Indonesian Journal of Electrical Engineering and Informatics (IJEEI)
Vol. 12, No. 2, June 2024, pp. 344~359
ISSN: 2089-3272, DOI: 10.52549/ijeei.v12i2.5118

Trust-based Enhanced ACO Algorithm for Secure Routing in IoT

Afsah Sharmin[1], S. M. A. Motakabber[2], Aisha Hassan Abdalla Hashim[3]
[1, 2,3]Department of Electrical and Computer Engineering, International Islamic University Malaysia, Malaysia

Article Info

Article history:

Received Sep 26, 2023
Revised Dec 19, 2023
Accepted Jun 24, 2024

Keywords:

Ant Colony Optimization
Internet of Things
Sensors
Secure Routing
Trust Evaluation
Energy efficiency

ABSTRACT

The Internet of Things (IoT) is an expanding paradigm of object connectivity using a range of resource types and architectures to deliver ubiquitous and requested services. There are security issues associated with the proliferation of IoT-connected devices, allowing IoT applications to evolve. In order to provide an energy-efficient and secure routing method for sensors deployed within a dynamic IoT network, this paper presents a trust-aware enhanced ant colony optimization (ACO)-based routing algorithm, incorporating a lightweight trust evaluation model. As it is challenging to implement security in resource-constrained IoT networks, the presented model adopted bio-inspired approaches, offering an improved version of ACO towards secure data transmission cost-effectively while taking into consideration residual energy and the trust score of the sensor to be optimized. The trust evaluation system has been enhanced in the development of the proposed routing algorithm and the node trust value is evaluated, sensor node misbehavior is identified, and energy conservation is maximized. The performance evaluation is demonstrated utilizing MATLAB. In comparison to the standard bio-inspired algorithms and existing secure routing protocols, the proposed system reduces average energy consumption by nearly 50% regardless of the increase in the number of nodes and end-to-end delay of 40%, while finding the secure and optimal path in unison is designed to ensure trust in the IoT environment.

Corresponding Author:

Afsah Sharmin,
Department of Electrical and Computer Engineering,
International Islamic University Malaysia,
53100 Kuala Lumpur, Malaysia
Email: afsahsharmin@gmail.com

1. INTRODUCTION

An ever-evolving technology, the Internet of Things (IoT) plays a vital role in integrating the intelligent things or interconnecting devices and objects that surround us into a network. The sensors are a crucial component of IoT entities that collect environmental data and transmit it in real time via the hosted IoT network. An extensive range of application areas that influence the lives of people are made possible by the incorporation of IoT and wireless sensor networks (WSNs). IoT continues to shift into ubiquitous networking, providing smart connectivity and context-aware computation with autonomous and smart behavior. This transformation from the static internet into a fully integrated future internet is being enabled by the widespread use of IoT things or objects made possible by wireless technologies [1]. For example, radio frequency identification (RFID), LPWANs, Wi-Fi, Zigbee, and cellular. From an IoT standpoint, a sensor contributes to collating information about the physical world and sending it to a sink node where analysis is done. But the deployed sensors are energy-constrained and typically distinguished by lower processing and computing abilities with limited resource availability. Energy efficient communication, security, scalability, mobility, autonomy, computational complexity, changing environmental issues, resource restraints, and quality of service (QoS) measures are all crucial considerations and challenges throughout IoT routing.

Considering the rapidly growing number of known and unknown security threats in IoT, implementing secure routing in IoT is a very challenging task to attain in the modern era and existing routing protocols have not yet been thoroughly tested for trustworthiness [2]. The primary reason for this is the use of resource-constrained devices in IoT with limited battery life, memory, and processing capacity. The existence of dynamic topology, which allows many sensors or other IoT devices to leave or join without predefined information, is another factor contributing to this security risk in IoT. As a result, it has enough negative consequences on security protocols. Although the utmost robust cryptographic algorithms are now offered, it is difficult to implement those in restrictive environment of IoT as they require more computing power and demand more resources. On the contrary, the extensive array of intricate encryption and complex hashing techniques found in cryptographic solutions are not offered in trust management; consequently, trust management is a practical choice for enhancing security in IoT nodes. Particularly when the number of linked devices rises to a level that cannot be managed by a central controlling system, trust-based systems are more intuitive and can be utilized to improve security in IoT [3]. Nonetheless, the existing trust management schemes are usually designed considering predefined information of adversaries, which makes the model robust in one environment but not applicable if the adversary environment is altered.

In order to mitigate security threats, vulnerabilities and malicious attacks, numerous research models and methodologies currently provide security in data transmission and services hosted in IoT. The security problems are associated with data privacy, IoT device vulnerabilities, malware attacks, and physical security where any form of such attempt to access the sensor illegitimately can lead to unauthorized tampering of sensed information, substituting with malicious program/data. Another more significant set of problems is associated with Distributed Denial-of-Service (DDoS) attacks, which is much prevalent in the cloud and IoT networks where a large number of traffic floods up the sensor by an attacker, leading them to be unresponsive, thereby disrupting the ongoing communication or services. Security attacks in the network layer against the IoT consist of sinkhole and blackhole attacks, which end up resulting in a DoS circumstance by discarding all the packets. Greyhole attacks, on the other hand, cause routing errors by only forwarding certain packets to the subsequent node. Furthermore, security threats like Rank attacks, in which malevolent nodes convert the rank to transmit packets through it, and Sybil attacks, in which packet forging is used to assume many identities, are troublesome to detect until they have an impact on IoT routing performance. A secure routing protocol must guarantee that information is routed securely to the deliberate recipients rather than an attacking node, ensuring no illegitimate access. These threats and hostile attacks will be alleviated by using trust-based secured routing protocols [3].

Though a wide variety of secure routing algorithms have been proposed, they are unable to balance energy and security demands effectively in a dynamic IoT communication environment. It is preferred when designing security mechanisms, notably routing protocols, that are lightweight since security is perceived as cost-intensive. The adoption of bioinspired techniques contributes towards the finding of the optimal secure routing path by adopting the different cognitive principles of organisms to achieve optimal security cost-effectively. Bio-inspired algorithms are robust, adaptive, and scalable, making them perfectly suited for highly dynamic network topologies. A bio-inspired algorithm, the ant colony optimization (ACO) system, employs the idea of self-organization to support ants' cooperation in problem resolution and can offer highly optimal secure routes. Unfortunately, the issues related to premature convergence and higher sensitivity towards parameters by conventional bioinspired approaches have not yet been addressed. Furthermore, trust management, an associated security solution, has been implemented and enhanced towards finding trustworthy neighbors. However, the existing trust management scheme needs to be more reportedly designed considering the restricted resources in IoT, e.g., processing power, energy, etc., which makes it quite challenging even to execute the sophisticated security protocols in sensors. A bio-inspired routing algorithm based on ACO is proposed here that associates a trust evaluation scheme while intending to optimize the residual energy and trust grade of the sensor by taking them into account. Local and global pheromone updating rules are further subjected to acquiring highly optimal solutions. ACO uses the probability formula to determine routes through a probabilistic progression and the pheromone update expression to update pheromone trails [4].

With regard to the trust management strategy, a uniquely designed trust model is presented in [5], employing theoretical knowledge-based framework through several trust-oriented determinants. Though the factors collaborate in order to exhibit the heterogeneity and uncertainty of trust relations from different aspects, the factors' weights are not indicated in this technique. Also, this model consumes substantial energy to restore a node's trust score before taking the subsequent choice. In [6], a highly adaptive and distinctive routing method that combines a small figure of redundant systems through a secret sharing mechanism has been suggested. Although it can guarantee routing reliability, energy constraints have not been considered. The authors in [7] developed a trust-associated threshold strategy for selecting a parent node which provides secured control to Rank attacks during Routing Protocol for Low Power Lossy Network (RPL) routing procedure. The benefit of this method is that the Rank attacks are minimized as the attacker node is recognized at the selection stage of

a parent node. The weakness of the approach is that it is failing to detect and mitigate newly vulnerable attacks like Sybil and blackhole attacks.

