https://doi.org/ 10.33472/AFJBS.6.10.2024.3850-3859

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

A Reliable Behavior Centric Secure Routing for Improved QoS Performance in WSN Using IoT

Dr.Dev Ras Pandey, Assistant Professor, Faculty of CS & IT, Kalinga University, Naya Raipur, Chhattisgarh, India.
Mail ID:ku.devraspandey@kalingauniversity.ac.in
ORCID ID: 0009-0004-4161-2369
Sushree Sasmita Dash, Assistant Professor, Faculty of CS & IT, Kalinga University, Naya Raipur, Chhattisgarh, India.
Mail ID:ku.sushreesasmitadash@kalingauniversity.ac.in
ORCID ID: 0009-0004-9662-595X

Article History

Volume 6,Issue 10, 2024

Received:13 Apr 2024

Accepted : 05 May 2024

doi: 10.33472/AFJBS.6.10.2024. 3850-3859

Abstract:

Secure routing in Wireless Sensor Network (WSN) towards QoS development has been well studied. There exist number of approaches to support secure routing in WSN, which consider the energy of sensor nodes, transmission range, latency and traffic on different sensor nodes as the key in measuring the trust of the route being used for data transmission. However, the methods suffer to achieve higher performance in secure routing and QoS performance. To handle this issue, a Reliable Behavior Centric Secure Routing (RBCSR) model is presented in this paper. The method focused on performing routing by measuring the trust of various sensor nodes present in the route. Also, the method considers the presence of IoT (Internet of Things) devices in data transmission. The method considers behavior of different sensor and devices to measure the trust of the routes available. The RBCSR algorithm consider the factors like energy, transmission range, previous transmission, number of retransmission, latency, number of drops and so on. By considering the above mentioned features, the method computes Device Incorporated Trust (DIT) and Non-Device Incorporated Trust (NIT) for different routes. Based on the value of DIT and NIT, the method computes the value of Route Reliable Trust (RRT) based on which a single route is selected to perform data transmission. The proposed RBCSR algorithm introduces higher QoS performance than other approaches.

Index Terms:WSN, Secure Routing, QoS, RBCSR, IoT, RRT

1. Introduction:

.Wireless sensor network has been used for variety of purposes like for public and private services. Any sensor network contains number of sensor nodes and each have been fabricated with a transmitter and receiver to support data transmission. But, the sensor nodes have limitation on their radio range and energy in joules. This restrict the sensor nodes in communicating directly to a faraway node, which encourages the nodes to perform cooperative transmission to complete the task. The sensor nodes are used for different applications and the data sensed by the sensor has been transmitted to a particular point where the data has been processed to perform required action. To perform data transmission, the nodes identify a secure route and forward the packet through the route selection. In this case, presence of malicious node performs different threats on data as well as routing. In case data attacks, the malicious node may perform eavesdrop attack by dropping whatever the packet comes. On the other side, the malicious node would transmit all the packets to a specific node which involve in learning the streaming to perform blockhole attack. Also, the nodes may perform routing attack by choosing a long route where there is a necessity to forward the packet through a short one. In case of energy efficient routing, the malicious node would transmit the packet where the nodes do not have enough energy to support the routing. Presence of such malicious nodes should be identified to perform secure routing as well as to increase the QoS of the network.

On the other side, the WSN contains set of IoT devices which are not part of the network. They are similar to the sensor nodes but have higher energy constraints and possible to perform different number of transmission. The IoT devices are private nodes which cannot be trusted for direct communication. However, in some situations where there is no sensor node available to support the data transmission and to provide seamless transmission, the presence of IoT devices can be included for data transmission. This denotes that the sensor nodes which are part of the network as well as IoT devices can perform any kind of threat to degrade the performance of the network.

It is necessary that, the routing process should identify a secure route by measuring the trust of the nodes. The node trust are measured according to different factors like previous history, behavior in transmission and other factors. There exist number of approaches which consider different features like number of transmission, energy and so on. But suffer to achieve higher performance in secure routing as well as QoS maximization. By considering all these, this article present a novel Reliable Behavior Centric Secure Routing (RBCSR) which consider number of features of sensor nodes and behavior of both sensor and IoT devices to compute Device Incorporated Trust (DIT), Non-Device Incorporated Trust (NIT) to measure the value of Route Reliable Trust (RRT). Based on the value of RRT, the method performs route selection and data transmission. The working of the proposed model is clearly sketched in Section 3. The Section 1 briefs the general introduction about WSN and secure routing in WSN. Section 2, analyzed different methods of secure routing in WSN. Section 4, presents the detailed analysis of secure routing towards QoS maximization. Section 5, details the conclusion of the research.

