Secure IoT Routing through Manifold Criterion Trust Evaluation using Ant Colony Optimization

Afsah Sharmin[1], Rashidah Funke Olanrewaju[2], Burhan Ul Islam Khan[3*], Farhat Anwar[4], S.M.A. Motakabber[5], Nur Fatin Liyana Mohd Rosely[6], Aisha Hassan Abdalla Hashim[7]

Department of ECE, Kulliyyah of Engineering, International Islamic University Malaysia, Kuala Lumpur, Malaysia[1, 2, 4, 5, 7]
Department of CST, Faculty of Computer Science and Information Technology, Universiti Malaya, Kuala Lumpur, Malaysia[3]
Faculty of Data Science and Information Technology, INTI International University, Nilai, Malaysia[6]

***Abstract*—The paper presents a simplified yet innovative computational framework to enable secure routing for sensors within a vast and dynamic Internet of Things (IoT) environment. In the proposed design methodology, a unique trust evaluation scheme utilizing a modified version of Ant Colony Optimization (ACO) is introduced. This scheme formulates a manifold criterion for secure data transmission, optimizing the sensor's residual energy and trust score. A distinctive pheromone management is devised using trust score and residual energy. Concurrently, several attributes are employed for constraint modeling to determine a secure data transmission path among the IoT sensors. Moreover, the trust model introduces a dual-tiered system of primary and secondary trust evaluations, enhancing reliability towards securing trusted nodes and alleviating trust-based discrepancies. The comprehensive implementation of the proposed integrates mathematical modeling, leveraging a streamlined bioinspired approach of the revised ACO using crowding distance. Quantitative results demonstrate that our approach yields a 35% improvement in throughput, an 89% reduction in delay, a 54% decrease in energy consumption, and a 73% enhancement in processing speed compared to prevailing secure routing protocols. Additionally, the model introduces an efficient asynchronous updating rule for local and global pheromones, ensuring greater trust in secure data propagation in IoT.**

Keywords*—Internet of things (IoT); secure IoT routing; manifold criterion trust evaluation; ant colony optimization (ACO); bioinspired computing; pheromone management

I. Introduction

Sensors are an integral part of the IoT landscape. They acquire environmental data and perform real-time transmission over the hosted IoT network [1]. These compact electronic devices can sense various environmental attributes, such as chemical composition, motion, sound, light, pressure, humidity, and temperature, depending on their application or the environment in which they are deployed [2–5]. In the context of IoT, sensors acquire information from the physical world and forward it to a sink node for analysis [6]. This acquired information might be used for research purposes or to trigger specific actuators for automated actions [7–10]. However, despite their capabilities, these sensors often have limited processing and computing abilities, and ensuring their extended lifespan remains challenging [11].

Among the various issues associated with sensors, security is the most critical concern for IoT sensors [12]. The first issue is data privacy, ensuring data is stored securely and transmitted to the intended terminal without unauthorized access [13]. The second pertains to vulnerabilities in IoT devices; sensors often fall prey to cyber-attacks due to unpatched vulnerabilities, outdated software, or weak passwords [14]. The third challenge relates to malware attacks in the form of Trojans, worms, and viruses, which can hinder data transmission, steal data, or corrupt device functionalities [15]. Physical security represents the fourth concern; unauthorized access to a sensor can lead to data tampering, malware introduction, or functionality disruption [16]. The fifth challenge involves Distributed Denial-of-Service (DDoS) attacks, where overwhelming traffic incapacitates sensors, disrupting their communication or services [17]. The sixth pertains to Man-in-The-Middle attacks, where attackers can intercept and potentially modify or steal data [18]. Numerous studies have proposed security mechanisms for IoT to address these vulnerabilities [19–23], but comprehensive solutions that tackle all these challenges remain elusive, with each approach having its strengths and weaknesses.

Securing routing in IoT has become a complex endeavor in today's landscape, marked by an ever-increasing array of known and emerging threats [24, 25]. One core challenge arises from the use of resource-constrained devices in IoT, characterized by limited battery life, memory, and computing power. This limitation precludes the deployment of robust cryptographic algorithms on such devices [26]. The dynamic topology of IoT, where devices can spontaneously join or leave the network, further complicates security protocols. Incorporating diverse IoT devices with specific service requirements complicates implementing universal security protocols. Challenges also arise from issues with mobility and localization; accurate localization information is hard to obtain, and the legitimacy of mobile nodes is difficult to verify. The need for standardization in IoT devices and security protocol management further complicates matters. Most current IoT security research is conducted in controlled environments, distinct from real-world scenarios. Thus, the reliability of their applications in practical deployments remains to be determined.

The manuscript is structured as follows: Section II delves into current methodologies for secure routing in IoT, emphasizing various bioinspired approaches and their

*Corresponding Author

This research was supported by the INTI IU Research Seeding Grant Phase 1/2023 initiative under Project No: INTI-FDSIT-01-01-2023.

contributions. Section III outlines the research problem identified from insights gleaned from these existing methodologies. The proposed methodology to address these issues is detailed in Section IV. An analysis of the results is presented in Section V, while Section VI concludes the paper.

II. Existing Approaches

Over time, several schemes have been developed to investigate secure routing within IoT. Among these, trust-based schemes have emerged as an essential tool for a simplified defense against security breaches [27, 28]. Liu *et al.* [29] devised a secure aggregation model for a Wireless Sensor Network (WSN), ensuring increased trust when operated with a single mobile sink node. Additionally, some research has focused on optimizing trust factors through bioinspired approaches. For instance, Mangalampalli *et al.* [30] employed a whale optimization scheme for enhancing task scheduling. Muzammal *et al.* [32] introduced a trust-based protocol to counter blackhole attacks in static and mobile IoT environments. However, these approaches often need to pay more attention to the dynamic nature of IoT networks and may not be efficient in real-time scenarios.

Awan *et al.* [33] embraced a blockchain-based model for secure routing in WSN, aiming to refine trust management. Notably, their model incorporated the Rivest Shamir Algorithm to safeguard data propagation. However, blockchain's inherent latency issues could limit its practicality in specific IoT setups. Nagaraju *et al.* [34] combined energy optimization with a traditional hybrid approach for secure IoT routing within heterogeneous WSNs. While energy-efficient, such models might compromise on real-time response. Bakhtiari *et al.* [35] proposed a two-way trust strategy using Bayesian learning automata for fog computing in IoT. It improves efficiency, reduces latency, and enhances trust calculations compared to existing methods. However, it's sensitive to initial trust accuracy, potentially impacting performance in dynamic networks. Also, implementing this two-way trust management strategy may introduce increased computational complexity as a potential limitation. Concurrently, Rakesh and Sultana [36] designed a neural network-empowered quantum scheme for mobile sink selection, employing the sailfish optimization approach for enhanced route security. However, this approach might demand more computational resources, impacting resource-constrained IoT devices. Additionally, its effectiveness may vary based on network conditions and the presence of malicious nodes, with reliance on initial trust assessments potentially limiting performance in dynamic environments. Gladkov *et al.* [37] championed a novel routing technique merging the residual number of redundant systems with a secret sharing scheme. However, the complexity associated with such hybrid approaches might lead to higher computational overheads. These diverse strategies enhance security in IoT and WSNs, but careful consideration of their computational requirements and adaptability to dynamic networks is crucial during implementation. Balancing security with resource constraints remains an ongoing challenge in these technologies.

Ramaswamy and Norman [38] introduced a trust model targeting network longevity and internal attacks in IoT. The exploration of bioinspired methods for secure IoT routing has seen algorithms like ACO applied in secured routing (Wang [39], Saleem & Ahmad [40]), decentralized traffic management (Nguyen and Jung [41]), electric vehicle selection (Ajinappa and Prabhakar [42]), and malware detection (El-Ghamry *et al.* [43]). While ACO's adaptive nature is commendable, it may struggle with large-scale, dynamic IoT environments due to its iterative nature. Particle Swarm Optimization (PSO), as documented by Alterazi *et al.* [44], Lin *et al.* [45], and Rajeshwari & Ramakrishnan [46], has also been harnessed for secure data transmission. Other notable bioinspired techniques include the Mayfly Optimization Algorithm (MOA) by Janani and Ramamoorthy [47], the Dragonfly Algorithm (DA) by Hosseinzadeh *et al.* [48], and Glowworm Swarm Optimization (GSO) by Selvaraj *et al.* [49]. Although these bioinspired strategies offer unique solutions, their scalability and adaptability in diverse IoT ecosystems might be limiting factors. The summary of strength and weakness of the reviewed literature is presented in Table I to state that existing methodologies towards secure routing in IoT is associated with beneficial features as well as shortcomings, which are required to be addressed in future upcoming series of research work.

