ASTES

Advances in Science, Technology and Engineering Systems Journal Vol. 7, No. 3, 95-105 (2022)

www.astesj.com

Special Issue on Multidisciplinary Sciences and Engineering

ASTESJ

ISSN: 2415-6698

A Secure Trust Aware ACO-Based WSN Routing Protocol for IoT

Afsah Sharmin*, Farhat Anwar, S M A Motakabber, Aisha Hassan Abdalla Hashim

Faculty of Engineering, Department of Electrical and Computer Engineering, International Islamic University Malaysia, Kuala Lumpur, 53100, Malaysia

ARTICLE INFO

Article history:
Received: 14 April, 2022
Accepted: 16 May, 2022
Online: 27 May, 2022

Keywords:
Internet of Things
Wireless Sensor Network
Routing algorithms
Ant Colony Optimization
Security
Trust Value
Energy consumption

ABSTRACT

The Internet of Things (IoT) is the evolving paradigm of interconnectedness of objects with varied architectures and resources to provide ubiquitous and desired services. The popularization of IoT-connected devices facilitating evolution of IoT applications does come with security challenges. The IoT with the integration of wireless sensor networks possess a number of unique characteristics, so the implementation of security in such a restrictive environment is a challenging task. Due to the perception that security is expensive in terms of computation, power and user-interface components, and as sensor nodes or low-power IoT objects have limited resources, it is desired to design security mechanisms especially routing protocols that are light weighted. Bio-inspired mechanisms are shown to be adaptive to environmental variations, robust and scalable, and require less computational and energy resources for designing secure routing algorithms for distributed optimization. In IoT network, the malicious intruders can exploit the routing system of the standardized routing protocol, e.g., RPL (The Routing Protocol for Low-Power and Lossy Networks), that does not observe the node's routing behavior prior to data forwarding, and can launch various forms of routing attacks. To secure IoT networks from routing attacks, a secure trust aware ACO-based WSN routing protocol for IoT is proposed here that establishes secure routing with trustworthy nodes. The trust evaluation system, is enhanced to evaluate the node trust value, identify sensor node misbehavior, and maximize energy conservation. The performance of the proposed routing algorithm is demonstrated through MATLAB. Based on the proposed system, to find the secure and optimal path while aiming at providing trust in IoT environment, the average energy consumption is minimized by nearly 50% even as the number of nodes has increased, as compared with the conventional ACO algorithm, a current ant-based routing algorithm for IoT-communication, and a present routing protocol RPL for IoT.

1. Introduction

The IoT (Internet of Things) is an evolving technology that performs a significant role in interconnecting intelligent devices or objects that surround us into a network. Integration of wireless sensor networks (WSNs) and IoT, offer a wide variety of applications domains that contour human life and also have influence on economic benefits. The IoT applications have touched its presence in many spaces, such as smart homes, smart cities, smart grid systems, banking, healthcare, environmental monitoring, transportations, data management and analysis and agriculture etc. The evolution of novel applications, systems, and technologies are intensifying attention from the research perception as well. Fueled by the extensive use of systems of interconnected intelligent objects or things enabled by wireless technology such as radio frequency identification (RFID), Wi-Fi, Bluetooth, embedded sensor and actuator nodes, cell phones, IoT is transforming into a fully integrated future internet from the static internet that would provide autonomous, smart behavior and pervasive communication networks for smart connectivity and context-aware computation. This paper is an extension of work originally presented in ICCCE'21 [1].

The present network protocols for wireless communications become inadequate when it comes to the IoT because of the large upsurge of IoT objects, diversity of continually emerging devices and possessions, and heterogeneity among objects' architectures.

*Corresponding Author: Afsah Sharmin, Faculty of Engineering, Department of Electrical and Computer Engineering, International Islamic University Malaysia, 53100 Kuala Lumpur, Malaysia Tel: +60142217380
Email: afsahsharmin@gmail.com

Especially, when the objects or nodes in the IoT system have limited resources in term of energy, memory and processor and the topology changes due to the mobility of the nodes. There are numerous applications, systems, and services from diverse manufacturers, as well as a wide range of hardware and software requirements, making a comprehensive compliance process for efficient and secure IoT-communication difficult to achieve. Also, the adaptation process of conventional communication protocol to take into account the structural and logical characteristics of the IoT modules is also very challenging.

During IoT routing, which influences and aids the interconnectivity of devices, a crucial deliberation focuses on energy efficiency, secure communication, scalability, computational complexity, autonomy, changed environmental issues, node mobility, resource constraints, and QoS (quality of service) requirements for specific applications. The sensors deployed in an IoT system, are energy-constrained and characterized by their self-organization; they sense, monitor and collect data, and perform computational functions while communicating over wireless networks and lossy channels. Because of the distinctive features of IoT networks, the system is subject to a variety of attacks, and many IoT devices are low-powered and computationally weak, and are not built to address security and privacy issues, a security breach could occur in such a system. Despite the fact that various IoT-specific routing protocols have been designed for providing routing decisions, within satisfying resource consumption, they have not been exhaustively verified for trustworthiness [2]. A secure routing protocol is essential for secure exchange of data with the intended parties rather an attacker and a mechanism is required for the stipulation of predetermined participants or discovering trustworthy nodes to collaborate with. Wireless sensor network which is constructed on autonomous nodes collaboration, plays a vital role in providing ubiquitous computing facilities to the diversification of IoT. There are numerous threats and challenges in the area of communication security, and wireless communication is particularly vulnerable to data exposure. The importance of route security is likewise high because the nodes are spatially scattered over a large area and the base station may be located distant from the information-carrying sensor node or device, requiring multi-hop communication to cooperatively send data over the network to a main location or the sink node for which routing path is necessary [3].

To protect the information in IoT devices, a significant range of secure routing algorithms and security mechanisms, including cryptographic techniques for message integrity, have been proposed by the scientific community. When malicious nodes or internal adversarial nodes or internal compromised nodes are present, the keys exchanged for interactions with the other nodes in the network are compromised as well. Most of the secret keys distribution algorithms are computationally expensive and take additional resources such as large memory space and CPU cycles, and that would result in performance degradation, while making it difficult to distinguish between malicious and non-malicious nodes using solely cryptographic measures. As a result, they are inappropriate for resource-constrained network systems. The notion of providing security is pricy with regard to compute, electrical energy, and user-interface components due to low-powered IoT objects, sensor and actuator nodes. If the encryption keys are accessed by the attackers, the whole network's data could be susceptible to exposure. If the protocol does not take the node's behavior into account throughout the routing process, security attacks like Rank attacks and Sybil attacks can be carried out without difficulty, paving the way for further insider attackers. These attacks can be mitigated by employing trust-aware secure routing protocols.