2. Related Works:

The methods related to secure routing in WSN and QoS development are detailed in this section.

A Blockchain Security IoT (BSI) is presented in [1], towards security in WSN, which authenticates the nodes using blockchain between base station and clusters. A detailed analysis on secure routing protocols in WSN is conducted in [2], which analyze the performance of various approaches according to energy, security and reliability. An trust based secure routing strategy is presented in [3], which measures direct and indirect trust in a collaborative way according to the signal strength received

from any node to perform efficient routing. A blowfish algorithm based secure routing scheme is presented in [4], which identifies link state multiple paths and uses crossover mutated marriage in Honey Bee (CM-MH) algorithm for route selection. A QoS aware energy balancing secure routing (QEBSR) is presented in [5], which applies ant colony optimization based secure routing with energy balancing scheme for route selection. A hierarchical routing metric secure routing (HRMS) is presented in [6], which uses Advanced Encryption Standard Methodology (IAFSM) to provide a data security over transmissions. The performance of hierarchical routing protocols for WSN is analyzed in [7], under different performance metrics. A trust based secure and energy efficient routing protocol (TBSEER) is presented in [8], which measures the trust value in direct, indirect, and energy values to identify the blackhole in the network to perform secure routing. A lightweight trust management scheme (LTMS) is proposed in [9], which works according to the binomial distribution of nodes to defend against internal attacks. Trust-aware secure routing protocol is proposed in [10], which computes trust value based on the direct, indirect trust, volatilization factor and energy. A low complexity energy efficient data securing model is presented in [11], which uses linearly complex voice encryption mechanism. A particle water wave optimization based secure routing (P-WWO) is presented in [12], which uses PSO and water wave optimization algorithm for secure routing. A trust based secure routing model is presented in [13], which uses safety trust evaluation mechanism towards secure routing in WSN. A hierarchical trust management scheme is presented in [14], to support node cooperation in software defined WSN. A histogram gradient boost (HGB) based node classifier is presented in [15], to handle different security issues.

3. Reliable Behavior Centric Secure Routing (RBCSR) Model:

The proposed reliable behavior centric secure routing (RBCSR) algorithm starts with discovering the routes by broadcasting the route request and collects set of routes with few details about different sensor nodes. Using these details, the method performs RBCSR routing by computing Device Incorporated Trust (DIT) and Non-Device Incorporated Trust (NIT) to measure the value of Route Reliable Trust (RRT). Using the value of RRT, the method selects a trusted route to deliver the packet to the destination. The detailed working of the RBCSR algorithm is sketched in this section.