TABLE I. Summary of Existing Schemes

Author	Problem	Methodology	Advantage	Limitation
Liu *et al.* [29]	Security in WSN, IoT	Trust-based secure data aggregation	• Trust-based secure data aggregation mechanism. • Real-time and accurate data acquisition. • Robust aggregation tree algorithm for efficient data gathering. • Enhanced network performance, including improved accuracy and reduced delay.	• Possibility of contradiction in indirect trust. • Scalability challenges in large-scale Industrial Internet of Things (IIoT) settings. • High implementation complexity. • Limited consideration for mobile sensor nodes. • Need more focus on energy efficiency.
Mangalampalli *et al.* [30]	Task scheduling with trust	Whale Optimization	• Enhanced task scheduling efficiency. • Reduced makespan. • Lower energy consumption. • Improved quality of service. • Increased trust in cloud service providers.	• Parameter sensitivity. • Implementation complexity. • Scalability issues. • Input data dependency. • Workload-driven performance variations. • Setup-specific fine-tuning. • Lack of real-world validation.

Muzammal *et al.* [31,32]	Resisting routing attacks	Trust-based protocol	• Improved security against Routing Protocol for Low-Power and Lossy Network (RPL) attacks. • Tailored for mobile IoT environments with trust and mobility metrics. • Superior performance in packet loss rate, throughput, and topology stability. • Meets consistency, optimality, and loop-freeness requirements. • Better throughput.	• Increased computational resource demands. • Sensitive to network size and setup. • Limited real-world IoT testing. • Protocol implementation complexity. • Requires further assessment in highly dynamic IoT scenarios. • Relies on trust and mobility metrics' accuracy.
Awan *et al.* [33]	Secure data transmission	Trust model, Asymmetric encryption	• High delivery ratio. • Enhanced security through blockchain-based authentication. • Extended network lifespan and reduced packet loss. • Effective malicious node detection and removal. • Secure routing based on residual energy and trust. • High packet delivery ratio in simulations.	• Increased key size. • Blockchain dependency may add complexity. • Scalability issues in more extensive networks. • Lack of real-world validation. • Computational resource demands. • Limited scope beyond trust assessment. • Latency potential in real-time applications. • Ongoing trust monitoring is required.
Nagaraju *et al.* [34]	Security, energy issues	Multipath link routing, hybrid protocol	• Satisfactory network lifetime. • Improved energy efficiency in heterogeneous WSNs. • Enhanced network lifetime. • Secure routing for confidential IoT data. • Load balancing capability. • Improved data storage capacity.	• Cannot sustain dynamic threats. • Limited real-world validation. • Dependence on specific routing protocols. • Possible sensitivity to network dynamics. • Lack of consideration for scalability in large-scale deployments.
Bakhtiari *et al.* [35]	Trust issues in Fog and IoT	Bayesian-based learning automata	• Faster response time. • Improved energy consumption. • Efficient network usage. • Reduced latency. • Enhanced trust management.	• Induces complexity for an extensive network. • Limited real-world validation. • Possible sensitivity to network dynamics. • Dependence on specific trust management methods. • May require fine-tuning for different IoT applications.
Rakesh and Sultana [36]	Trust issues	Sailfish optimization, Neural Network	• Can mitigate multiple attacks. • Improved node reliability with the introduction of a mobile sink. • Secure routing implemented using the sailfish optimization algorithm. • Data encryption for increased data security.	• Consumes higher memory to retain trust values. • Limited real-world validation and scalability considerations. • Network dynamics and computational resource dependencies. • Complexity in implementation. • Emphasis on specific optimization algorithms.
Gladkov *et al.* [37]	Routing reliability	Secret sharing scheme	• Highly adaptive. • Enhanced speed and reliability in data transmission. • Improved security through Secret Sharing Schemes (SSS). • Enhanced fault tolerance and reliability. • Adaptive multipath secured transmission for route attack prevention.	• No consideration of energy constraints. • Possible complexity in implementing SSS and RRNS. • Dependency on adaptive multipath secured transmission. • Scalability needs to be fully addressed. • Limited evaluation in dynamic heterogeneous networks.
Ramaswamy [38]	Energy issues	Trust model	• Secured clustering	• Extensive analysis is needed further.
Wang [39], Saleem and Ahmad [40], Nguyen and Jung [41], Ajinappa and Prabhakar [42], El-Ghamry *et al.* [43]	Security issues in IoT	ACO	• Higher accuracy	• Inferior convergence speed.
Alterazi *et al.* [44], Lin *et al.* [45], Rajeshwari [46]	Trust/security in IoT	PSO	• Faster performance	• High dimensional space issue needs to be addressed.

Janani and Ramamoorthy [47]), Hosseinzadeh *et al.* [48], Selvaraj *et al.* [49]	Secure data transmission in IoT	MOA, DA, GSO	• Flexible performance	• Highly iterative scheme leading to complexity.

From the highlights of the methodologies, their advantages, and limitations in the table above, it can be noted that existing secured routing methodologies are associated with various shortcomings in the perspective of deployment in an IoT environment. Following are some of the significant research problems related to the existing methods towards secure routing in IoT:

- Issues in Trust-based IoT Security: Various trust-based secure routing schemes are formulated in existing systems. Most of these techniques offer better throughput; however, the majority are also witnessed by their non-sustainability towards dynamic threats. Furthermore, the existing trust management schemes are usually designed considering the predefined information of adversaries. This makes the model robust in one environment but not applicable if the adversary environment is altered.
- Imbalance between Energy and Security Demands: Existing approaches favor energy or security retention. The security schema presented in existing schemes uses various sophisticated operations that can offer more security but at the cost of uncertain resource consumption. There has yet to be a benchmarked study model to prove this in the presence of the dynamic environment of IoT.
- Usage of Bioinspired Approach: The adoption of bioinspired approaches towards secure routing is less abundant in archives of technical publications. However, the available publications on the use of bioinspired strategies contribute towards findings of the secured path by adopting the varied cognitive principles of organisms to attain optimal security. Unfortunately, the issues related to premature convergence and higher sensitivity towards parameters by conventional bioinspired approaches have not yet been addressed. Moreover, there is no report of any study model where novel features of organisms' cognitive behavior have been attempted to be modified and investigated.
- Non-inclusion of Constraint in Trust Management: 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. This yet-to-solve challenge acts as a potential impediment to computing and establishing trust between all the entities and IoT devices in large and dynamic environments. For secure routing to occur correctly, it is necessary to formulate a better form of constraint modeling with a clear definition of the attributes that need to be added to the existing system.
- The tradeoff between Model Effectiveness and Scalability: Scalability is a different set of problems in IoT to be resolved. It demands a smart and highly planned processing for secure routing in IoT. Unfortunately, none of the existing study models has been designed considering its optimization parameter or problem space mapping with the large environment of an IoT with more interconnected devices. For this purpose, the outcome of model effectiveness doesn't match the sensors' scalable performance in increased traffic flow over an IoT.

From the above-stated highlights of the identified research problem, it can be inferred that trust modeling is one of the complex issues that demand the inclusion of various intrinsic and extrinsic attributes and effective constraint modeling. Apart from this, it is necessary to optimize the problem space to increase the change of optimal outcome of the secured path. Bioinspired algorithms are a potential alternative to address this problem, but they demand a novel inclusion of characteristics that can balance security and resource demands. The proposed solution addresses all these research issues, and its associated methodology towards implementation is discussed next.

III. Research Problem

The rapid proliferation of the IoT heralds both transformative opportunities and notable security challenges. With its expansive network of devices, IoT underscores the urgency for reliable, secure routing. Emerging as a promising avenue, trust-based secure routing strategies aim to buttress IoT's security framework. However, IoT's dynamic and resource-limited nature has often rendered traditional trust-based methods inadequate.

A significant limitation of extant trust-based IoT security methodologies is their inability to adapt to evolving threats, often designed around known adversarial models. The quest to harmonize energy conservation with security amplifies this challenge, as current systems lean towards one, often sacrificing the other. This compromise becomes more palpable when high-security measures, despite their efficacy, devour substantial resources.

The contemporary research landscape needs to display bioinspired strategies for secure IoT routing. Drawing inspiration from natural systems to fortify security, these approaches appear promising. Nevertheless, prevalent bioinspired models grapple with issues like early convergence and parameter sensitivity. This highlights a pressing need to refine and adapt these methods, tailoring them for IoT's unique challenges.

Further complicating the scenario is the design of trust management systems. The intrinsically limited resources of IoT devices, in terms of energy and processing power, hinder the execution of comprehensive security protocols. This challenge intensifies in the sprawling IoT ecosystems, where fostering trust amongst various devices is vital and daunting.

Scalability further accentuates these problems. While effective in a controlled setting, an approach might need to be revised under IoT's expansive and interconnected structure, especially when encountering unexpected traffic surges.

While trust modeling offers a promising foundation for IoT security, its practical deployment is beset with multifaceted challenges. This study aspires to address these gaps, employing the bioinspired ACO technique to architect an adaptive and secure IoT routing paradigm adeptly poised to navigate the intricate challenges of IoT.

IV. Materials and Methods

The prime agenda of the proposed study model is to introduce a novel computational model that ensures robust trust-based security while transmitting data among the sensor nodes in IoT. The prime basis of the proposed study model is based on the fact that the severity degree of security threat for sensor nodes deployed in an IoT environment is comparatively higher in contrast to conventional WSN. Therefore, the security aspect of WSN deployed in IoT is subjected to improvement by balancing the demand for increased security along with energy consumption. Hence, various criterion-based schemes is implemented, harnessing ACO along with constraint consideration towards secure trust evaluation.

