International Journal on Semantic Web and Information Systems
Volume 18 • Issue 1

Chaotic Whale Crow Optimization Algorithm for Secure Routing in the IoT Environment

Meghana Gopal Raj, KIIT University (deemed), Bhubaneswar, India*
Santosh Kumar Pani,KIIT University (deemed), Bhubaneswar, India

ABSTRACT

This paper solves the internet of things (IoT) security issues by introducing a chaotic whale crow (CWC) optimization, which is the integration of chaotic whale optimization algorithm (CWOA) in crow search algorithm (CSA). The framework operates on two crucial aspects: one is to select the secure nodes, and the other is to implement secure routing using the selected trusted nodes. First, the selection of trusted nodes is performed based on trust factors like direct, indirect, forwarding rate, integrity, and availability factors. Then, the selected trusted nodes are adapted for trust-based secure routing, which is optimally performed using the proposed CWC, based on the fitness parameters trust and energy. Finally, the proposed CWC is evaluated, which revealed high performance with a minimal delay of 191.46ms, which shows 14.87%, 7.35%, 6.82%, 4.19%, and 5.74% improved performance compared to existing LaSeR, PM Ipv6, secTrust-RPL RISA, and LSDAR techniques. Similarly, the proposed method obtained the maximal energy of 71.25J and maximal throughput of 129.77kbps.

KEYWORDS

Energy, Internet of Things (IoT), Secure Routing, Security, Trust Management

1. INTRODUCTION

The innovation of advanced services and the development of information on the internet have escorted to novel ideas, conceptions, and paradigms, like the Internet of Things (IoT). However, the conventional network infrastructures require high-level configuring protocols and network policies and are ineffective and pose noteworthy drawbacks for supporting high level scalability, huge traffic, and mobility (Liu, *et al.,* 2017). IoT is considered an advanced technology whose goal is to connect anything, anywhere, and anytime. The objects connected with the IoT must be addressable and hold a unique Identifier (ID) for connecting the internet. An IoT can be anything, which includes humans, light bulbs, computers, and cars. IoT offers a virtual image of the physical objects that are connected with the internet. IoT is progressed in various domains, like machine-machine technologies, networking,

DOI: 10.4018/IJSWIS.300824 *Corresponding Author

hardware, and software, contributing to the emergence of IoT (Kalkan & Zeadally, 2017). IoT is the extensive usage of systems that poses heterogeneous technologies and novel paradigms for connecting the devices with the help of Transmission Control Protocol/Internet Protocol (TCP/IP) (Bellovin, 1989) using the physical environments (Airehrour, *et al.,* 2016). IoT is applicable in water grids, management automation, building, industrial smart grid systems, smart cities, and agriculture. The sensors are deployed in the energy-constrained networks, and they achieve computational functions and storage by communicating through the lossy channels (Airehrour, *et al.,* 2019).

IoT has significantly implicated people's day-to-day lives with heterogeneous devices, like homogeneous devices that include most sensor networks and smart homes. IoT produced tremendous convenience in handling the energy-constrained sensors (Rathee, *et al.,* 2019). The dynamic forces of IoT in networking and routing provide effective device interconnections (Airehrour, *et al.,* 2019; Miorandi, *et al.,* 2012). The foremost contemplation in IoT routing is autonomy, scalability, energy efficiency, and secured communication. However, the exceptional features of IoT networks made them susceptible to attacks. As a result, secure data communication and routing are the two barriers in the IoT network. These barriers need to be resolved using the network topologies with different networks for general understanding. Consistency plays a vital role in routing a packet that arrives from the IoT-enabled device. Thus, the security of an IoT system is a major aspect that engages in detailed research due to the secure networks that are imperative in the IoT systems (Airehrour, *et al.,* 2019). In secure routing, the reputation computes the routing and forwarding rate based on the authentication and encryption mechanisms with the appropriate broadcast of acknowledgments per transmitted packet (Hatzivasilis, *et al.,* 2017). Trust is considered as the confidence level of an entity, which holds about others in routing. Moreover, trust is considered the collection of all reputation values, which the entity holds for other contributors (Hatzivasilis, *et al.,* 2017). The Semantic technologies integrate and the interoperability of sensor nodes and hence the organization, management, and controlling of high level specifications. The IoT is flexible and has good scalability of processing applications. However, the semantic solution requires more mechanisms. Besides, in the romantic review, the searching of the title doesn't provide all related publications. Real time data streaming is not available in the IoT (Harlamova,*et al*., 2017).