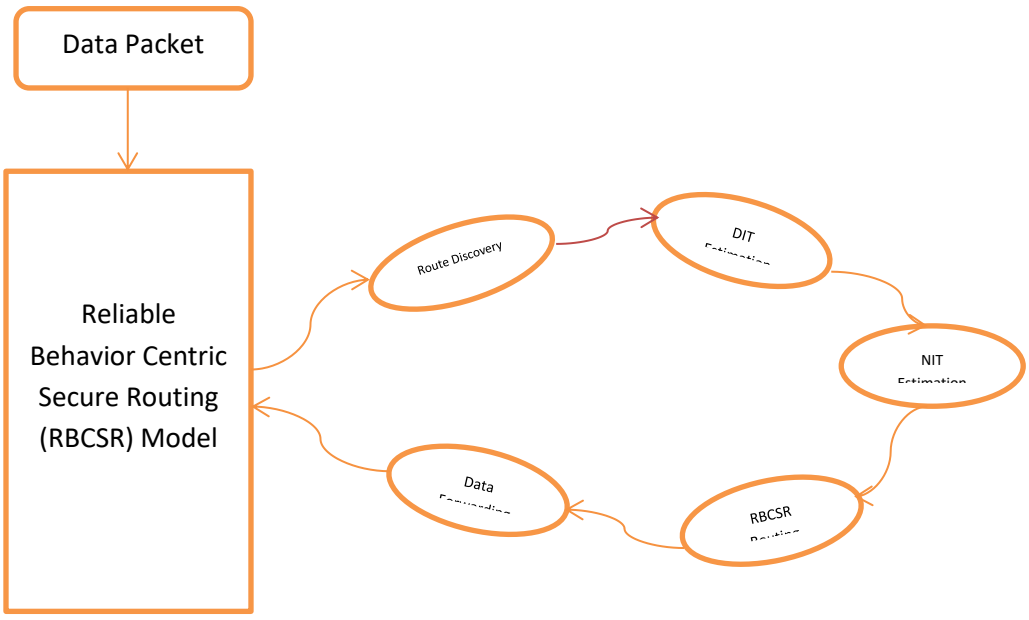

Figure 1: Architecture of Proposed RBCSR Routing Model

The working model of the proposed RBCSR routing model is presented in Figure 1, where the functions of the model are sketched in detail in this section.

Route Discovery:

The proposed RBCSR routing protocol starts by discovering the routes available between any two sensor nodes or a route between a source and service point. By the time the source nodes have a packet to be transmitted towards a destination, the sensor node performs route discovery. The route discovery is initiated by generating a route request packet RBCSR_RR with a source id and destination id. Generated packet has been broadcast in the network which has been received by the neighbors of the source. By receiving the route request packet, the neighbors verify their route table for the availability of route to reach the destination mentioned in the request packet. If there is a route, then it send a reply packet with different details of its own like energy, transmission range, previous transmission, number of retransmission, latency, number of drops and so on. Updated route request packet is forwarded to the source node. Otherwise, the packet is broadcasted in the same way and the node which has a route will update the route and other details with the reply packet and will be sent to the source node. Upon receiving the route reply packet, the source will extract the route and other features available from the reply packet and updated to the table maintained. The updated tables and their features are used to perform routing in a secure way.

DIT Estimation:

The routes identified by the route discovery procedure would contain N number of routes in their route table. Also, the node table contains different information like energy, transmission range, previous transmission, number of retransmission, latency, number of drops about each node present in the route. The nodes are comes with their id which denotes their id as well as type of node. The security of the route is greatly depending on the number of sensor nodes present in the route and number of IoT devices present in the route. Also, the security of the route is depend on the number of transmissions involved by any IoT device present in the route and number of retransmission happened. Further, the method consider the average number of IoT devices present in other routes and number of IoT devices present in the current route. The DIT measure represents the security or trust of route when including the IoT devices for the data transmission. To measure the trust, the method computes number of IoT present in the route NI, Number of Transmission NT, Number of Retransmission NR, Average Device Count ADC, Average Residual Energy ARE, Average Latency AL, and Average Drops AD. Using all these values, the method computes DIT value as the trust to be used on routing.

Algorithm:

Given: Route Table RT, Route R, Node Table NT, Transmission set Ts

Obtain: DIT

Start

Read RT, R, NT, Transmission set Ts.

Identify Device set Ds = $\sum_{i=1}^{Size(R)} R(i).Type == IoT$

For each device Di

Count Number of Transmission NT = $\sum_{i=1}^{size(Ds)} \sum_{j=1}^{Size(Ts)} Count(Ts(i).Route \in Ds(i))$

Count Number of retransmission Rt.

$$RT = \sum_{i=1}^{size(Ds)} \sum_{j=1}^{Size(Ts)} Count(Ts(i).Route \in Ds(i) \;\&\&\; Ts(i).state == retransmit)$$

End

Compute Average Device Count ADC = $\frac{\sum_{i=1}^{size(RT)} Count(RT(i).Ds)}{size(RT)}$

Compute Average Residual Energy ARE = $\frac{\sum_{i=1}^{size(RT)} \sum_{j=1}^{size(RT(i).Ds)} Sum(Ds(j).Energy)}{\sum_{i=1}^{size(RT)} Sum(RT(i).Ds.size)}$

Compute Average Latency AL = $\frac{\sum_{i=1}^{size(RT)} \sum_{j=1}^{size(Ts(RT(i)))} Sum(Ts(j).Ds(k).Latency)}{\sum_{i=1}^{size(RT)} Sum(RT(i).Ds.size)}$

Compute average drop count ADrC = $\frac{\sum_{i=1}^{size(RT)} \sum_{j=1}^{size(Ts(RT(i)))} Sum(Ts(j).Ds(k).DropCount)}{\sum_{i=1}^{size(RT)} Sum(RT(i).Ds.size)}$

Compute DIT = $\frac{\sum RT}{\sum NT} \times \frac{ADrC}{ADC} \times \frac{ARE}{AL}$

Stop

The above pseudo code represents how the trust of route with IoT devices is measured. The method computes different values according to the behavior of the devices. Based on the measures, the method computes the value of DIT to support secure routing.