From the exhibited methodology in Fig. 1, it can be noted from the declaration of the proposed scheme that it uses a manifold criterion modeling towards trust-based secure routing in an IoT environment. Adopting an optimization agenda towards manifold criteria is simultaneously challenging due to the surfacing possibilities of various conflicts. Moreover, unlike managing unit criterion-based routing improvement strategy, the multiple criterion schemes usually seeks to obtain compromised outcomes, yet another sub-optimal solution towards secure routing. Therefore, the proposed system constructs a manifold criterion-based trust modeling in IoT to address the issue of energy drainage and security threats as follows:

$$arg_{max}\varphi(t) = [\varphi_1(t)\varphi_2(t)] \quad (1)$$

In Eq. (1), the manifold criterion function $\varphi(t)$ is represented by two sub-criteria, i.e., $\varphi_1(t)$ and $\varphi_2(t)$, representing the mean criterion for remnant energy and the mean value of trust of the sensor nodes associated with the routing path in IoT. Two processes follow for this purpose:

- The above expression is required to be satisfied for its remnant energy score $R_i(t) > 0$ for the i^{th} the sensor at t instance of time such that acquired data by the sensor is $AD_{ij}(t) > 0$ from the i^{th} sensor to the j^{th} sensor while forwarding data $FD_{ji}(t) > 0$ from the j^{th} sensor to the i^{th} sensor.
- This task is carried out considering $0 < t < t_{max}$. From Eq. (1), it can be noted that the proposed scheme considers
  - $\varphi_1(t)$ as a function for mean remnant energy,
  - $\varphi_1(t)$ as a function for trust score that is considered towards the selection of an optimal path,
  - Multiple constraints as a maximal time of communication t_{max}, the quantity of forwarding data $FD_{ji}(t)$, the quantity of acquired data $AD_{ij}(t)$, and remnant energy $R_i(t)$.

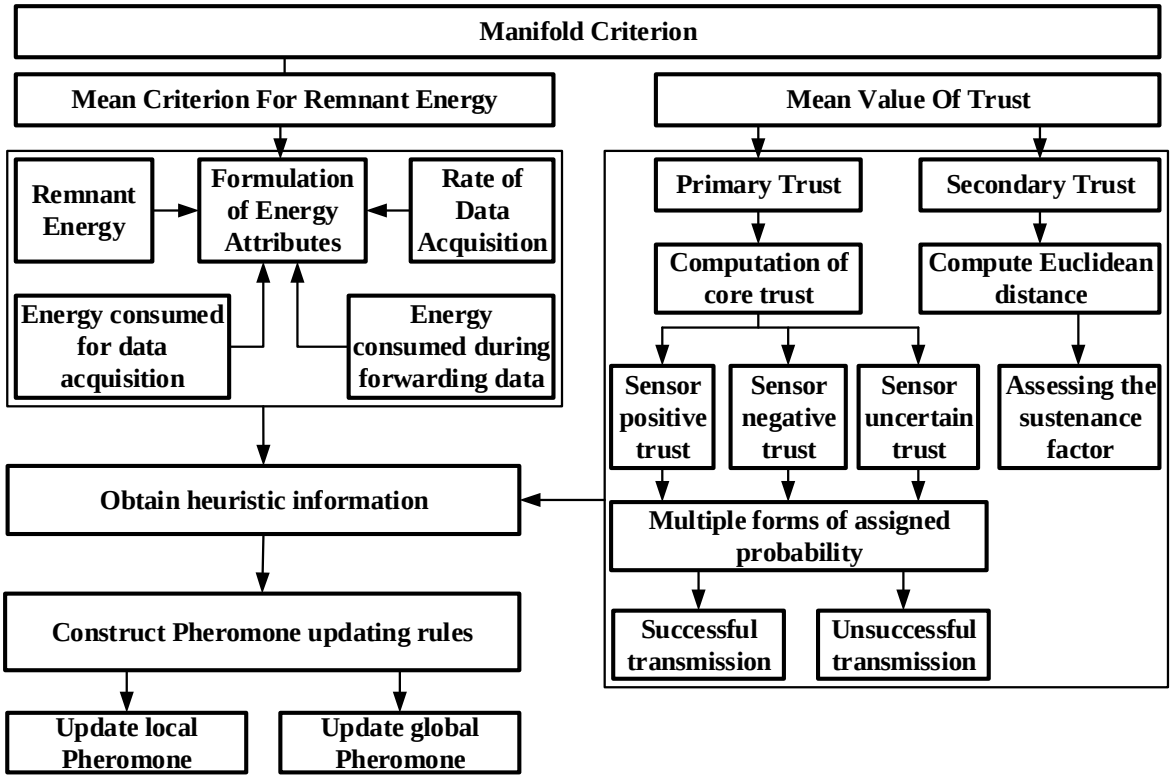

Fig. 1. Proposed methodology.

The complete formulation of the proposed study is based on two essential functions toward meeting the objectives, i.e., $\varphi_1(t)$ and $\varphi_2(t)$ towards energy and trust, respectively. It also includes four conditions of constraint. It should be noted that adopting these two essential functions is deployed for opting for the best path for data propagation, where the performance of nodes is selected as an indicator. This section further elaborates on the formulation of the proposed scheme. Further discussion of the formulation of the proposed modeling is carried out in subsequent sections.

A. Formulation of Manifold Criterion

Energy is one of the essential attributes considered in the proposed scheme whose consumption is generally recorded for multiple events of a sensor being in an idle state, sleep state, or either in receiving or transmission state. The formulation of energy attribute $R_i(t)$ is carried out as follows:

$$R_i(t) = \eta_1 + \eta_2 \tag{2}$$

To obtain information on the consumed energy of IoT nodes, any conventional mechanism can be adopted considering software and hardware components. The proposed scheme considers this an energy input value and contributes towards further optimized routing. Besides energy, the proposed method chooses to initiate its design implementation considering any conventional trust evaluation scheme that can vary based on application and use case. However, the system relies not much on device-specific trust computation mechanisms but more on behavioral analysis based on historical reports of security breaches, violations /adherence to security protocols, and compliance with access control protocols. Like the consumed energy metric, the proposed scheme also considers this trust score to act as an input to its model toward working in the direction of proof-of-concept. In Eq. (2), the computation of energy attribute $R_i(t)$ is carried out using two sub-entities, i.e., η_1 and η_2.

$$\eta_1 = R_j(t-1) - \lambda_{ij}(t).R_j^{\lambda}(t) \tag{3}$$

As shown in Eq. (3), the formulation of η_1 is carried out by differentiating the product of $\lambda_{ij}(t)$ and $R_j^{\lambda}(t)$ from $R_j(t-1)$, where the entities $R_j(t)$ and $R_j(t-1)$ represent remnant energy of the j^{th} sensor at instant t and $(t-1)$, respectively. The entity $\lambda_{ij}(t)$ represents the data acquisition rate from the i^{th} sensor to the j^{th} sensor. In contrast, $R_j^{\lambda}(t)$ represents the energy consumed for data acquisition for the j^{th} node at the t-instance.

$$\eta_2 = \lambda_{ij}(t).R_j^{C}(t) - R_j^{C}(t) \tag{4}$$

On the other hand, the formulation of η_2 shown in (4) is carried out by differentiating energy dissipated by the j^{th} sensor, $R_j^{C}(t)$ from the product of the data acquisition rate from the i^{th} sensor to the j^{th} sensor, $\lambda_{ij}(t)$ and energy consumed while forwarding data for the j^{th} sensor, $R_j^{C}(t)$. Therefore, the criterion function for mean energy associated with the path of routing considering α number of sensors in IoT can be represented as:

$$\varphi_1(t) = \sum {R_j(t)}/{\alpha} \tag{5}$$

In Eq. (5), the suffix j resided between (1, α). After formulating the energy attribute, the next task is developing the trust attribute of a sensor deployed in an IoT environment. The notion of trust attribute represents the degree of consistency in data packet transmission and receiving by the sensors when exposed to different severity levels of attacks in IoT (e.g., DDoS). The trust attribute is computed based on the evidential traces furnished by the neighboring sensors or by observing trust attributes from the adjacent sensors. Therefore, the proposed scheme formulated two types of trust attributes, i.e., primary and secondary.