Numerous trust-based systems are adapted for attaining secure routing (Liu, *et al.,* 2017). Trust-based methodologies are utilized in wireless networking to provide secure routing functionality. The reputation is devised from the past behavior of nodes and discloses the cooperativeness. The node with the highest reputation values is termed a trustworthy node. The genuine nodes are based on trustworthy entities, which helps to complete the communication tasks. Moreover, the lesser reputation can reveal the malicious entities and is utilized for detecting the intrusions. The legitimate node tries to evade notorious entities and does not serve the traffic (Hatzivasilis, *et al.,* 2017). Secured Trust-aware Routing Protocol for Low-Power and Lossy Networks (SecTrust-RPL) in the IoT determines and detaches routing attacks by offering improved network performance (Airehrour, *et al.,* 2019). Secure routing protocols, like Expected Forwarded Counter (EFW) (Paris, *et al.,* 2013), Semi-Distributed Reputation-based Intrusion Detection System (S-D RepIDS) (Trivedi, *et al.,* 2010), Trusted based routing using Dominating Set Approach (TRDSA) (Kukreja & Reddy, 2012), Secure Resilient Reputation-based Routing (SR3) (Altisen, *et al.,* 2013), reputation-based Framework for Sensor Networks (RFSN) (Ganeriwal, *et al.,* 2008), and Ad Hoc On-Demand Distance Vector Reputation Extension (AODV) (Over MANET, 2012)are illustrated. Secure Resilient Reputation-based Routing (SR3), Expected Forwarded Counter (EFW), and Trusted based routing using Dominating Set Approach (TRDSA) use reputation methods for core deductive components (Hatzivasilis, *et al.,* 2017). In TRDSA, a group of trusted nodes with adequate enduring energy is needed for operating in the promiscuous mode and capture malevolent activity reducing overall energy consumption. The Semi-Distributed Reputation-based Intrusion Detection System for mobile ad-hoc networks (S-D RepIDS) for mobile ad-hoc networks executes several reputation measures for secure routing and is liberal to malfunction due to traffic congestion (Hatzivasilis, *et al.,* 2017). The usage of a secure session key and lightweight

approach offers security in smart homes. Multilevel authentication is a solution for addressing privacy and security issues in automation systems of smart homes. Distributed security solutions improve the security of channels in smart homes by operating the system using IoT devices (Shin, *et al.,* 2017).

1.1 Need for Secure Routing in IoT

The IoT is widely used in several applications like industry, education, commerce, and military-related applications and can be controlled anywhere and anytime. However, the challenges faced by the IoT are hacker intrusion, malicious attacks, and data damages in the networks. Hence, there is a need for secure communication in IoT for the authentication and the security of information sharing. Thus, this paper introduces a trust-aware routing framework in IoT by proposing a hybrid optimization algorithm named CWC algorithm. A Trust-based model is developed such that the IoT nodes, which participate in the routing, ensure security. Initially, the secure node selection process is carried out in which the node is selected for initiating secured group communication in IoT based on the trust factors. Thereafter, trust-based routing is performed using the proposed hybrid Optimization algorithm named CWC, which integrates CWOA in CSA, imputing the merits of both approaches. The solution encoding shows that it supports trust-aware routing from the current node to the destination to forward the data and maintain trust among the nodes. The optimal solution selection is based on the newly-defined fitness function, which considers trust and energy as parameters. The global optimal convergence and less-intensive computations, and higher search speed of the proposed algorithm enable the effective performance and selection of feasible and secure routes.

The major contributions of the paper are:

- ***Proposed CWC algorithm for trust-aware routing***- Design a novel hybrid optimization algorithm named CWC by integrating the update position of CWOA and CSA to acquire global optimal solutions for trust-based routing. By using this, the fast convergence rate is obtained with premature convergence. Thus, the more efficient, secure optimal path is identified for the routing.
- ***Fitness function for optimal routing-*** A newly devised fitness function is utilized for initiating a trust-aware routing between the trusted nodes. The fitness function utilizes trust factors and energy as its parameter for assisting secure routing in IoT networks.

The rest of the paper is organized as: Literature review is deliberated in section 2, and the proposed model of trust aware routing is devised in section 3. Then, the results, comparative analysis, and effectiveness of the framework are deliberated in section 4, and finally, section 5 concludes the paper.

2. MOTIVATIONS

The section deliberates the literature survey of trust-based routing techniques along with the disadvantages of the methods. Here, the review of eight existing methods is done, which motivated the researcher to establish an effective trust-based routing method. At the end of the section, the challenges of the existing methods are deliberated.

2.1. Literature Survey

The eight existing methods based on trust-based routing in the IoT network are illustrated in this section. Mick, *et al.,* (2017) developed a secured routing framework named Lightweight Authentication and Secured Routing protocol (LASeR) for providing trusted routing in IoT systems. The scalability was attained by a hierarchical network design along with cryptographic designs. As a result, the method faced fewer network overhead and attained satisfactory onboard convergence times. However, the method was unable to implement real IoT devices in a testbed deployment.

Hatzivasilis, *et al.,* (2017) developed a trust-based system named Self-Channel Observation Trust and Reputation System (SCOTRES) for secure routing in ad-hoc networks. The energy parameter contained the resource consumption of each node by the same daunting amount of collaboration and maximizing the network lifetime. The method preserved the network against jamming attacks. Thus, it offered more security in the IoT devices, but the performance of the channel conditions degraded the overall system performance.

