IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Revue d'Intelligence Artificielle
Vol. 36, No. 1, February, 2022, pp. 31-39
Journal homepage: http://iieta.org/journals/ria

# An Efficient Swift Routing Model with Node Trust Identity Factor (SRM-NTIF) to Perform Secure Data Transmission Among IoT Gadgets

Srilakshmi Puli*, Smitha Chowdary Chaparala

Department of CSE, Koneru Lakshmaiah Education Foundation, Vaddeswaram, Guntur 522 502, Andhra Pradesh, India

Corresponding Author Email: srilakshmipuli77@gmail.com

https://doi.org/10.18280/ria.360104

**Received:** 20 October 2021
**Accepted:** 3 December 2021

***Keywords:***
*node validation, trust factor, secure routing, internet of things, routing model, secure data transmission*

**ABSTRACT**

According to a United Nations survey, the number of users using the internet has increased to 3 billion in recent years. The Auto-ID Center is a research organisation that coined the word "Internet of Things" (IoT) a decade ago, describing how it utilises wired or wireless networking technologies to create a channel of communication among technologies and networks available over the Internet. Despite the fact that a swing of routing protocols has been proposed in the literature, safe and energy-efficient routing protocol is still a work in progress. Many routing protocols expressly designed for resource limited wireless devices take the same approach and have nearly achieved their full improvements. The Internet of Things (IoT) has recently gained prominence as a result of the increasing number of connected devices being used in everyday human life with network lifetime constraints. Routing expertise is essential for establishing communication between nodes. A node should be capable of self-learning, self-configuring, and self-managing by gathering local knowledge and sharing it with its neighbours. The degree of trust determines the degree of cooperation between scattered mobile nodes. The term "trust" refers to a level of assurance based on node behavior. To ensure secure and proper data transmission in IoT network, the trust level of the nodes is calculated based on node behaviour. Because of the unexpected changes in the network structure, the complex existence of IoT network, and the underived prior trust relationship between the nodes, trust computation in IoT network is a difficult task. All IoT nodes willing to engage in data transmission are given a Digital Unique Identifier (DUI), and the proposed model must define their trust identity factors. Using the DUI, the proposed Swift Routing Model with Node Trust Identity Factor (SRM-NTIF) model, node authentication is performed to verify natural and malicious nodes in the network. The proposed model is compared with the traditional methods and the results show that the proposed model performance is better in security and trust levels.

## 1. INTRODUCTION

Customers are no longer confined to building relationships with other users to communicate; they now expect to be able to link people with objects, things, which led to the introduction of the Internet of Things. Anything around can be linked to the communications system and connected to the conventional internet, allowing them to openly interact and share information [1]. The "data" in the Internet of Things are intelligent machines with contact and internet access; the equipment has vast quantities, constant switching, and limited resources [2]. To manage and coordinate these smart devices for reliable and scalable networks, as well as to integrate them with the traditional internet, a special routing protocol is needed [3].

To meet the demand, the Internet Engineering Task Force (IETF) developed the RPL routing protocol [4], a lightweight IPv6 network algorithm for the internet of things [5]. RPL routing protocols enable smart devices to make better use of their energy and processing resources while also enabling the creation of diverse topologies and data routing [6]. The RPL routing protocol, on the other hand, does not recognise network protection throughout the network stage and does not provide network security through routing regulatory mechanisms when the network is installed, resulting in the network's inability to respond to an attack in a timely manner.

**Figure 1.** Internet of Things

Because of their widespread usage in the understanding of smart mobile devices such as smartphones, laptops, notebooks, Personal Digital Assistants (PDA), and other similar devices, the Internet of Things (IoT) is a fast-growing and common

technology in everyday life. In the digital world, these devices have become a part of everyone's life and have been used in a number of circumstances [7]. The primary goal of IoT-enabled devices is to be "linked anywhere, at any time," as seen in Figure 1, which depicts the interaction between IoT-enabled objects.

The routing protocol that detects the routes between nodes facilitates communication within the IoT network [8]. The routing protocol identifies the efficient routing of messages in the right timing between nodes in the IoT enabled network. It is designed with minimal overhead consumption and bandwidth. The nodes communicate with the neighbouring nodes and find the way to the destination [9]. WSN is composed of small communication nodes, lower calculation capacity and lower environmental memory that are used to detect the events and report back to the central monitoring device or node. Since the nodes are wireless, different attacks can be carried out. It is thus very important to establish the framework that addresses wireless sensor networks stability, reliability, safety, robustness, authentication and authorization.

The degree of assurance is defined in literature as an individual's faith in or confidence in another object [10]. The amount or level of trust that a node can have in the network is the amount or degree of trust that a node can have in the network in the absence of any other node. WSN trust could be regarded as a combined paradigm for mobility safety, reliability, and privacy [11]. "Building trust and analysing IoT network trust enables the node to communicate with other nodes or networks based on its trust values in security, dependability, and security [12]." The network node's trust solves the challenge of safe routing by providing the packet with a stable path and secure mobility model selection. The trust value is critical for sensor nodes in unattended and military contexts. To be confident, the assessment of trustworthiness must take place between the network's nodes [13]. To ensure node mobility in the sensor network, the security issue and trust evaluation are monitored [14].

Trust in the field of wireless networks can be described as the degree of confidence in the future comportment of other nodes based on past experience and observations of the action of nodes. The fundamental concept of a trust-based scheme is to measure trust in order to characterise individual nodes' confidence, trustworthiness or competence [15, 16]. In different applications for security management, trust management systems can be introduced such as the secure protocol, secure data aggregation trusted routing and an intrusion detection system [17]. Many states of the art models have been proposed in recent years in this field. The current achievements have certainly greatly encouraged research related to the enhancement of IoT network safety. Nevertheless, trust assessment in WSNs remains a challenge [18]. There are some drawbacks that need to be resolved more carefully.