NIT Estimation:

The Non-Device Incorporate Trust (NIT) represents the trust of any route according to the behavior of the sensor nodes. This measure the trust of node based on the sensor nodes present in the route. To measure the trust of the route in this way, the method consider the factors like energy, transmission range, previous transmission, number of retransmission, latency, number of drops about each node present in the route. Using these features, the method computes the Average transmission rate (ATR), Average Retransmission Rate (ARTR), Average Latency (AL), Average Sensor Count (ASC), Average Drop Count (ADrC) and Average Residual Value (ARV). Using all these measures, the method computes the value of NIT to support secure routing.

Algorithm:

Given: Route Table RT, Route R, Node Table NT, Transmission set Ts

Obtain: DIT

Start

Read RT, R, NT, Transmission set Ts.

Identify Sensor set Ss = $\sum_{i=1}^{Size(R)} R(i).Type == Sensor$

Count Average Transmission Rate ATR = $\frac{\sum_{i=1}^{size(Ss)} \sum_{j=1}^{Size(Ts)} Count(Ts(i).Route \in Ss(i))}{size(ss)}$

Compute Average retransmission rate ARTR.

ARTR = $\frac{\sum_{i=1}^{size(Ss)} \sum_{j=1}^{Size(Ts)} Count(Ts(i).Route \in Ss(i)\ \&\&\ Ts(i).state == retransmit)}{size(ss)}$

Compute Average Sensor Count ASC = $\frac{\sum_{i=1}^{size(RT)} Count(RT(i).S.size)}{size(RT)}$

Compute Average Residual Energy ARE = $\frac{\sum_{i=1}^{size(RT)} \sum_{j=1}^{size(RT(i).Ss)} Sum(Ss(j).Energy)}{size(RT)}$

Compute Average Latency AL = $\frac{\sum_{i=1}^{size(RT)} \sum_{j=1}^{size(Ts(RT(i)))} Sum(Ts(j).Ss(k).Latency)}{\sum_{i=1}^{size(RT)} Sum(RT(i).Ss.size)}$

Compute average drop count ADrC = $\frac{\sum_{i=1}^{size(RT)} \sum_{j=1}^{size(Ts(RT(i)))} Sum(Ts(j).Ss(k).DropCount)}{\sum_{i=1}^{size(RT)} Sum(RT(i).Ss.size)}$

Compute NIT = $\frac{ARTR}{ATR} \times \frac{ADrC}{ASC} \times \frac{ARE}{AL}$

Stop

The above discussed algorithm computes NIT value based on different measures computed based on the transmission trace available. Estimated value of NIT has been used to perform secure routing.

RBCSR Routing:

The reliable behavior centric secure routing algorithm receives the incoming packet initially. With the packet received, if it has a route to reach the destination, then it forwards the packet through the route. Otherwise, it perform route discovery to identify set of all routes available. For each route

identified, the method computes two trust values like DIT and NIT. Based on these values, the method computes the value of Route Reliable Trust (RRT). Based on the value of RRT, the method selects a most valued route to perform data transmission.

Algorithm:

Given: Route Table RT, Node Table NT, Transmission set Ts, Packet P

Obtain: Null

Start

Read RT, NT, Ts, P.

If Node has route to P.destination then

Transmit the packet

Else

Perform route discovery.

For each route R

Compute DIT = Perform DIT estimation

Compute NIT = Perform NIT Estimation

Compute RRT = $NIT \times (\text{DIT} \times \frac{1}{7})$

End

Route R = Choose the route R with maximum RRT.

Transmit packet on the selected route R.

End

Stop

The above RBCSR routing algorithm computes RRT value for different routes to identify most secure route to transmit the data packet.