Sun, *et al.,* (2019) developed a Lightweight Anonymous Geometric Routing (LAGER) to preserve node-related private data. The LAGER employed a coordinate confusion mechanism for providing anonymous coordinates of virtual nodes so that the private data was decoupled from the coordinate of nodes. In addition, LAGER employed a hybrid routing method by integrating a source and greedy routing to support the data transmission with unnamed coordinates. The method was effective in dealing with scalability issues. However, the length of the path computed by the LAGER was adversely affected by the hybrid routing.

Shin, *et al.,* (2017) developed a secure protocol that utilized the trust between the PMIPv6 domain and smart home to facilitate security and performance concerning the paths between mobile nodes and home IoT devices. The proposed protocol contained specific steps for securing Route optimization (RO) and handover management, where mutual authentication, perfect forward secrecy, key exchange, and privacy were supported. However, the method failed to consider distributed mobility management with 5G, using different traffic and mobility methods.

Airehrour, *et al.,* (2019) developed a time-based trust-aware RPL routing protocol named SecTrust-RPL for securing the IoT networks from routing attacks. The SecTrust was designed by embedding the RPL routing protocol for protecting Sybil and rank attacks. The method utilized a trusted method for determining and isolating the attacks while optimizing the performance of networking. The method used an effective security system for mitigating the attacks in the IoT networks. However, the method failed to address other attacks, like Blackhole, Sybil, or Selective Forwarding attacks.

Das, *et al.,* (2019) developed a lightweight access control and key agreement protocol (LACKA) in the IoT environment, which used collision-resistant one-way cryptographic hash function and Elliptic Curve Cryptography (ECC) for the route selection. The method preserved different attacks and was needed for a secure device access control mechanism in the IoT. The method provided an effective trade-off between the functionality and security features, but the network parameters were not effectively measured.

Liu, *et al.,* (2017) designed a Software-defined Network (SDN)-based data transfer security model using a Middlebox-Guard (M-G) for trust-based routing. The method effectively managed the network latency and data flow for ensuring safer network processing. An offline Integer Linear Program (ILP) pruning algorithm was devised for tackling the switching constraints. Moreover, an online Linear Program (LP) formulation was used to balance the IoT networks' loads. At last, secure methods were devised for handling different types of attacks. The method was helpful for determining the feasible solutions using the switching tunnels.

Bu, *et al.,* (2019) developed a secure and robust scheme for facilitating the shared information in the IoT networks. This method provided two crucial characteristics for facilitating the routing in the network. This method used Threshold Secret Sharing (TSS) for splitting the information into shares considering all the devices present in the system. This method facilitated the integrity and privacy of the information using many collusive attackers, who can seize the devices. The method was able to recognize the compromised devices by keeping the secret anonymous and impressive to attackers. However, this method was ineffective in identifying the compromised nodes.

Aakanksha Tewari and B.B. Gupta (2018) developed security, trust, and privacy layers in the IoT framework. In this, each layer analyzed the security issues, and the solution for the security issues was identified. The trust factors need to employ for the trustworthiness in IoT. However, they failed to analyze the security and privacy requirement in the heterogeneous environment.

Christos *et al.,* (2021) developed IoT-based secure data management. In this, an innovative framework was developed for managing the big data in the buildings, which is obtained through the cache decision system (CDS). However, they failed to analyze the extremely scale analytics system (ESAS).

Aakanksha Tewari and B. B. Gupta (2016) developed the IoT-based authentication protocol. In this, ultra weight mutual authentication was developed for the efficient communication cost and the storage based on the bitwise operation. However, they failed to analyze them in depth cryptanalysis.

Daming Li *et al.,* (2019) developed the secure image watermarking generating approach. In this, the synergic neural network was developed for secure digital watermarking. As a result, they obtained high precision and high-speed recognition. However, they failed to evaluate the performance using other databases.

Christian *et al.,* (2021) developed the authentication and the authorized protocol for blockchain-based applications. Here, the distributed approach for the authentication in smart cites. However, they failed to check the correctness of the stored policies.

2.2. Challenges

The challenges faced by the existing methods are enlisted below. These challenges are taken into consideration for designing an effective trust-based strategy in the IoT network.