Existing WSN and IoT routing protocols are unable to adequately set of scales security and energy consumption, resulting in routes that are not globally optimum and might fail to function in the face of malicious attacks, threats and vulnerabilities. Bio-inspired processes offer low-cost options for developing secure routing algorithms that find the optimal path. Furthermore, finding trustworthy neighbors is a critical responsibility. Thus, an accompanying security solution known as trust management has been applied and enhanced [4]. In order to manage the network's highly dynamic topology while preserving energy efficiency during data transfer, various intelligent systems and biological systems, as well as the techniques by which they solve their everyday challenges, are used in the construction of secure routing algorithms. The ant colony optimization (ACO) system is a bio-inspired algorithm that uses the notion of self-organization to aid ants' coordination for solving problems. This technique is notably inspiring for addressing security issues in IoT network routing, as ants create paths that satisfy precise constraints in a graph. Bio-inspired processes are robust, adaptive, and scalable, and they aid in the design of optimal algorithms and distributed systems. The probability formula is utilized for route selection in ACO, which is a probabilistic process, while the pheromone update formula is used for pheromone trail updating [5].

EICAntS (Efficient IoT communications based on ant system) is an ant-inspired routing strategy for optimizing IoT communications that was proposed in [6]. The energy parameter is used in the calculation of the global efficiency factor, which represents the ant colony system's pheromone estimations. This approach extends network lifetime while reducing energy usage. The energy impact concentrates the data class that the node manipulates. The various difficulties afflicting the energy factor, for instance small-scale multi-path fading and large-scale fading, free-space path loss in wireless communications are not indicated here. Furthermore, no precise details for calculating the energy level of the nodes are provided. Three routing metrics, ETX (Expected Transmission Count), load or content, and residual energy, are utilized separately and in combination in [7] to enhance the design of the proactive routing protocol RPL (Routing Protocol for Low Power Lossy Network) objective function (OF), that is used to automate the route development method, for IoT applications. Residual energy (RE) in conjunction with ETX (EE) and an upgraded timer setup is effective for energy consumption. On the other hand, unlike the ant colony based approach, which employs the mechanism at work in ant-colony foraging, there is no optimization model used. Using the principles of rank threshold limitations and hash chain authentication, a secure-RPL (SRPL) protocol is suggested in [8] to minimize the influence of rank manipulation. This technique is seemed to be computationally expensive as it combines cryptography with hash chain authentication. In addition, nodes are vulnerable to insider attacks. In [9], the authors suggested a trust-based threshold method for the selection of a parent node to provide security countermeasures to Rank attacks amid RPL routing. The scheme's benefit is that the attacking node is recognized in the course of selection process of

the parent node, which mitigates Rank attacks. The scheme's downside is that additional susceptible attacks, such as blackhole and Sybil attacks, cannot be identified and alleviated well. The authors proposed approaches for the detection and mitigation of Rank attacks that are inconsistent with RPL-supported IoT in [10]. The node's trustworthiness is not considered by the technique, which leads to further security issues, targeting network traffic and resources.

In RFSN [4] framework, the sensor nodes keep reputation about other nodes in the system. Within this framework, a beta reputation system that uses Bayesian formulation has been employed. Using a watchdog mechanism, a node observers the behavior of other nodes. In this way, their reputation is built over a period which help to evaluate their trustworthiness to collaborate. Also, their future behavior is predicted. Direct and indirect reputation are built up using direct observations and second hand information respectively. The statistical expectation of the probability distribution signifies the reputation, which is used to calculate trust. However, this schema does not include a provision for distributing information about a bad reputation. As a result, it is unable to cope with uncertainty. Secure alternate path routing in sensor network (SeRINS) detects and isolates the compromised nodes by providing key management system along with the neighbor report system where the inconsistent routing information have been injected by those nodes [11]. Here, the compromised node is found out using neighbor report technique. The base station then broadcasts the compromised node's ID, key ring to the entire network and that malicious node is excluded using revocation of its cryptographic keys network-wide. However, the proposed technique needs huge changes to apply in the network as it is majorly embedded in the routing arrangement and neighboring nodes can eavesdrop.

A hybrid tree-based search approach called ANT-BFS is presented in [12] to determine the best and shortest information transmission route in order to enhance network performance. ACO is used in conjunction with breadth first search algorithm to investigate the neighbors so as to identify the solution or the requisite node. The amount of energy used is reduced with this strategy. The execution of BFS in ACO, on the other hand, necessitates more memory and computation time. In [13], quantum computation method is introduced and a new WSN routing algorithm, named the Quantum Ant Colony Multi-Objective Routing (QACMOR), is proposed to monitor in complex manufacturing environments. The node pheromone is characterized by quantum bits and to update the pheromone concentration of the path, the quantum gates are rotated. This method improves convergence performance and saves energy consumption. However, the computational complexity of the algorithms and effects on QoS are not addressed in this technique and need to be considered as QoS is posed by real-time applications. In [14], a routing protocol REL for IoT based on residual energy and wireless link quality estimate is suggested to improve reliability and energy efficiency. It enhances the quality of service (QoS) of IoT applications. To improve protocol reliability, received signal strength indication (RSSI) and signal to noise ratio (SNR) are used to generate the link quality estimate for wireless links. To reduce protocol overhead, an opportunistic piggyback technique is implemented, and the residual energy is transmitted to adjacent nodes to increase energy consumption. Despite this, no better approach is used, as opposed to the ant-inspired routing algorithm, which makes use of the ant-based system.

The proposed system of ours [15] has been analyzed more here to efficiently balance security and energy consumption. The proposed routing algorithm has considered important communication parameters for data transmission in an IoT network, such as mobility and energy parameters. This paper extends the work reported in [1], where a secure bio-inspired routing protocol based on ant colony optimization (ACO) systems is proposed, with the intension of providing trust in WSNs while improvising efficient IoT communications.

The relevant work is introduced in Section 1 and the rest of this paper is organized as follows. The system model and energy consumption model are discussed in Section 2. Section 3 depicts the proposed scheme in detail, including the proposed secure ACO algorithm and its design concept, the trust model used as a security mechanism, and trust assessment. The performance of the proposed system is evaluated in Section 4. Finally, some concluding remarks are provided in Section 5.

2. System Model and the Energy consumption model

The chosen network system is based on an IoT sensor organization in which the deployed nodes, sensors and actuators M_i are dispersed throughout the monitored area at random. The graph G linked with the nodes and symmetrical communication links makes up the system model for an IoT communication network. The energy and computational resources available to the sensor nodes in the region are the same. The received signal strength indication (RSSI) can be used by the nodes to calculate the estimated distance of the transmitters, where the transmission power must be acknowledged. The nodes can adjust transmission power and keep records of their neighbors' information updates. The presented system uses the radio energy model of wireless communications [16] and is implemented utilizing (1) to analyze the energy consumption. The quantity of energy consumed is determined by the distance between transmitting and receiving nodes, the size of the packets, and a distance-threshold value, d_0. The two types of energy consumption models applied here are free-space (the transmission power attenuates inversely proportional to d^2) and multi-path fading (the received power is falling off inversely with d^4) models. The following equations are used to calculate the energy consumption (E_{tran}) by the sensors during the transmission of an m-bit data:

$$E_{tran}(m,d) = \begin{cases} mE_{elec} + m\epsilon_{fs}d^2 & if\ d < d_0 \\ mE_{elec} + m\epsilon_{mp}d^4 & if\ d \geq d_0 \end{cases} \quad (1)$$

where ϵ_{fs} and ϵ_{mp} are the amplifying radio's energy consumption in the free-space and multi-path fading models, respectively. The distance is denoted by d, while the threshold value for the distance is denoted by d_0. Electronic devices' circuitry is powered by energy dissipation, E_{elec}. Now, $E_{Rx}(m)$, the reception energy for an m-bit data for a node, can be calculated as follows:

$$E_{Rx}(m) = mE_{elec} \quad (2)$$

The following equation is used to compute the residual energy (E_{res_i}) of a node n_i :

$$E_{res_i} = E_{tot_i} - E_{tran_i} \quad (3)$$

where E_{res_i} denotes the residual energy, E_{tot_i} represents the total initial energy and E_{tran_i} represents the transmission energy.