To resolve the above problems, an effective Swift Routing Model with Node Trust Identity Factor (SRM-NTIF) model for IoT network is proposed in this research work. The trust value is measured according to multi trust variables in the proposed trust model, an effective trust assessment can be achieved.

## 2. LITERATURE SURVEY

Through wireless transactions with adjacent nodes, sensor nodes develop a node trust model. Debroy et al. [1] proposed the first RFSN model in which nodes used reputations to assess the trustworthiness of others. The System employs a watchdog method to monitor the contact behaviour of neighbouring nodes and reflects node credibility distribution using beta values. The trust value is then calculated using statistical expectations about the probability distribution of credibility. However, faith in the recommendation is not taken into account, and some internal attacks are unavoidable.

Pan and Yang [2] proposed an agent-based trust model. The agent node was used to track sensor node behaviours and to classify behaviours into good or malicious ones. Agent nodes count all the positive behaviours and the malicious behaviours and save three-fold the data. ATSN's system uses agents that can save energy and computing resources. In ATSN, however, only the value of the direct trust is determined if the trust recommendation is ignored. Furthermore, the trust value updating mechanism is not taken into account. The new lightweight trust management scheme for clustered WSNs proposed by Hasan and Al-Turjman [3]. The value of trust is obtained by neighbouring node contact. It operates on three levels of trust: node, cluster head and base station level. The model sets up a framework for trust to withstand attacks from malicious nodes. GTMS is able to efficiently avoid malicious node attacks and needs no massive data store and complicated calculations. However, it is not possible to represent a sound trust value only by analysing the amount of good and failing interactions.

Dayal et al. [6] proposed a multi-factor dynamic trust assessment process. The trust of the nodes is dynamically calculated by the combination of direct trust and indirect trust. Moreover, it depends on the interaction times between nodes, which are present under Hoeffding's unpredictable probability theory, both on the classification standards and dynamic weight allocations concerned. The results of the simulation show that this approach is susceptible to many attacks. But the trust value update mechanism is not taken into account.

Jhaveri et al. [7] proposed a model for clustered WSNs, a lightweight and reliable trust scheme. The trust-decision system is suggested on the basis of the functions of the nodes in clustered WSNs. By cancelling feedback between cluster members or between cluster heads, it improves device performance. The trust system also specifies a self-adaptive method for the aggregation of trust at cluster level. This methodology goes beyond conventional methods of weighting trust factors, in which weights are subjectively assigned.

Gupta et al. [10] described a trust management scheme called ReTrust which is immune to attack and lightweight routing. This framework, based on the hierarchical architecture, consists of master nodes and sensor nodes, is directed to a medical sensor network. To find and remove the on-off attack, ReTrust uses sliding times and ageing factor. After gathering recommendations bad-data transmission attacks are stopped, outliers are eliminated. It is immune to blackmail assaults. The disadvantage, however, is that main nodes must be stored extensively and have an abundance of resources. A credible Bayesian trust management system was proposed by Kolade [11]. Direct and indirect trust is taken into account in the trust management system. Direct trust is determined using an adaptive forgetting factor by means of a modified Bayesian equation with penalties and a sliding window update. In addition, a third party invokes the indirect trust calculation. In resistant attacks, BTMS performs better.

Khan et al. [12] initiated an assessment of the

trustworthiness of sensor nodes by different factors based on contact behaviours. Direct and indirect trust is achieved by the weighted average trust factors. In the meantime, the fuzzy configuration approach is used to determine the importance of a node with any trust level. The discrepancy between the evidence and the indirect trust is determined, which links the revised D-S proof mix to synthesise the integral trust value of the nodes.

Jain et al. [14] suggested a trust assessment approach for distributed cloud-based sensor networks. The method includes a contact, messages and energy factor to get a trust factor cloud. The method includes many variables. The trusted cloud is determined by assigning and combining weights for every trust cloud factor. The final trust cloud is determined by the synthesis of the trust cloud recommendation and the immediate trust cloud, and by trust cloud decision making is translated into a trust level. In different WSN applications, this method can detect malicious nodes according to different secure requirements and provide a safe operating environment for various applications. The trusted decisions and its dynamics, which were crucial for stabilising the entire network by evolutionary game theory, were investigated by Chhabra et al. [15]. For the field of trust development in WSNs, evolutionary game theory is utilised. It creates a WSN trust game on trust evolution dynamics during the decision-making phase of the sensor node. When sensor nodes decide to pick action with trust or suspicion, a WSN trust game is developed to mirror their utilities. It will determine the conditions for sensor nodes to select trust level as their final comportment to ensure the security and stability of WSNs.

Abdel-Azim et al. [17] proposed Effective Emergency Routing Protocol for Internet of Things. The author had designed an IoT connection based on the Global Information Decision and an advanced emergency response protocol known as Emergency Response IoT (ERIoT). They proposed an ERIoT protocol to enhance displays of solid bundles of knowledge transfer and efficient response to crucial situations in IoT arrangements. They displayed a portion of the Delay Iterative Method (DIM), based on an adjournment assessment that determines the issue of overlooking relevant and valid system courses.

Trivedi and Malhotra [18] proposed a multicast regulatory protocol based on IoT device placement. Through its goals, it reduces the frequency of source access and the shorter duration of multi-component systems. The conspiracy suggested comprises the call-up process, the restructuring phase and the reform phase. The local hubs get the total number of hubs to reach their destination in the Aid Request portion. Multi-cast modes can then be added by modifications of programmed techniques during the updated refresh and transfer phases. Simulation and survey results show that the suggested system will minimise the number of transmission connections and transmission delays on both sides effectively and change their versatility to allow modular travel.

