SSRG International Journal of Electronics and Communication Engineering
ISSN: 2348-8549/ https://doi.org/10.14445/23488549/IJECE-V10I6P108

Volume 10 Issue 6, 92-103, June 2023
© 2023 Seventh Sense Research Group®

Original Article

Dynamic IoT Specific Inclusion Exclusion Strategic Secure Routing for Improved QoS Development in Industrial Networks

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

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

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

Received: 01 April 2023 Revised: 27 May 2023 Accepted: 15 June 2023 Published: 30 June 2023

Abstract *- Industrial network-based secure routing has been investigated in many articles. Also, the entry of IoT devices has been adapted to different industrial environments. The presence of Internet of Things (IoT) devices would support the performance development in data transmission. Numerous approaches are discussed in the literature but struggle to achieve the expected performance. IoT devices are standalone devices not part of the network, and trust in such devices is highly questionable. However, the QoS metrics can be improved by including such devices in data transmission. On the other side, measuring the trust of such IoT devices is most important in the routing procedure. Considering this, an IoT-specific Inclusion and Exclusion Strategic Secure Routing scheme (IESSR) is presented in this article. The routes available to reach the destination are identified initially. Further, a list of IoT devices in each route is identified. Also, the transmission frequency encountered is computed on different nodes and IoT devices. According to the status of transmission, and other features, the method computes the General Secure Route Measure (GSRM), Inclusion Specific Secure Route Measure (ISSRM), and Exclusion Specific Secure Route Measure (ESSRM). Using both measures, the method would compute the value of transmission strength for different routes. According to transmission strength, the optimal route for data transmission is selected.*

Keywords *- Industrial network, Secure routing, IoT, Inclusion, Exclusion, IESSR, ISSRM, ESSRM, QoS.*

1. Introduction

Growing technology in the communication sector has been used on several occasions. The organizations have their units which are distributed in different locations. However, connecting them to enable communication between various units is essential, which smoothens the functioning of the industries. The industrial networks are designed to support the functioning of different industrial units. It has been framed by deploying different networks within the units of the organization. Wireless sensor networks are generally deployed to support communication between different industrial units. The support of WSN in rapidness and least costs has been highly incorporated in different industries.

The industrial network covers the nodes for communication through several networks, not just WSN and several other networks. In any network, there are many constraints to consider regarding routing. Any node in the network cannot directly communicate with other nodes as they have boundaries in terms of communication, transmission range, and energy. So, all these restrict the communication of nodes directly with the other nodes. In general, the nodes of any network or the user accesses different services the network provides to perform any process. Such network services are converted as transmission packets to be transmitted through various nodes. This is where the security issue comes in. When a malicious node exists in the transmission route, it performs different attacks at both service and data levels. In service-level attacks, the packets belonging to a specific service would be targeted. In contrast, in the case of data level, all the data will be targeted to perform different malicious actions.

Security and Energy efficiency, both of which perform crucial roles in Quality of Service (QoS), remain hard in the WSN-assisted Internet of Things because of the resource-constrained and open nature of the network. Many sensor nodes make up a WSN to carry out their functions. In most cases, these nodes have limited resource availability due to the limited time their battery energy can be maintained. As a result, the most critical concern in WSN is energy efficiency.

In the same way, the Internet of Things is a developing paradigm that enables the introduction of even more intelligent applications. The Internet of Things is combined with WSN, which has applications in smart cities, transportation, healthcare, etc. However, this combination brings several issues, including security, interoperability, scalability, and energy efficiency. In addition, the sink node of mobile, effective clustering, routing, and data aggregation in WSN contribute to enhanced energy efficiency. In this regard, cluster formation is applied in many research activities to improve energy efficiency. The sensor nodes in a cluster-based network are divided into smaller clusters according to various criteria. The formation of clusters improves the quality of service and energy efficiency through data aggregation. In addition, constructing the network in the most efficient possible structure increases the network's energy efficiency. The fact that the WSN-IoT network includes both IoT devices such as RFID and sensors as well as users of IoT who may access the data from IoT devices is the primary characteristic of this type of network. As a result, a significant amount of research is being done on networks of WSN-IoT to enhance energy efficiency and service quality. In addition, optimal routing was carried out in the network to improve service quality and energy efficiency. The amount of data that is lost and the amount of energy that is consumed will both be significant if an effective routing method is not implemented. The signal's travel distance increase is the root cause of this degradation. Therefore, appropriate routing is required for WSN-IoT networks to use energy efficiently. The effectiveness of Internet of Things applications can also be improved using optimal routing. The presence of threats can be overlooked by performing secure routing.

Industrial network routing uses energy, traffic, and hops-however, the methods struggle with security achievements. Also, the QoS of the network greatly depends on how routing is performed, the throughput performance, energy, and so on. To improve the QoS of the network, a novel real-time inclusion and exclusion secure strategic routing (IESSR) are sketched here. Recently, IoT devices have been primarily used in different private locations. Such devices can be used in support of QoS development. However, the IoT devices are not part of the network and cannot be trusted. So, selecting a route must be performed by considering different constraints. It is necessary to analyze the impact of including the IoT device and excluding the IoT device in data transmission. Factors like IoT devices, traffic, and bandwidth must be considered to develop the QoS performance of industrial networks. By considering all this, the proposed model has been designed for QoS development and secure routing [1, 2].

The objectives of this research work include:

- Improving the QoS metrics and measuring the trust of IoT devices is most important in the routing procedure.
- To propose the real-time inclusion and exclusion secure strategic routing (IESSR) model for the QoS network.
- To measure the status of transmission and other features, the method computes the General Secure Route Measure (GSRM), Inclusion Specific Secure Route Measure (ISSRM), and Exclusion Specific Secure Route Measure (ESSRM).
- The performances of the research model are evaluated based on packet delivery ratio (PDR), secure routing performances (SRP), throughput, and packet drop ratio.
- The performances of this research model are validated by comparing it with various routing models analyzed from the related works.