1) Evaluation of primary trust: The primary trust is the value obtained directly from the i^{th} sensor to the j^{th} sensor. In contrast, the secondary trust is the value obtained from the i^{th} node to different relay sensors, and then it reaches the j^{th} sensor. The initial assessment towards the trust modeling is carried out for primary trust that considers that every possibility of evaluation of the sensor's trust consists of information associated with the degree of consistency associated with data transmission, rate of transmission, and rate of acquiring the data packet. The proposed scheme considers the evaluation of the core trust score γ_{ij} of the target i^{th} sensor on the j^{th} sensor to be assessed at t-instance of time as follows:

$$\gamma_{ij}(t) = \left[spt_{ij}(t), snt_{ij}(t), sut_{ij}(t)\right] \tag{6}$$

In Eq. (6), the computation of core trust γ_{ij} is carried out based on sensor positive trust, sensor negative trust, and sensor uncertain trust represented by $spt_{ij}(t)$, $snt_{ij}(t)$, and $sut_{ij}(t)$, respectively. It can be noted that all these three types of trust variables are equivalent to probability factors associated with multiple forms of assigned probability $\omega_{ij}^{c}(\pi)$, $\omega_{ij}^{c}(-\pi)$, and $\omega_{ij}^{c}(\pi,-\pi)$, where π represents a possible secured route for data propagation. It will eventually mean that the variable $\gamma_{ij}(t)$ represents the summation of the success rate of data acquiring, i.e., $\lambda_{ij}^{s}(t)$. In contrast, the success rate of data forwarding $F_{ij}^{s}(t)$ and $\beta_{ij}^{s}(t)$ denotes consistency in data packet transmission. Therefore, the expression in Eq. (6) can now be rewritten as:

$$\gamma_{ij}(t) = [\omega_{ij}^{c}(\pi), \omega_{ij}^{c}(-\pi), \omega_{ij}^{c}(\pi,-\pi)] \tag{7}$$

where, $\omega_{ij}^{c}(\pi) = [\theta_1.\lambda_{ij}^{s}(t) + \theta_2.F_{ij}^{s}(t) + \theta_3.\beta_{ij}^{s}(t)]$

$\omega_{ij}^{c}(-\pi) = [\theta_1.\lambda_{ij}^{us}(t) + \theta_2.F_{ij}^{us}(t) + \theta_3.\beta_{ij}^{us}(t)]$

$\omega_{ij}^{c}(\pi,-\pi) = [1 - spt_{ij}(t) - snt_{ij}(t)]$

In Eq. (7) in its expanded form, the power variable of the expression, i.e., s and us, represents successful and unsuccessful transmission in the IoT environment, while the variables θ_1, θ_2, and θ_3 represent weight values associated with different modes of transmission, which are subjected to training using first-order iterative optimization to arrive at the local value of the defined function. With the aid of Eq. (7), the formulation of the primary trust PT_{ij} between the i^{th} sensor and j^{th} sensor can be carried out as follows:

$$PT_{ij}(t) = [P1_{ij}(t), P2_{ij}(t), P3_{ij}(t)] \tag{8}$$

$$= [\omega_{ij}(\pi), \omega_{ij}(-\pi), \omega_{ij}(\pi, -\pi)]$$
$$= h_1 + h_2$$

In Eq. (8), the variables $P1$, $P2$, and $P3$ are primary values of trust, which are nearly similar to the notion of the variables $spt_{ij}(t)$, $snt_{ij}(t)$, and $sut_{ij}(t)$, while the variables h_1 and h_2 are empirically represented as follows:

$$h_1=\left[(1-\eta).\gamma_{ij}(t)\right]$$
$$h_2=\left[\eta.\gamma_{ij}(t)(t-1)\right] \quad (9)$$

From Eq. (9), the variable η further represents the temporal attribute of adaptivity used to evaluate the significance of heuristic data over the existing routing data to assess the trust among the sensors while deployed in an IoT environment.

2) Evaluation of secondary trust: The next part of the implementation is associated with formulating secondary trust $ST_{ij}(t)$, which is essentially meant to process any form of conflict. The empirical formulation of the secondary trust $ST_{ij}(t)$ is expressed as:

$$ST_{ij}(t) = [S1^l_{ij}(t), S2^l_{ij}(t), S3^l_{ij}(t) \quad (10)$$
$$= [\omega^l_{ij}(\pi), \omega^l_{ij}(-\pi), \omega^l_{ij}(\pi, -\pi)]$$

From Eq. (10), it can be seen that the formulation of secondary trust bears a similar strategy as noted in Eq. (8) for primary trust computation, including a variable l representing the common sensor node that resides within the transmission region for both the i^{th} and j^{th} sensors. A closer look into Eq. (10) for secondary trust evaluation will show that it is an n-ary circled times operation between two primary trusts, i.e., $ST_{ij}(t) = PT_{i,1}(t) \otimes PT_{1j}(t)$. The variables $S1^l_{ij}(t)$, $S2^l_{ij}(t)$, and $S3^l_{ij}(t)$ represent secondary positive trust, secondary negative trust, and secondary uncertain value of trust, respectively. These are also corresponding to $\omega^l_{ij}(\pi)$, $\omega^l_{ij}(-\pi)$, and $\omega^l_{ij}(\pi, -\pi)$.

Fig. 2 highlights the pictorial representation of primary and secondary trust evaluation. As the secondary trust evaluation is carried out by the other relay nodes, which are neither source nor destination nodes, there is always a possibility of evolving contradiction in the trust computation. Therefore, the next part of consecutive implementation is associated with evaluating the conflicts in the secondary trust. For this purpose, the proposed scheme constructs a reference matrix towards assessing the equivalency of the trust attributes of secondary trust where the variable μ represents the steadiness score between two secondary trusts and hence $\mu_{a,b}$ indicates the steadiness score for a^{th} and b^{th} relay sensors with a Euclidean distance of $dis_{a,b}$ between two secondary values of trust of ST^{lb}_{ij} and ST^{la}_{ij}, where la and lb represent common a and b sensors between i^{th} transmitting sensor and j^{th} receiving sensor. Empirically, it will be designated as follows:

$$dist_{ab} = |sqrt\left[\left(ST^{lb}_{ij} - ST_{ij}\right)^2 + \left(ST^{la}_{ij} + ST_{ij}\right)^2\right]| \quad (11)$$

After evaluating distance in Eq. (11), the next task is to assess the sustenance factor of secondary trust σ_a, which is obtained by summing up all steadiness scores, i.e., $\mu_{a,b}$. Further, towards attaining secondary trust value, there is a need for one more dependable attribute, i.e., indicative weight g_a, which is obtained from the standard weight of secondary trust (i.e., $ST^{l)}_{ij}$, i.e., O_a. This variable of normal weight of ST^l_{ij} is obtained by dividing sustenance score σ_a with the cumulative sustenance score of secondary trust, i.e., $\sum \sigma_a$. Therefore, the suggested indicative weight of secondary trust, i.e., g_a, is obtained by dividing the normal weight O_a with $arg_{max}(O_a)$. Thus, the final empirical expression towards attaining the value of secondary trust is as follows:

$$ST^l_{ij}(t) = [b_1, b_2, b_3] \quad (12)$$

In Eq. (12), the computation of secondary trust $ST^l_{ij}(t)$ is carried out using three dependable attributes, i.e., b_1, b_2, and b_3 representing $[g_a.S1^l_{ij}(t)]$, $[g_a.S2^l_{ij}(t)]$, and $[1 - g_a.(S1^l_{ij}(t) + S2^l_{ij}(t))]$ respectively.

$$ST^l_{ij}(t) = [(g_a.S1^l_{ij}(t)), (g_a.S2^l_{ij}(t)), (1 - g_a.(S1^l_{ij}(t) + S2^l_{ij}(t)))] \quad (13)$$

Finally, the primary and secondary trust (shown in Eq. (13)) values are combined to yield the joint trust score. It should be noted that the computation of primary trust is carried out directly between the two communicating nodes. In contrast, the secondary trust is evaluated using associated neighboring nodes, as shown in Fig. 2.

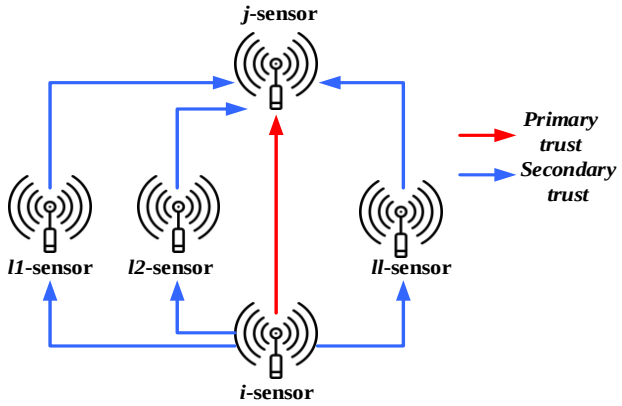

Fig. 2. Primary and secondary trust evaluation.