Ali Zardari et al. [19] proposed two calculations with $K>2$ constraints to manage a difficult problem of multicast routing communication within the IoT network. The proposed calculations dramatically decrease the multifaceted nature of a multi-constrained routing problem and allow some important calculations to deal with the issue when applied to the sum of multiple constraints in an exhaustive measurement. The entropy method showed the multifaceted existence of the proposed calculations hypothetically and approximately, as well as large simulations to test the calculation presentation. Exploratory consequences have shown that a measurement of both speed and precision was better than a multi-limited multi-cast routing calculation.

Saudi et al. [20] designed a "Reliable Communication Energetic Efficient Device Discovery for the use of 5G IoT based vehicles and for the use of aerial vehicles. A method for IoT and BSNs with UAVs based on 5G has been introduced in this paper. The suggested approach uses a power model to generate the impression that the next 5G-PPP that is optimally used. It provides an interactive framework using XML charts to discover resources due to the expense of the state-owned network and the power available.

Baker et al. [21] showed a random walking distance determined using the nodes and the ranks of the nodes from other nodes. The inputs are node alignments of high scores. With their accurate random walk distance and built model with a random motion principle, each network node couple in the product diagram can be distinguished from other high-scoring alignments and, if the model is based on a clustering mechanism, the chances of energy consumption will increase. A model using Cluster-based Energy Efficient Secure routing to address power consumption issues is discussed in this model.

AbuMansour et al. [22] introduced a new TESRP in WSN that employs a decentralised system of trust in the detection and isolation of malicious nodes. To calculate residual energy and hop counts with trusted nodes, TESRP has integrated Composite Routing Feature (CRF). In the communication path, nodes with high CRF were considered. In this work the author used different loads and measured simulation metrics. The results of the simulation show that the performance of black hole attacks has deteriorated packet delivery rate, although the access points avoid all data packets passing through the path.

## 3. PROPOSED MODEL

Wireless sensor networks are the primary means for IoT device control systems. There is a large number of sensor nodes in a wireless sensor network [23]. Each sensor node has the capacity to communicate sensing, computing. With wireless transfer techniques, the sensor nodes transmit the data to a base station Sensor network system, however, need an appropriate lifetime routing structure [24]. Taking into account the constraints; for example, the need for significant capabilities and energy; the conventional routing solutions to these networks cannot be properly addressed [25]. In recent years too much research has been conducted to improve the restricted conventional solutions. The problems and routing algorithms must be changed in order to use the IoT in ordinary human life. It is a major challenge to route data from source to destination through vast IoT networks [26]. Communication devices with different network standards introduce new problems and limitations in the IoT, which are not taken into account in previous routing protocols. This requires routing that continuous changes in network topologies can be handled dynamically [27].

The interaction of sensors and actuators between devices is performed in IoT. For collecting, saving and processing data, a sensor will be used. In IoT, stored information is sent to a remote server to store and process the information on a remote server. Often, due to size constraints, energy consumption and computational capacity of IoT objects the storage and processing is limited to certain available resources. In IoT devices, routing plays a critical role [28]. Routing is a very

difficult feature of IoT due to its intrinsic characteristics. Routing protocol [29] is often referred to as a routing policy to specify how routing devices interact in the network, by dividing control data that selects the best routes for any two nodes between multiple routes [30]. Data can be shared from a source node through closer neighbours in the routing protocol and reaches the destination node. It determines the best route between the source and the target node on the basis of algorithms when routing [31].

The proposed model uses Swift Routing Model with Node Trust Identity Factor (SRM-NTIF) model for finding the best and trusted route by considering the trusted factors of each and every node involved in routing process by verifying the Digital Unique Identifier (DUI) of every node. When a group of IoT devices are connected, then the computational capabilities of all the nodes are calculated, energy levels are calculated, past malicious behaviour is considered and cluster sets are calculated for every single group of nodes and a cluster head is selected among the group. The node which has less malicious behaviour, high computational capabilities and high energy levels are considered as Nodes Cluster Head (NCH). All the NCH nodes again has a IoT Network Head (IoTNH) which monitors all the NCH nodes. The DUI is generated by the IoTNH node and distributed to the NCH nodes. Based on the DUI, if any malicious device tries to enter the network, it is easily detected and it is not allowed to involve in communication that provides a secure environment in IoT network for secure data transmission. The structure of the proposed model is represented in Figure 2.

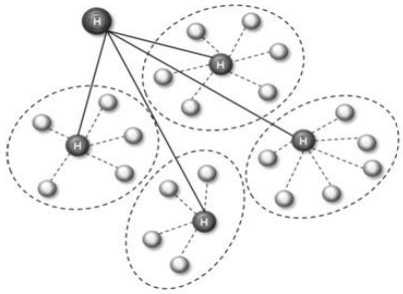

**Figure 2.** Proposed network structure

### 3.1 Digital unique identifier (DUI) calculation

Cryptography is the Semantic and mathematical techniques to secure information during data transmission in particular in communications in wireless networks. Cryptography was historically only concerned with encryption, that is with the transformation of data into an inexplicable and unreadable state of information from the normal stage with the use of a secret key. Keys are an important element in the cryptographic process to create and manage data. The IoTNH node in the proposed model generates a Digital Unique Identifier (DUI) for every IoT gadget. The IoT nodes that needs to involve in data communication has to request the DUI from the NCH node. The node provided with DUI will be continuously monitored by the NCH node during data transmission and malicious actions are monitored.

**Algorithm DUI Generation**

{

Step-1: Input all the IoT Nodes for establishing a wireless network and provide an ID for each IoT device.

Step-2: All nodes send a Digital Unique Identifier Request (DUIREQ) to the NCH Node where the request from every node has a REQ_ID.

Step-3: The NCH node verifies the request is received from the node in its range or not.