3. Proposed Secure Routing Protocol based on ACO

3.1. Proposed improved ACO Algorithm

a) The state-transition formula:

By examining the nodes' stable energy consumption while keeping in consideration the security issues for next-hop routing to determine the most trustable route getting to the node that delivers the certain required provision, an enhanced network routing algorithm based on ACO is proposed here. Hence, the next hop selection by the ants depends upon residual energy level of the neighbor nodes, i.e., the node with greater energy level possessing more probability of being selected higher, and their trust value, i.e., regarding the nodes' high trust value as probabilistic next-hop for routing. Assume if an ant *m* is located at node *i* at time *t*, it will comply to the following probability formula to choose the subsequent node *j* as the information forwarding node of the ensuing route for the proposed improvement of our ant colony optimization based routing algorithm [15]:

$$P_{ij}^{m} = \begin{cases} \frac{[\tau_{ij}(t)]^{\alpha}[\eta_{ij}(t)]^{\beta}[\vartheta_{ij}(t)]^{\gamma}[T_{ij}(t)]^{\psi}E_j}{\sum_{s\subset allowed_m}[\tau_{is}(t)]^{\alpha}[\eta_{is}(t)]^{\beta}[\vartheta_{is}(t)]^{\gamma}[T_{is}(t)]^{\psi}E_s} & , j \subset allowed_m \\ 0, \quad others & \end{cases} \quad (4)$$

$$\text{here,} \quad \eta_{ij}(t) = \frac{1}{d_{ij}} \quad (5)$$

where $\tau_{ij}(t)$ is the amount of pheromone deposited on edge (i, j) and $\eta_{ij}(t)$ is the state transition desirability of edge (i, j). A priori knowledge, typically the heuristic value $\eta_{ij}(t)$ is $1/d_{ij}$ and d_{ij} is the distance between *i* and *j*. There are two impact factors, α and β, that control the influence of the pheromone intensity and heuristic value respectively. In accordance with the average node mobility or speed, the stability factor, $\vartheta_{ij}(t)$, is determined, where γ is the mobility constant. $T_{ij}(t)$ is the high trust value of nodes at time *t* or the trust metric and ψ is the impact factor that control the influence of trust level among the nodes to further communication. The calculation of the trust metric will be provided below. E_j represents the node residual energy that ant *m* would visit.

a) The local update:

After an ant finish mapping a node *i* to node *j*, the corresponding pheromone intensity $[\tau_{ij}(t)]$ is updated by a local pheromone updating rule according to (6). Besides enhancing diversity of the algorithm, local pheromone update is augmented here in case a large quantity of pheromone value is accumulated down the pathways, while preventing faster local convergence. As a result, the pheromone measure is restored and controlled through the use of a threshold rating, and the updating rule which is assessed by following equation:

$$\tau_{ij}(t+1) = \begin{cases} T, & \tau_{ij}(t+1) > T \\ (1\text{-}\rho)\tau_{ij}(t) + \Delta\tau_{ij}(t) & else \end{cases} \quad (6)$$

$$\Delta\tau_{ij}(t) = \sum_{k=1}^{m} \Delta\tau_{ij}^{k} \quad (7)$$

where ρ signifies the local pheromone decay parameter, $\rho \in (0,1)$, a threshold value T is provided to restrict excessive pheromone accumulation, $\Delta\tau_{ij}(t)$ is the appended pheromone deposition of link (i, j), which is typically specified as below:

$$\Delta\tau_{ij}^{k} = \begin{cases} \frac{S}{L_k} & if\ kth\ ant\ travels\ on\ the\ edge\ (i,j) \\ 0 & otherwise \end{cases} \quad (8)$$

where *S* is a constant represents the strength of pheromone, L_k is the cost of the k^{th} ant's tour known as length, and *m* is the number of ants.

3.2. Trust Model used as a Security Mechanism

Trust framework involves two participants: trustors and trustees, who work associatively to accomplish a particular job based on a node's estimated trust value to determine its trustworthiness. A weighed value index, denoted as the node's trust rating, is assessed depending on the judgement of a node's prior behaviour, which also establishes the node's reputation [4]. The trust management approach identifies malicious and other attackers and compromised nodes in the communication network by evaluating their trust value in order to deal with unpredictability about the nodes' future activities. This reflects a node's trustworthiness while engaging with its neighbors, either directly or indirectly, to complete a set of specified activities. Consequently, the behaviour of a node is observed and that defines the positive or negative interactions over time, which is demonstrated as expressions to represent the calculable range of values, such as the trust value rating, while also indicating a node's reputation metric. For secure routing, neighbors or adjacent nodes with greater trust metric values are chosen, whereas nodes having lower values of trust or if trust values of these suspect nodes do not increment with time, then these nodes are identified as malicious. The security mechanism described in [4], manipulating a watchdog mechanism, is utilized and expanded upon here, where a beta reputation system based on Bayesian formulation is applied via direct/indirect observations to signify reputation metric.

The direct trust (DT_{ij}) is the rating of the latest activities of node *j* by node *i*. and it is calculated through the expected value of the probability distribution function. While allowing for consideration of the beta distribution and beta function, as a previous distribution property in the communications between the nodes, yields the direct trust value that node *i* has on node *j*. The direct trust is represented as follows:

$$DT_{ij} = \frac{\acute{\alpha}_j + 1}{\acute{\alpha}_j + \acute{\beta}_j + 2} \quad (9)$$

where $\acute{\alpha}_j$ indicates the successful or cooperative interactions and $\acute{\beta}_j$ indicates the unsuccessful or non-cooperative interactions or interactive behaviors between node *i* and *j* accordingly from the perspective of node *i*.

While an entity can make a precise direct trust judgement based on direct observation without a third party involvement for its adjacent nodes, it relies on the recommendations of trusted nodes to assess trust for packet transmission to nodes that are not directly connected. In case of uncertainty, presume that the evaluating node *i* needs the recommendation from a third entity and acquires reputation rating of node *j*, via their commonly adjoining nodes *k*. According to the principle of trust transfer decline, the recommended trust metric is calculated by following equation:

$$RT_{ij}^{k} = DT_{ik} * DT_{kj} \tag{10}$$

here, RT_{ij}^{k} gives the recommended trust value that node *i* possesses about node *j* offered by the common neighbor nodes *k*, and is derived by the product of the direct trust values, DT_{ik} and DT_{kj}. Accordingly, DT_{ik} represents direct trust rating between nodes *i* and *k*, and DT_{kj} represents direct trust rating between nodes *k* and *j*.