B. Formulation of Proposed ACO

After the trust computation, the next part of implementing the proposed scheme consists of applying the ACO scheme to arrive at an optimal solution for enhancing network lifetime and accomplishing a higher degree of resiliency from varied threats in the IoT environment. It should be noted that the proposed scheme introduces dual criteria and optimal solutions to amend the conventional ACO scheme to be used in secured routing in IoT. The novelty of the proposed ACO approach is that it constructs logic of manifold heuristic data and manifold pheromones to accomplish the discussed concept of manifold criterion in IoT routing by sensor nodes. The proposed scheme makes use of the idea of crowding distance to boost the algorithm to yield optimal solution diversity. The idea of the proposed ACO approach using crowding distance is to perform

an optimal selection of solutions required for the next generation to map with secure and energy-efficient routing among the sensors in IoT. If the crowding distance is more for a specific set of solutions, then the algorithm considers that set of solutions further for the next generation. Therefore, the proposed ACO approach offers a diversified and optimal solution to accomplish both secured trustworthy routes for data transmission with higher residual energy. According to the proposed scheme, the first set of operations is towards selecting the j^{th} sensor by k number of ants in the form of the i^{th} sensor present in the next hop. This computation offers the probability of change from one state to another. The proposed scheme constructs dual heuristic information that is associated with remnant energy and trust value, which can be empirically exhibited as follows:

$$\sigma_{ij}^{1}(t) = R_j(t) \text{ and } \sigma_{ij}^{2}(t) = \pi_j(t) \quad (14)$$

From Eq. (14), it should be noted that the first heuristic information $\sigma_{ij}^{1}(t)$, i.e., $R_j(t)$, is evaluated considering energy dissipated by the data acquired divided by the initialized energy of the sensor. In contrast, the second heuristic information $\sigma_{ij}^{2}(t)$ depends on a set of candidate routes for optimal data transmission performance with higher trust. The proposed scheme implements two types of pheromone information to fit the model with two heuristic information. The idea is to jointly study the value of trust and the associated remnant energy of a sensor. When an ant constructs a candidate solution using Eq. (15), the scheme instantly updates the pheromone associated with each heuristic. The following are the empirical expressions:

$$\left[\rho_{ij}^{1}(t), \rho_{ij}^{2}(t)\right] = [\chi_1, \chi_2] \quad (15)$$

In Eq. (15), the first attribute of pheromone, i.e., $\rho_{ij}^{1}(t)$, is associated with the criterion for remnant energy, i.e., χ_1. In contrast, the second attribute of pheromone, i.e., $\rho_{ij}^{2}(t)$, is related to the criterion for the mean value of trust, i.e., χ_2. It should be noted that the maximization of the pheromone score is relative to the mean quantity of resource availability and trust score associated with the propagation routes. The inference is that increased resource availability on the communication routes can only ensure a higher degree of pheromone retention. The conclusive remark of this logic is that nodes with reported higher value of trust and resources will eventually have higher feasibility to be opted as participating routing nodes. However, this empirical expression is in abstract form, and it demands more clarity in terms of the actual updating mechanism of pheromone in ACO, which is given as follows:

$$\rho_{ij}^{n}(t+1) = funct(e, \rho_{ij}^{n}) \quad (16)$$

In Eq. (16), the updating of local pheromone ρ_{ij}^{n} is stated considering the unique function $funct$ of coefficient of pheromone evaporation e mainly. The function $funct$ performs extractions of two operators using arguments of e and ρ_{ij}^{n}, i.e., i) $(1-e).\rho_{ij}^{n}(t)$ and ii) $e.\Delta\rho_{ij}^{n}(t)$, where the values of suffixes i and j are associated with π, while the value of power variable n is (1, 2) owing to consideration of two heuristic information. The variable $\Delta\rho_{ij}^{n}(t)$ is incremented, further proportional to the heuristic information of mean trust and energy score. The prominent inference of this implementation concept is that the maximum score of the function χ_1 associated with mean remnant energy will mean higher retention of pheromone on the routing path. It will also mean that if the value of the function χ_2 associated with the mean trust value is found to be maximal, then it will mean that a large quantity of pheromone will be retained. Hence, the routing operation in IoT will always choose only those sensors with a higher value of remnant energy and higher trust. The implementation concept of updating the local pheromone is completed when the data reaches the sink node, followed by further updating of enhanced crowding distance by sub-optimal solutions in the sink node. The system finally yields a backward-moving ant from the forward-moving ant upon completion of the local updating operation of the pheromone.

Finally, the proposed scheme performs updating of the global pheromone by subjecting all the sub-optimal solutions presented by the sink node. The backward-moving ant in the proposed ACO approach carries out this task of updating the sub-optimal solution. An empirical expression for this global pheromone updating is similar to that of Eq. (12) only with the difference of $\Delta\rho_{ij}^{n}(t)$ equivalent to $1/\varsigma$, where the variable ς represents the quantity of the sensors traversed by the k number of backward-moving ants considering a set of sub-optimal solutions as routing paths to update the global pheromone.

The contributions of this methodology can be seen by two significant results: (a) The primary contribution of the proposed method is to design and develop a simplified yet robust secure data propagation scheme in IoT. It is simplified as it doesn't consist of any sophisticated mechanism or involve a higher number of complex processing routing schemes. It is robust as the method can realize the dynamic vulnerabilities present in links connecting IoT nodes without any dependencies on the apriori information of an attacker. The scheme is highly secured as the formulation of the system is carried out considering manifold criteria in the form of an essential function associated with trust and resources of IoT nodes as well as various practical constraints related to time, forwarding, and receiving data, and remnant resources of IoT nodes, (b) The second prime contribution is associated with the mechanism of deploying an ACO approach where novel pheromone management is presented. The credibility of the data propagation and exchange among the IoT nodes is carried out by proposed ACO-based routing, where the selection of cost-effective and secured routes is based on heuristic and pheromone information of manifold type. It should be noted that the proposed scheme considers heuristic information and pheromone information derived from remanent information and the trust score of IoT nodes. The main contributions of the study can be briefly summarized as:

1) The proposed scheme balances trust computation with the selection of optimal nodes possessing substantial residual energy, ensuring they have the requisite resources for extensive secure data propagation within IoT.

2) The trust evaluation mechanism of the proposed system is scalable and viable for both compact and expansive IoT environments. Its resilience is evident as it can function even

in the presence of unknown-origin attackers. This resilience stems from the fact that, regardless of an attacker's strategy, the proposed scheme ensures all standard sensors compute an optimal solution that remains inscrutable to potential intruders.

3) The proposed ACO approach addresses and rectifies the traditional issues of slow convergence and parameter sensitivity, which plague conventional ACOs. By providing a broader problem scope, it aptly aligns with the expansive nature of IoT.

The ensuing section delves into the results derived from implementing the proposed scheme.

V. RESULT

This section presents the results achieved after implementing the proposed model. Since the proposed implementation introduces a novel ACO-based secure routing method, emphasis has been placed on investigating data transmission performance. Additionally, the trust management scheme has been executed for the system. The primary objective of the result analysis is to establish an extensive test environment using variable performance metrics. This is done to gauge the impact of the proposed secure routing conducted by sensors within the IoT environment. The results are then analyzed to provide insights into how the model's performance compares to existing secure routing schemes.

A. Assessment Strategy

The entire implementation is conducted in MATLAB on a standard 64-bit Windows machine. The simulation environment selected for the experiment spans an area of 1000x1000 m^2, with the specific simulation parameters detailed in Table II. This environment replicates a smart city setting where numerous clusters of wireless sensor nodes are interconnected, facilitating data aggregation with a predetermined energy level. While the initial energy assigned to each node is 10 J, it can be adjusted based on the specific IoT application in use. Thus, the proposed simulation environment offers considerable flexibility, accommodating modifications to parameter values to fit various scenarios.

TABLE II. SIMULATION PARAMETERS ADOPTED FOR ASSESSMENT

Parameters	Values
No. of Sensors	500-1000
Initialized energy	10 J
Rate of data transmission	400 kbps
Data packet size	5000 byes
Communication Radius	200 m
Antenna	Omni-directional
MAC	802.11
Simulation Time	100 s

To gauge the effectiveness of the proposed scheme, a benchmarked analysis against existing secure routing schemes in the IoT environment is essential. This comparative analysis examines specific performance metrics across the proposed and existing secure routing schemes. The conventional secured routing schemes selected for comparative analysis in IoT include:

- Routing Protocol for Low-Power and Lossy Network (RPL): This standard IoT routing scheme is tailored for networks with lossy features and low-powered nodes. Its secure variant, Secure RPL (SRPL), employs authentication of messages and encryption operations to ensure data freshness, integrity, and confidentiality [32].
- Routing using 6LoWPAN: Another conventional IoT routing method closely aligned with RPL, this protocol leverages the IPv6 scheme for routing. It adopts 6LoSec, primarily designed to guard against replay attacks and ensure data integrity and confidentiality [50].
- Secured routing using Zigbee Cluster Library (ZCL): Zigbee's prevalence in IoT-based wireless communication systems is notable. However, ZCL is designed to provide secure routing exclusively for Zigbee-based networks. This scheme uses authentication and encryption to ensure authentic communication, data integrity, and confidentiality [51].
- Secure routing using Constrained Application Protocol (CoAP): This protocol facilitates data transmission for resource-constrained devices within the IoT framework. It incorporates Datagram Transport Layer Security (DTLS) to provide authentication, data integrity, and confidentiality [52].

The aforementioned secure routing schemes and proposed method have been implemented in comparable test environments and under similar simulation parameters. Moreover, the conventional ACO and PSO algorithms have been employed to evaluate the performance enhancements ushered in by the proposed scheme relative to existing bioinspired approaches.