This paper is structured as follows with the remaining sections: Section 2 presents the analysis of the literature review of the related works. Section 3 explains the proposed Inclusion Exclusion Strategic Secure Routing (IESSR) model, including the presentation of General Secure Route Measure (GSRM), Inclusion Specific Secure Route Measure (ISSRM), and Exclusion Specific Secure Route Measure (ESSRM).

Section 4 evaluates the performances of the IESSR model by comparing it with various models analyzed from the literature review, and finally, section 5 discusses the conclusion and future works.

2. Literature Review

Several approaches exist towards secure routing in industrial networks, and this section details a set of approaches to the problem. In [3], a geographic routing with a biometric authentication approach is sketched, which adapts the Biometrics based Authenticate Geographical Opportunistic Routing (BAGOR) model for handling DoS attacks with the help of Biometrics. The work in [4-6] provided a conceptual outline of a cryptographic technique for secure routing that is based on digital certificates. Using a hybrid secure routing strategy incorporating reactive and proactive strategies was suggested. To create routes, the protocol periodically worked to develop the MANET topology and MST proactively while simultaneously working to generate source-destination routes reactively.

The security association (SA) was created among the pair of source and destination to authenticate each party, and a secret key was generated by employing either Shamir's (2,2) threshold secret sharing or Diffie-Hellman keys exchanges protocol. This was done for the sake of ensuring the data's integrity. With the implementation of this protocol, each node was verified via a digital certificate, each neighbour cluster was verified by using a node that was the centre of formation for the cluster, and the MANET became dependable. Asymmetric decryption and encryption method, employing the secret keys determined in SA, was utilized to transmit data securely.

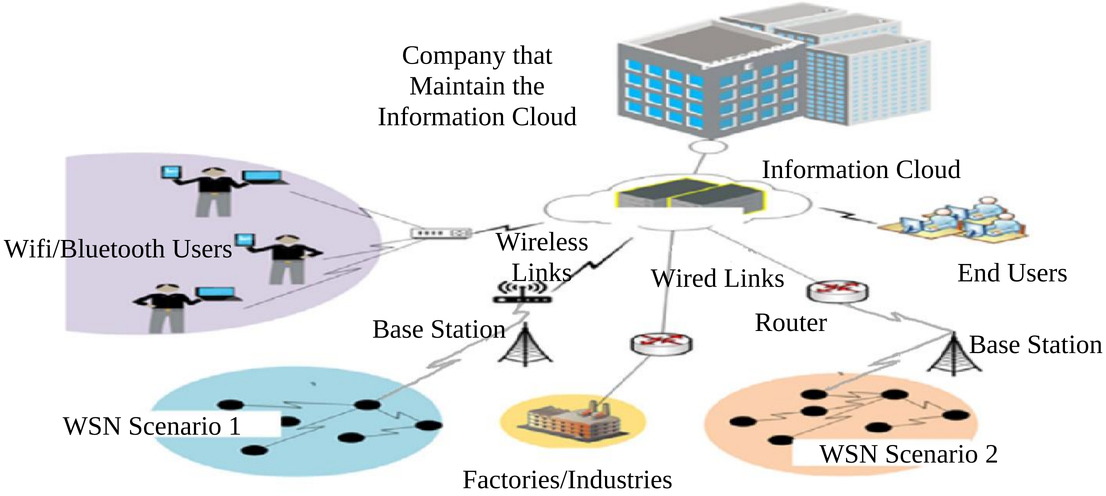

Fig. 1 WSN-IoT-based industrial networks architecture

A strategy to handle numerous attacks using forensics based on neural networks is provided in [7]. In a MANET, forensic methods were used to detect and prevent various assaults along with neural networks, such as User-to-Root (U2R), probe, vampire, and Denial-of-Service (DoS) attacks. This strategy identified potential threats to the network, took preventative measures against those threats, and reduced energy usage, all indicators of the network's increased longevity. More advanced approaches in machine learning may have been utilized to secure the network against multiple attacks [8].

In [9], there is a presentation of a differentiated secure opportunistic routing (DSOR) based on game theory. A trust calculation scheme was presented in DSOR. This scheme considers both the forwarding capability of a node and the status of various flows simultaneously. The transmission was given a flow priority determination technique in addition to multiple types of flows-oriented forwarding candidate selection. Both of these were developed using a game theoretic approach.

A QoS-based energy balancing secure routing (QEBSR) protocol was proposed in [10]. This type of routing was carried out by assessing trust based on the delay factors. The QEBSR strategy considered the quality of service, security criteria, and the necessity for energy balancing. It adapted ACO to choose the routing path in the network. The QEBSR protocol improved performance by extending the network's lifetime, lowering latency, and routing data through trusted nodes.

A blockchain-based intrusion prevention framework was proposed in [11] as a lightweight, dependable, end-to-end secure approach for safe routing in mobile IoT based on WSN. This approach was described as being lightweight. This intrusion prevention framework was designed to extend network lifetimes with lightweight, secure data routing among mobile IoT devices based on WSN [12, 13]. A secure routing strategy that can handle black hole attacks is addressed based on a modified version of AODV's sequence number. An algorithm was proposed [14] based on transforming the sequence numbers in control packets, specifically the route reply packets (RREP), in the widely utilized AODV routing protocol. The goal of this algorithm was to identify black hole nodes and reduce the amount of data that was lost as a result by discarding routes that contained black hole nodes.