4. Results and Discussion:

The proposed RBCSR routing algorithm has been implemented with Network Simulator 2, with different simulation conditions. The performance of the method is measured on different parameters and compared with the results of other methods.

Key	Value
Tool	Network Simulator 2
Number of Nodes	150
Simulation Time	20 seconds
Residual Energy	200 joules
Mobility Speed	1 meters / second

Table 1: Evaluation Details

The details of evaluation have been presented in Table 1, which has been used to measure the performance of the proposed model. The results obtained are compared with the result of other approaches.

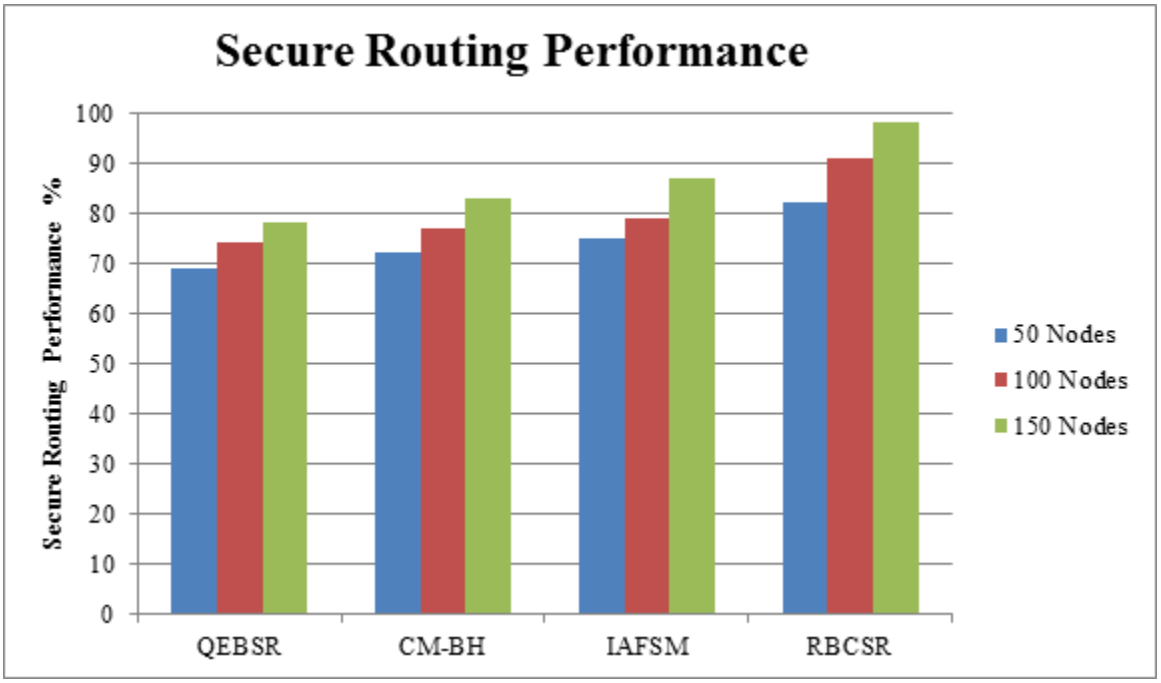

Figure 2: Analysis on Secure Routing vs No of Services

The performance of the methods in secure routing is measured for various approaches and presented in Figure 2. The proposed RBCSR model introduces higher performance compare to others.