B. Discussion of Result

The initial performance metric examined is network throughput, calculated as the volume of data packets transmitted from one node to another within the IoT environment over a specific time. A detailed examination of the proposed secure routing scheme reveals that it encompasses various mathematical and logical operations based on the manifold criterion-based model. This design ensures a robust defense against manipulation or unauthorized access. Given these intricacies, potential delays or added computational demands might impact throughput. Consequently, benchmarking based on throughput provides a clear insight into whether the inherent security operations compromise network performance and data transmission. Additionally, thorough throughput assessment can highlight potential bottleneck areas within the routing path.

Fig. 3 presents the average throughput observed during a series of evaluations over specified simulation duration. It indicates that the proposed scheme outperforms existing methods in terms of throughput. The RPL protocol emerges as the next best performer in current systems, primarily due to its dynamic path selection capabilities. However, it needs help to balance traffic load during dynamic events within the IoT landscape. Following RPL, conventional ACO, PSO, and

CoAP algorithms rank next in terms of throughput. It's worth noting that traditional ACOs have a limitation, needing help to provide optimal solutions amidst heavy traffic flow. PSO faces a similar challenge, grappling with increased memory dependencies as traffic surges, reducing throughput. The CoAP protocol, because it utilizes User Datagram Protocol (UDP), is prone to packet loss, primarily when data packets are transmitted in an unordered sequence within IoT.

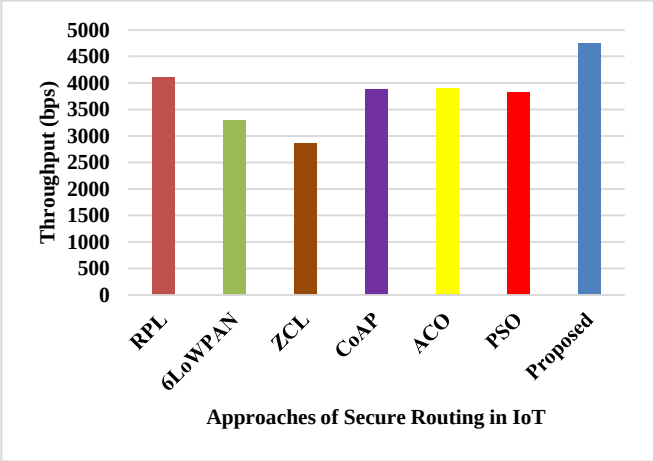

Fig. 3. Comparative analysis of throughput.

Moreover, 6LoWPAN and ZCL underperform in throughput within the IoT environment due to complexities arising from header compression. In contrast, the proposed system remains unaffected by such challenges. Its constraints concerning energy and trust, combined with its modeling, are adept at identifying vulnerabilities and pinpointing alternative optimal paths for propagation based on the manifold criterion. Consequently, even without encryption, the proposed scheme achieves superior secure data transmission throughput compared to conventional secure IoT routing strategies that predominantly depend on encryption and authentication.

The subsequent performance metric evaluated is a delay, calculated as the latency encountered during the data bit transmission across the network from one sensor to another within the IoT framework. Evaluating delay is paramount for secure data transmission, given the diverse applications and services housed within the IoT environment. It's essential to highlight that the proposed scheme incorporates several mathematical procedures for trust calculation, where local and global parameters play pivotal roles. Conversely, most extant secure routing schemes lean heavily on encryption and message authentication to ensure data security. Thus, it becomes imperative to ascertain that these intrinsic security processes don't detrimentally influence network performance by augmenting delay. For optimal network efficiency, it's crucial to maintain low delay, as extended latency often signals network bottlenecks or areas compromised by security vulnerabilities, consequently impinging on data transmission durations.

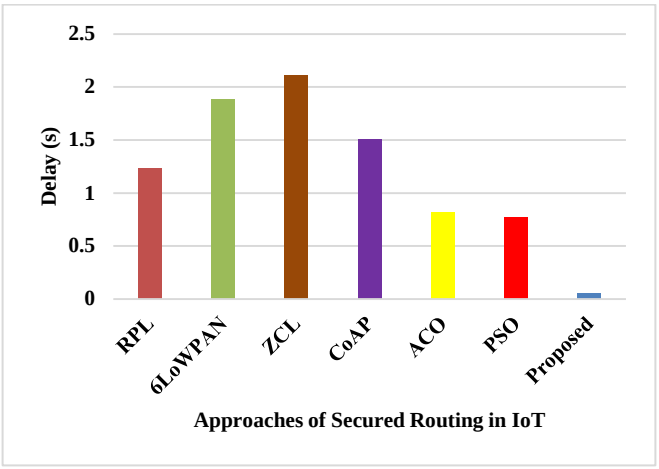

Fig. 4. Comparative analysis of delay.

Examining Fig. 4 reveals that the proposed scheme considerably reduces delay compared to existing systems. ZCL displays a higher delay due to its conventional architecture's slower transmission rate tailored to meet Zigbee transmission requirements. 6LoWPAN outperforms ZCL in delay, but it sacrifices some security; it possesses a weaker immunity to interference. A significant cause of delay in 6LoWPAN is its repeated retransmissions due to packet loss from IPv6 data chunks. CoAP, being optimized for peer-to-peer communication, has an inevitable delay. However, RPL shines the best in reducing delay compared to other secure transmission methods. This is attributed to its auto-configuration capabilities and dynamic path selection, vital for large-scale IoT devices with resource-constrained sensors. Yet, RPL's delay becomes significant in IoT's mobile environments. Conventional ACO and PSO also underperform due to i) increasing iteration counts as they seek optimal solutions in constrained problem areas and ii) premature convergence resulting in sub-optimal routing paths, leading to increased delay. In contrast, our proposed scheme excels in delay performance, being more progressive, less iterative, and encompassing a broader problem area, thereby reducing the effort needed for optimal solutions and achieving a superior delay score.

The third performance metric is energy consumption. The rationale behind selecting this metric hinges on two factors: i) our mathematical model prioritizes residual energy as a primary constraint, with manifold criterion modeling also considering residual energy apart from the trust attribute as a heuristic. This necessitates evaluating the model's impact on energy consumption, and ii) our scheme primarily focuses on sensors as essential IoT devices. Given their limited energy resources, it becomes crucial to ascertain the energy expended during secure data transmission in IoT. The objective is to balance trust-based security and energy efficiency, ensuring a prolonged network lifespan. Here, "energy" denotes the power expended on cumulative sensor operations, which encompasses data transmission and reception, data processing, and internal circuit functions. We rely on the first-order radio energy model [53] to assess this, which provides a comprehensive formula for sensors' total energy consumption.

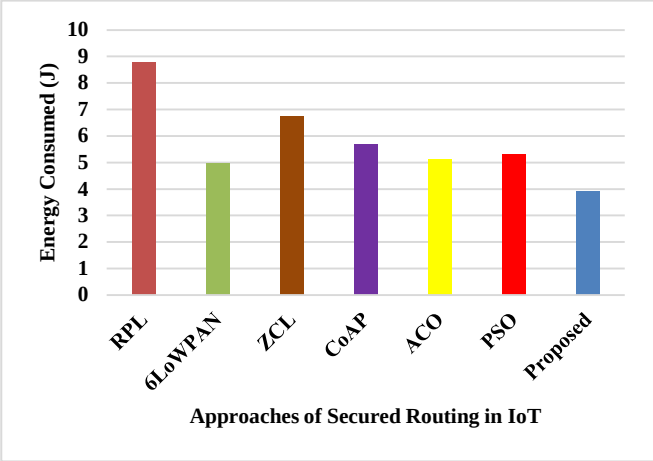

Fig. 5. Comparative analysis of energy consumption.

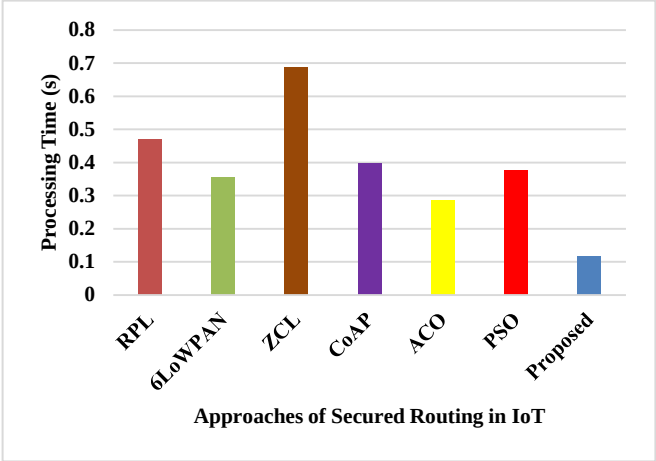

Fig. 6. Comparative analysis of algorithm processing time.