Similarly, an outlier identification approach utilizing AODV is provided in [15] to deal with black hole attacks. A trust-based routing protocol, S-DSR, has been presented to provide secure routing. This protocol measures trust by gathering feedback from neighbours. This protocol assists in determining the most reliable path for the safe transmission of files based on the trust information provided by the nodes in the surrounding area. This work successfully built the load-balancing mechanism to use the network's resources efficiently. This effort solved many problems that were experienced in the presence of attacks. However, it does not eliminate all the security challenges associated with an ad hoc network. A black hole attack detection and prevention strategy based on outlier identification was developed in [16] to protect the AODV routing protocol used in MANET.

The work in [17] provided a high-level overview of a model for detecting and preventing case study-based intrusions. An algorithm was proposed that uses profile (behaviour)-based analysis to detect intrusions, and for multi-attack scenarios, a distributed-trust-based preventive strategy was suggested. Both of these ideas were developed. Elliptic Curves were combined with energy-efficient secure routing (EESR) to create this technology proposed in [18]. Elliptic Curves are used in the process of key exchange. The EESR protocol made the network more reliable and extended its lifespan, benefiting the system. Using sequence numbers, a trust and energy-aware secure routing paradigm, also known as TESRP, was developed to increase the system’s level of security and protect it from wormhole attacks [19]. The TESRP protocol was the finest trust-based protocol available; nevertheless, this protocol did not protect against wormhole attacks. The document referred to above presents a trust sensing secure routing mechanism (TSSRM) that takes advantage of a characteristic of nodes. TSSRM was able to increase network security in comparison to TSR in situations when numerous errors were identified occurrences. This was possible because TSSRM considered both direct and indirect trust, which gave much resistance against error-detected incidents.

In [20-22], an iterative filtering (IF) system was used to handle Collusion attacks on nodes. Based on the information obtained from various sources, it gives a trust valuation for the sensor nodes. The SHA1 hashing algorithm was utilized to ensure the confidentiality of the data. It checked the data integrity on the cluster head (CH) and found evidence of an assault on the CM, aggregator node (AN), and CH. [23] presents the Q learning-based secured routing protocol called ESRQ that measures individual nodes’ trustworthiness based on their behaviour. Because this methodology is not based on the neighbour nodes’ suggestion, it was not subject to attack types like the Bad-Mouth or Good-Mouth assaults. Additionally, this method could increase energy efficiency by minimizing the suggested trust.

A game-theoretic approach was proposed in [24] to routing to reduce overall energy usage while maintaining the layer of protection. The network had been given increased durability due to the combination of load balancing and power control. The elliptic curve digital signatures algorithm (ECDSA) controls the power of transmission, ensures the traffic load is balanced, and provides security for the interactions. Following the trust values, a trust model was constructed to ensure secure routing, and the path was followed. Detecting and localizing malicious nodes was investigated and carried out as an expansion and improvement [25, 26]. The number of issues identified from the above literature survey motivated me to design novel approaches in secure routing.

3. Inclusion Exclusion Strategic Secure Routing (IESSR) Model

The proposed model uses the network topology to find the list of routes over the node range in the network. With the routes discovered, the method finds the nodes set in the route and the IoT devices set present. The value of general secure route measure (GSRM) is measured with the node’s behaviour in the past times. Further, each route’s transmission strength (TS) value is measured according to the ISSRM and ESSRM values. Based on the values, both the value of TS is measured. With the TS value measured, route selection is performed towards secure routing in maximizing the QoS of the network. The working of the proposed IESSR model is sketched in Figure 2, and its elements are detailed in this part.

3.1. Route Discovery

The process involves identifying the routes with the network’s topology to reach the destination. Using the network topology, a set of wireless nodes is identified. For each node, the location and transmission range are identified. With the information on nodes, their types, and transmission range, the method discovers the list of routes by identifying each neighbour. Further, the list of nodes toward the destination is identified with the neighbours and their neighbours. Such identified chain of nodes has been framed as a route to reach the destination.