The trust metric $T_{ij} \in [0,1]$ of node *i* holds for *j* is the operational trust rating that is computed by collecting interactive records from third parties through direct observation or indirect observation. The weighted average, an associatory trust aggregation function, is computed by combining the estimates RT_{ij}^{k}, where distinct recommenders' provisions are brought into consideration for computing RT_{ij}^{k} particularly from each trusted edge. The trust metric is given as follows:

$$T_{ij} = \sum_{k \in N_i} \left(RT_{ij}^{k} * w_k \right) \tag{11}$$

$$\text{here, } w_k = \frac{DT_{ik}}{\sum_{k \in N_i} DT_{ik}}, \; k = 1,2, \ldots, N_i. \tag{12}$$

$$DT_{ik} = \frac{\acute{\alpha}_k + 1}{\acute{\alpha}_k + \acute{\theta}_k + 2} \tag{13}$$

where the weight w_k is assigned depending on recommenders' trust levels to lessen the influence of personal choice. In the above equation, $w_k (0 \le w_k \le 1, \sum_{k=1}^{N_i} w_k = 1)$ is the weight of RT_{ij}^{k}. The direct or indirect recommendations for node *j* received by node *i* from a set of trusted nodes denoted as N_i. It also indicates the number of received recommendations that is utilized. DT_{ik} represents the direct trust values between nodes *i* and *k*, while $\acute{\alpha}_k$ and $\acute{\theta}_k$ represent the prior recommendation or reputation metric, successful and unsuccessful interactive records accordingly that node *i* already possesses about node *k*.

In the proposed system, every sensor node manages and controls its own pheromone traces while not adding too much overload to the network, and maintaining the lightness of the model. Moreover, to gather ratings, there is not any central or supervising entity and each transmitted ant carries the sensors' identifications along with the pheromone traces.

On the contrary, a reputation rating depending upon pheromone value, τ_{ij}, of a communication route can be established here where the higher is the pheromone trace, the quality of the path, the higher is the security. Every node saves its own pheromone traces and the pheromone traces for its neighbors. In this sense, a more secured route is with more pheromone deposits, implying that a linked node holds greater packet forwarding or collaborative capabilities. The deterministic factor as well as this pheromone measure, $\tau_{ij} \in [0, 1]$, will determine the probability of ants selecting one path or another and the trust value in association with reputation metric provided by an entity to another node specifies the deterministic factor. If the reputation of a node at time *t* is denoted by $\varphi_{ij}(t)$, then the following equation can be applied for the detection of a malicious node:

$$\tau_{minimum} = \frac{\sum_{i=1}^{n_k} \tau_{ij}(t)}{n_k} \tag{14}$$

where τ_{ij} represents the pheromone quantity in between nodes *i* and *j*, and the number of *i*'s neighbors is n_k. If $\varphi_{ij}(t) < \tau_{minimum}$, which indicates the node's reputation falls below the minimum reputation conditions, $\tau_{minimum}$, then security threat or node's misbehavior is detected, and this node is identified for its malicious tasks, and will have fewer forwarding capabilities.

3.3. Trust Assessment

High-trust level nodes are used for routing decisions or secure communications by the proposed method. During the trust calculation process when the trust values have been determined, a trust assessment system is further adopted for ranking the highest to the lowest trust values, T ([0, 1]). This will further help to detect and eliminate the misbehaving node, where nodes with lower trust values are categorized as malicious. The membership degree and fuzzy classification of nodes' trust are implemented here. Three grades or level of trust have been provided for trust evaluation of a node by using fuzzy judgment as: distrust, uncertain and completely trust level or state which is represented in Table 1. Three fuzzy subsets T1, T2 and T3, as shown in Fig. 1, and the corresponding membership functions are defined as m1 (t), m2 (t) and m3 (t) and m1 (t) + m2 (t) + m3 (t) = 1.

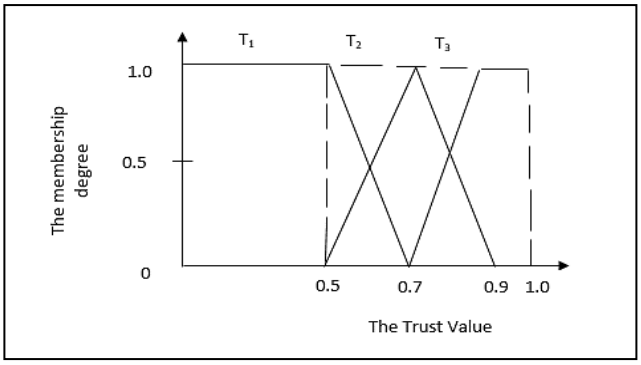

Figure 1: The membership function of node's trust

Table 1: Trust States

Three fuzzy subsets (T)	Trust level
$\boldsymbol{T_1}$	Distrust

T_2	Uncertain
T_3	Completely trust

3.4. The global update and the fitness-function

The global updating of pheromone concentration is worked out after all of the ants have constructed their solutions, finishing their search and have appeared at the target node. In addition, after the search is completed, each ant corresponds to a routing path. To begin, the path estimation rating, which is a route assessment function, is provided as (15) using the existing node energy, route length [m^{th} ant's route length L_m^k in k^{th} iteration], and trust metric. Some nodes will die prematurely if the residual energy [E_{res_i} for a sensor node n_i] is not analyzed as it is in the typical ACO method, reducing the network's overall lifespan. The path's fitness value can be calculated as follows:

$$f_{(fitness)_m^k} = \frac{E_{res_i}}{L_m^k} * T_{ij} \tag{15}$$

here T_{ij} is the trust metric of node i holds for j. Then the global pheromone updating applies on the optimum path which is the best-so-far solution, offering the largest fitness value. The pheromone intensity is updated globally according to the following equation:

$$\tau_{ij}(t+1)=(1-\delta)\tau_{ij}(t)+\sum_{m=1}^{n}\Delta\tau_{ij}^m \tag{16}$$

$$\Delta\tau_{ij}^m = \begin{cases} R * f_{(fitness_{best})_m^k}, & if\ mth\ ant\ visits\ the\ edge\ i,j \\ 0, & otherwise \end{cases} \tag{17}$$

where $0< \delta <1$ is the global pheromone decay parameter, R is the constant for recompensing the pheromone, n denotes the total number of ants, and $\Delta\tau_{ij}^m$ is the increase of pheromone concentration of the edge (i,j) utilized by m^{th} ant, which is proportionate to the maximal cost of fitness equation, $f_{(fitness_{best})_m^k}$, if edge (i,j) is associated with the global best route.

3.5. Proposed Improvement

Clustering is contemplated on attaining scalability while maintaining security. As a result, the routing protocol presented in [15] can be used in conjunction with a clustering based routing approach, such as LEACH [16], a hierarchical clustering protocol. It takes into account the data forwarding probability, nodes' current residual energy, the trust metric, and nodes distance from the base station (BS) and improves the optimal cluster head (CH) selection technique. The flow diagram representing the proposed enhancement is shown in Figure 2.