Different strategies have been devised for exploring secure routing in the IoT. Directed Acyclic Graph (DAG), a topology resembling a tree, is produced by the RPL proactive routing protocol. The transmission and residual energy factors, Expected Transmission Count (ETX) metric, and contented load are routing parameters that are used entirely and in conjunction in [8] to upgrade the design of objective function (OF) for the RPL protocol, which is utilized to organize the route progression method. Operating residual energy (RE) combined with ETX (EE), and an optimized timer setup may substantially lower energy use. Contrarily, unlike the ant colony-grounded system, which applies the ant colony foraging technique, this method does not employ an optimization model. A secure-RPL (SRPL) protocol, presented in [9], is used for performing authentication of messages as well as encryption operation to ensure new information, data integrity, and confidentiality and to lessen the effects of rank manipulation. It is founded on the concepts of hash chain authentication and rank threshold constraints. This method turns out to be pricey computationally because it binds cryptography to hash chain authentication. Nodes are also susceptible to insider attacks and security breaches. In [10], trust-based secure data aggregation with a single mobile sink in WSN-based IIoT is provided. This method considers both direct and indirect trust, but the possibility of contradiction in indirect trust may arise. The authors offer methods for identifying and thwarting rank attacks that conflict with RPL-assisted IoT in [11]. The method disregards the nodes' trustworthy behaviors, which causes additional security vulnerabilities that target network traffic and resources.

Though the use of bio-inspired approaches aids in the development of secure routes for information exchange, their implementation for secure routing appears less abundant in existing research. An ant colony-based routing method Efficient IoT communications based on the ant system (EICAntS) is presented in [4]. The energy effect and data class are considered in figuring the global effectiveness factor and ultimately correspond to the pheromone dosage in the ant framework. Although the system expands network lifetime and reduces energy consumption, the energy effect is calculated taking into account the data class, but several concerns related to path loss due to fading in wireless communications are not detailed for obtaining the node remnant energy. In [12], to address the issue of energy hole problem, a routing algorithm based on ACO and residual energy of the terminals is presented. This approach, named AERO, deposits pheromones into the terminals, whereas the conventional ACO secretes pheromone into the paths between the terminals. This technique allows to balance traffic loads and achieves improved routing efficiency. However, the terminal statuses need to be considered while designing routing strategy.

The proposed scheme sets up secure routing with reliable nodes in order to protect IoT networks from routing attacks while optimizing the sensor's residual energy and trust score. Here, a more in-depth analysis of our suggested system [13] has been conducted to competently attain a stability between consumed energy and security. The recommended routing algorithm has taken into account major communication aspects for information forwarding in an IoT network, for instance mobility and energy concerns. This paper follows up on the research presented in [14], which presents a secured bio-inspired routing protocol constructed on Ant Colony Optimization (ACO) systems accommodating a trust model with the objective of improving IoT communications effectually while establishment of trust in WSN incorporated IoT. The trust evaluation method of the proposed system can be implemented in both small and large-scale IoT environments, even in the presence of attackers of unknown origin. This is because, regardless of the attacker's strategy, the proposed approach ensures that all regular sensors follow a specific process for computing the optimal solution, which an intruder cannot trace.

Section 1 introduces the relevant work and the rest of this paper is organized as follows. Section 2 presents the proposed scheme in detail, including the proposed enhanced ACO algorithm and its design concept, the secure trust-based system, and algorithm for the selection of trusted parent. The suggested system's performance is assessed in Section 3. Finally, Section 4 provides some concluding remarks.

2. PROPOSED ACO-BASED SECURE ROUTING ALGORITHM

2.1. Proposed Enhanced ACO Algorithm

The implemented IoT communication network system is grounded on an IoT sensor configuration in a graph G_i networked with nodes, sensors, and actuators (M_i) and symmetrical edges distributed at random throughout the observing zone. This paper presents an improved ACO-based secure network routing algorithm that chooses the most reliable path to the hop that provides the specific requested supplies while also considering security and residual energy considerations for next-node routing. The ants decide which node to route traffic through next based on the remnant energy and trust grades of nearby nodes that have to be optimized (the node with a larger level of energy and trust value has a greater chance of being preferred for routing). For the suggested development of our ant colony optimization based routing algorithm [13], suppose

that an ant *m* appears at node *i* at time *t* and uses the state-transition probability formula here to choose node *j* as the information passing node of the approaching route:

$$P_{ij}^{m} = \begin{cases} \frac{[\tau_{ij}(t)]^{\alpha}[\eta_{ij}(t)]^{\beta}[\vartheta_{ij}(t)]^{\gamma}[T_{ij}(t)]^{\psi E_j}}{\sum_{s \subset allowed_m}[\tau_{is}(t)]^{\alpha}[\eta_{is}(t)]^{\beta}[\vartheta_{is}(t)]^{\gamma}[T_{ij}(t)]^{\psi E_s}} & , j \subset allowed_m \\ 0, \quad others \end{cases} \quad (1)$$

$$\text{here,} \quad \eta_{ij}(t) = \frac{1}{d_{ij}} \quad (2)$$

Where $\tau_{ij}(t)$ is the extented pheromone held on link (i, j) and $\eta_{ij}(t)$ is the state transition heuristic score of link (i, j), a priori information in general is $1/d_{ij}$. Here, d_{ij} is the path distance connecting *i* and *j*. The effect of the pheromone concentration and heuristic cost are impacted by two factors, α and β, respectively. In accord with the mean node velocity specifying motion, the steady factor, $\vartheta_{ij}(t)$, is settled, where γ is the mobility constant. $T_{ij}(t)$ is the integrated/high trust rating of nodes at time *t*, denoted as the trust metric and ψ is the influencing factor that determines the effect of trust measure among the nodes to aid interaction. The trust metric computation is being provided accordingly in the succeeding discussion. E_j denotes the node residual energy that ant *m* traverses. For this system, the radio energy model introduced in [15] is applied. The residual energy, E_{res_i}, of a node n_i, is calculated as follows:

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

where E_{res_i} is the remnant energy, E_{tot_i} is the total initial energy and E_{tran_i} is the transmission energy.

2.2. The Secure Trust-based System

In order to facilitate secured interaction in the Internet of Things, a trust-based model is provided here that establishes secured routing with trustworthy nodes. It is a security solution that provides secure communication while calculating a node's trust value to decide its reliability, recognizing, and isolating malevolent and other attackers, as well as compromising adversarial nodes from the network. The prediction of a node's trustworthy behavior is based on how the node interacts with its neighbors in the network. Trust management assists IoT participants, e.g., trustors, in coping with the unpredictability throughout the future conducts of other members, e.g., trustees, by evaluating a node's trust value based on its prior behavior. The trustor analyzes the trustee to determine its reliability to carry out some stated actions. An index of weighted value and progressively gathered facts make up a node's trust rating, which further acts as an indication of the node's reputation. In other words, as a reflection of the positive or negative interaction experiences of a node's observed prior behavior over time in two adjacent collaborations, namely, cooperation and non-cooperation, while communicating directly or indirectly with its neighbor(s), reputation exhibits a computable range of values and serves as the foundation for the entity value perceived as trust.

Neighbors with greater trust metric scores are preferred for secured routing, but nodes with lower trust values or if the trust values of the suspicious nodes are not incrementing over time are considered malicious. Assuming that only cooperation and non-cooperation in the process of interaction between nodes, the beta distribution represents the node's reputation and trust [16]. Here, the security mechanism proposed in [3], building on a watchdog mechanism, is enhanced through a beta reputation system grounded on Bayesian conceptualization that is employed via direct and indirect observations, signifying reputation metric.