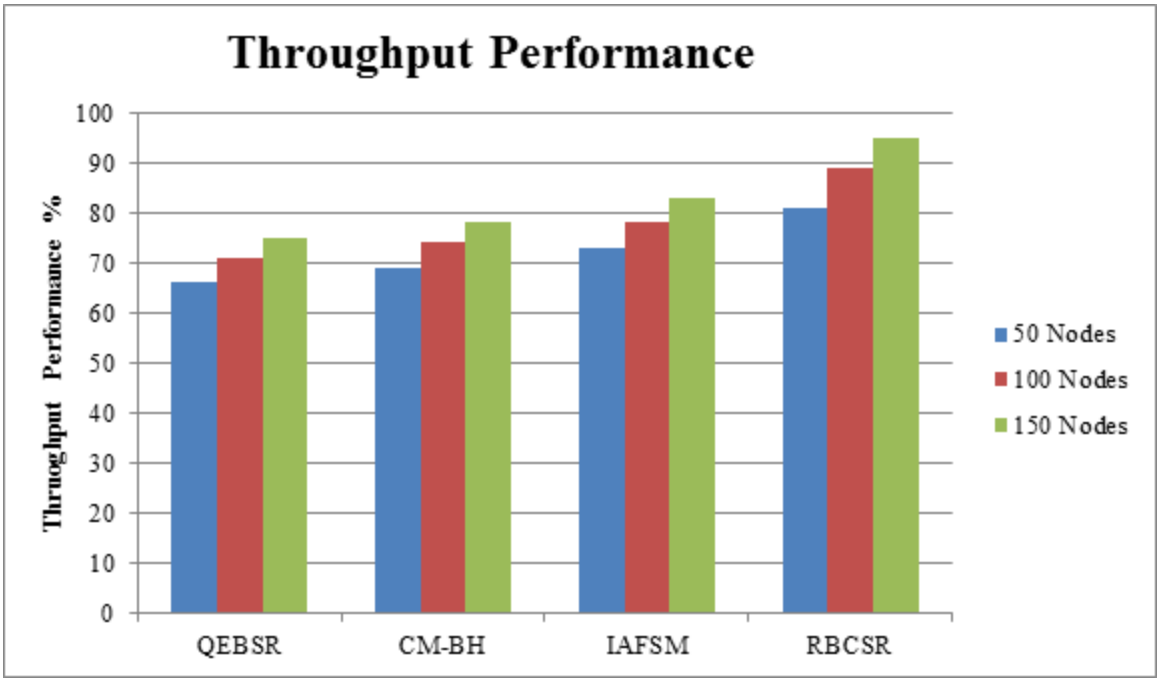

Figure 3: Throughput Performance

The performance of methods in achieving throughput is measured at the presence of different number of nodes. The proposed RBCSR model introduces higher performance than others.

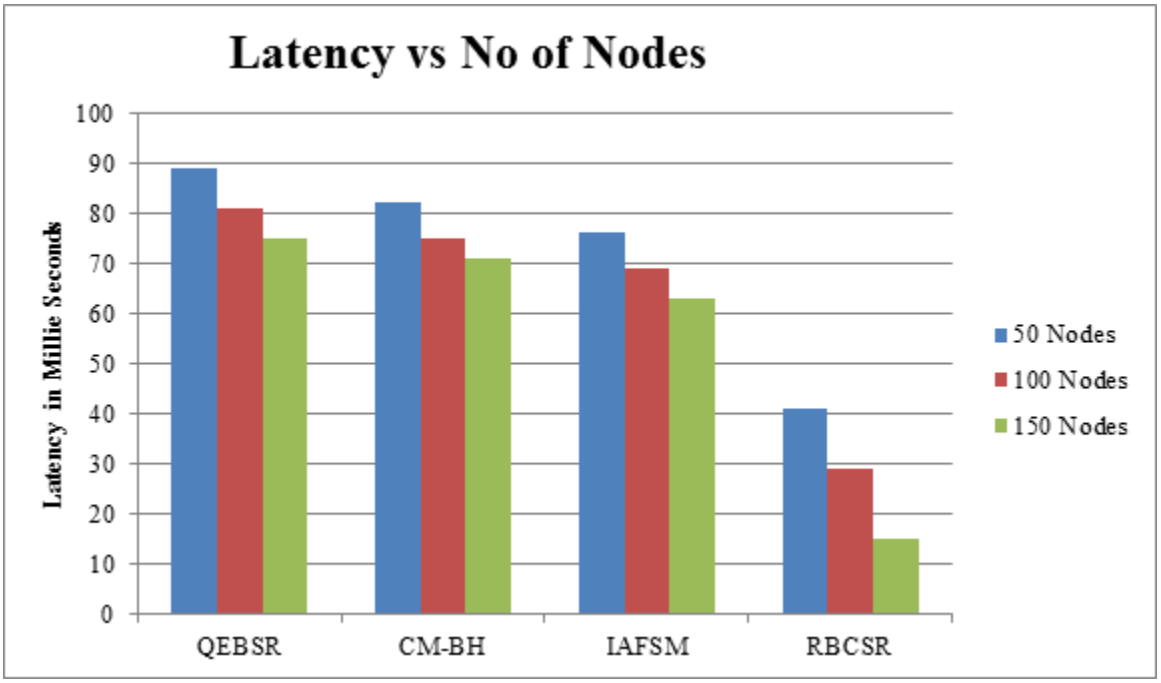

Figure 4: Latency vs No of Nodes

The value of latency introduced by the methods in data transmission is measured for various approaches and presented in Figure 4. The proposed RBCSR algorithm produces less latency compare to others.