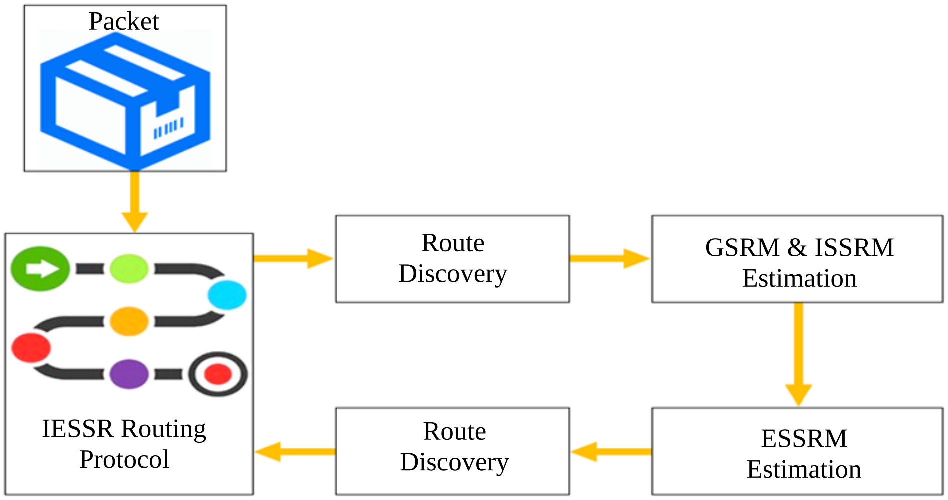

Fig. 2 Functional structure of the IESSR model

Similarly, for each first hop node, the method traverses till all the nodes being visited other than the previous hops to find the set of routes. Such identified nodes are framed as a route and added to the route set. Generated route set was utilized for selecting routes toward QoS maximization. The algorithm for route discovery is as follows:

```
Input    : Network Topology NTop, Packet P.
Output   : Route Set Rs.
Start
Read NTop, P
Destination D = P.Dest.
Find all nodes in topo Anlist = $\sum_{i=1}^{size(NTop)} Nodes \in NTop(i)$
For each node N
Fetch location LocN = $\sum_{i=1}^{size(Anlist)} Loc(Anlist(i) \rightarrow NTop)$
Fetch Transmission Range NTr = $\sum_{i=1}^{size(Anlist)} TransmissionRange(Anlist(N) \rightarrow NTop)$
End
Find neighbour list of Source S as Nlist = $\sum_{i=1}^{Size(AnList)} AnList(i).Location < TransmissionRange(S) >$
For each node Fn
Find neighbours of  Fn as FNlist = $\sum_{i=1}^{Size(AnList)} AnList(i).Location < TransmissionRange(Fn) >$
For each node Fn
If Fn==D then
Generate route.
Add to the route set Rs.
else
Through each node Sn from FNlist
Find neighbours and verify the destination.
Add to node list.
Continue.
End
End
End
Stop
```

The route discovery procedure picks the routes to deliver the packet to the destination and adds them to the route set.

3.2. GSRM Estimation

The general secure route measure represents the node's trust in the past few days. It has been measured based on the node's behaviour in transmitting or forwarding the data packets. According to the model's transmission history, the method fetches the nodes of the selected route and fetches the transmission histories. Using them, the method computes the total number of transmissions the route has supported as total transmission supported (TTS) and the number of them sent successfully as the Number of Secure Transmission (NST). With the value of TTS and NST, the GSRM value is measured. The algorithm for GSRM estimation is represented as follows:

```
Given    : Route R, Transmission History TH.
Obtain GSRM.
Start
Read TH and R.
Route History RH = $\sum_{i=1}^{Size(TH)} TH(i).Route == R$
Compute TTS = $\sum_{i=1}^{Size(TH)} Count(TH(i))$
Compute NST = $\sum_{i=1}^{Size(TH)} TH(i).Route == R$ && $TH(i).State ==$ Finished.
Compute GSRM = $\frac{NST}{TTS} \times \frac{\sum_{i=1}^{Size(RH)} RH(i).Latency}{Size(RH)}$
Stop
```

The algorithm discussed shows how the value of GSRM is measured. The value of GSRM is computed according to the value of NST and TTS. Also, it has been measured based on the latency value of such transmissions.

3.3. ISSRM Estimation

The inclusion-specific secure route measure represents the trust of the route, which contains a set of IoT devices. It has been measured according to the condition when including such devices.

It is measured by computing the overall transmission performed through the route, overall successful transmission, the Number of transmissions the IoT device involved in total, and the Number of them that become successful independent of the route considered.

The measures mentioned above are used to compute ISSRM value towards secure routing. The algorithm for the ISSRM Estimation is given as follows:

```
Input    : Transmission History TH, Route R.
Output   : ISSRM.
Start
Read TH and R.
Find IoT in route R as IList = $\sum IoTDevices \in R$
Route History RH = $\sum_{i=1}^{Size(TH)} TH(i).Route == R$
Compute Overall Transmission OTr = Size (RH)
Compute Overall Success Transmission OST = $\sum_{i=1}^{Size(RH)} RH(i).State == Success$
```

```
For each IoT device, I in Ilist
    Compute Number of Transmission NoT = $\sum_{i=1}^{Size(TH)} TH(i).Route \in IoT$
    Compute the Number of Success as NoS = $\sum_{i=1}^{Size(TH)} TH(i).Route \in IoT \&\& TH(i).State == Success$
    Compute Node Inclusion Support (NIS) = $\frac{NoS}{NoT}$
End
Compute ISSRM = $\frac{OsT}{OTR} \times \frac{\sum NIS}{Size(Ilist)}$
Stop
```

The inclusion-specific secure route measure estimation algorithm computes different measures for different IoT devices. According to them, the ISSRM value is measured towards secure routing.

3.4. ESSRM Estimation

The trust in the route has been measured in another way in this part. By excluding the specific IoT device, the trust measure is computed.

It has been performed by measuring the trust of the route without the presence of a specific IoT device. For each IoT device identified, the method computes how good the earlier transmission was with the presence of the IoT device considered and without the presence of the same.

Rk with the IoT device I is measured for each route, and Rk without the IoT device I is measured for the same route. Using the measures mentioned above, the value of ESSRM is measured. The algorithm for ESSRM Estimation is given as follows:

```
Input   : Transmission History TH, Route R, Route List RL
Output  : ESSRM
Start
Read TH, RL, and R.
Find the list of IoT present in the route R as IList = $\sum IoTDevices \in R$
Route History RH = $\sum_{i=1}^{Size(TH)} TH(i).Route == R$
For each IoT device I
    Compute Node Inclusion Support NIS = $\frac{\sum_{i=1}^{Size(TH)} TH(i).Route \in IoT \&\& TH(i).State==Success}{\sum_{i=1}^{Size(TH)} TH(i).Route \in IoT}$
    Compute Exclusion Routes ER = $\sum_{i=1}^{size(RL)} RL(i) \in \forall(Nodes(R) excluding\ I)$
    For each excluded route E
        Compute Transmission factor TF = $\frac{\sum_{i=1}^{Size(TH)} TH(i).Route==E \&\& State==Success}{\sum_{i=1}^{Size(TH)} TH(i).Route==E}$
    End
    Compute Exclusion Support ESup = $\frac{NIS}{\sum TF / size(ER)}$
End
Compute ESSRM = $\frac{\sum ESup / size(ER)}{size(Ilist)}$
Stop
```

The above-discussed approach represents how the exclusion-specific secure route measure (ESSRM) is measured for any given route. It has been measured by computing both inclusion support and exclusion support values.