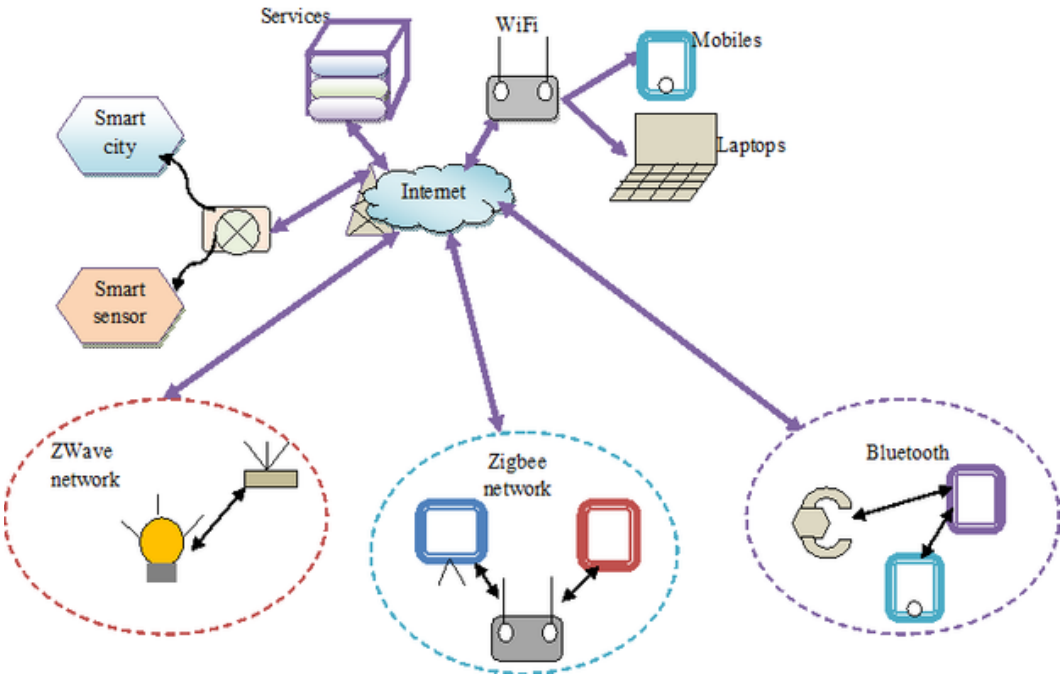
- In (Das, *et al.,* 2019), the key agreement protocol and lightweight access control are devised in the IoT environment. This protocol efficiently executes the formal and informal security verification, but the cost of communication and computation is very high.
- Best-Fit Traversing (BFT) algorithm was designed for enhancing the accessibility of the device in a specific manner. The method enhanced the application's performance by reducing the redundancy, transmission delay with high communication rates. However, the performance analysis of IoT networks with range-adaptive aggregators was ineffective while dealing with message gathering and distribution (AlZubi, *et al.,* 2019).
- In (Hatzivasilis, *et al.,* 2017), a trust-based system is devised for secure routing to advance network entities' intellect. The channel-health metric offers tolerance in periodic malfunctioning that bad channel conditions and preserves the network against jamming attacks. Moreover, the system offers high protection but degrades the performance of the system.
- In (Shin, *et al.,* 2017), Secure and Efficient Protocol was developed, which utilizes trust amongst the Proxy Mobile IPv6 (PMIPv6) domain and smart home to ensure security and performance between the mobile nodes and IoT devices. It was able to provide secure transmissions by addressing the Route Optimization (RO) issues in the PMIPv6 and reducing latency. However, the method failed to evaluate the performance with different mobility models.
- The Data transfer security model was devised in (Liu, *et al.,* 2017) to reduce network latency. The network routing is addressed by flexibility using dataflow management protocol, formulated using the combined tags and tools. However, the method failed to manage the stability of the network.
- IoT exhibits new factors of security challenges in the network topology, and the non-uniformity of the IoT networks makes them vulnerable to suspicious attacks in the networks. In addition, the susceptibility of resource-constrained properties, mobility, and communication channels makes IoT security challenges. To provide secure data transmission, trust mechanisms are employed in IoT systems.

The challenges faced by the existing techniques are high computation and communication cost, higher transmission delay, degrading the system, reduced latency, and lower stability.

3. SYSTEM MODEL OF IOT NETWORK

IoT consists of different objects, like smart devices, which are connected to exchange the accumulated data through the network. Many smart devices in the IoT are resource-constrained, which poses processing and communication capabilities for exchanging data. Figure 1 portrays the system model of the IoT network, wherein several smart devices and actuators are installed for processing. In the IoT network, the smart devices are connected to the internet using the gateway node. The users can acquire real-time information from the IoT devices through the gateway for which the user needs to be authorized to the IoT network. IoT is speckled between different low-power networking protocols, like Bluetooth, ZigBee, and ZWave. These protocols are developed for domain-specific applications with unique characteristics. Therefore, numerous devices should be designed for supporting different networking protocols by accumulating the hardware components. The device offers direct network connectivity through access networks like ZigBee and Bluetooth. However, the smart objects are energy and resource-constrained, and thus, the gateway should be responsive for the management. Hence, the IoT must adapt caching techniques and intellectual routing protocols for routing the data across constrained paths. In mobility cases, such as routing networks are significantly important so that the architecture can deal with ad hoc network information and the movement of data from one node to another. The issues like the transmission delay, higher computation complexity and the stability of the method is enhanced using the proposed CWC algorithm because, the proposed method has the capability of fast convergence with the avoidance of local minima. Besides, the trust management using the trust factors provides more secure communication. Thus, routing and data transmission are crucial on the internet, which motivates the network for efficient data delivery that uses processing functions and network caches.