5. Conclusion:

This article presented a novel Reliable Behavior Centric Secure Routing (RBCSR) algorithm for the performance development of WSN. The method discovers the routes available between any two nodes. With the routes identified, the value of trust on the inclusion of IoT devices is measured by computing DIT value where the trust of sensor nodes in the route is measured by computing NIT value. Using both of them, the method computes the value of RRT and based on that a single route is identified to perform data transmission. The proposed RBCSR protocol improves the performance of routing as well as improves the overage QoS performance.

References:

1. W. Jerbi, O. Cheikhrouhou, A. Guermazi, A. Boubaker and H. Trabelsi, "A Novel Blockchain Secure to Routing Protocol in WSN," IEEE (HPSR), 2021, pp. 1-6.
2. M. Biradar and B. Mathapathi, "Secure, Reliable and Energy Efficient Routing in WSN: A Systematic Literature Survey," IEEE (ICAECT), 2021, pp. 1-13.
3. P. Rani and N. K. Gupta, "Composite Trust for Secure Routing Strategy through Energy based Clustering in WSN," IEEE (ICAECT), 2021, pp. 1-6.
4. M. Alotaibi, "Improved Blowfish Algorithm based Secure Routing Technique in IoT based WSN," IEEE, PP 1-1, 2021.
5. M. Rathee, S. Kumar, A. H. Gandomi, K. Dilip, B. Balusamy and R. Patan, "Ant Colony Optimization Based Quality of Service Aware Energy Balancing Secure Routing Algorithm for Wireless Sensor Networks," IEEE (TEM), Volume. 68, Number. 1, pp. 170-182, 2021.
6. S. C, G. Ramkumar, A. G, S. M and M. Ayyadurai, "Experimental Analysis of Secured Routing Protocol Establishments over Wireless Sensor Network," IEEE (ICOEI), 2021, pp. 691-698.

7. Muhammad K. Khan, Hierarchical Routing Protocols for Wireless Sensor Networks: Functional and Performance Analysis, HINDAWI (JS), Volume 2021, PP 18, 2021.
8. H. Hu, Y. Han, M. Yao and S. Xue, "Trust Based Secure and Energy Efficient Routing Protocol for Wireless Sensor Networks," IEEE, 2021.
9. Weidong Fang, MSCR: multidimensional secure clustered routing scheme in hierarchical wireless sensor networks, SPRNGER Open (WCN), Number 14, 2021.
10. Huangshui Hu, Trust-aware secure routing protocol for wireless sensor networks, ETRI, Volume 43, Issue 4, PP 674-683, 2021.
11. M. Saud Khan, A low-complexity, energy-efficient data securing model for wireless sensor network based on linearly complex voice encryption mechanism of GSM technology, SAGE (IJDSN), Volume 17, Issue 5, 2021.
12. Pradeep Sadashiv Khot, Particle-Water Wave Optimization for Secure Routing in Wireless Sensor Network Using Cluster Head Selection, SPRINGER LINK (WPC), Volume 119, PP 2405-2429, 2021.
13. Qingzeng Xu, Wireless sensor networks secure routing algorithm based on trust value computation, (IJIPT), Volume 14, Number 1, 2021.
14. M. Bin-Yahya, O. Alhussein and X. Shen, "Securing Software-Defined WSNs Communication via Trust Management," in IEEE Internet of Things Journal, vol. 9, no. 22, pp. 22230-22245, 15 Nov.15, 2022, doi: 10.1109/JIOT.2021.3102578.
15. M. Nouman, U. Qasim, H. Nasir, A. Almasoud, M. Imran and N. Javaid, "Malicious Node Detection Using Machine Learning and Distributed Data Storage Using Blockchain in WSNs," in IEEE Access, vol. 11, pp. 6106-6121, 2023, doi: 10.1109/ACCESS.2023.3236983.