3.5. IESSRM Secure Routing

The proposed IESSRM-based securing routing model discovers the routes to reach the destination using the topology. The route discovery procedure not just discovers the route but also identifies various features of nodes like location, energy, and transmission range.

Further, the method performs GSRM estimation according to the history of the route. With the routes and features, the value of ISSRM and ESSRM is measured, and the transmission strength (TStr) value is computed.

Based on the TStr value, a suitable route is identified for data transmission. The algorithm of IESSRM secure routing is represented as follows:

```
Input   : Transmission History TH, Packet P, Network Topology Topo
Output  : Null
Start
Read TH, Topo, and P.
Route List Rl = Perform Route Discovery (P)
For every route R
    ISSRM = Perform ISSRM Estimation
    ESSRM = Perform ESSRM Estimation
    GSRM = Perform GSRM Estimation
    Compute Transmission Strength Tstr = $\frac{ESSRM}{ISSRM} \times GSRM$
End
Route R = Select route with maximum Tstr.
Perform data transmission using R
Stop
```

The algorithm discovers the routes and estimates various measures to compute transmission strength. Accordingly, an optimal route is selected to support data transmission.

4. Results and Discussion

The inclusion and exclusion-specific secure routing measure-based routing model has been simulated with NS2. The model's performance is measured on nodes, transmission range, and energy in different conditions. The results populated are compared with other schemes.

Table 1. Simulation parameters

Feature	Value
Tool Used	Network Simulator NS2
Total Nodes	500
Transmission Range	100 meters
Energy	100 Joules

The performance of different approaches has been measured and evaluated according to the simulation conditions mentioned in Table 1. According to that, the method compared the performances of the research model with the various approaches.

4.1. Performance Evaluation

For performance analysis, four parameters are used, which are secure routing performances (SRP), throughput, packet delivery rate (PDR), and packet drop rate. These parameters are computed using the following equations.

$$\text{SRP} = \frac{\text{No.of Threats Detected}}{\text{Total Threats Generated}} \times 100 \quad (1)$$

$$\text{Throughput} = \frac{\text{Total bytes delivered}}{\text{Total bytes transferred}} \times 100 \quad (2)$$

$$\text{PDR} = \frac{\text{No.of Packets Delivered}}{\text{Total Packets Sent}} \times 100 \quad (3)$$

$$\text{Packet Drop Ratio} = \frac{\text{No.of Packets Dropped}}{\text{Total Packets Sent}} \times 100 \quad (4)$$

Table 2. Comparison of SRP performances

Models	Nodes		
	100	300	500
HCBS	71.42	75.51	77.97
TSSRM	73.65	77.26	79.02
ESRQ	76.04	78.90	80.55
BAGOR	78.89	80.34	82.71
CBCSR	80.11	82.98	86.46
IESSR	83.75	89.20	96.00

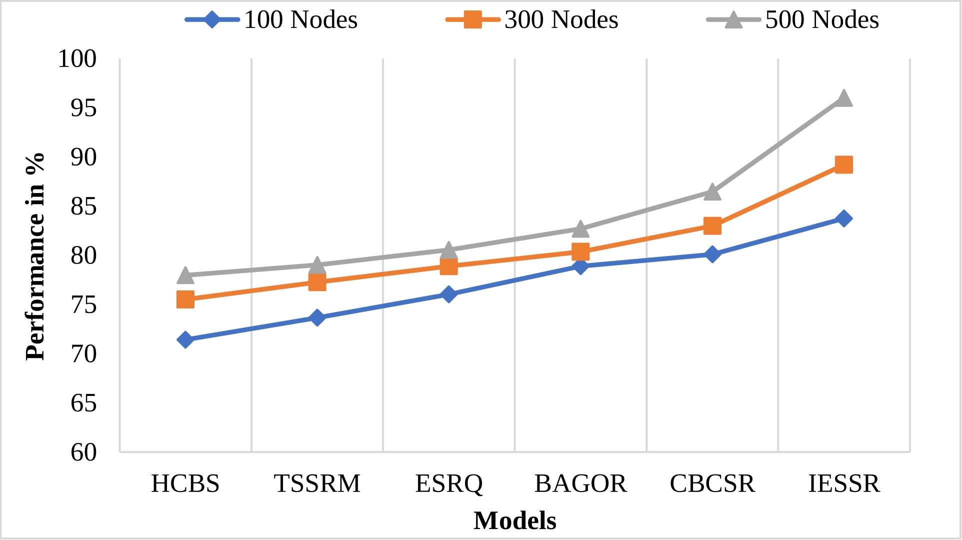

Fig. 3 SRP performance comparison

Table 2 represents the IESSR's SRP performance analysis comparison with other models. The compared models are Heterogeneous Cluster Based Secure routing (HCBS), TSSRM, ESRQ, BAGOR, and Continuous Behavior Class Secure Routing (CBCSR). The performances are measured based on three levels of nodes such as 100, 300, and 500.

The IESSR model obtained 83.75% SRP at 100 nodes, 89.20% SRP at 300 nodes, and 96% SRP at 500 nodes. Compared to other models, the IESSR model has obtained a higher SRP rate on all the categories of nodes. With 100 nodes, the IESSR model has an SRP difference of 3.64% to 12.33%, 6.22% to 13.69% with 300 nodes, and 9.54% to 18.03% higher than other models. The CBCSR was the second leading performance model, and the least performed model was HCBS. Figure 3 represents the graphical plot of the IESSR's comparison of SRP performance. The IESSR's throughput performance analysis comparison with other models is represented in Table 3. The throughput performances are measured based on three levels of nodes such as 100, 300, and 500. The IESSR model obtained 82.97% throughput at 100 nodes, 88.70% throughput at 300 nodes, and 97% throughput at 500 nodes. Compared to other models, the IESSR model has obtained a higher throughput rate on three categories of nodes.