Figure 1. System model of IoT network



3.1. Energy Model of IoT Network

This section deliberates IoT's energy model (Chen, *et al*., 2015) while transmitting data from one node to another node. IoT possesses a number of distributed sensors operating with the batteries. With the increase in the number of rounds, the energy drains affect the network lifetime. Let us assume that the initial energy of the nodes is, ε_0 specifying that the batteries are non-rechargeable. When the data receives the transmitter, some energy is lost depending on the distance of communication. The transmission in the network relies on the protocol, and the dissipation in the energy is due to the presence of the power amplifier and radio electronics available in the transmitter. Thus, it is clear that the energy dissipates at the time of data transmission concerning the distance and nature of the node. Whenever the normal sensor node transmits y bits of data packet then, the model for energy consumption is based on the following formula as,

$$\varepsilon_t(y) = \varepsilon_e(y) + \varepsilon_a(y,m) \tag{1}$$

where, $\varepsilon_t(y)$ represents the transmitted energy, ε_a denote the consumed energy when node sends 1 bit data, ε_e specifies consumed energy when node receives and sends 1 bit data, m indicates communication distance, y is the data bits.

$$\varepsilon_t(y) = \begin{cases} y \times \varepsilon_e + y \times \varepsilon_j \times m^2; \; if \;\; m \le m_0 \\ y \times \varepsilon_e + y \times \varepsilon_i \times m^4; \; if \;\; m > m_0 \end{cases} \tag{2}$$

where, ε_i is the consumed energy when the node transmits "1" bit data in the free space model, ε_j refers to the consumed energy when the node transmits "1" bit data in the multipath fading model.

$$m_0 = \sqrt{\frac{\varepsilon_j}{\varepsilon_i}} \tag{3}$$

The energy consumed by the sensor nodes for receiving y bit of data is given as,

$$\varepsilon_r(y) = y \times \varepsilon_e \tag{4}$$

where, $\varepsilon_r(y)$ is the received energy.

4. PROPOSED CWC ALGORITHM FOR TRUST-BASED ROUTING IN IOT NETWORK

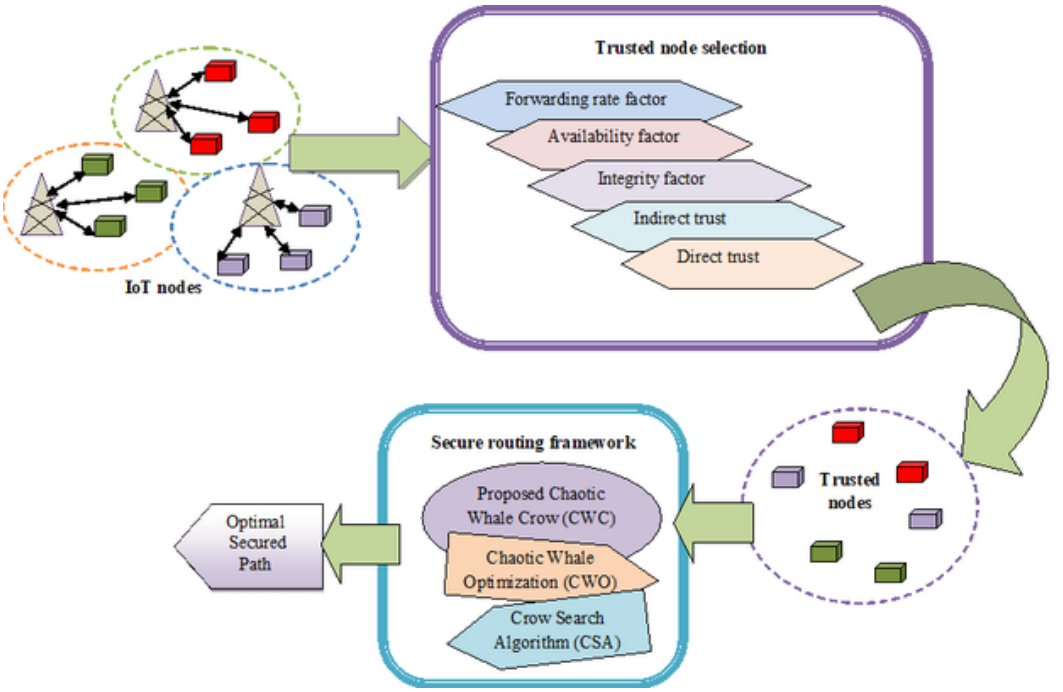
The routing protocols are employed in determining the optimal path for undergoing routing in IoT, and there exist several protocols for routing. However, the trust and energy factors are the significant constraints that should be considered for enabling secure routing in IoT. Moreover, the computational complexities of the conventional methods remained high. Hence, a trust-aware method is developed to relieve the computational overhead and the ability to deal with complex attacks. Thus, to enable security in the network, the trust-aware routing algorithm, namely CWC, is developed, which is the combination of CWOA (Kaur &Arora, 2018) and CSA (Askarzadeh, 2016). The developed method

acquires the trustworthy and adaptive routing framework structure, which tackles the attacks and provides a greater degree of defense from the attacks. The proposed algorithm generates greediness in packets, and in addition, the utilization of network resources, such as node memory and reliability of end-to-end transmission, are optimized. The network is simulated with numerous sensor nodes, and the trusted nodes are selected for further routing processes. The selection of the trusted nodes is modeled based on the trust parameters, like direct trust, indirect trust, integrity factor, and availability factors. The secure nodes are taken to the next step for initiating trust-based routing. The routing is performed optimally using the proposed CWC algorithm. Secure routing is a significant task, which is based on trust factors. Thus, the optimal way of trust-based routing is progressed in the IoT environment. There are N number of nodes in the sensor environment initially, and the secure nodes are chosen based on the trust factors. Figure 2 depicts the schematic view of the trust-aware routing framework in the IoT environment. The major concern of IoT is the energy crisis that is due to the presence of the battery-operated sensor nodes as the energy of the nodes drains with the increase in the number of rounds. Let us establish the IoT with N the number of sensor nodes, number of trusted nodes, and a base station (BS) so that the route is established using the trusted nodes. During data communication between trusted nodes and BS, the communication occurs through the optimal routes, chosen based on the fitness function modeled depending on the energy and trust.

