Wireless Sensors Network (WSNs)," *International Journal of Engineering Research and Technology*, vol. 10, no. 3, pp. 196-202, 2021. [Google Scholar] [Publisher Link]

[17] Pradeep Sadashiv Khot, and Udaykumar Laxman Naik, "Cellular Automata-Based Optimized Routing for Secured Data Transmissions in Wireless Sensors Network," *Journal of Experimental and Theoretical Artificial Intelligences*, vol. 34, no. 3, pp. 431-449, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[18] Xueli Wang, "Low-Energy Secured Routing Protocols for WSN Based on Multi-Objective Ant Colony Optimization Algorithms," *Journal of Sensor*, vol. 2021, pp. 1-9, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[19] Oladayo Olufemi Olakanmi, "A Lightweight Security and Privacy-Aware Routing Scheme for Energy-Constraints Multi-Hop Wireless Sensors Network," *International Journal of Information and Computers Security*, vol. 15, no. 2, pp. 231-253, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[20] Tayyab Khan, and Karan Singh, "TASRP: A Trust Aware Secured Routing Protocols for Wireless Sensors Network," *International Journal of Innovative Computing and Application*, vol. 12, no. 2, pp. 108-122, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[21] Aditya Pathak, Irfan Al-Anbagi, and Howard J. Hamilton, "An Adaptive QoS and Trusts-Based Lightweights Secured Routing Algorithms for WSNs," *IEEE Internet of Thing Journal*, vol. 9, no. 23, pp. 23826-23840, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[22] Sandeep Verma et al., "Intelligent and Secured Clustering in Wireless Sensors Networks (WSN)-Based Intelligent Transportations System," *IEEE Transaction on Intelligent Transportations System*, vol. 23, no. 8, pp. 13473-13481, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[23] Adeel Ahmed et al., "An Energy-Efficient Data Aggregation Mechanisms for IoT Secured by Blockchains," *IEEE Access*, vol. 10, pp. 11404-11419, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[24] Manaf Bin-Yahya, Omar Alhussein, and Xuemin Shen, "Securing Software-Defined WSNs Communications via Trusts Managements," *IEEE Internet of Things Journal*, vol. 9, no. 22, pp. 22230-22245, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[25] Muhammad Nouman et al., "Malicious Nodes Detections Using Machine Learning and Distributed Data Storages Using Blockchains in WSN," *IEEE Access*, vol. 11, pp. 6106-6121, 2023. [CrossRef] [Google Scholar] [Publisher Link]

[26] C. Narmatha, "A New Neural Network-Based Intrusion Detection System for Detecting Malicious Nodes in WSNs," *Journal of Computational Science and Intelligent Technologies*, vol. 1, no. 3, pp. 1-8, 2020. [CrossRef] [Google Scholar] [Publisher Link]