The data presented in Fig. 5 reveals that our proposed scheme significantly reduces power consumption compared to most existing systems. What stands out is that both conventional ACO and PSO demonstrate slightly higher energy consumption. The main reasons for this are: i) the increased use of attributes to achieve higher convergence performance and ii) a stronger focus on the local search optimization problem, often at the expense of global search space. The distinction between the proposed ACO and the conventional ACO lies in the former's formulation of pheromone management based on multiple criteria intertwined with an adaptive operational principle. A detailed examination of our ACO scheme further shows that their functionalities are mostly preserved despite the utilization of numerous parameters. The only variation arises from their use cases to enhance trust and energy retention. Due to the calculated global update formulation, local operatives' reliance on extensive operations diminishes as simulation time increases, leading to energy conservation. IoT secure routing schemes, such as RPL, ZCL, CoAP, and 6LoWPAN, incorporate encryption in their security variants. This inclusion demands a significant energy allocation for the ciphering and deciphering processes, which our proposed secure routing scheme avoids.

The final performance metric assessed for the proposed scheme is the processing time, an essential measure that reflects the time complexity inherent in algorithmic processing during secure routing. This metric is determined by evaluating a sensor's time to complete its operations. An efficient system model, especially one with lightweight characteristics, should display reduced processing times. If the processing time is extensive, the security scheme in use might benefit from some refinement to boost its overall efficiency. It is also crucial to note that, given sensors' limited computational capabilities, their processing time can increase when more complex operations are introduced. As a result, gauging the system's efficacy in terms of computational complexity by assessing its processing time becomes vital.

Fig. 6 illustrates that the proposed scheme significantly reduces processing time compared to other secured routing schemes. The processing time for ZCL is notably higher, as this scheme necessitates performing extensive iterative operations for massive data transmission in IoT. On closer examination, 6LoWPAN, CoAP, and conventional PSO performance reveal similar processing times. This similarity arises because these approaches segment and chunk data into smaller portions, leading to packet loss in a heterogeneous IoT network that necessitates retransmission. Additionally, the conventional PSO requires iterative computation of particles and velocities to identify optimal results. While this is effective for homogeneous systems, it is less so for heterogeneous ones, causing them to amalgamate all data packets and conduct routing. Such operations demand significant processing time and deliver sub-optimal data quality.

Furthermore, RPL displays a longer processing time, slightly more than CoAP. This is attributed to RPL's formation of a directed acyclic graph, eventually resulting in a singular link from the leaf node to the route. While this might be suitable for smaller IoT networks, the RPL graph operation must be repeated to achieve data transmission within the context of more extensive IoT networks. This repetition expends excessive resources and consumes considerable processing time for data transmission. Therefore, the proposed scheme promises minimal processing time, primarily due to diminished resource dependencies and fewer iterative operations, as emphasized in the proposed mathematical modeling.

VI. Conclusion

The landscape of the IoT is both exciting and challenging, marked by tremendous opportunities and, in parallel, considerable security vulnerabilities. In the modern age, when digital interconnectedness is both a boon and a bane, the urgency to fortify IoT against burgeoning threats cannot be overstated. The paper has addressed this urgency, providing a novel and streamlined approach that leverages a modified version of ACO toward achieving optimal security in the vast and dynamic IoT ecosystem. This bioinspired approach symbolizes our attempt to mimic nature's intuitive problem-solving methodologies. Through our process, not only is data

transmission secured, but the dual challenges of optimizing sensor energy and ensuring high trust scores are simultaneously addressed. A particular innovation in our work is the unique pheromone management system, which holistically considers residual energy and trust scores. Coupled with our manifold criterion and the dual-tiered trust evaluation system, the methodology provides an unparalleled framework for IoT security. Our research has showcased its merits, delivering impressive performance metrics compared to prevailing secure routing protocols. With a 35% improvement in throughput, 89% reduction in delay, 54% decrease in energy consumption, and 73% surge in processing speed, the approach is theoretically sound and practically efficacious. The current work, however, has its limitations. While it has achieved a balance between energy conservation and security, nuances to this balance need exploration. The inherently dynamic nature of IoT means that newer devices with diverse capacities are continually entering the ecosystem, presenting evolving challenges for security protocols. The future work of this study model will be to formulate a hybrid modeling of a bioinspired approach to optimize the security and resource management performance in a large IoT environment. Furthermore, integrating Artificial Intelligence and Machine Learning algorithms could further enhance our initial results. These can help the system to adaptively learn from emerging threats and respond proactively, ensuring a more agile and dynamic security mechanism.

ACKNOWLEDGMENT

The authors express their appreciation for the effort of Ms. Gousia Nissar in proofreading and editing the paper.

REFERENCES

[1] R. F. Olanrewaju *et al.*, "The internet of things vision: A comprehensive review of architecture, enabling technologies, adoption challenges, research open issues and contemporary applications," *Journal of Advanced Research in Applied Sciences and Engineering Technology*, vol. 26, no. 1, pp. 51–77, 2022. doi:10.37934/araset.26.1.5177

[2] R. K. Gangawar, S. Kumari, A. K. Pathak, S. D. Gutlapalli, and M. C. Meena, "Optical fiber based temperature sensors: A Review," *Optics*, vol. 4, no. 1, pp. 171–197, 2023. doi:10.20944/preprints202302.0180.v1

[3] S. K. Ghosh *et al.*, "Temperaturepressure hybrid sensing all-organic stretchable energy harvester," *ACS Applied Electronic Materials*, vol. 3, no. 1, pp. 248–259, 2020. doi:10.1021/acsaelm.0c00816.s002

[4] N. V. Krishna Prasad *et al.*, "Ceramic sensors: A mini-review of their applications," *Frontiers in Materials*, vol. 7, p. 593342, 2020. doi:10.3389/fmats.2020.593342

[5] A. M. Rahmani, S. Bayramov, and B. Kiani Kalejahi, "Internet of things applications: Opportunities and threats," *Wireless Personal Communications*, vol. 122, no. 1, pp. 451–476, 2021. doi:10.1007/s11277-021-08907-0

[6] S. A. Siddiqui, A. Ahmad, and N. Fatima, "IoT-based disease prediction using machine learning," *Computers and Electrical Engineering*, vol. 108, p. 108675, 2023. doi:10.1016/j.compeleceng.2023.108675

[7] H. S. Kim, Y. J. Park, and S. J. Kang, "Secured and deterministic closed-loop IoT system architecture for sensor and Actuator Networks," *Sensors*, vol. 22, no. 10, p. 3843, 2022. doi:10.3390/s22103843

[8] J. Yun, I. Y. Ahn, J. Song, and J. Kim, "Implementation of sensing and actuation capabilities for IoT devices using onem2M platforms," *Sensors*, vol. 19, no. 20, p. 4567, 2019. doi:10.3390/s19204567

[9] G. M. Kapitsaki, A. P. Achilleos, P. Aziz, and A. C. Paphitou, "SensoMan: Social Management of context sensors and actuators for IoT," *Journal of Sensor and Actuator Networks*, vol. 10, no. 4, p. 68, 2021. doi:10.3390/jsan10040068

[10] C. Stolojescu-Crisan, C. Crisan, and B.-P. Butunoi, "An IoT-based Smart Home Automation System," *Sensors*, vol. 21, no. 11, p. 3784, 2021. doi:10.3390/s21113784

[11] 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*, vol. 20, no. 22, p. 6420, 2020. doi:10.3390/s20226420

[12] B. U. I. Khan, R. F. Olanrewaju, F. Anwar, R. N. Mir, A. Oussama, and A. Z. B. Jusoh, "Internet of Things—The Concept, Inherent Security Challenges and Recommended Solutions," in *Smart Network Inspired Paradigm and Approaches in IoT Applications*, Springer, Singapore, 2019, pp. 63-86. doi: 10.1007/978-981-13-8614-5_5

[13] B. U. I. Khan, R. F. Olanrewaju, F. Anwar, R. N. Mir, and A. R. Najeeb, "A critical insight into the effectiveness of research methods evolved to secure IoT ecosystem," *International Journal of Information and Computer Security*, vol. 11, no. 4/5, pp. 332–354, 2019. doi:10.1504/ijics.2019.101908

[14] P. Ferrara, A. K. Mandal, A. Cortesi, and F. Spoto, "Static analysis for discovering IoT vulnerabilities," *International Journal on Software Tools for Technology Transfer*, vol. 23, no. 1, pp. 71–88, 2020. doi:10.1007/s10009-020-00592-x

[15] A. H. Celdrán *et al.*, "Intelligent and behavioral-based detection of malware in IoT spectrum sensors," *International Journal of Information Security*, vol. 22, no. 3, pp. 541–561, 2022. doi:10.1007/s10207-022-00602-w

[16] A. Attkan and V. Ranga, "Cyber-physical security for IoT Networks: A comprehensive review on traditional, blockchain and artificial intelligence based key-security," *Complex & Intelligent Systems*, vol. 8, no. 4, pp. 3559–3591, 2022. doi:10.1007/s40747-022-00667-z

[17] U. Kumar, S. Navaneet, N. Kumar, and S. C. Pandey, "Isolation of DDoS attack in IoT: A new perspective," *Wireless Personal Communications*, vol. 114, no. 3, pp. 2493–2510, 2020. doi:10.1007/s11277-020-07486-w