4.1. Selection of Trusted Nodes using Trust Factors for Secure Routing

This section explains the trust model that offers security in the proposed algorithm during routing. Trust refers to the fact that the unit believed to be trustful will not go wrong. The nodes in the network communicate with each other using a mutual relationship based on trust. Each node in IoT has a trust degree that estimates the trust level of the node and its neighbors. It provides scalability, as the value is evaluated based on local network topology information. The trust factor of each node is computed for evaluating the set of trusted nodes. Thus, the trust factor employed for determining

Figure 2. Schematic view of proposed CWC algorithm for Trust-based secure routing



the trusted nodes is formulated based on four factors, namely direct trust, indirect trust, availability factor, forwarding rate factor, and integrity factor, and is given as,

$$T_{k,l}^{f} = D_{h}^{g}(k,l) + I_{h}^{g}(k,l) + F_{h}(k,l) + J_{h}(k,l) + A_{h}(k,l) \tag{5}$$

where, $D_{h}^{g}(k,l)$ represents the direct trust of node k on node l , $I_{h}^{g}(k,l)$ represents the indirect trust of node k on node l , k is the evaluation node and l is the node to be evaluated, $F_{h}(k,l)$ specifies the forwarding rate factor, $J_{h}(k,l)$ refers the integrity factor, $A_{h}(k,l)$ indicate acknowledgment factor, the time interval is given by h , and the transaction is given as h.

4.1.1. Direct Trust

The direct trust (Das & Islam, 2011) is otherwise referred to as the local trust, which depends on the satisfaction between node interactions. The direct trust between the nodes k and l is based on the degree of satisfaction between the nodes. Whenever the node k feels satisfied concerning the node l then, the degree of satisfaction is high, rendering a local trust. The direct trust is based on the degree of satisfaction between the nodes k and l and is given as,

$$D_{h}^{g}(k,l) = Sat_{h}^{g}(k,l) \tag{6}$$

where, $Sat_{h}^{g}(k,l)$ is the degree of satisfaction that the node k has upon node l. The satisfaction function computes the degree of satisfaction that a node has upon other nodes to provide secure transmission. The satisfaction function is formulated as,

$$Sat_{h}^{g}(k,l) = \beta \times Sat_{C} + (1-\beta) \times Sat_{h-1}^{g}(k,l) \tag{7}$$

where, Sat_{C} indicates the satisfaction value of the most recent transaction, β refers to the weight. The satisfaction value of the most recent transaction is further formulated as,

$$Sat_{C} = \begin{cases} 0; If\ transaction\ is\ unsatisfactory \\ 1; If\ transaction\ is\ satisfactory \\ 0,1; Otherwise \end{cases} \tag{8}$$

The weight β is varied based on the accumulated deviation $\gamma_{h}^{g}(k,l)$,

$$\beta = R + q \times \frac{\alpha_{h}^{g}(k,l)}{1 + \gamma_{h}^{g}(k,l)} \tag{9}$$

where, q is the constant, $\gamma_{h}^{g}(k,l)$, represents the accumulated deviation, and $\alpha_{h}^{g}(k,l)$ specifies the recent error.

$$\alpha_{h}^{g}(k,l) = \mid Sat_{h-1}^{g}(k,l) - Sat_{C} \mid \tag{10}$$

$$\gamma_h^g(k,l) = q \times \alpha_h^g(k,l) + (1-q) \times \gamma_{h-1}^g(k,l) \tag{11}$$

4.1.2. Indirect Trust

The indirect trust (Das & Islam, 2011) is acquired based on the recommendation. It is evaluated from the experience of other agents in the system for making effective decisions with the target nodes. Firstly, the node requests other nodes to offer recommendations about the target node. The evaluated node collects the recommendations from other nodes along with the feedback credibility of the recommenders. The indirect trust acquired by the node k upon node l is given as,

$$I_h^g(k,l) = \begin{cases} \dfrac{\sum_{d \in S-\{k\}} C_h^g(k,d) \times D_h^g(d,l)}{\sum_{d \in S-\{k\}} C_h^g(k,d)}; if \mid S-\{k\} > 0 \mid \\ 0; if \mid S-\{k\} = 0 \mid \end{cases} \tag{12}$$

where, S indicates the set of agents interacted with l , D_h^g represents the direct trust and C represents the feedback credibility.