The predicted value of the probability distribution function is used to construct the direct trust (DT_{ij}), which is a rating of node *j*'s recent actions by node *i*. The direct trust value that node *i* has on node *j* is determined while taking into account the beta distribution and beta function as a prior distribution property in the communications between the nodes. The following is how the direct trust is shown:

$$DT_{ij} = \frac{\acute{\alpha}_j + 1}{\acute{\alpha}_j + \acute{\beta}_j + 2} \quad (4)$$

Where $\acute{\alpha}_j$ and $\acute{\beta}_j$ denote the cooperative and non-cooperative interactions between nodes *i* and *j* respectively from the perception of node *i.*

Whereas an entity may accurately determine direct trust for its neighboring nodes based on direct observation without the help of a third party, it depends on the recommendations of trustable nodes to evaluate trust indirectly for sending messages to nodes that are not immediately linked. If there is any ambiguity, assume that the assessing node *i* requires the recommendations from a third party and obtains the reputation score of node *j* through their common adjacent connecting nodes *k*. The recommended trust metric is computed by the following equation in accordance with the trust transfer decline principle:

$$RT_{ij}^{k} = DT_{ik} * DT_{kj} \quad (5)$$

By multiplying the direct trust values, DT_{ik} and DT_{kj}, the recommended trust value, RT_{ij}^{k}, that node *i* has regarding node *j* is provided by the common neighboring nodes *k*. Consequently, DT_{ik} stands for the direct trust score relating nodes *i* and *k*, and DT_{kj} stands for the direct trust score relating nodes *k* and *j*. The trust model aggregates recommendations using a weighted calculation of direct trust values between connected nodes, as demonstrated in (5).

The indirect trust is provided as follows:

$$IDT_{ij} = \sum_{k \in N_i} \left(RT_{ij}^{k} * w_k\right) \quad (6)$$

$$\text{here, } w_k = \frac{DT_{ik}}{\sum_{k \in N_i} DT_{ik}},\ k = 1,2, \dots, N_i. \quad (7)$$

$$DT_{ik} = \frac{\acute{\alpha}_k + 1}{\acute{\alpha}_k + \acute{\beta}_k + 2} \quad (8)$$

Where the weight of RT_{ij}^{k} is represented by $w_k (0 \le w_k \le 1, \sum_{k=1}^{N_i} w_k = 1)$. To lower the consequence of individual preferences, the weight w_k is ascribed dependent on the recommenders' level of trust. The number of received recommendations or reputations for node *j* collected by node *i* from a set of trustworthy nodes indicated as N_i. Here, DT_{ik} denotes the direct trust scores involving nodes *i* and *k*, whereas $\acute{\alpha}_k$ and $\acute{\beta}_k$ signify the prior reputation score, cooperative and non-cooperative interactive behaviors correspondingly that node *i* already holds about node *k*.

The operational trust rating, the trust metric $T_{ij} \in [0,1]$ of node *i* retains for *j*, is determined by gathering interaction evidences and conducts from third parties by means of direct monitoring or indirect observation. Incorporating the estimations RT_{ij}^{k} yields the weighted average, an associative trust aggregate function that takes into account the recommendations of individual recommenders in particular for computing RT_{ij}^{k} from each trusted link.

The total/integrated trust value (Ω_j) is typically expressed as:

$$T_{ij} = \Omega_j = \lambda DT_{ij} + (1 - \lambda) IDT_{ij} \quad (9)$$

Where, T_{ij} corresponds to the total trust degree, a confidence factor signified as λ is utilized to offset the erroneous, or fake recommendations rendered by the malicious nodes. It can be denoted as:

$$\lambda = 1 - y^{-x}, \quad x \in (0,1) \quad (10)$$

Where *y* indicates the number of successful/ unsuccessful interactions involving nodes *i* and node *j* that ensued cooperative or non-cooperative. The value of *x* changes within the range of (0, 1) depending on application setting. Let τ be the trust threshold, typically $0.8 \le \tau \le 1$. If $\lambda \ge \tau$, then $T_{ij} = DT_{ij}$; otherwise, the indirect trust calculation is carried out.

A trust assessment procedure is then constructed for rating the maximal to minimal trust scores, T ([0, 1]), once the trust estimates have been determined all through the trust computation phase. This will aid in identifying and removing the mischievous node since nodes with lower trust levels are labeled as malicious nodes. There are three classes according to how trustworthy a node is: entirely distrust (T_1), uncertain (T_2), and completely trust (T_3) grades. Here, the membership trust-assessment rating along with fuzzy categorization and evaluation of nodes' trust are applied. Three fuzzy subsets, T1, T2, and T3, are illustrated in Figure 1. The related membership functions, f1 (t), f2 (t) and f3 (t), are provided as f1 (t) + f2 (t) + f3 (t) = 1. Table 1 shows the trust states.

Table 1. Phases of Trust

Fuzzy categorization subsets (T)	Grades of Trust
T_1	Entirely Distrust
T_2	Uncertain
T_3	Completely trust

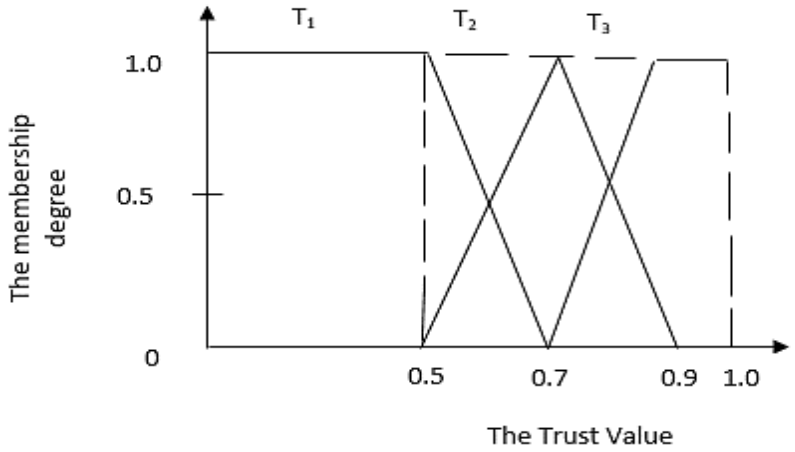

Figure 1. The degree of membership and function with the trust value

The currently implemented strategies for identifying multiple attacks do not provide a suitable method for distinguishing attacks when they are embarked on simultaneously. This study investigated a number of secured RPL routing protocols, but to the best of our knowledge, none effectively, in all important respects, inscribes concurrently Rank and Sybil attacks in an IoT environment. Consider the case when Rank attacker nodes are impersonated by Sybil attacker nodes as normal nodes in order to send numerous fictitious data packets after masquerading their identities. The resolution to this issue can be achieved using a parameter in the trust computation that takes into account both the nodes' forwarded and dropped data packets. The following is the DT_{ij} computation for disregarding the false identification or conflating of the Rank attacking node as a normal node in the course of a Sybil attack:

$$DT_{ij} = \left[\left(\frac{PFDs}{PRDs}\right) \times \left(\frac{PRDs - PDDs}{PRDs}\right)\right] \quad (11)$$

Here PDDs = The total number of Data Packets Dropped, PRDs = The total number of Data Packets Received and PFDs = The total number of Data Packets Forwarded.

Every sensor node in the suggested system directs and regulates its own pheromone trails while minimizing network overload and sustaining the lightness of the model. Additionally, each transmitted ant bears the identifications of the sensors together with the pheromone traces, and there is no central or overseeing unit for the purpose of collecting the grades.

2.3. Algorithm for the selection of Trusted Parent

Algorithm 1: Computation of Trust and choosing a trustworthy parent

Let $M_1 \leftarrow$ any attainable object in the Neighbouring_List[ ]

Let $M_2 \leftarrow$ another attainable object next to M_1 in the Neighbouring_List[ ]

Compute

$$T_{ij} = \lambda DT_{ij} + (1 - \lambda) IDT_{ij}$$

while node does not appear in the Malicious_Level_List do
If (*M1.ETX_score* <= *ETX_score-limit*) & (*M2.ETX_score* <= *ETX_score-limit*)
If (*M1.Rank_order* <= *Self_Rank_order*) & (*M2.Rank_order* <= *Self_Rank_order*)
Selected_Trusted_Parent = $M_1.\ T_{ij} > M_2.\ T_{ij}$? *M1:M2*;
else
if (*M1.Rank_order* <= *Self_Rank_order*) || (*M2.Rank_order* <= *Self_Rank_order*)
Selected_Trusted_Parent = *M1.Rank_order* < *M2.Rank_order* ? *M1: M2*
else
Selected_Trusted_Parent = NULL;
end if
else
If (*M1.ETX_score* <= *ETX_score-limit*) || (*M2.ETX_score* <= *ETX_score-limit*)
Selected_Trusted_Parent = *M1.ETX_score* <= *M2.ETX_score* ? *M1: M2*;
else
Selected_Trusted_Parent = NULL;
end if
e**nd** while
return Selected_Trusted_Parent
End. //of the program.