[18] T. B. Josey and D. S. Misbha, Man-in-the-Middle attack mitigation in IoT sensors with hash-based multidimensional Lamport digital signature," in *Lecture Notes in Electrical Engineering*, Springer Nature Singapore, 2023, pp. 47–56

[19] B. U. I. Khan, F. Anwar, R. F. Olanrewaju, B. R. Pampori, and R. N. Mir, "A novel multi-agent and multilayered game formulation for intrusion detection in internet of things (IoT)," *IEEE Access*, vol. 8, pp. 98481–98490, 2020. doi:10.1109/access.2020.2997711

[20] R. Sharma and R. Arya, "Secure transmission technique for data in IoT Edge Computing Infrastructure," *Complex & Intelligent Systems*, vol. 8, no. 5, pp. 3817–3832, 2021. doi:10.1007/s40747-021-00576-7

[21] U. Panahi and C. Bayılmış, "Enabling secure data transmission for wireless sensor networks based IoT Applications," *Ain Shams Engineering Journal*, vol. 14, no. 2, p. 101866, 2023. doi:10.1016/j.asej.2022.101866

[22] E. Refaee *et al.*, "Secure and scalable healthcare data transmission in IoT based on optimized routing protocols for mobile computing applications," *Wireless Communications and Mobile Computing*, vol. 2022, pp. 1–12, 2022. doi:10.1155/2022/5665408

[23] B. U. I. Khan *et al.*, "SGM: Strategic game model for resisting node misbehaviour in IoT-Cloud Ecosystem," *Information*, vol. 13, no. 11, p. 544, 2022. doi:10.3390/info13110544

[24] V. K. Quy, V. H. Nam, D. M. Linh, and L. A. Ngoc, "Routing algorithms for Manet-IoT Networks: A comprehensive survey," *Wireless Personal Communications*, vol. 125, no. 4, pp. 3501–3525, 2022. doi:10.1007/s11277-022-09722-x

[25] M. Majid *et al.*, "Applications of wireless sensor networks and internet of things frameworks in the industry revolution 4.0: A systematic literature review," *Sensors*, vol. 22, no. 6, p. 2087, 2022. doi:10.3390/s22062087

[26] B. Aslan, F. Yavuzer Aslan, and M. T. Sakallı, "Energy consumption analysis of lightweight cryptographic algorithms that can be used in the security of internet of things applications," *Security and Communication Networks*, vol. 2020, pp. 1–15, 2020. doi:10.1155/2020/8837671

[27] M. Aaqib, A. Ali, L. Chen, and O. Nibouche, "IoT trust and reputation: A survey and taxonomy," *Journal of Cloud Computing*, vol. 12, no. 1, pp. 1–20, 2023. doi:10.1186/s13677-023-00416-8

[28] Y. Liu, J. Wang, Z. Yan, Z. Wan, and R. Jäntti, "A survey on Blockchain based trust management for internet of things," *IEEE Internet of Things Journal*, vol. 10, no. 7, pp. 5898–5922, 2023. doi:10.1109/jiot.2023.3237893

[29] 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 Networks*, vol. 136, p. 102956, 2022. doi:10.1016/j.adhoc.2022.102956

[30] S. Mangalampalli, G. R. Karri, and U. Kose, "Multi Objective Trust aware task scheduling algorithm in cloud computing using whale optimization," *Journal of King Saud University - Computer and Information Sciences*, vol. 35, no. 2, pp. 791–809, 2023. doi:10.1016/j.jksuci.2023.01.016

[31] S. M. Muzammal, R. K. Murugesan, N. Jhanjhi, M. S. Hossain, and A. Yassine, "Trust and mobility-based protocol for secure routing in internet of things," *Sensors*, vol. 22, no. 16, p. 6215, 2022. doi:10.3390/s22166215

[32] S. M. Muzammal *et al.*, "A trust-based model for secure routing against RPL attacks in internet of things," *Sensors*, vol. 22, no. 18, p. 7052, 2022. doi:10.3390/s22187052

[33] S. Awan *et al.*, "Blockchain based Secure Routing and Trust Management in Wireless Sensor Networks," *Sensors*, vol. 22, no. 2, p. 411, 2022. doi:10.3390/s22020411

[34] R. Nagaraju *et al.*, "Secure routing-based energy optimization for IoT application with heterogeneous wireless sensor networks," *Energies*, vol. 15, no. 13, p. 4777, 2022. doi:10.3390/en15134777

[35] N. B. Bakhtiari, M. Rafighi, and R. Ahsan, "TTLA: Two-way trust between clients and fog servers using Bayesian Learning Automata," *The Journal of Supercomputing*, vol. 79, pp. 16152–16180, 2022. doi:10.21203/rs.3.rs-1744138/v1

[36] B. Rakesh and P. S. H, "Novel authentication and Secure Trust based RPL routing in Mobile Sink supported internet of things," *Cyber-Physical Systems*, vol. 9, no. 1, pp. 43–76, 2021. doi:10.1080/23335777.2021.1933194

[37] A. Gladkov *et al.*, "DT-RRNS: Routing protocol design for secure and reliable distributed smart sensors communication systems," *Sensors*, vol. 23, no. 7, p. 3738, 2023. doi:10.3390/s23073738

[38] S. Ramaswamy and J. Norman, "Social and QoS based trust model for secure clustering for Wireless Body Area Network," *The International Journal of Electrical Engineering & Education*, 2020. doi:10.1177/0020720920953133

[39] X. Wang, "Low-energy secure routing protocol for WSNS based on multiobjective ant colony optimization algorithm," *Journal of Sensors*, vol. 2021, pp. 1–9, 2021. doi:10.1155/2021/7633054

[40] K. Saleem and I. Ahmad, "Ant colony optimization ACO based Autonomous Secure Routing Protocol for Mobile Surveillance Systems," *Drones*, vol. 6, no. 11, p. 351, 2022. doi:10.3390/drones6110351

[41] T.-H. Nguyen and J. J. Jung, "ACO-based traffic routing method with automated negotiation for connected vehicles," *Complex & Intelligent Systems*, vol. 9, no. 1, pp. 625–636, 2022. doi:10.1007/s40747-022-00833-3

[42] G. Anjinappa and D. Bangalore Prabhakar, "A secure IoT and Edge Computing based EV selection model in V2G systems using ant colony optimization algorithm," *International Journal of Pervasive Computing and Communications*, 2022. doi:10.1108/ijpcc-06-2022-0245

[43] A. El-Ghamry, T. Gaber, K. K. Mohammed, and A. E. Hassanien, "Optimized and efficient image-based IoT malware detection method," *Electronics*, vol. 12, no. 3, p. 708, 2023. doi:10.3390/electronics12030708

[44] H. A. Alterazi *et al.*, "Prevention of cyber security with the internet of things using particle swarm optimization," *Sensors*, vol. 22, no. 16, p. 6117, 2022. doi:10.3390/s22166117

[45] H. C. Lin, P. Wang, and W. H. Lin, "Implementation of a PSO-based security defense mechanism for tracing the sources of DDoS attacks," *Computers*, vol. 8, no. 4, p. 88, 2019. doi:10.3390/computers8040088

[46] R. R. K and M. Ramakrishnan, "Internet of trust things using particle-swarm optimisation (PSO-IoT)," *SSRN Electronic Journal*, 2021. doi:10.2139/ssrn.3769174

[47] K. Janani and S. Ramamoorthy, "Threat analysis model to control IoT network routing attacks through deep learning approach," *Connection Science*, vol. 34, no. 1, pp. 2714–2754, 2022. doi:10.1080/09540091.2022.2149698

[48] M. Hosseinzadeh *et al.*, "A cluster-tree-based secure routing protocol using Dragonfly Algorithm (DA) in the internet of things (IoT) for Smart Agriculture," *Mathematics*, vol. 11, no. 1, p. 80, 2022. doi:10.3390/math11010080

[49] P. Selvaraj *et al.*, "An enhanced and Secure Trust-aware improved GSO for encrypted data sharing in the internet of things," *Applied Sciences*, vol. 13, no. 2, p. 831, 2023. doi:10.3390/app13020831

[50] M. Tanveer *et al.*, "S6AE: Securing 6lowpan using authenticated encryption scheme," *Sensors*, vol. 20, no. 9, p. 2707, 2020. doi:10.3390/s20092707

[51] K. Nichols, V. Jacobson, and R. King, "Defined-Trust Transport (DEFTT) protocol for limited domains," IETF Datatracker, https://datatracker.ietf.org/doc/draft-nichols-tsv-defined-trust-transport/ (accessed Jul. 30, 2023).

[52] J. Granjal, J. Silva, and N. Lourenço, "Intrusion detection and prevention in CoAP wireless sensor networks using anomaly detection," *Sensors*, vol. 18, no. 8, p. 2445, 2018. doi:10.3390/s18082445

[53] F. Liu, "Majority decision aggregation with binarized data in wireless sensor networks," *Symmetry*, vol. 13, no. 9, p. 1671, 2021. doi:10.3390/sym13091671.