Feedback credibility is employed for computing the preciseness of the feedback information provided by the recommenders to the evaluator. It is considered that the good agents offer true feedbacks and suspicious nodes provide false feedbacks. However, it is not true all-time as good nodes may provide false feedback for competitors. Thus, feedback credibility is essential for determining the trusted nodes and is formulated as,

$$C_h^g(k,l) = \begin{cases} 1 - \dfrac{\ln(Sim_h^g(k,l))}{\ln \theta}; If\ Sim_h^g(k,l) > 0 \\ 0;\ else \end{cases} \tag{13}$$

where, $Sim_h^g(k,l)$ is the similarity measure to describe the extent to which the two nodes are similar. Here, the similarity is evaluated by finding the personalized difference in satisfaction for describing the degree of similarity. For evaluating the similarity between node k on node l , the node k computes the difference $B_h^g(k,l)$ with the deviation constant κ and is formulated as,

$$Sim_h^g(k,l) = \begin{cases} Sim_{h-1}^g(k,l) + \dfrac{1 - Sim_{h-1}^g(k,l)}{\eta}; If\ B_h^g(k,l) < \kappa \\ Sim_{h-1}^g(k,l) - \dfrac{Sim_{h-1}^g(k,l)}{\rho}; else \end{cases} \tag{14}$$

The difference $B_h^g(k,l)$ with the deviation constant κ is given as,

$$\mathrm{B}_{\mathrm{h}}^{\mathrm{g}}(k,l) = \sqrt{\frac{\sum_{d \in G(k,l)} (Sat_h^g((k,d) - Sat_h^g(l,d))}{\mid G(k,l) \mid}} \tag{15}$$

where, $G(k,l)$ refers to the set of nodes in which both k and l has made interactions.

4.1.3 Forwarding Rate Factor

The nodes in the IoT networks pose less energy, which needs to be dissipated while sending and receiving data. Thus, it is essential to evaluate and judge if the node is attacked or not by evaluating the data forwarding of the nodes. The forwarding rate factor (Zhu, 2018) from node k to node l is given as,

$$F_h(k,l) = \frac{H_h(k,l)}{K_h(k,l)} \tag{16}$$

where, $H_h(k,l)$ represents the number of feedback packets and $K_h(k,l)$ indicates the number of packets to be forwarded.

4.1.4. Integrity Factor

Whenever the data packet is sent to the other node, the source nodes inspect if the data packet is corrupted or not and determines whether the data packet is forwarded within a specific time, and ensure integrity and data correctness. Thus, the integrity factor (Zhu, 2018) is given as,

$$J_h(k,l) = \frac{E_h(k,l)}{P_h(k,l)} \tag{17}$$

where, $E_h(k,l)$ indicate the number of forwarded packets, and $P_h(k,l)$ indicates the number of packets to forward.

4.1.5. Availability Factor

The node is not utilized for the transmission due to the interference of the network channel and harsh case, and so it is essential to compute the evaluated node by transmitting and inspecting data. The availability factor (Zhu, 2018) is given as,

$$A_h(k,l) = \frac{H_h(k,l)}{H_h(k,l) + H_h^{'}(k,l)} \tag{18}$$

where, $H_h^{'}(k,l)$ indicate the number of unresponded packets and $H_h(k,l)$ indicates the number of responded packets.

4.2. Proposed Trust-based Routing Based on the Optimization Algorithm

This section elaborates on the proposed CWC for attaining secure routing in the IoT environment. Initially, IoT nodes are simulated in a distributed environment, and as a point of assuring security, the trust of the nodes is being computed. The trust is computed for all the simulated IoT nodes to facilitate secure communication in the network. The trust, namely direct trust, indirect trust, forwarding rate factor, integrity factor, availability factor, and energy, is computed for all the simulated IoT nodes. Once the trust factor is computed, the secure routing framework is established using the secure IoT nodes. The secure routing framework is progressed using the proposed CWC optimization algorithm, which integrates the CWOA (Kaur &Arora, 2018) algorithm and the CSA (Askarzadeh, 2016). Thus,

the optimal way of routing is progressed in the IoT environment. The solution encoding, fitness function, and the proposed CWC algorithm are illustrated in the subsections.

4.2.1. Solution Encoding

The solution vector is the representation of the solution to be determined using the proposed CWC algorithm. The solution vector comprises the intermediate nodes taking part in the routing process. The number of intermediate nodes is denoted as, o where o varies between 1 to b , and b is the total number of the trusted nodes in the path. Assume S and D be the source and destination pair and the number of nodes required for reaching the destination from the source be given as o. Figure 3 represents the solution encoding,when $k = 3$, the routing between the source and the destination nodes takes place through three intermediate nodes and from figure 3, it is clear that the data transmission from the source node occurs through nodes, node-5, node-3, and node-6, respectively, to reach the destination. The selection of the optimal intermediate nodes is based on the M-CSO algorithm, executed using the fitness function. Figure 3 shows the solution vector between a source node and destination node, and this format is similar for all the other possible paths generated for routing.