Step-4: The DUI is generated by the IoTNH node as:

$$IV_{Node(i)} = M^{N(ID)_n} \bmod P*Q + Threshold\_Vector$$

Here Intermediate Vector IV is calculated for all the nodes, $M$ is the REQ_ID of a node that is maintained by NCH node. $P$, $Q$ are randomly selected values of a node where $P<Q$ and $Q$ must be prime and a Threshold_Vector is considered.

$$IK_{Node(i)} = (M * Node(ID) + REQ\_ID)^{Q_n} \bmod P + Threshold\_Vector$$

The IoT device chooses a random number $P \in Z_n^*$, set $Z_n$ IoT NH nodes computes a DUI as:

$$compute\, K1_{N(i)} \leftarrow N(i)_i^n \,(\bmod P*Q)$$

$$compute\, K2_{N(i+1)} \leftarrow N(i)_i^n \,(\bmod IK_{Node(i)})$$

$$IK_{Node(i+1)} = \frac{\Sigma_{i=1}^{n}\left(K1_{N(i)} - K2_{N(i+1)}\right)\left(M - REQ\_ID_n\right)}{\Sigma_{i=1}^{n} N(i)_i^n \,(\bmod P*Q)^2 \Sigma_{i=1}^{n} REQ\_ID(N(i))}$$

$$DUI\,(N(i))_n^1 = \left(IK_{Node(i)} + IK_{Node(i+1)}\right) \oplus P \parallel Q + REQ\_ID(Node(i))$$

In the proposed model, the node once used should not be reused. The similarity of the keys is calculated and the unique keys are updated in the model that improves the security level of the system.

$$sim_{num}(DUI\,(N(i)), DUI\,(N(i+1))) = Uniq_k\,(DUI\,(N(i))_n, DUI\,(N(i+1))_n)$$

$$where\, DUI\,(N(i), N(i+1)) = \sqrt{\Sigma_{i=1}^{N}\left(DUI\,(N(i))_n\left[IK_{Node(i)}\right] - DUI\,(N(i+1))_n\left[IK_{Node(i+1)}\right]\right)^2}$$

Step-5: The IoTNH node will distribute the DUIs to the NCH nodes.

Step-6: If the node is valid, the NCH node send a DUIACK(DUI Acknowledgement) to the node back.

Step-7: The DUI node is used for the node trust factor calculation and its behaviour detection.

}

### 3.2 Trusted node detection

Based on the approximate trust value calculated, the trust function in routing avoids/includes nodes in routing operations. The establishment of trust and the credibility system are both components of a Trust Calculation system. Trust Calculation is characterised as an entity that deals with trust relationship management, such as information gathering, making trust-related decisions, assessing trust-related criteria, and observing and reassessing established relationships. Trust Calculation deals with tracking neighbouring nodes during transmissions, detecting misbehaviour, evaluating trust values based on performance accuracy and propagating trust values to complete the routing process.

**Algorithm Trust Calculation**

{

Step-1: Input the node_id, REQ_ID, DUI and NCH_ID.

Step-2: Initial node trust level is calculated as:

If (node_id ε $Z_n$)

{

If (REQ_ID==getrequest(NCH(ID))

{

If (PDR(N(i))>Threshold)

{

If (DUI (N(i)) ε DUIset(IoTNH(ID))

{

$$Tf\left(N(i)\right)=\frac{1}{PDR\left(N(i),Threshold\right)}DUI\left(N(i)\right)^{P-1}Node\_id^{Q-1}$$

The probability expectation value for trust factor is calculated as:

$$\lambda n(Tf\left(N(i)\right)=\frac{1}{\left|Tf\left(N(i)\right)_n\right|}+$$

$$\sum_{DUI_n\in IoTNH_n}\left|\frac{PDR_{N(i)}(Threshold)-}{\frac{Node\_id+\Sigma_{DUI\in IoTNH}\,N(i)}{\left|N_i\right|+NCH\_ID}}\right|$$

}

}

}

}

Step-3: If the node is having less packet delivery rate or malicious behaviour, such kind of nodes are not involved in communication.

Step-4: After calculating the nodes trust values, each node is assigned with a labelling trust vector for checking whether it is a trusted node or not.

Step-5: The nodes whose trust factors are more than the specific threshold, such kind of nodes are considered for routing and data communication.

}

### 3.3 Route detection process

Internet of Things are gaining significance because of its popularity and advantages for achieving quick data transmission and making the humans life easier. Few applications require fast data transmission with minimal interruption, despite the widespread use of sensor networks. Awareness of the network structure and routing protocol is essential, and it must be suitable for the user requirements. The routing protocol is a method for selecting an appropriate route for data to pass from source to destination. While selecting the path, which is dependent on the type of network, channel characteristics, and performance metrics, the process encounters many difficulties. The proposed model considers only trusted nodes to involve in data communication by considering the trust factors of nodes.

**Algorithm SRM-NTIF**

{

Step-1: All the nodes establish a IoT network for data communication

Step-2: NCH node is selected for every cluster.

Step-3: The sender will send Trusted Route Request (TRREQ) message to all the neighbour nodes.

**For each** N(i) ∈ Network set **do**

$$N(i)\leftarrow"TRREQ"+\left|\left(N(i).X-dest.X\right)\right|+\left|\left(N(i+1).Y-dest.Y\right)\right|$$

$$route\_table\leftarrow null$$

$$next\_hop\leftarrow null$$

$$Trust\_status\leftarrow null$$

Step-4: The NCH node will distribute DUIs to all the nodes that want to involve in communication.

**For each** N(i) ∈ Network set **do**

$$N(i)\leftarrow DUI\left(NCH\left(N(i)\right)\leftarrow IoTNH\left(set(DUI\left(N(i)\right)\right)\right)$$

Step-5: Neighbor nodes will send Node_Trust_Status to the NCH node to verify whether they received the TRREQ message from a trusted node or not.

Step-6: The NCH node will verify and update the status to the nodes. If the sender is trusted node, then the neighbours will send DUI Reply message (DUIREP) along with its node_id.