The algorithmic process applied here to select the trusted parents has been provided above. It comprises calculating the nodes' trust scores and choosing parents using a trust-based methodology. The ETX metric as detailed in [17], is utilized by the algorithm. The minimal necessary variation of the calculated trust score for a node is indicated as M1. T_{ij} for the purpose of initiating the optimal parent swap. The algorithm searches over all possible routes in search of the node with the maximum trust score along the node's routing path, while simultaneously ensuring that the path has the minimum ETX values possible, as specified in (12). The ETX limit denotes the maximal ETX rating determined to be the optimum potential parent, whereas a node will not choose its neighbors that possesses superior rank than it as probable selected parents. Additionally, it will make sure there exists no loop. While performing the trust estimation for choosing the node as the selected parent, the trust threshold (the membership trust-assessment rating provided above) is applied for a preferred trusted parent. Also retained is the rank order as stated in [18]. When a malevolent node is recognized as a parent, the child node changes its assignment to another parent from the list provided when choosing a parent node. The expected transmission count, or ETX metric, is determined as follows:

$$ETX_{(i,j)} = \frac{1}{D_f * D_r} \tag{12}$$

Where the forward data delivery is defined by D_f and the acknowledgement or reverse data delivery from the receiver is represented as D_r.

2.4. Updating of Pheromone and the Fitness Function

In case a substantial pheromone amount gathers on the routes and to prevent earlier local convergence, a local pheromone updating rule is applied afterwards an ant has mapped node *i* to node *j* to restore and manage pheromone measures, along with the employing of a threshold rating according to:

$$\tau_{ij}(t+1) = \begin{cases} T_r, & \tau_{ij}(t+1) > T_r \\ (1-\rho)\tau_{ij}(t) + \Delta\tau_{ij}(t) & else \end{cases} \tag{13}$$

$$\Delta\tau_{ij}(t) = \sum_{k=1}^{m} \Delta\tau_{ij}^{k} \tag{14}$$

where ρ implies the local pheromone degrade restraint, a threshold value T_r is used for restricting excess pheromone deposition, and $\Delta\tau_{ij}(t)$ is the accumulated pheromone of edge (*i*, *j*), which is consistently asserted as follows:

$$\Delta\tau_{ij}^{k} = \begin{cases} \frac{S}{L_k} & if\ kth\ ant\ travels\ on\ the\ path\ (i,j) \\ 0 & otherwise \end{cases} \tag{15}$$

Where the pheromone's influence constant is S, the k^{th} ant's track length is L_k, and the total ants' sum is m.

The global update of pheromone accretion is resolute when paths exploration is completed, and solutions are built after reaching the destination by all the ants. To estimate the path rating, the fitness score is computed by including the node residual energy, node distance, L_m^k, and trust metric in the route evaluation function as provided below:

$$f_{(fitness)}{}_m^k = \frac{E_{res_i}}{L_m^k} * T_{ij} \quad (16)$$

Here is the assessed trust metric T_{ij} that node i upholds for j. The global updation of the pheromone intensity then takes place on the optimal resultant path, which contains the highest fitness rating according to the following expression:

$$\tau_{ij}(t+1)=(1\text{-}\delta)\tau_{ij}(t)+\sum_{m=1}^{n}\Delta\tau_{ij}^m \quad (17)$$

$$\Delta\tau_{ij}^m = \begin{cases} R * f_{(fitness_{best})}{}_m^k, & if\ mth\ ant\ uses\ the\ path\ i,j \\ 0, & otherwise \end{cases} \quad (18)$$

Where δ is the global pheromone decline parameter, the pheromone recoup constant is R, the overall ants' figure n, and $\Delta\tau_{ij}^m$ is the intensified pheromone of the path i,j exploited by m^{th} ant, which is proportionate to the foremost measure of fitness estimate, $f_{(fitness_{best})}{}_m^k$, if path i,j is related with the global best route.

3. RESULTS AND DISCUSSION

For performance measurement, the implementation is done in MATLAB, and 100 nodes are distributed in a monitored area measuring 100m by 100m. The improved secure routing protocol is contrasted to the benchmark existing routing protocols, which include the standard bio-inspired algorithms [4], and a current RPL routing protocol for IoT networks [8]. Also, the malicious nodes are dispersed throughout the area in an arbitrary manner. Keeping track of the interactions is necessary in order to calculate the initial trust value, which is set at 0.6. Setting a reasonable value is crucial for this. The input parameters for simulation are set as: $\alpha = 1$, $\beta = 1$, $\gamma = 1$, $\rho = 0.05$, $\delta = 0.05$. Table 2 lists other factors.

Table 2. Simulation Parameters

Parameters	Corresponding Values
Initial node energy	0.5 joule
T_r	100
Data packet size	500 bytes
Transmission radius	50 m
Consumed Energy of TX/RX	50 nJ/bit
Node speed	5 m/s ~ 10 m/s
MAC	802.11

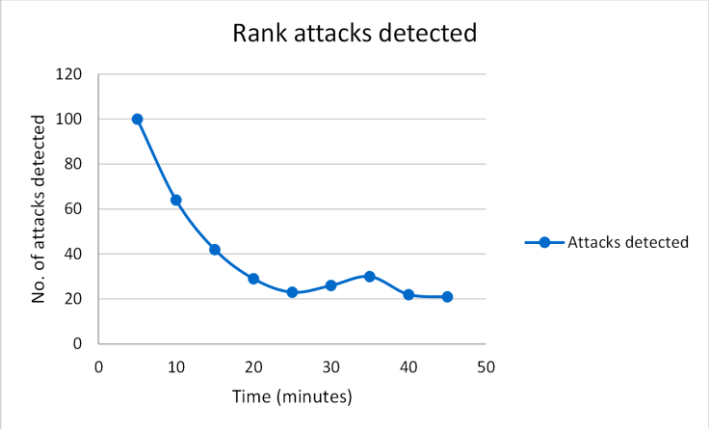

Figure 2. Rank attacks detection

In the Trust calculation process a trustor node evaluates a trustee node using the computed trust value. The trust metric score is employed to assess whether the trustee node is sufficiently trustworthy for carrying out the allotted task, where the trust threshold process is applied for the evaluation. In a rank attack, a malicious node modifies its rank to forward packets through it and to disrupt the network topology, whereas a Sybil node, by exploiting packet forging to subterfuge as many fake identities as possible, attempts to interrupt the network functionality. This secure trust-based scheme notices unusual and inconsistent route communication approaching towards a node and detects the threat managing node overhearing and promiscuous observing techniques. This perception could be a sign of a rank attack. A Sybil attacking node is identified and isolated through the assignment of higher weight to a node's current trust rating than to its apparent record. In RPL routing, when a Rank attack proceeds, the neighbors are drawn to and duped by the adversary because it gives the appearance of having a better rank value than the nodes immediately surrounding it.