The probability ($Prob_i$) of a node being selected as a cluster head, an ant m can apply the probability calculation equation given in (18). Node i is presumed to be the present cluster head node then the next node j to be selected as the subsequent cluster head, where the trust metric (T_{ij}), P_{ij}^m , the node distance ($dist_i$), as well as two control parameters (α and β) are used, and the following probability equation is applied:

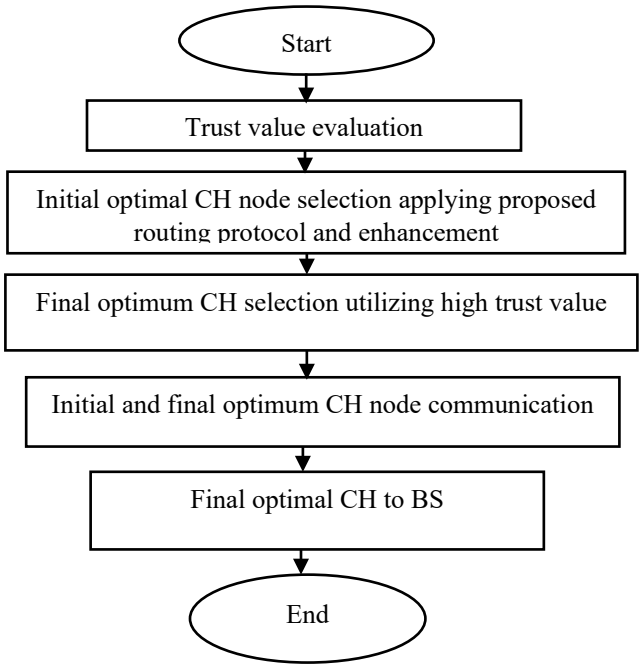

Figure 2: The flow diagram of the proposed improvement

$$Prob_i(t)=\frac{dist_i*\alpha+[P_{ij}^m(t)]*\beta}{\sum_1^{N_i} dist_i*\alpha+[P_{ij}^m(t)]*\beta} * T_{ij} \tag{18}$$

here T_{ij} signifies the trust metric, P_{ij}^m is computed from (4), and N_i is the set of nodes in the cluster.

3.6. Trusted Parent Selection

Algorithm 1: Trust Calculation and selection of trusted parent

Let $M_1 \leftarrow$ any obtainable entity in the Neighbour_List[ ]
Let $M_2 \leftarrow$ another entity next to M_1 in the Neighbour_List[ ]
Calculate

$$T_{ij} = \sum_{k \in M_i} \left(RT_{ij}^k * w_k\right)$$

while node is not found in Malicious_Class_List do
If (M_1.*ETX_metric*<= *ETX_metric-limit*) & (M_2.*ETX_metric*<= *ETX_metric-limit*)
If (M_1.*Rank* <= *Self_Rank*) & (M_2.*Rank* <= *Self_Rank*)
Selected_Parent = $M_1.T_{ij} > M_2.T_{ij}$? M_1:M_2;
else
if (M_1.*Rank* <= *Self_Rank*) || (M_2.*Rank* <= *Self_Rank*)
Selected_Parent = M_1.*Rank* < M_2.*Rank* ? M_1: M_2
else
Selected_Parent = NULL;

end if
else
If (M_1.*ETX_metric* <= *ETX_metric-limit*) ||
(M_2.*ETX_metric* <= *ETX_metric-limit*)
Selected_Parent = M_1.*ETX_metric* <= M_2.*ETX_metric* ?
M_1: M_2;
else
Selected_Parent = NULL;
end if
end while
return Selected_Parent
End. //of program.

The algorithmic procedure implemented here has been given above for selecting the trusted-parents. It includes calculation of the trust values of the nodes and a trust-based method for the selection of parents. The algorithm utilizes the ETX metric as specified in [17]. For the initiation for the optimum parent swap, the minimum required variation of the computed trust value for a node is denoted as $M_1.T_{ij}$. The node having the maximal trust rating along the node's routing path is searched for by the algorithm among all the routes, while the path would also have minimum ETX values, given in (19). The ETX limit represents the maximum ETX rating assessed to be the optimal prospective parent, whereas a node will not select its neighbours that have superior rank as its possible chosen parents. It will also ensure that there is no loop. The trust threshold (Trust assessment Table 1) is utilized for a trusted parent preference, during trust calculation for selecting the node as the chosen parent. Moreover, the rank order is maintained as specified in [18]. Upon identification of a malicious node as a parent, the child node reassigns itself with a different parent from the offered list for selecting a parent node.

The ETX metric, or expected transmission count is calculated as:

$$ETX_{(i,j)} = \frac{1}{D_f * D_r} \tag{19}$$

where D_f defines the forward data delivery and D_r is the reverse data delivery or acknowledgement from the receiver.

4. Result and Discussion

MATLAB is used to accomplish the performance evaluation and simulation. The routing protocol proposed here is compared to the benchmark protocols, where the conventional ACO algorithm, EICAntS algorithm [6], a current ant-based routing method for IoT communication, and a present proactive routing protocol for low power lossy network (RPL) [7] for IoT have been considered as benchmark protocols. There are 100 nodes dispersed in a $100m \times 100m$ area. Some malicious nodes are also deployed across the network at random. The initial trust value is calculated which is set as 0.6, observing the number of interactions, and for that taking reasonable value is crucial. The simulation parameters are set as: $\alpha = 1, \beta = 1, \gamma = 1, \rho = 0.05, \delta = 0.05$. More parameters are presented in the Table 2.

Table 2: Simulation Parameters

Parameters	Values
T	100
Initial trust value	0.6
Initial energy per node	0.5 joule
Node-speed	2 m/s ~ 5 m/s
Transmitted message bits	4000 bits
Distance of transmission	50 m

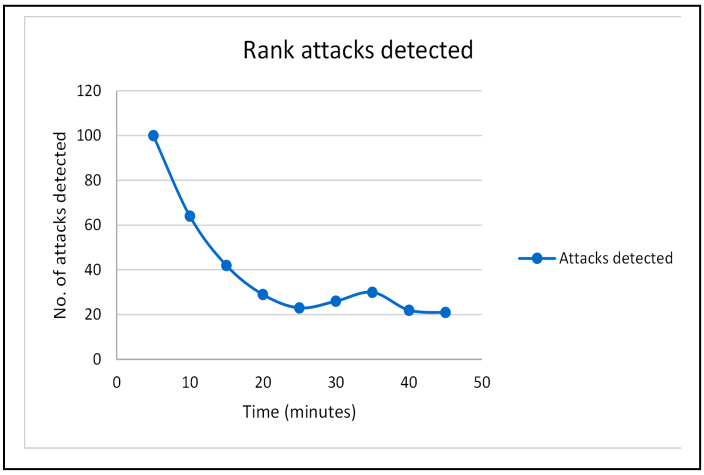

Figure 3: Rank attack detected by proposed secure ACO algorithm

In Trust calculation process, by using the computed trust value, a trustor node assesses a trustee node. It employs the trust metric value to evaluate whether the trustee node is adequately reliable enough of fulfilling an allotted task, and the trust threshold system (Trust assessment Table 1) is utilized for the assessment. Each node collects the direct trust value of directly connected neighbours and recommended trust value of indirectly connected neighbours. The focus of this research is on detecting and isolating internal attacks, particularly Rank and Sybil attacks. A malicious node modifies its rank in a rank attack for disrupting the network route topology, whereas a Sybil node, by using fake identities, tries to subvert the network process. The malicious nodes, taking part in internal attacks of the network, are more challenging to detect as they are aware of the system information of the network. By using node overhearing and monitoring methods, this secure trust-based system perceives unusual route transmission towards a node, and that might be an indication of a rank attack. By assigning a greater weight to a node's existing trust value, a Sybil attack node is detected and isolated. It is also needed not to attribute its observed prior behavior too much weight while defending against a Sybil node as its initial behaviour might be well. So, if it does not have any worthy packet sending behavior that can be observed, its trust value will remain below the threshold, which is necessary for secured communication.