Step-7: The node will again verify whether it received reply from the trusted neighbour node from the NCH node to update the routing table and to update the trust status.

**For each** N(i) ∈ Network set **do**

$$N(i)\leftarrow"DUIREP"+\left|\left(N(i).X-dest.X\right)\right|+\left|\left(N(i+1).Y-dest.Y\right)\right|$$

$$route\_table[]\leftarrow Seq(N(i),N(i+1))$$

$$next\_hop\leftarrow N(i+1)$$

$$Trust\_status\leftarrow True$$

$$available\_routes[]\leftarrow Seq(N(i),N(i+1)+Seq(N(j),N(j+1))$$

Step-8: If the node fails to get verified at NCH node level, it is marked as malicious and then removed from the network communication.

$$Malicious\_nodes[]\leftarrow N(i)$$

$$Trust\_status\leftarrow False$$

Step-9: The process is repeated until the routing table is updated from source to destination and all nodes are labelled with the status.

Step-10: All the available routes are updated and the route having highest trust factor nodes are considered for data communication. If any link/node failure occurs, the next available route is considered.

}

The routing process in the proposed model is represented in Figure 3. The network considers only trusted nodes for initiating the data communication.

Route maintenance is a mechanism to detect the discovered path's node failure or topological transition. It begins the process of route exploration when the path breaks. This process enables the stable and fault tolerant network to be maintained. Data is transmitted hop by hop, via the neighbour's nodes present in the topology of the network. Effective transfer is not possible even if a node is dead on the rout. The preceding nodes are unable to know the next node's failure. The transmission of control packets in the IoT network is shown in Figure 4. The node mobility in the transmission

period results in a breakdown. The proposed model maintains a list of available routes. If there is any link or node failure identified, the new route is automatically selected and the data transmission is continued. The failed node is terminated from the route and the transmission path is updated with the other available routes in the sorted list. Thus, a periodic route update and maintenance process prevent interrupting the transmission of data and the overload of node failure.