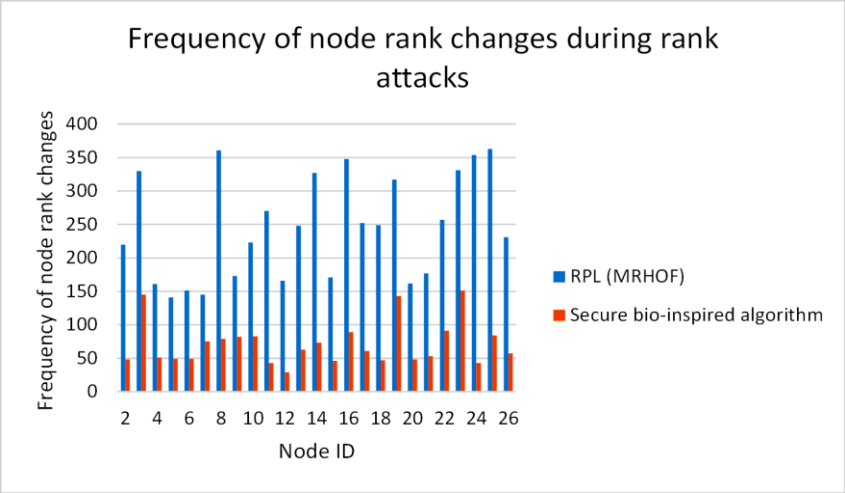

Figure 3. Comparison of frequency of node rank changes throughout rank attacks

For simulation analysis, at the beginning, a malicious node keeps its prior behavior favorable for 5 to 10 seconds while the Rank attack is being applied. Then it starts its attack and broadcasts falsely low Rank records throughout every cycle. The suggested secure routing technique can recognize and isolate Rank assaults, as shown in Figure 2. The first five minutes of the routing operations caught about 100 attacks. Nevertheless, as the simulation has gone on, the number of attacks detected has constantly decreased. Figure 3 shows the frequency of node rank changes. When the secure system demonstrated here and Minimum Rank with Hysteresis Objective Function-RPL (MRHOF-RPL) [18] are compared, the suggested algorithm is significantly more resistant to node rank changes than the benchmark protocol, indicating a susceptibility to Rank attacks. Nonetheless, over the whole simulation period, the presented strategy consistently upheld a relatively low node rank change in frequency. Figure 4 demonstrates how the proposed secure routing protocol may recognize and isolate Sybil attacks. During the first five minutes of the routing operations, around 272 Sybil attacks are discovered; however, as time goes on, fewer attacks are discovered.

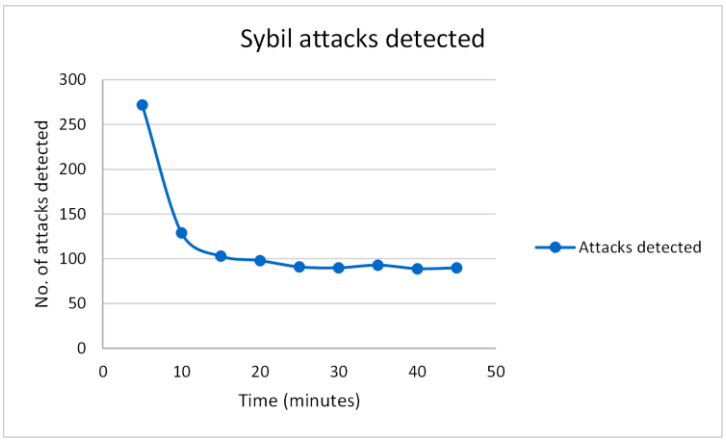

Figure 4. Sybil attacks detection using proposed secure ACO-based routing algorithm

The identification of mischievous nodes in the network's functionality is not taken into account by the existing standard routing protocols here. Consequently, the systems are unable to identify any hostile nodes, which results in lesser trust or security in the IoT, and system performance deteriorates. However, by taking into account crucial transmission parameters as well as the usage of trust for improving security, the suggested approach not only results in convergence into the best route so far but also the most secured path for communication. Every node in the network has its trust assessed, and the attacker nodes are detected based on the overall trust rating. It outperforms benchmark protocols in the isolation and detection of malicious nodes through employing a trust evaluation method to discover and interact with trustable nodes. The ratio of the sum of mischievous nodes discovered to the total simulation time is used to define the detection time. Figure 5 compares the percentage of malevolent nodes presented on the abscissa with the ordinate's representation of a mischievous node's detection times, with a value of 1 for detection time denoting there were no malevolent nodes identified.

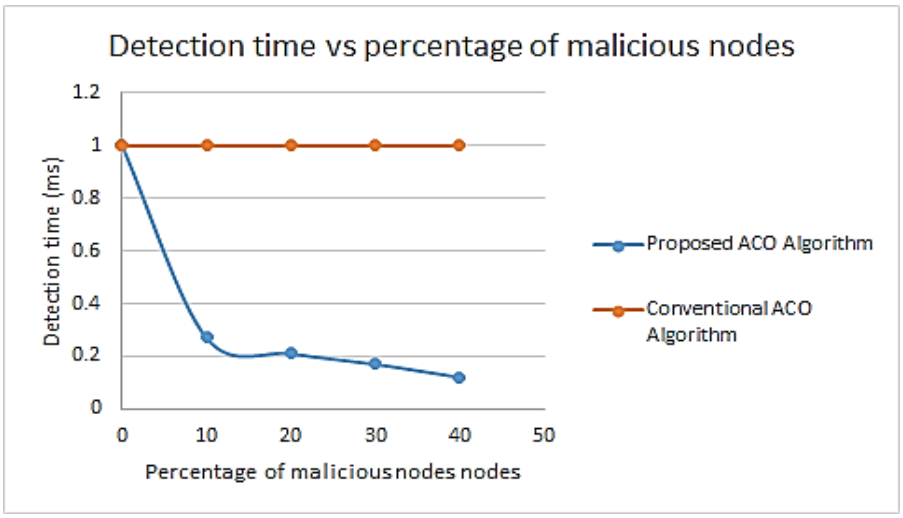

Figure 5. A malicious node's detection times comparison

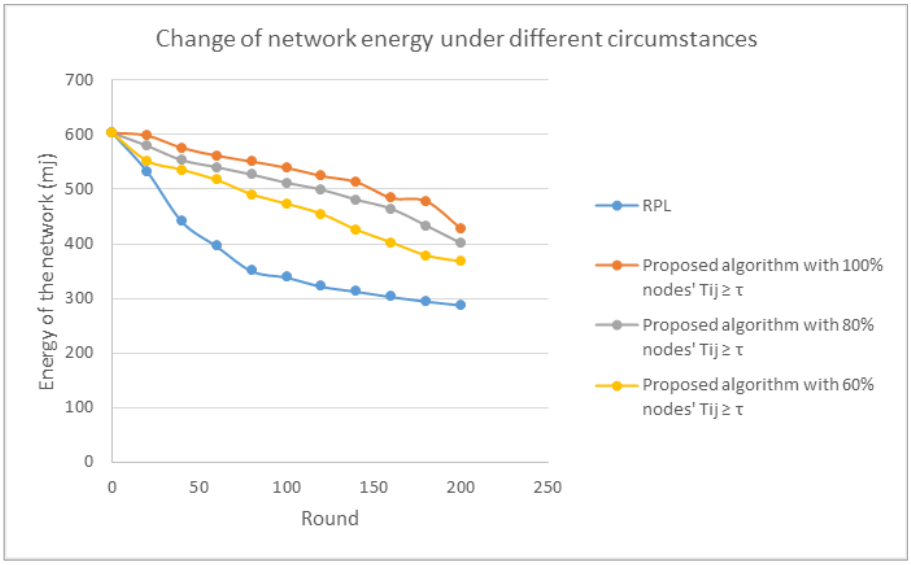

Figure 6. Change of network energy under different circumstances

The most reliable, optimum energy-efficient route is discovered and secured path to forward a message from the information originating node to the desired node is identified by the routing algorithm presented here. Figure 6 demonstrates how the offered algorithm exploit less energy than the benchmark protocol does under various conditions (as illustrated here using the trust threshold value as given by τ). This makes the algorithm more lightweight. Whether the direct trust is reliable enough to constitute the integrated trust needs to be determined based on the confidence level of the direct trust value. When there is a high degree

of certainty in the direct trust, it is not essential to compute indirect trust from indirect observations and reputation score. It suggests that the method is lightweight, can conserve more energy, resources and will prolong the network life. Regardless of scenarios with an increasing number of nodes, as illustrated in Figure 7, the presented routing approach constructed on ACO consumes less energy than the mainstream ACO, EICAntS, and RPL protocols, resulting in an average reduction in energy consumption of about 50% and making the algorithm lightweight. For the proposed strategy, the functionalities of the parameters are nearly retained similarly, with only a change in the different use-cases of optimality towards higher trust and energy retention. As the number of nodes in the network surges, the proposed scheme offers scalability by using less energy than the benchmark standard protocols.