For the simulation study, in the phase of implementing Rank attack, a malicious node initially keeps up with a fine prior behaviour for roughly 5 to 10 seconds. After that during every cycle, it broadcasts spuriously low Rank values and initiates its attack.

From Figure 3, it can be seen that the proposed secure routing protocol is effective at detecting and isolating the Rank attacks. In the course of routing operations, about 100 attacks have been

detected in the first five minutes. Although with the simulation progress, the number of attacks detected has steadily decreased.

In RPL routing operation, a node examines potential parents that have lower rank values than itself and then selects as its chosen parent. In this way, the rank of a node changes and realignment takes place for a child node to another selected parent node that has a smaller rank value. A Rank attack proceeds where the attacker takes advantage of this attribute in RPL routing. It presents itself with a superior rank value to its adjacent nodes and the neighbours are attracted and deceived by this.

The frequency of node rank changes is shown in Figure 4. From the comparison in between MRHOF-RPL (Minimum Rank with Hysteresis Objective Function-RPL) [18] and the secure system presented here, it is observed that the benchmark protocol has notably higher vulnerability to node rank changes than the proposed algorithm, demonstrating a vulnerability to Rank attacks. However, this proposed scheme, persistently has maintained low frequency of node rank changes during all of the simulation period.

From Figure 5, it can be observed that the proposed secure routing protocol is effective at detecting and isolating the Sybil attacks. During the routing procedures, about 272 attacks have been detected in the first five minutes but the number of attacks detected have decreased with time.

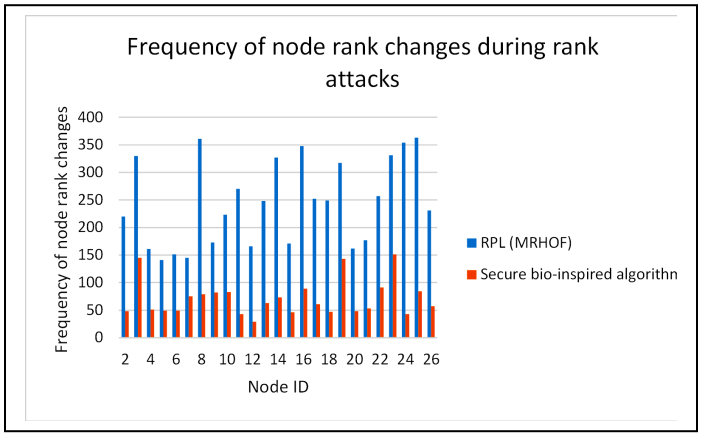

Figure 4: Frequency of node rank changes comparison

The offered ant colony metaheuristic-based routing method is used to discover the optimum pathway for routing packets from the originating node to the target node with the least amount of energy consumption and the highest level of security. The trustworthy nodes are chosen for data transfer in order to build a secure routing path. The graph in Figure 6 shows the relationship between the detection times of a malicious node and the number of nodes in the network. The detection time is defined as the number of malicious nodes found in relation to the simulation time. The percentage of malicious nodes has been retained fixed in this graph, and the value 1 for detection time indicates that no malicious nodes have been found.

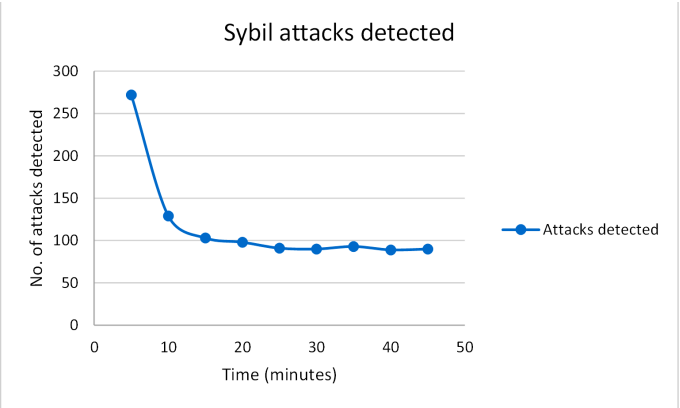

Figure 5: Sybil attack detected by proposed secure ACO algorithm

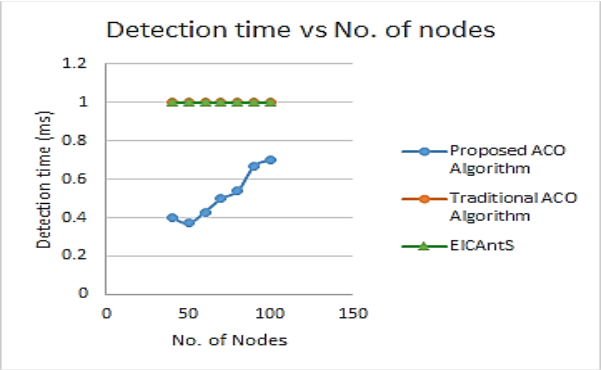

Figure 6: Detection times comparison of a malicious node to the No. of nodes.

The detection of malicious nodes in the network is not considered by the traditional ACO algorithm and EICAntS protocol. As a result, the systems fail to detect any malicious nodes, resulting in lower security and performance. However, the proposed scheme not only converges into the best-so-far path but also the most secure route by taking into account essential transmission factors along with the use of trust to improve security. With the detection and isolation of malicious nodes, it outperforms benchmark protocols while discovering and collaborating with trustworthy nodes via utilizing a trust assessment system. Figure 7 shows the comparison of a malicious node's detection times represented on the ordinate to the percentage of malicious nodes represented on the abscissa accordingly.

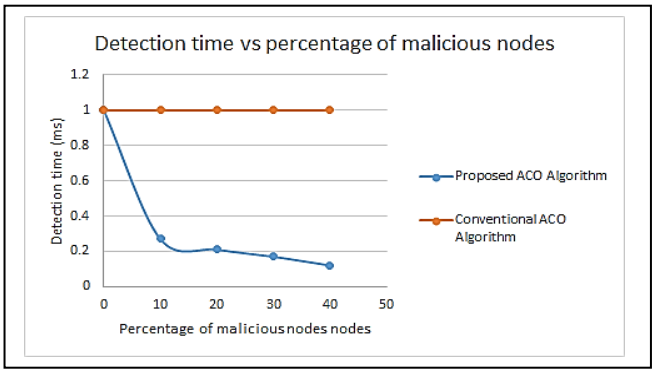

Figure 7: Detection times comparison of a malicious node to the percentage of malicious nodes.