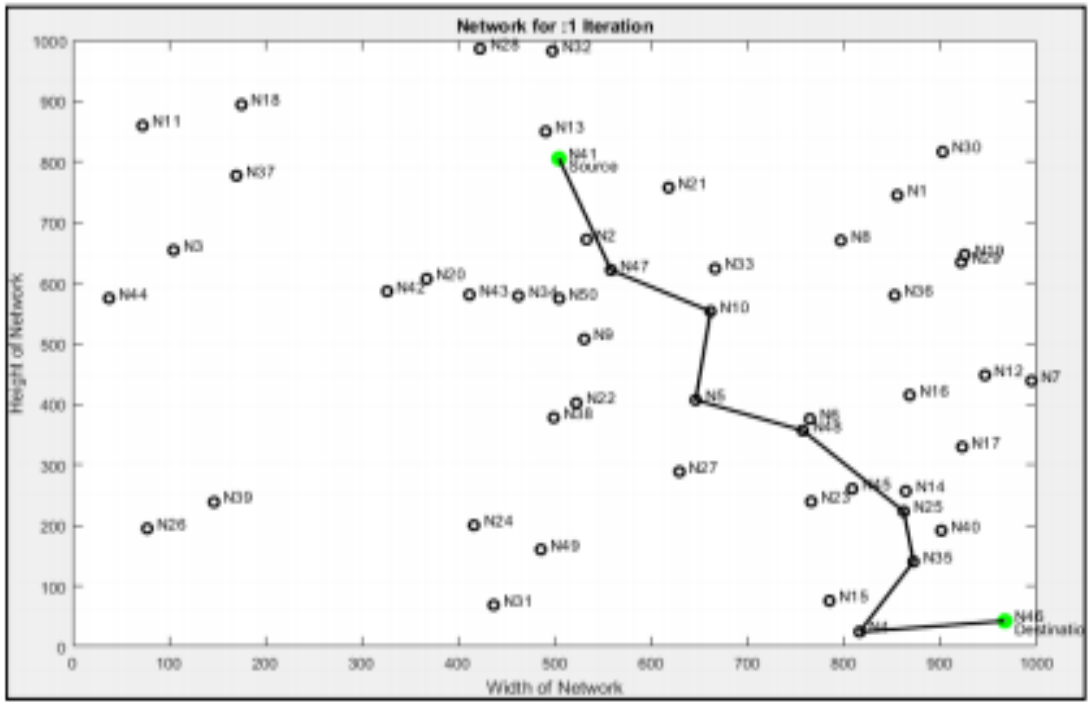


**Figure 3.** Routing process in IoT network

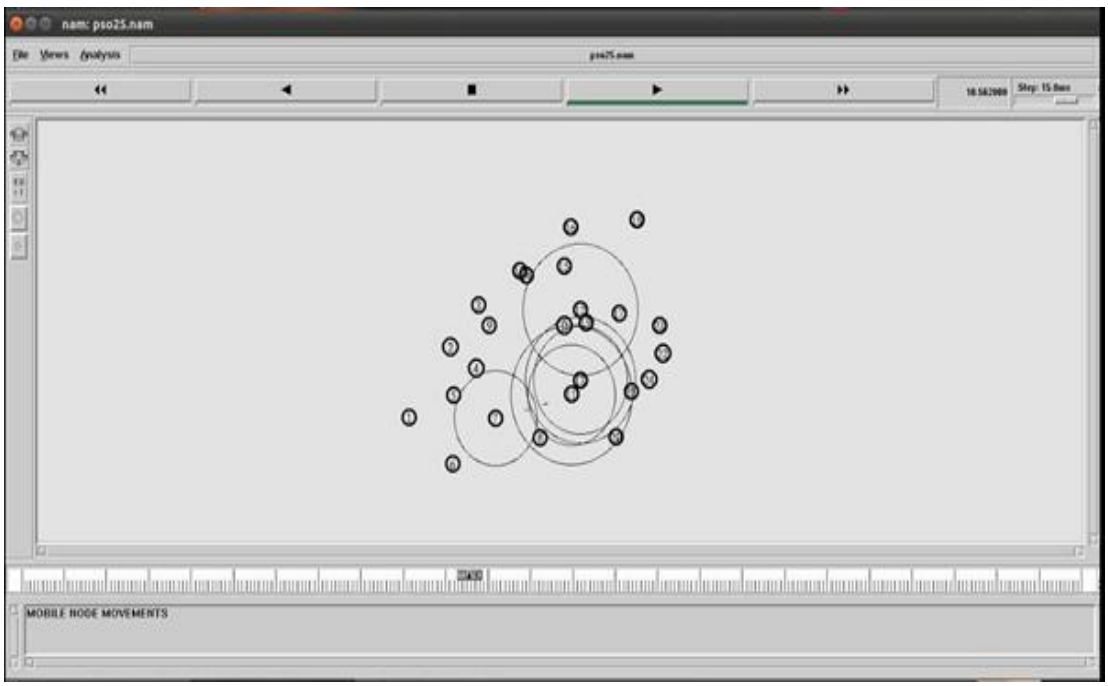


**Figure 4.** Data transmission in IoT network

## 4. RESULTS

This design uses NS2 as a simulation method for the verification of trust mechanism for secure routing to establish a IoT network. The trust levels of all the devices are calculated and then routing process is initiated using only trusted nodes for secure data transmission. The proposed Swift Routing Model with Node Trust Identity Factor (SRM-NTIF) model is used for establishing a secure route among the IoT gadgets for secure data transmission. Network Simulator 2 (NS2) offers extensive support for the modelling of many protocols over wired and wireless networks. It offers a highly modular

architecture for wired and wireless simulations that supports many network elements, protocols, traffic, and routing types [20]. It offers a number of features that make it a useful tool, including compatibility for numerous protocols and the ability to graphically display network activity. NS2 also supports a number of routing and queuing methods. Routing algorithms include LAN routing and broadcasting.

**Table 1.** Parameters used

| Parameter | Value |
|---|---|
| Initial energy/J | 0.5 |
| Initial trust value | 0.5 |
| Packet length/bit | 2000 |
| d/m | 37 |
| Number of behaviours in each time unit | 10 |
| Trust estimation period/s | 10 |
| Simulation time/s | 1000 |
| θ | 0.5 |
| m | 4 |
| A | 0.7 |

The proposed model is compared with the Incentive Jamming-based Secure Routing (IJbSR) model. The proposed model is compared with the traditional methods in terms of routing time levels, trust factor calculation time levels, trusted nodes labelling time levels, node validation time levels and total route security levels. The parameters used in the simulation is depicted in Table 1.

Because of the fundamental characteristics of these networks that distinguish them from other wireless networks, such as mobile Ad Hoc networks or mobile networks, IoT routing is particularly complex. First, developing a global address system for deploying a large number of sensor nodes is not practical since the network management overhead is considerable due to the relatively large number of sensor nodes. Figure 5 depicts the routing time levels of the proposed and traditional approaches. The routing time levels of the proposed model is low when compared to existing method.

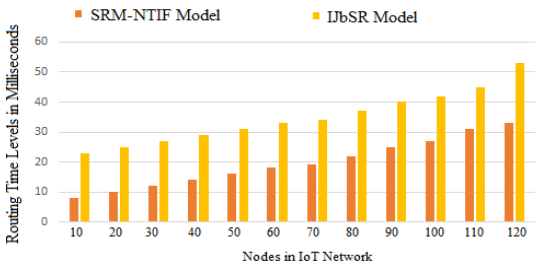


**Figure 5.** Routing time levels

The lack of knowledge in the process of cooperation on the other nodes contributes to the shared resources of trustworthy and untrustworthy nodes. Consequently, it is necessary to establish trust such that only the trusted nodes can share resources. The complex and unpredictable character of IoT makes some attacks vulnerable and results in less safety. Trust for building the safe IoT network is a challenging task for providing an environment for secure data transmission. The trust factor calculation time levels of the proposed and the traditional models are indicated in Figure 6.

The growth of trust management protocol identification methods ignores malicious behaviour discovered by direct and indirect systems. The active subject of research to eliminate the influence of rogue nodes in IoT networks is trust updating and the adoption of reputation protocols. The main variables restricting node activity are energy, processing capability, and battery capacity, and the impacted nodes are selfish nodes. The trusted nodes are labelled in the proposed work for future usage and the trusted node labelling time intervals are represented in Figure 7.

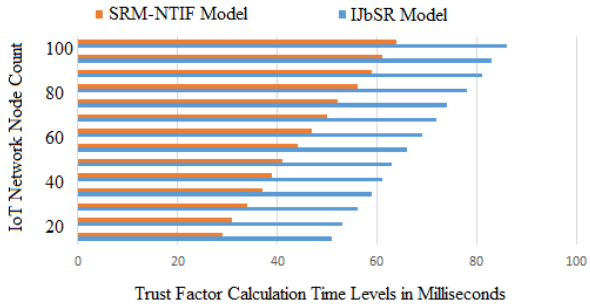


**Figure 6.** Trust factor calculation time levels

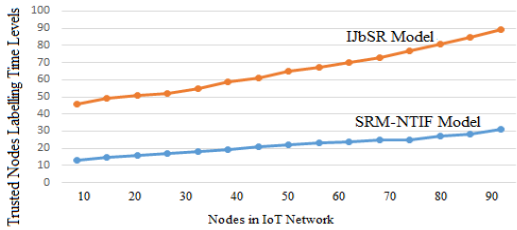


**Figure 7.** Trusted nodes labelling time levels

The mobility and movement of malicious nodes in an IoT network have a significant impact on the prevention of malicious nodes. The attacker learns about the complicated changes that occur as a result of data transfer in the routing path. As a result, trust protection in many applications requires immediate attention. The nodes in the network need to be validated before the data transmission is initiated. The proposed and traditional model node validation time levels are indicated in Figure 8.