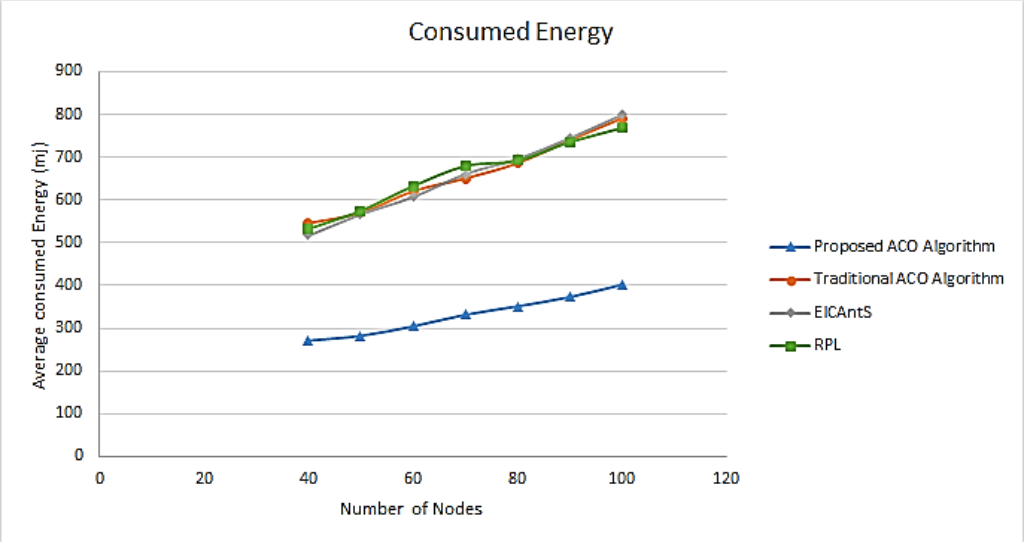

Figure 7. The average consumed energy comparison

Figure 8 demonstrates how the secure protocol proposed here performs better at resisting attacks set up by the compromised nodes than RFSN [3] and BTMS [16] in terms of how rapidly total trust of the suggested algorithm decreases. The trust degradation of the system model is quicker than the benchmark techniques. Which indicates that, particularly when the malicious node exhibits undesirable behavior, this technique might cause the node's trust value to drop quickly. Figure 9 illustrates how the suggested technique can functionally resist the collusion attack, whereas RFSN (Reputation based Framework for WSNs) and BTMS (binomial-based trust management system) perform poorly in this regard. Evidently, this technique can cause the trust grade of the mischievous node to drop rapidly when the compromised node behaves badly in the case of resisting the collusion attack where a node intentionally enters into a secret provision with the attacking node.

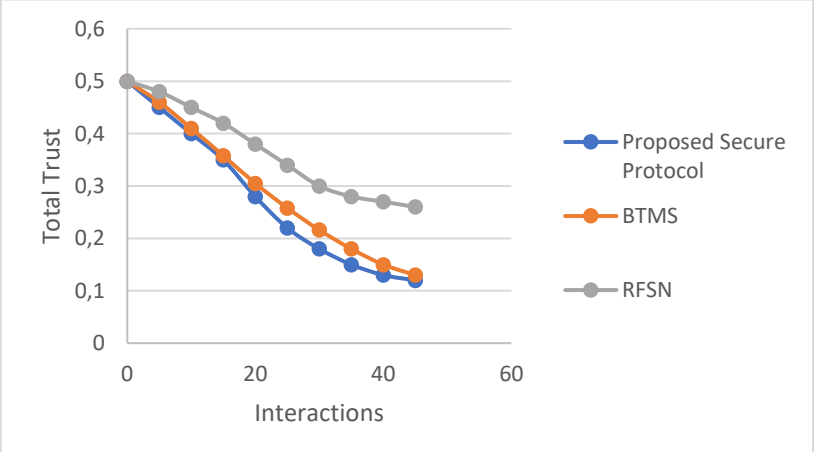

Figure 8. The total trust degree of compromised nodes

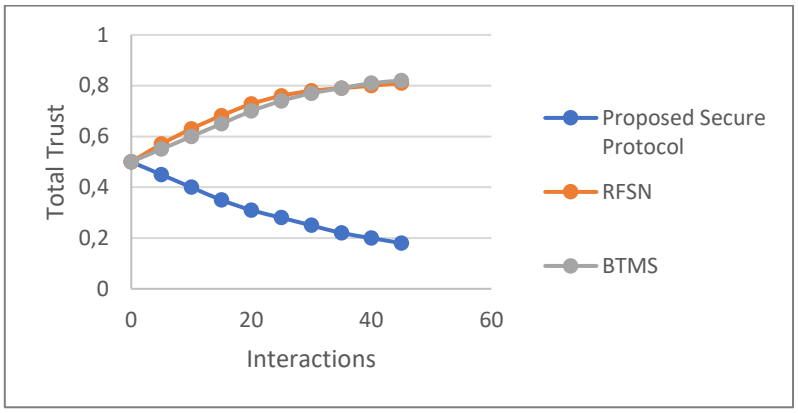

Figure 9. The total trust degree of adversarial/ compromised nodes under collusion attack

The suggested routing method lessens the repetition problem while enhancing the route-selection procedure. The proposed scheme offers reduced end-to-end time, mainly due to reduced dependencies of resources and reduced iterative operations. When compared to the existing benchmark routing protocols, the recommended method accomplished adequately regarding average end-to-end delay, attaining a close to 40% reduced end-to-end time, as shown in Figure 10. The results of the presented system's estimate of the packet delivery ratio are shown in Figure 11. Many packets are diverted or lost out when hostile nodes are adopting different tactics. Packets attempting to reach the target node fail to reach it successfully, and attackers and adversarial nodes cannot be found. But owing to security precautions, the majority of the data gets transmitted through the indicated method.

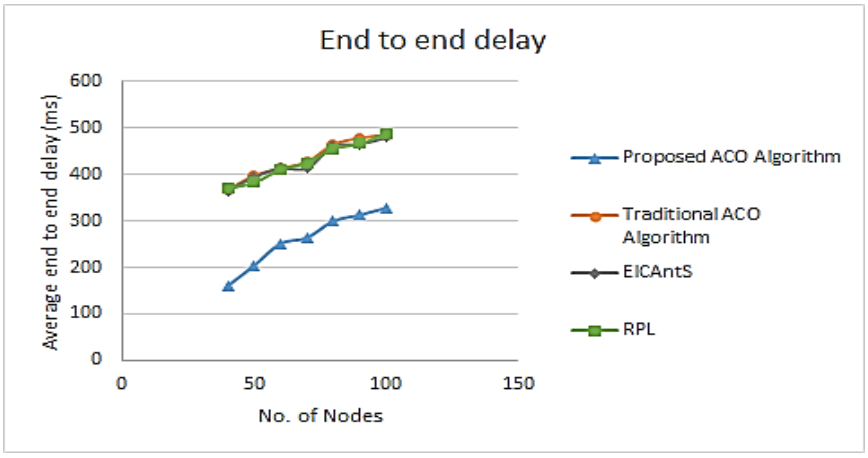

Figure 10. The comparative analysis of average end-to-end delay using fitness function