With 100 nodes, the IESSR model has a throughput difference of 3.86% to 9.95%, 5.06% to 13.48% with 300 nodes, and 7.75% to 19.36% higher throughput than other models. The CBCSR was the second leading performance model, and the least performed model was HCBS. Figure 4 represents the graphical plot of the IESSR's throughput performance comparison.

Table 3. Comparison of throughput performances

Models	Nodes		
	100	300	500
HCBS	73.02	75.22	77.64
TSSRM	72.30	77.89	78.80
ESRQ	75.06	78.07	79.98
BAGOR	77.24	79.82	87.60
CBCSR	79.11	83.64	89.25
IESSR	82.97	88.70	97.00

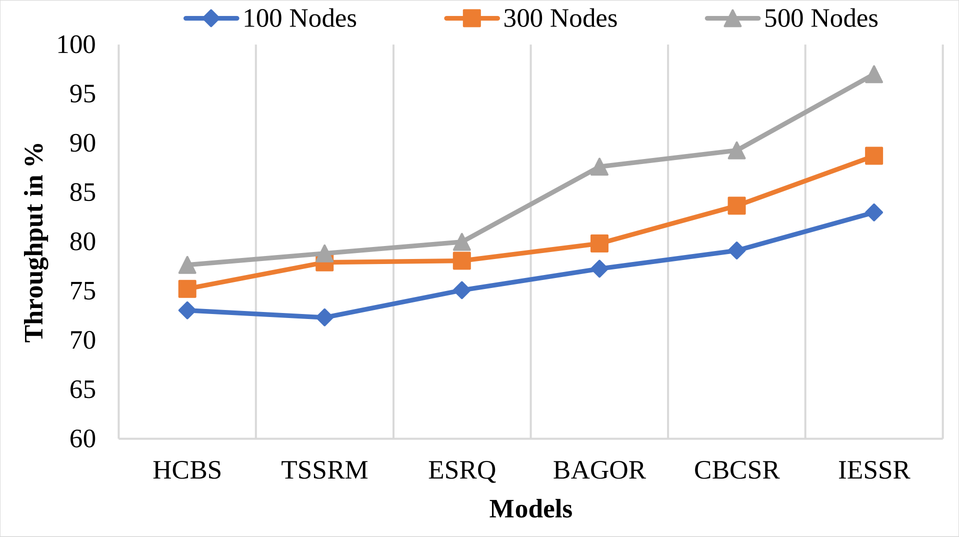

Fig. 4 Throughput performance comparison

The IESSR's packet drop rate performance analysis comparison with other models is represented in Table 5. The packet drop rates are measured based on three levels of nodes such as 100, 300 and 500. The IESSR model obtained an 18.39% packet drop rate at 100 nodes, a 13.47% packet drop rate at 300 nodes and a 3.01% packet drop at 500 nodes.

Compared to other models, the IESSR model has obtained a lower packet drop rate on three categories of nodes. With 100 nodes, the IESSR model has a packet drop rate difference of 3.06% to 10.22%, 4.18% to 13.33% with 300 nodes, and 11.98% to 19.86% lower packet drop rate than other models. The CBCSR was the second leading performance model, and the least performed model was HCBS. The packet drop rate measured with 500 nodes obtained a significantly lower one. Figure 6 represents the graphical plot of the IESSR's packet drop rate performance comparison. As per the comparison, the proposed IESSR model was the best-performed model in all the parameters compared to all the other models. Table 4 represents the IESSR's PDR performance analysis comparison with other models. The PDR performances are measured based on three levels of nodes such as 100, 300, and 500. The IESSR model obtained 82.09% PDR at 100 nodes, 87.70% PDR at 300 nodes, and 97.17% PDR at 500 nodes.

Compared to other models, the IESSR model has obtained a higher PDR rate on all the categories of nodes. With 100 nodes, the IESSR model has a PDR difference of 2.77% to 9.77%, 5.12% to 12.74% with 300 nodes, and 8.05% to 19.15% higher than other models. The CBCSR was the second leading performance model, and the least performed model was HCBS. Figure 5 represents the graphical plot of the IESSR's comparison of PDR performance.

Table 4. Comparison of PDR performances

Models	**Nodes**		
	100	**300**	**500**
HCBS	72.32	74.96	78.02
TSSRM	72.83	76.18	78.90
ESRQ	75.57	78.06	80.00
BAGOR	77.91	79.35	86.20
CBCSR	79.32	82.58	89.12
IESSR	82.09	87.70	97.17