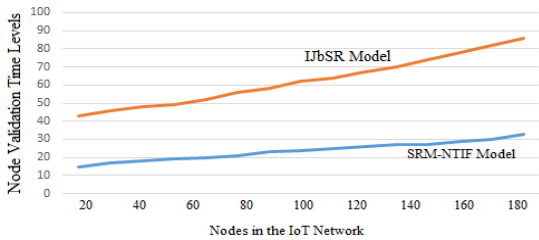


**Figure 8.** Node validation time levels

The distribution ratio for packets is the ratio of successfully received packets at destinations to the maximum amount of packets sent by source. The number of data packets sent to the destination reflects the level of data supplied to the destination. The packet delivery ratio of the proposed and existing models is represented in the Figure 9.

The proposed routing model performs secure data transmission by considering the trust factor of all the IoT nodes involved in communication. The security levels of the proposed model are high when compared to the traditional method. Figure 10 represents the total route security levels.

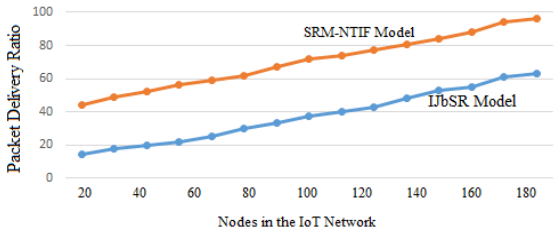


**Figure 9.** Packet delivery ratio

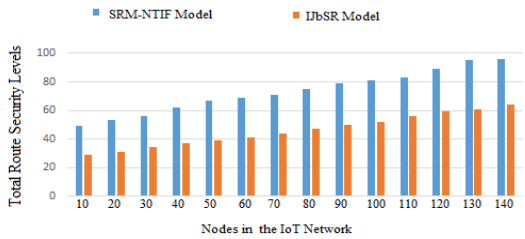


**Figure 10.** Total route security levels

## 5. CONCLUSIONS

The trust calculation is a challenge issue in any network because of impermissible changes in the network structure, IoT network dynamic existence and the association of trust between non-derived nodes increases the complexity for establishing a trusted route among the gadgets. This paper introduced a Swift Routing Model with Node Trust Identity Factor for establishing a secure route for secure data transmission among the IoT gadgets by considering the trusted nodes. In order to improve the accuracy of the network, the trust Factors are calculated for all the IoT nodes that involved in communication. Based on the trust factor, a node with trust value more than the threshold range are considered to involve in data communication. In addition, a dynamic weight factor for overcoming a defect caused by the arbitrary allocation of weight in the integrated trust calculation is also implemented. The proposed dynamic model of trust allows precise and objective trust assessment of nodes based on node behaviour. Factors such as the invalid path selection and content changes can be considered as a potential improvement during packet transmission for safe network packet transmission. The proposed model performance levels are better when contrasted with the existing models. In future, the trust factor calculation can be still improved and a central authority node will also be maintained for the monitoring of the entire network to improve the security levels of the network.

## REFERENCES


[1] Debroy, S., Samanta, P., Bashir, A., Chatterjee, M. (2019). SpEED-IoT: Spectrum aware energy efficient routing for device-to-device IoT communication. Future Generation Computer Systems, 93: 833-848. https://doi.org/10.1016/j.future.2018.01.002

[2] Pan, M.S., Yang, S.W. (2017). A lightweight and distributed geographic multicast routing protocol for IoT applications. Computer Networks, 112: 95-107. https://doi.org/10.1016/j.comnet.2016.11.006

[3] Hasan, M.Z., Al-Turjman, F. (2017). Optimizing multipath routing with guaranteed fault tolerance in Internet of Things. IEEE Sensors Journal, 17(19): 6463-6473. https://doi.org/10.1109/JSEN.2017.2739188

[4] Meng, Y., Jiang, C., Chen, H.H., Ren, Y. (2017). Cooperative device-to-device communications: Social networking perspectives. IEEE Network, 31(3): 38-44. https://doi.org/10.1109/MNET.2017.1600081NM

[5] Li, X., Li, D., Wan, J., Liu, C., Imran, M. (2018). Adaptive transmission optimization in SDN-based industrial Internet of Things with edge computing. IEEE Internet of Things Journal, 5(3): 1351-1360. https://doi.org/10.1109/JIOT.2018.2797187

[6] Dayal, N., Maity, P., Srivastava, S., Khondoker, R. (2016). Research trends in security and DDoS in SDN. Security and Communication Networks, 9(18): 6386-6411. https://doi.org/10.1002/sec.1759

[7] Jhaveri, R.H., Patel, N.M., Zhong, Y., Sangaiah, A.K. (2018). Sensitivity analysis of an attack-pattern discovery based trusted routing scheme for mobile ad-hoc networks in industrial IoT. IEEE Access, 6: 20085-20103. https://doi.org/10.1109/ACCESS.2018.2822945

[8] Ma, H., Liu, L., Zhou, A., Zhao, D. (2015). On networking of Internet of Things: Explorations and challenges. IEEE Internet of Things Journal, 3(4): 441-452. https://doi.org/10.1109/JIOT.2015.2493082

[9] Arya, N., Singh, U., Singh, S. (2015). Detecting and avoiding of wormhole attack and collaborative black hole attack on MANET using trusted AODV routing algorithm. In 2015 International Conference on Computer, Communication, and Control (IC4) IEEE, pp. 1-5.