Figure 8 shows a contrast of the consumed energy per transmission of the nodes for the protocol proposed here, the ant-based routing method for IoT communication, i.e., EICAntS, the standard ACO algorithm, and the RPL protocol, demonstrating that the suggested ACO algorithm is better in terms of consuming a lesser amount of energy. The cumulative energy consumption of each node is displayed here every transmission for each individual search operation. In comparison to the previous benchmark protocols, the suggested calculation has clearly achieved refinement, resulting in a substantially lower energy consumption, nearly 50% less for the majority of nodes.

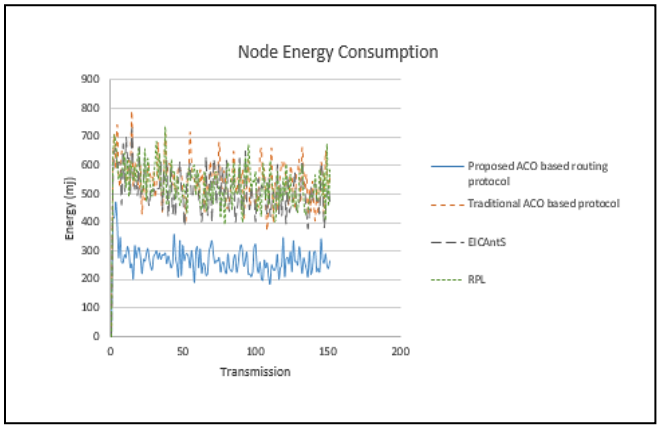

Figure 8: The energy consumption per transmission of the nodes comparison

The presented routing technique based on ACO consumes less energy compared to the traditional ant colony optimization metaheuristic algorithm, proactive routing protocol for low power lossy network (RPL), and efficient IoT communications based on ant system (EICAntS) routing protocol, even in the situations where the number of nodes increases, as shown in Figure 9, where the average energy consumption is lower. When contrasted to the benchmark routing techniques, it is clear that using the suggested ACO-based routing algorithm as an explication reduces average energy consumption, by approximately 50% less and makes the algorithm lightweight. Because the proposed approach enables the optimum packet forwarding path for transmission to be determined, and retransmissions are avoided, providing reliable communication. This method likewise reduces the number of updating phases while optimizing the route selection strategy. According to the outcomes, the more nodes there are, the higher the energy consumption. Another result is that the more malicious nodes there are, the more energy is consumed. The presented framework retains scalability by using less power than the standard protocols taken as the benchmark, even as the number of nodes in the network expands.

As demonstrated in Figure 10, the average End-to-end delay performance metric rises when the number of nodes grows. The proposed routing protocol lessens the repetition issue while also enhancing the procedure for selecting a route because numerous packets have to be sent again to the intended destination if the optimal path is not found and utilized to deliver the packets. Compared to the mentioned benchmark algorithms here, the suggested technique performed well with regard to average End-to-end delay, achieving a nearly 40% decrease in end-to-end delay. Figure 11 shows the throughput results. The network throughput is measured by calculating the total number of packets sent over the complete simulation time, or the measure of digital data transmitted per time unit via a communication link. It is usually expressed in bits per second (bps), although it can also be expressed as data packets delivered per-second or per-time-slot. From the contrast, it is clearly shown that the results obtained by the method proposed here are better than the results recorded by the other network.

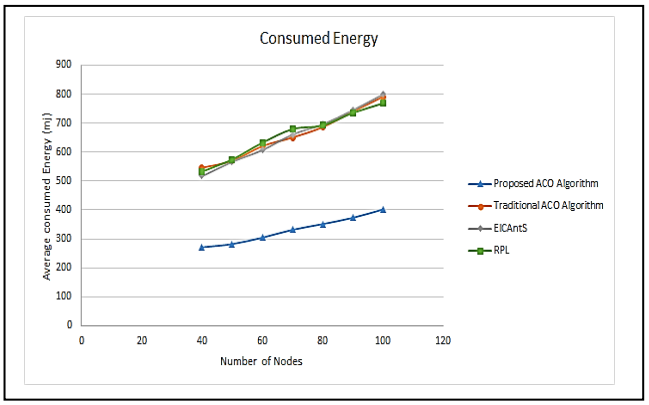

Figure 9: The average energy consumption comparison.

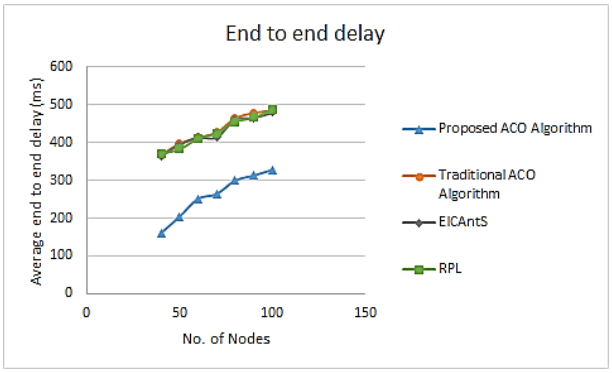

Figure 10: Comparison of the average End-to-end delay with regard to the number of nodes using fitness function

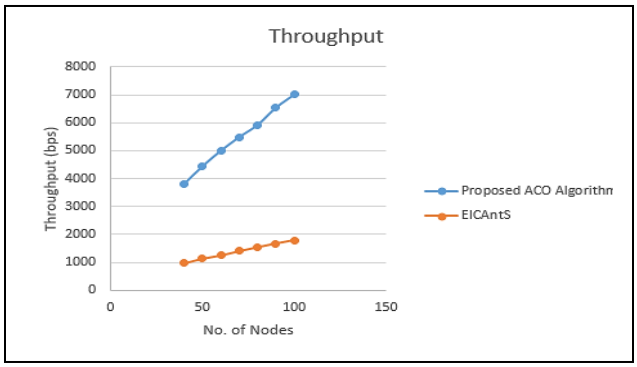

Figure 11: Comparison of Throughput

The findings of the proposed algorithm's calculation of packet delivery rates are shown in Figure 12. Since the protocol devises the ability to deliver numerous packets shortly while also reaching the destination, the proposed approach achieved satisfactory outcomes despite the crucial node quantity. It offers a system for determining the most secure information-transmission path among the network's several routes. Many packets are diverted or

dropped out when there are malicious nodes utilizing other strategies. However, due to security mechanisms, the proposed technique is used to deliver most of the data.

The packet loss ratio is also seen in Figure 13 when malicious nodes are present. The packet delivery ratio diminishes when the percentage of nodes that are malicious rises or as other attackers and compromised nodes exist in the pathways amid communication nodes. When attackers and compromised nodes cannot be detected and packets outreaching the target node successfully decline, the ratio of packet loss or misdirection is significant in the case of the specified benchmark methodologies.