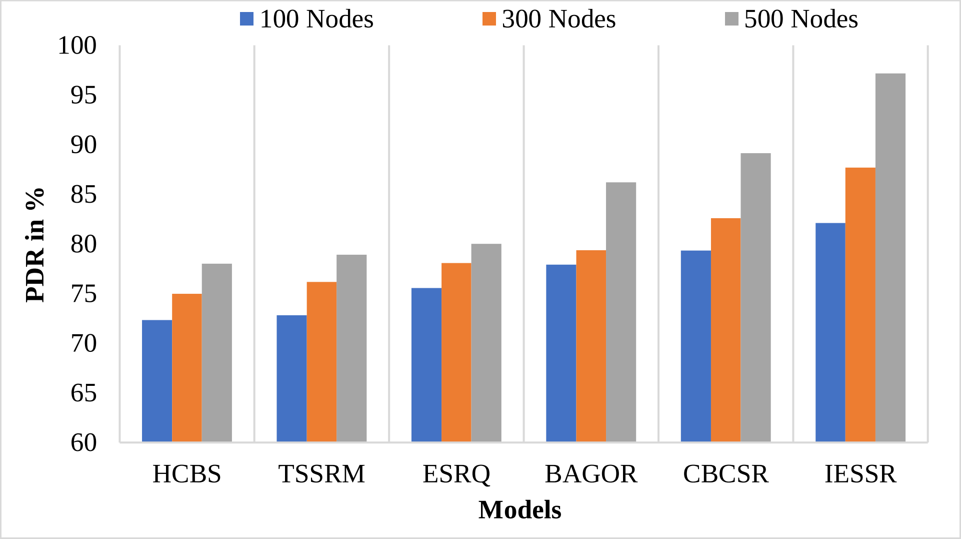

Fig. 5 PDR performance comparison

Table 5. Comparison of packet drop ratio performances

Models	Nodes		
	100	300	500
HCBS	28.61	26.80	22.87
TSSRM	27.34	23.54	21.73
ESRQ	25.00	22.07	19.98
BAGOR	23.58	21.50	17.43
CBCSR	21.45	17.65	14.99
IESSR	18.39	13.47	3.01

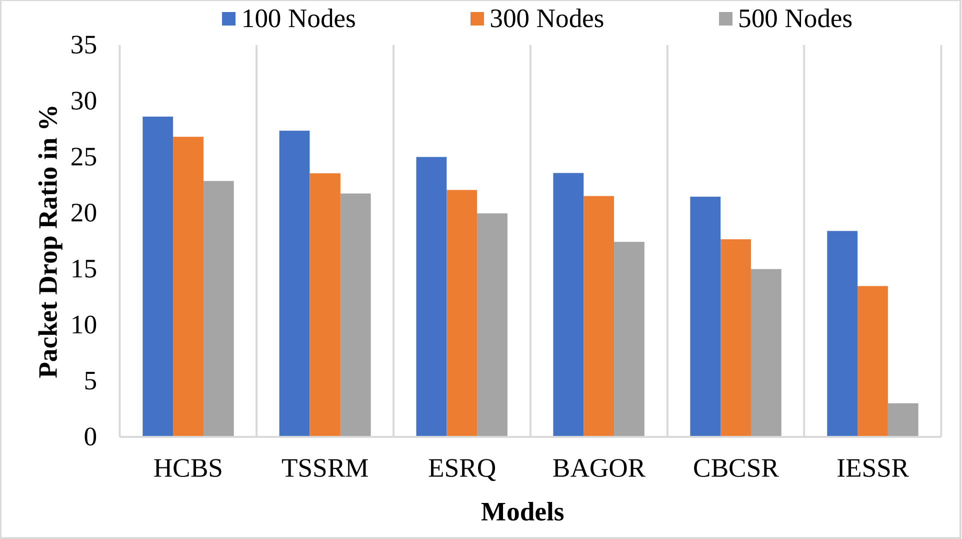

Fig. 6 Packet drop ratio performance comparison

5. Conclusion

The research presents the design and development of a novel IESSR model to improve the QoS metrics and measure the trust of IoT devices. This article presented the IESSR model for QoS development. Towards this, the proposed model discovers the available routes between the source and destination. The status of transmission, and other features, the method computes the General Secure Route Measure (GSRM), Inclusion Specific Secure Route Measure (ISSRM), and Exclusion Specific Secure Route Measure (ESSRM).

The research model computes GSRM, ISSRM, and ESSRM values for all detected routes. Based on these values, the method computes the value of Transmission Strength. According to the values of Transmission strength, the research model selected the most weighted route for transmitting data. The performances of the research model are evaluated based on secure routing performances (SRP), throughput, packet delivery rate (PDR), and packet drop rate.

The performances of this research model are validated by comparing it with various routing models analyzed from the related works. The research model enhanced the routing performances by up to 96%, and throughput performance has been hiked up to 97%. In the future, we plan to extend this work to maximize the PDR and throughput further and minimize the packet drop rate. We have also interested in evaluating IESSR in a large-scale environment.

Acknowledgments

Authors 1 and 2 contributed equally to this work. The authors would like to thank St. Peter's Institute of Higher Education and Research, Chennai, for their support in completing this research work.

References

[1] Rashmita Khilar et al., “Artificial Intelligence-Based Security Protocols to Resist Attacks in Internet of Things,” *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1-10, 2022. [CrossRef] [Google Scholar] [Publisher Link]

[2] Mugesh Ravi, “A Survey on Security Risks in Internet of Things (IoT) Environment,” *Journal of Computational Science and Intelligent Technologies*, vol. 1, no. 2, pp. 1-8, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[3] S. Menaga et al., “An Efficient Biometric Based Authenticated Geographic Opportunistic Routing for IoT Applications using Secure Wireless Sensor Network,” *Materials Today: Proceedings*, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[4] Anindya Kumar Biswas, and Mou Dasgupta, “A Secure Hybrid Routing Protocol for Mobile Ad-Hoc Networks (MANETs),” *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1-7, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[5] Duvvada Shreya Sri, and R. V. L. S. N. Sastry, “An Efficient and Secure Data Transmission of Common Randomness Routing in Adhoc Wireless Network,” *International Journal of P2P Network Trends and Technology*, vol. 9, no. 1, pp. 1-4, 2019. [Publisher Link]