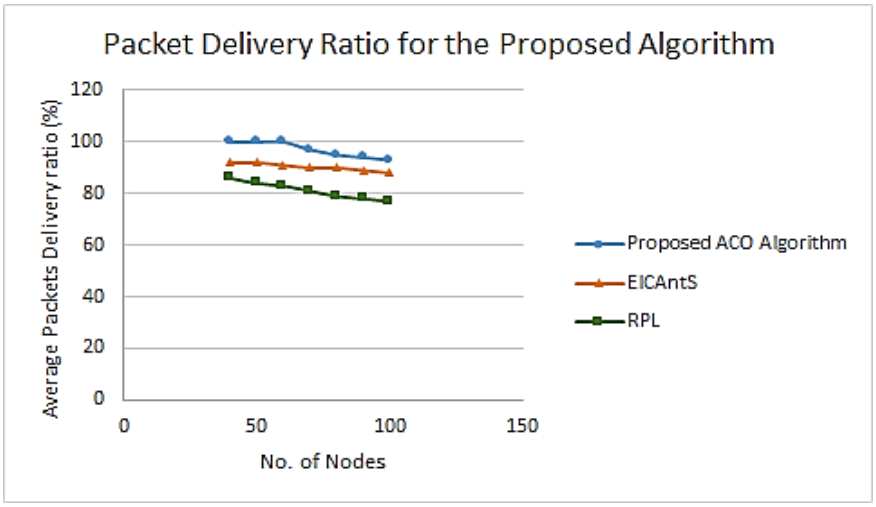

Figure 11. Packet Delivery Ratio (PDR) for the proposed system

For further comparative analysis, taking different values for the simulation parameters, the existing standard secured routing schemes in IoT considered are Routing Protocol for Low-Power and Lossy Network (RPL) [19], Routing using 6LoWPAN [20], Secured Routing using Zigbee Cluster Library (ZCL) [21], and Secure Routing using Constrained Application Protocol (CoAP) [22]. Moreover, conventional ACO and PSO algorithms are implemented to assess the performance improvement introduced by the proposed scheme in contrast to the existing bioinspired approach. Setting the initialized energy of each node at 10J and considering 500 sensor nodes with an increased rate of data transmission of 400 Kbps, the assessment is conducted to figure out how much energy is consumed during secured data transmission in the desired IoT system. Figure 12 shows that the proposed scheme offers minimal energy consumption compared to most existing systems. The suggested IoT secure routing strategy does not involve encryption, unlike other IoT secure routing schemes like RPL, ZCL, CoAP, and 6LoWPAN, which require significant energy allocation to perform ciphering and decoding processes. Moreover, with the computed global update formulation, the outcomes of decreased energy consumption are obtained by a decreasing dependence on more extended operation by local operatives with increasing simulation duration, whereas conventional ACO and PSO are shown to exhibit somewhat higher energy consumption.

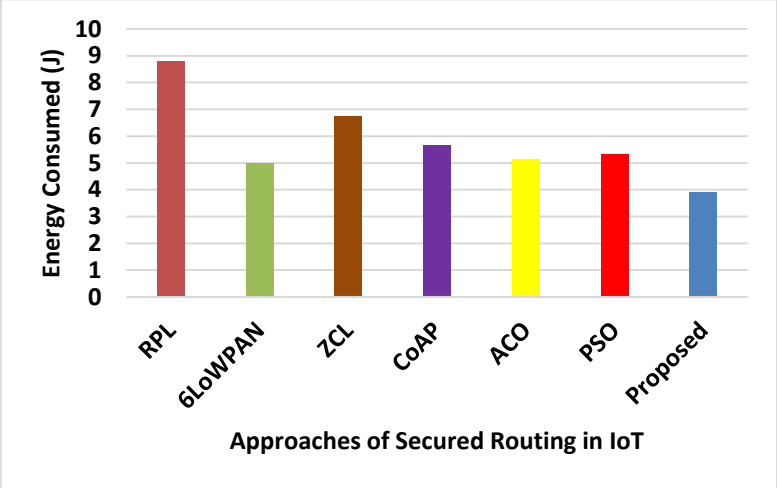

Figure 12. Comparative analysis of energy consumption.

When compared to the existing systems, the proposed strategy gives a significant result for delay reduction that includes end-to-end delay and processing delay, as can be seen by taking a closer look at Figure 13. It is noted that the proposed scheme consists of a series of mathematical operations towards trust computation along with a probability equation following local and global pheromone revised formulas that are significant. In contrast, existing secured routing schemes usually use encryption and message authentication to ascertain secure data transmission. Hence, it is necessary to assess that the involvement of internal security operations does not affect the network performance by increasing its delay. The proposed scheme offers better delay performance as it is more progressive, less iterative, and reduces dependencies on resources while providing a more significant problem area to explore better outcomes. This lowers the dependencies of increased effort towards optimal solution leading to a much-reduced delay score.

Figure 14 highlights the mean throughput observed during the series of assessments for a specified simulation time to show that the proposed scheme offers significantly better throughput than the existing schemes. From the viewpoint of the current scheme, the RPL protocol is the next superior performer owing to its dynamic path selection; however, it cannot withstand the imbalance in the traffic load during dynamic events in IoT. It is to be noted that traditional ACO is characterized by its shortcoming of the inability to offer optimal solutions while working on a more significant flow of traffic. A nearly similar problem is also encountered with PSO, which faces more memory dependencies with increased traffic flow resulting in throughput degradation. Owing to the usage of UDP, the CoAP protocol has the highest possibility of losing its data packets, which are transmitted in an unordered structure in IoT. Furthermore, it is noted that 6LoWPAN and, specifically, ZCL do not offer better throughput in the IoT environment due to the complexity introduced while performing header compression. However, the proposed system has no such issues, rather without encryption it offers better secure data transmission throughput than prevailing standard secured routing protocols in IoT, which mainly rely on intricate encryption and hashing techniques and authentication schemes.

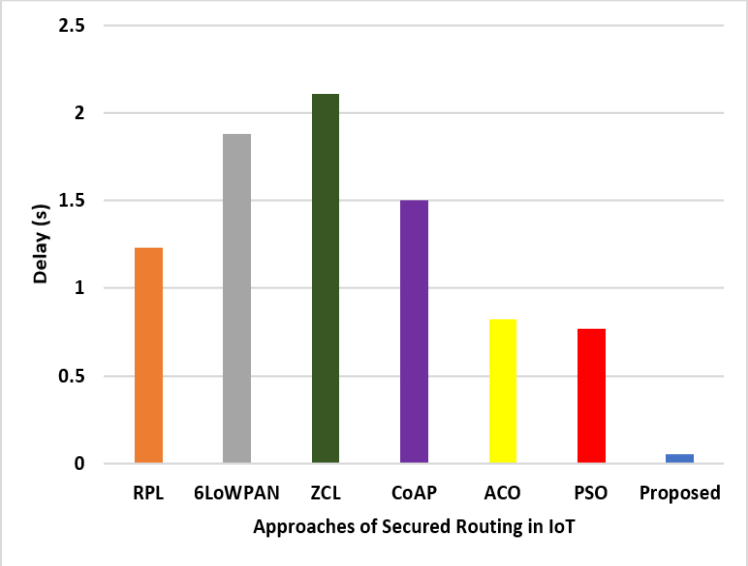

Figure 13. Comparative analysis of delay.

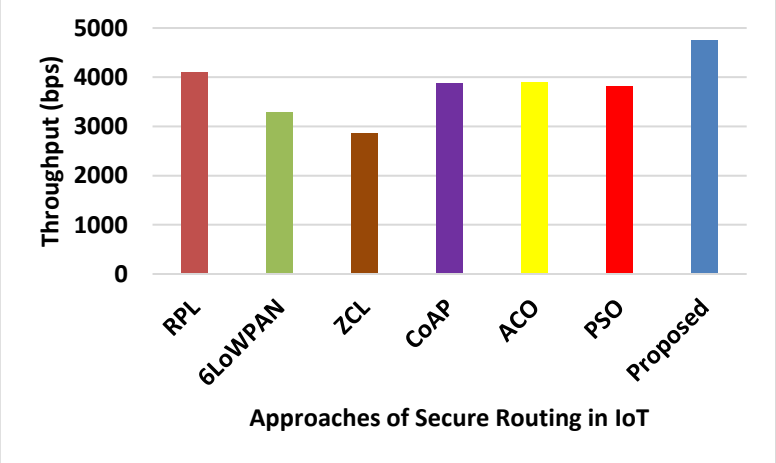

Figure 14. Comparative analysis of throughput.