[10] Gupta, P., Goel, P., Varshney, P., Tyagi, N. (2019). Reliability factor based AODV protocol: Prevention of black hole attack in MANET. In Smart Innovations in Communication and Computational Sciences, pp. 271-279. https://doi.org/10.1007/978-981-13-2414-7_26

[11] Kolade, T.A. (2018). A scheme for detecting and mitigating cooperative black hole attack in AODV-based MANET routing protocol. Ph.D. dissertation.

[12] Khan, A.A., Rehmani, M.H., Reisslein, M. (2017). Requirements, design challenges, and review of routing and MAC protocols for CR-based smart grid systems. IEEE Communications Magazine, 55(5): 206-215. https://doi.org/10.1109/MCOM.2017.1500744

[13] Bello, O., Zeadally, S. (2014). Intelligent device-to-device communication in the Internet of Things. IEEE Systems Journal, 10(3): 1172-1182. https://doi.org/10.1109/JSYST.2014.2298837

[14] Jain, A.K., Tokekar, V., Shrivastava, S. (2018). Security enhancement in MANETs using fuzzy-based trust computation against black hole attacks. In Information and Communication Technology, pp. 39-47. https://doi.org/10.1007/978-981-10-5508-9_4

[15] Chhabra, A., Vashishth, V., Sharma, D.K. (2018). A fuzzy logic and game theory based adaptive approach for securing opportunistic networks against black hole attacks. International Journal of Communication Systems, 31(4): e3487. https://doi.org/10.1002/dac.3487

[16] Gurung, S., Chauhan, S. (2018). A novel approach for mitigating gray hole attack in MANET. Wireless Networks, 24(2): 565-579. https://doi.org/10.1007/s11276-016-1353-5

[17] Abdel-Azim, M., Salah, H.E.D., Eissa, M.E. (2018). IDS against black-hole attack for MANET. International Journal of Network Security, 20(3): 585-592.

https://doi.org/10.6633/IJNS.201805.20(3).22
[18] Trivedi, M.C., Malhotra, S. (2019). Identification and prevention of joint gray hole and black hole attacks. International Journal of Ambient Computing and Intelligence (IJACI), 10(2): 80-90. https://doi.org/10.4018/IJACI.2019040106
[19] Ali Zardari, Z., He, J., Zhu, N., Mohammadani, K.H., Pathan, M.S., Hussain, M.I., Memon, M.Q. (2019). A dual attack detection technique to identify black and gray hole attacks using an intrusion detection system and a connected dominating set in MANETs. Future Internet, 11(3): 61. https://doi.org/10.3390/fi11030061
[20] Saudi, N.A.M., Arshad, M.A., Buja, A.G., Fadzil, A.F.A., Saidi, R.M. (2019). Mobile ad-hoc network (MANET) routing protocols: A performance assessment. In Proceedings of the Third International Conference on Computing, Mathematics and Statistics (iCMS2017), pp. 53-59. https://doi.org/10.1007/978-981-13-7279-7_7
[21] Baker, S.B., Xiang, W., Atkinson, I. (2017). Internet of things for smart healthcare: Technologies, challenges, and opportunities. IEEE Access, 5: 26521-26544. https://doi.org/10.1109/ACCESS.2017.2775180
[22] AbuMansour, H.Y., Elayyan, H. (2018). IoT theme for smart datamining-based environment to unify distributed learning management systems. In 2018 9th International Conference on Information and Communication Systems (ICICS), Irbid, Jordan, pp. 212-217. https://doi.org/10.1109/IACS.2018.8355469
[23] Aman, M.S., Quint, C.D., Abdelgawad, A., Yelamarthi, K. (2017). Sensing and classifying indoor environments: An Iot based portable tour guide system. In 2017 IEEE Sensors Applications Symposium (SAS), Glassboro, NJ, USA, pp. 1-6. https://doi.org/10.1109/SAS.2017.7894055
[24] Li, R., Asaeda, H., Li, J. (2017). A distributed publisher-driven secure data sharing scheme for information-centric IoT. IEEE Internet of Things Journal, 4(3): 791-803. https://doi.org/10.1109/JIOT.2017.2666799
[25] Wazid, M., Das, A.K., Odelu, V., Kumar, N., Conti, M., Jo, M. (2017). Design of secure user authenticated key management protocol for generic IoT networks. IEEE Internet of Things Journal, 5(1): 269-282. https://doi.org/10.1109/JIOT.2017.2780232
[26] Maheshwari, N., Dagale, H. (2018). Secure communication and firewall architecture for IoT applications. In 2018 10th International Conference on Communication Systems & Networks (COMSNETS), pp. 328-335. https://doi.org/10.1109/COMSNETS.2018.8328215
[27] Torre, I., Koceva, F., Sanchez, O.R., Adorni, G. (2016). A framework for personal data protection in the IoT. In 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), Barcelona, Spain, pp. 384-391. https://doi.org/10.1109/ICITST.2016.7856735
[28] Gochhayat, S.P., Kaliyar, P., Conti, M., Tiwari, P., Prasath, V.B.S., Gupta, D., Khanna, A. (2019). LISA: Lightweight context-aware IoT service architecture. Journal of Cleaner Production, 212: 1345-1356. https://doi.org/10.1016/j.jclepro.2018.12.096
[29] Li, Q., Gochhayat, S.P., Conti, M., Liu, F. (2017). EnergIoT: A solution to improve network lifetime of IoT devices. Pervasive and Mobile Computing, 42: 124-133. https://doi.org/10.1016/j.pmcj.2017.10.005
[30] Oh, S.R., Kim, Y.G. (2017). Security requirements analysis for the IoT. In 2017 International Conference on Platform Technology and Service (PlatCon), pp. 1-6. https://doi.org/10.1109/PlatCon.2017.7883727
[31] Conti, M., Kaliyar, P., Lal, C. (2017). REMI: A reliable and secure multicast routing protocol for IoT networks. In Proceedings of the 12th International Conference on Availability, Reliability and Security, pp. 1-8. https://doi.org/10.1145/3098954.3106070