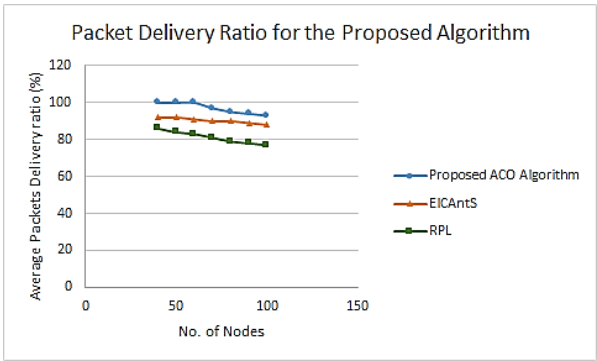

Figure 12: Packet Delivery Ratio (PDR) with the number of nodes

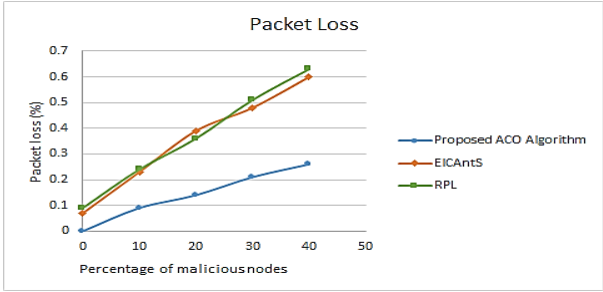

Figure 13: Packet Loss in the existence of malicious nodes

5. Conclusions

Though the IoT technology would be evolving in the coming decade, its multiple and complex aspects need to be considered in the process of developing effective communication protocols. An ACO-based WSN routing algorithm for IoT is proposed in this paper, which uses a trust-based security system while considering the limited resources restraints in sensors or low-power IoT objects, as well as the special necessity of security in the data forwarding process. The trust value is worked out to determine a node's trustworthiness for packet transfer. In order to evaluate route performance, the proposed enhancement and the route assessing function include the trust metric, as well as the existing energy of the nodes and the route length. The energy factor, the trust metric, and the average mobility of the nodes are all included in the ACO algorithm's probability formula as well. When compared to the benchmark methods, the presented ACO-based routing algorithm lowered energy consumption by almost 50% even as the number of nodes rose, making the algorithm lightweight and scalable. It also showed a nearly 40% reduction in end-to-end delay. The routing protocol generates a secure and globally optimal route based on the related information, which includes the neighboring nodes' trust value and residual energy, as well as the path cost from the adjacent node to the sink node. The proposed technique can retain a higher packet delivery ratio due to the security mechanism, which ensures the system's efficacy in addition to the global optimization. Furthermore, by providing trustworthy routing paths, the proposed routing protocol can efficiently balance energy consumption and security.

As future work, presented secure routing protocol would be improved to implement in a real-world setting to estimate the algorithm's performance. Moreover, it will be elaborated to deal with additional conspiring attacks such as a Rank attacking node colluding with Selective Forwarding attacks or having collusion with a Blackhole or a Sybil attack. Finally, previously trusted nodes will be re-assimilated based on their trust levels after having recouped their battery power. These nodes will be deployed administratively to ensure network's balanced secure communication.

References

[1] A. Sharmin, F. Anwar, S.M.A. Motakabber, A.H.A. Hashim, "Secure ACO-Based Wireless Sensor Network Routing Algorithm for IoT," in Proceedings of the 8th International Conference on Computer and Communication Engineering, ICCCE 2021, 190-195, 2021, doi:10.1109/ICCCE50029.2021.9467223.

[2] J. Granjal, E. Monteiro, J. Sa Silva, "Security for the internet of things: A survey of existing protocols and open research issues," IEEE Communications Surveys and Tutorials, **17**(3), 1294– 1312, 2015, doi:10.1109/COMST.2015.2388550.

[3] W. Dargie, C. Poellabauer, Fundamentals of Wireless Sensor Networks: Theory and Practice, 2011, doi:10.1002/9780470666388.

[4] S. Ganeriwal, M.B. Srivastava, "Reputation-based framework for high integrity sensor networks," in Proceedings of the 2004 ACM Workshop on Security of Ad Hoc and Sensor Networks, SASN'04, 66–77, 2004, doi:10.1145/1029102.1029115.

[5] L. Bianchi, M. Dorigo, L.M. Gambardella, W.J. Gutjahr, "A survey on metaheuristics for stochastic combinatorial optimization," Natural Computing, 8(2), 239-287, 2009, doi:10.1007/s11047-008-9098-4.

[6] S. Hamrioui, P. Lorenz, "Bio inspired routing algorithm and efficient communications within IoT," IEEE Network, **31**(5), 74-79, 2017, doi:10.1109/MNET.2017.1600282.

[7] S.S. Solapure, H.H. Kenchannavar, "Design and analysis of RPL objective functions using variant routing metrics for IoT applications," Wireless Networks, **26**(6), 4637–4656, 2020, doi:10.1007/s11276-020-02348-6.

[8] G. Glissa, A. Rachedi, A. Meddeb, "A secure routing protocol based on RPL for internet of things," in 2016 IEEE Global Communications Conference, GLOBECOM 2016-Proceedings, 1-7, 2016, doi:10.1109/GLOCOM.2016.7841543.

[9] I. Kenji, T. Matsunaga, K. Toyoda, I. Sasase, "Secure parent node selection scheme in route construction to exclude attacking nodes from RPL network," IEICE Communications Express, 299–303, 2015, doi:10.1587/comex.4.340.

[10] R. Stephen, L. Arockiam, "E2V: Techniques for Detecting and Mitigating Rank Inconsistency Attack (RInA) in RPL based Internet of Things," in Journal of Physics: Conference Series, **1142**(1), 012009, 2018, doi:10.1088/1742-6596/1142/1/012009.

[11] S.B. Lee, Y.H. Choi, "A secure alternate path routing in sensor networks," Computer Communications, **30**(1), 153–165, 2006, doi:10.1016/j.comcom.2006.08.006.

[12] R. Khoshkangini, S. Zaboli, "Efficient Routing Protocol via Ant Colony Optimization (ACO) and Breadth First Search (BFS)," International Conference on Internet of Things (IThings 2014), (March), 375–381, 2014, doi:10.1109/iThings.2014.69.

[13] F. Li, M. Liu, G. Xu, "A quantum ant colony multi-objective routing algorithm in WSN and its application in a manufacturing environment," Sensors (Switzerland), **19**(15), 3334, 2019, doi:10.3390/s19153334.

[14] K. Machado, D. Rosário, E. Cerqueira, A.A.F. Loureiro, A. Neto, J.N. de Souza, "A routing protocol based on energy and link quality for internet of things applications," Sensors (Switzerland), **13**(2), 1942–1964, 2013, doi:10.3390/s130201942.

[15] A. Sharmin, F. Anwar, S.M.A. Motakabber, "Energy-Efficient Scalable Routing Protocol Based on ACO for WSNs," 2019 7th International

Conference on Mechatronics Engineering, ICOM 2019, 1-6, 2019, doi:10.1109/ICOM47790.2019.8952053.

[16] W.B. Heinzelman, A.P. Chandrakasan, H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," IEEE Transactions on Wireless Communications, **1**(4), 660-670, 2002, doi:10.1109/TWC.2002.804190.

[17] J. Vasseur, M. Kim, K. Pister, N. Dejean, D. Barthel, "Routing metrics used for path calculation in low power and lossy networks," Draft-Ietf-Roll-Routing-Metrics, 2011.

[18] T. Winter and P. Thubert "RPL: IPv6 Routing Protocol for Low power and Lossy Networks," IETF Internet-Draft, 2010.