4. CONCLUSION

Even though IoT technology will advance over the decade that follows, it is crucial to consider all of its nuanced and intricate facets while implementing effective communication protocols. This paper proposes an ACO-based routing algorithm for IoT that utilizes a trust evaluation-based security system while taking into account the resource constraints of deployed sensors or low-powered IoT devices as well as the particular requirement of security during data transmission. It sets up secure routing with reliable nodes in order to protect IoT networks from routing attacks. The trust value is used to determine whether a node is reliable enough to transfer packets. A trust-based threshold mechanism is applied, and if the evaluated node's calculated direct trust value is not credible enough, the indirect trust value is calculated. This suggests that the presented model is lightweight and can conserve more energy. The offered system recommended employing bio-inspired methods to optimize the trust factors. The trust metric, along with the existing node energy and path cost, are included in the route assessment function for analyzing route behavior. The probability formula of the ACO algorithm considers the energy parameter, the trust metric, and the average node velocity. Even as the number of nodes expanded, the lightweight and scalable ACO-based routing system that is presented reduces average energy consumption by approximately 50% contrasted to the benchmark options. Additionally, it demonstrated a 40% reduction in end-to-end delay. The routing system offers a secured and globally optimum path based on the pertinent data, and can effectively optimize security and energy consumption. In future work, the proposed secure routing protocol will be expanded upon to deal with other conspiring attacks, such as those where rank attacking nodes colluding with blackhole or selective forwarding attacks, while formerly trusted nodes will be

reintegrated according to their trust levels after recovering their battery power. Additionally, incorporating Artificial Intelligence and Machine Learning algorithms could improve the preliminary outcomes even further, creating a more dynamic and flexible security system.

REFERENCES

[1] F. Pereira, R. Correia, P. Pinho, S. I. Lopes, and N.B. Carvalho, "Challenges in resource-constrained IoT devices: Energy and communication as critical success factors for future IoT deployment", Sensors (Basel) 2020, 20, 6420.

[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, vol. 17(3), pp. 1294–1312, 2015.

[3] S. Ganeriwal and M. B. Srivastava, "Reputation-based framework for high integrity sensor networks," in SASN'04: Proceedings of the 2nd ACM workshop on security of Ad hoc and sensor networks, New York: ACM, pp. 66–77, 2004.

[4] S. Hamrioui and P. Lorenz, "Bio inspired routing algorithm and efficient communications within IoT," IEEE Network, vol. 31(5), pp. 74-79, 2017.

[5] H. Xia, Z. Jia, and E. H.-M. Sha, ''Research of trust model based on fuzzy theory in mobile ad hoc networks,'' IET Inf. Secur., vol. 8 (2), pp. 88–103, March 2014.

[6] A. Gladkov, E. Shiriaev, A. Tchernykh, M. Deryabin, M. Babenko, S. Nesmachnow, "DT-RRNS: Routing protocol design for secure and reliable distributed smart sensors communication systems," Sensors (Basel), vol. 23(7), p. 3738, 2023.

[7] 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, pp. 299–303, 2015.

[8] S. S. Solapure and H. H. Kenchannavar, "Design and analysis of RPL objective functions using variant routing metrics for IoT applications," Wireless Networks, vol. 26, pp. 4637-4656, 2020.

[9] G. Glissa, A. Rachedi, and A. Meddeb, "A Secure Routing Protocol Based on RPL for Internet of Things," in 2016 IEEE Global Communications Conference (GLOBECOM), pp. 1-7, 2016.

[10] X. Liu, J. Yu, K. Yu, G. Wang, and X. Feng, "Trust secure data aggregation in WSN-based IIoT with single mobile sink", *Ad Hoc Netw.* 2022, *136*, 102956.

[11] 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.

[12] R. Yamamoto, S. Nishibu, T. Yamazaki, Y. Okamura, Y. Tanaka, "ACO-inspired energy-aware routing algorithm for wireless sensor networks," Journal of Telecommunications and Information Technology, 2019.

[13] 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, pp. 190-195, 2021.

[14] A. Sharmin, F. Anwar, S.M.A. Motakabber, A.H.A. Hashim, "A Trust Aware Secure Ant Colony Optimization Based Routing Algorithm for Internet of Things," In 2023 IEEE 9th International Conference on Computer and Communication Engineering, ICCCE 2023, pp. 58-63, 2023.

[15] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan, "An application-specific protocol architecture for wireless microsensor networks," IEEE Transactions on Wireless Communications, vol. 1(4), pp. 660-670, 2002.

[16] W. Fang, X. Zhang, Z. Shi, Y. Sun, and L. Shan, ''Binomial-based trust management system in wireless sensor networks,'' Chin. J. Sens. Actuators, vol. 28, no. 5, pp. 703–708, 2017.

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

[19] S. M. Muzammal, R. K. Murugesan, N. Z. Jhanjhi, M. S. Hossain, and A. Yassine, "Trust and mobility-based protocol for secure routing in Internet of Things", *Sensors (Basel)* 2022.

[20] M. Tanveer, G. Abbas, Z. H. Abbas, M. Waqas, F. Muhammad, and S. Kim, "S6AE: Securing 6LoWPAN using authenticated encryption scheme", Sensors (Basel) 2020.

[21] K. Nichols, V. Jacobson, and R. King, "Defined-Trust Transport (DeftT) Protocol for Limited Domains", Available online: https://datatracker.ietf.org/doc/draft-nichols-iotops-defined-trust-transport/ (accessed on 5 March 2023).

[22] J. Granjal, J. M. Silva, and N. Lourenço, "Intrusion detection and prevention in CoAP wireless sensor networks using anomaly detection", Sensors (Basel) 2018.

[23] G. Shafer, "A mathematical theory of evidence," Princeton university press, vol. 42, 1976.

[24] D. R. Dodds, "Fuzziness in knowledge-based robotics systems. Fuzzy sets and systems," vol. 26(2), pp. 179-193, 1988.

[25] A. Josang, and R. Ismail, "The beta reputation system," In Proceedings of the 15th bled electronic commerce conference, vol. 5, pp. 2502-2511, June 2002.

BIOGRAPHY OF AUTHORS

Afsah Sharmin received an M.Sc. in Telecommunications Engineering and Telecommunication Networks from the University of Technology Sydney (UTS), Australia in 2009 and a B.Sc. in Computer Engineering from American International University-Bangladesh (AIUB), Bangladesh in 2004. She received a second M.Sc. in Computer and Information Engineering from the International Islamic University Malaysia (IIUM), Malaysia in 2019. She is currently a PhD student in the department of Electrical and Computer Engineering at the International Islamic University Malaysia (IIUM). Her research interests are in wireless sensor networks, bio inspired WSN routing algorithm, energy-efficient communication, computer security, and IoT. She had been a faculty member of American International University-Bangladesh in the Department of Computer Science and Engineering.

Associate professor Dr. S. M. A. Motakabber was received the B.Sc. and M.Sc. Degrees in Applied Physics and Electronics from the University of Rajshahi, in 1986 and 1987, respectively, and the Ph.D. degree in Electrical, Electronic and Systems Engineering from the National University of Malaysia, in 2011. From 1993 to 2011, he was an Associate Professor in the Department of Applied Physics and Electronic Engineering at the University of Rajshahi, Bangladesh. He is now Associate Professor in the Department of Electrical and Computer Engineering at the International Islamic University of Malaysia. Dr. Motakabber is a Chartered Engineer UK (CEng). He is a senior member of the Institute of Electrical and Electronics Engineers (IEEE), His research interests are Analog & Digital Electronic System Design, Wireless Sensor Networking, Medical & Industrial Instrumentation, VLSI Design, RFID, Robotics, Automated Control System, Embedded System Design and IoT. He has published more than 70 research articles in peer-reviewed journals, 80 conference proceedings, one textbook for under grate students and two research books.

Professor Aisha Hassan Abdalla Hashim received her PhD in Computer Engineering (2007), M.Sc. in Computer Science (1996), and B.Sc. in Electronics Engineering (1990). She joined IIUM in 1997 and is currently working as a Professor at the Department of Electrical and Computer Engineering. Professor Aisha is actively involved in research and postgraduate programmes. Her research interests are in the areas of network communication, wireless computing, cloud computing, network management, and IoT. She has published more than 300 journal/conference papers. She received Promising Researcher Award in 2009 during IIUM Quality Day. She has also received "Top 30 Contributors, ranked number 6, to IIUM research performance (MyRA) 2017" award and the "Highest Number of Publications in Index Journal award (faculty level)" awarded during the University Quality Day, July 2018. She is a senior member of IEEE, a member of IEEE Women in Engineering and a member of IEEE professional bodies.