[6] S. Ranjithkumar, and N. Thillaiarasu, “A Survey of Secure Routing Protocols of Mobile AdHoc Network,” *SSRG International Journal of Computer Science and Engineering*, vol. 2, no. 2, pp. 34-39, 2015. [CrossRef] [Google Scholar] [Publisher Link]

[7] Gurveen Vaseer, “Multi-Attack Detection using Forensics and Neural Network Based Prevention for Secure MANETs,” *2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1-6, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[8] Majdi Alqdah, “Intrusion Detection Attacks Classification using Machine Learning Techniques,” *Journal of Computational Science and Intelligent Technologies*, vol. 2, no. 2, pp. 1-6, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[9] Xiaoxiong Zhong et al., “DSOR: A Traffic-Differentiated Secure Opportunistic Routing with Game Theoretic Approach in MANETs,” *2019 IEEE Symposiums on Computer and Communication (ISCC)*, pp. 1-6, 2019. [CrossRef] [Google Scholar] [Publisher Link]

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

[11] Khalid Haseeb et al., “Intrusion Prevention Framework for Secure Routing in WSN-Based Mobile Internet of Things,” *IEEE Access*, vol. 7, pp. 185496-185505, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[12] M. Supriya, and T. Adilakshmi, “Secure Routing using ISMO for Wireless Sensor Networks,” *SSRG International Journal of Computer Science and Engineering*, vol. 8, no. 12, pp. 14-20, 2021. [CrossRef] [Google Scholar] [Publisher Link]

[13] M. S. Krishnaveni, and K. Kavitha, “Secure Routing in Wireless Sensor Network using HTARF,” *SSRG International Journal of Computer Science and Engineering*, vol. 3, no. 5, pp. 27-30, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[14] Sijan Shrestha et al., “Securing Blackhole Attacks in MANETs using Modified Sequence Number in AODV Routing Protocol,” *2020 8th International Electrical Engineering Congress (iEECON)*, pp. 1-4, 2020. [CrossRef] [Google Scholar] [Publisher Link]

[15] V. Sesha Bhargavi, M. Seetha, and S. Viswanadharaju, “A Trust-Based Secure Routing Scheme for MANETS,” *2016 6th International Conference - Cloud Systems and Big Data Engineering (Confluence)*, pp. 565-570, 2016. [CrossRef] [Google Scholar] [Publisher Link]

[16] Sakshi Yadav et al., “Securing AODV Routing Protocol against Black Hole Attack in MANET using Outlier Detection Scheme,” *2017 4th IEEE Uttar Pradesh Section International Conferences on Electricals, Computers and Electronics (UPCON)*, pp. 1-4, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[17] Gurveen Vaseer, Garima Ghai, and Dhruva Ghai, “Novel Intrusion Detection and Prevention for Mobile Ad Hoc Networks: A Single- and Multiattack Case Study,” *IEEE Consumer Electronics Magazine*, vol. 8, no. 3, pp. 35-39, 2019. [CrossRef] [Google Scholar] [Publisher Link]

[18] C. Deepa, and B. Latha, “An Energy Efficient Secure Routing (EESR) using Elliptic Curve Cryptography for Wireless Sensor Networks,” *2018 Second International Conference on Inventive Communication and Computational Technologies (ICICCT)*, Coimbatore, India, pp. 1603-1608, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[19] Ranu Shukla, Rekha Jain, and P. D. Vyavahare, “Combating against Wormhole Attack in Trust And Energy Aware Secure Routing Protocol (TESRP) in Wireless Sensor Network,” *2017 International Conferences on Recent Innovation in Signals Processing and Embedded System (RISE)*, Bhopal, India, pp. 555-561, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[20] Rutuja Ashtikar, Deepali Javale, and Sujata Wakchaure, “Energy Efficient and Secured Data Routing through Aggregation Node in WSN,” *2017 International Conferences on Computing, Communications, Control and Automations (ICCUBEA)*, Pune, India, pp. 1-6, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[21] K. RupaRani, and K. Jagdeeshwara Rao, “An Improved Novel Design for User Authentication and Secure Transmission of Data in End to End Routing in Wireless Sensor Network,” *International Journal of P2P Network Trends and Technology (IJPTT)*, vol. 8, no. 2, pp. 8-13, 2018. [Publisher Link]

[22] C. Prasad Reddy, “Programmable Wireless Sensor Network for Industrial Automation and Environmental Safety,” *SSRG International Journal of Industrial Engineering*, vol. 1, no. 1, pp. 4-6, 2014. [CrossRef] [Publisher Link]

[23] Gaosheng Liu et al., “ESRQ: An Efficient Secure Routing Method in Wireless Sensor Networks Based on Q-Learning,” *2018 17th IEEE International Conferences on Trust, Security and Privacy in Computing and Communication/ 12th IEEE International Conferences on Big Data Sciences and Engineering (TrustCom/BigDataSE)*, New York, USA, pp. 149-155, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[24] Hilmi Lazrag, Rachid Saadane, and Driss Aboutajdine, “A Game Theoretic Approach for Optimal and Secure Routing in WSN,” *Proceedings of the Third International Afro-European Conferences for Industrial Advancements-AECIA 2016*, vol. 565, pp. 218-228, 2018. [CrossRef] [Google Scholar] [Publisher Link]

[25] G. M. Navami Patil, and P. I. Basarkod, “Trust Model for Secure Routing and Localizing Malicious Attackers in WSN,” *Computing and Network Sustainability*, pp. 1-9, 2017. [CrossRef] [Google Scholar] [Publisher Link]

[26] Danyang Qin et al., “Research on Trust Sensing Based Secure Routing Mechanism for Wireless Sensor Network,” *IEEE Access*, vol. 5, pp. 9599-9609, 2017. [CrossRef] [Google Scholar] [Publisher Link]