4.2.2. Fitness Function

The fitness measure assures the routes to pursue the routing in IoT, and the fitness should be a maximal value. In other words, the fitness is based on solving the maximization problem, which is formulated based on the trust, connectivity, and energy factors, between the nodes. The fitness is computed as,

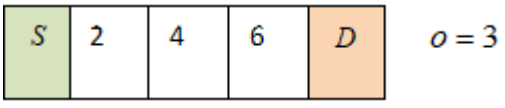
$$Fitness = \frac{1}{b}\sum_{\substack{k=1\\l=1}}^{b}\left[T_{k,l}^{f} + (\varepsilon_{t}^{k,l}(y) + \varepsilon_{r}^{k,l}(y))\right] \tag{19}$$

where, b is the number of trusted nodes in a path, $T_{k,l}^{f}$ is the trust factors considered for evaluating trusted nodes, $\varepsilon_{t}^{k,l}(y)$ indicates the transmitted energy, and $\varepsilon_{r}^{k,l}(y)$ is the received energy.

4.2.3. Proposed CWC Algorithm

CWC algorithm is developed by integrating CWOA in CSA, which balances both the algorithms' merits and demerits. The proposed CWC algorithm can acquire the global optimal solutions, and the computations associated with the algorithm are complex-free. The behavior of whales inspires the CWOA (Kaur & Arora, 2018) algorithm during hunting. The simplicity of the CWOA algorithm produces easy computations and helps to understand easily. CWOA controls the exploration and exploitation phases, which render global optimal solutions with higher convergence rates. On the other hand, CSA (Askarzadeh, 2016) algorithm is inspired by the intelligent behavior of crows, which leads to optimal solutions. In CSA, an awareness probability is utilized, which helps control the algorithm's diversity and is simpler to implement. Thus, the integration of CWOA and CSA helps to generate global optimal solutions in routing the data. The algorithmic procedure for routing data is given as,

Figure 3. Solution encoding based on proposed CWC algorithm



Step1: Initialization: The first step is the initialization of the whale population and other algorithmic parameters, like iteration counter n . The total whale population is z and is expressed as,

$$V = V_1, V_2, \ldots, V_x, \ldots, V_z \tag{20}$$

where, x is total number of whales, V_x is the x^{th} solution.

Step2: Evaluation of fitness function: The fitness of the solutions is computed using the fitness obtained in equation (19) under section 4.2.2.

Step3. Determination of update equation: To enhance the search space, the proposed algorithm utilizes the update rule of CWOA. As per CWOA (Kaur &Arora, 2018), the position update applied over the algorithm is represented as,

$$V_{n+1}^{p} = \begin{cases} \dfrac{V_n^p}{0.7} & ;V_n^p < 0.7 \\ \dfrac{10}{3}\left(1 - V_n^p\right) & ;S_u \geq Q_n^u \end{cases} \tag{21}$$

In order to obtain globally optimal solutions in secure routing, the CSA (Askarzadeh, 2016) is utilized in this algorithm. Thus, the updated position of crows based on the CSA algorithm is given as,

$$V_{n+1}^{p} = V_n^p + S_p \times M_n^p \times (W_n^u - V_n^p);\ S_u \geq Q_n^u \tag{22}$$

where, S_p is the random number, M_n^p is the flight length, Q_n^u represent the awareness probability of u at n^{th} iteration, w_n^u is the hiding place, V_{n+1}^p position of the crow p at iteration $n+1$, and V_n^p indicates the position of the crow p at iteration n.

$$V_{n+1}^{p} = V_n^p + S_p \times M_n^p \times W_n^u - S_p \times M_n^p \times V_n^p \tag{23}$$

$$V_{n+1}^{p} = V_n^p (1 - S_p \times M_n^p) + S_p \times M_n^p \times W_n^u \tag{24}$$

$$V_n^p = \frac{V_{n+1}^p - S_p \times M_n^p \times W_n^u}{(1 - S_p \times M_n^p)} \tag{25}$$

After substituting above equations in equation (21), the equation is given as,

$$V_{n+1}^{p} = \frac{1}{0.7}\left\{\frac{V_{n+1}^p - S_p \times M_n^p \times W_n^u}{(1 - S_p \times M_n^p)}\right\} \tag{26}$$

$$V_{n+1}^{p} = \frac{V_{n+1}^{p}}{0.7(1-S_{p} \times M_{n}^{p})} - \frac{S_{p} \times M_{n}^{p} \times W_{n}^{u}}{0.7(1-S_{p} \times M_{n}^{p})} \tag{27}$$

$$V_{n+1}^{p}\left(1-\frac{1}{0.7(1-S_{p} \times M_{n}^{p})}\right) = \frac{-S_{p} \times M_{n}^{p} \times W_{n}^{u}}{0.7(1-S_{p} \times M_{\boldsymbol{n}}^{p})} \tag{28}$$

$$V_{n+1}^{p}\left(\frac{0.7-0.7S_{p} \times M_{n}^{p}-1}{0.7(1-S_{p} \times M_{n}^{p})}\right) = \frac{-S_{p} \times M_{n}^{p} \times W_{\boldsymbol{n}}^{u}}{0.7(1-S_{p} \times M_{n}^{p})} \tag{29}$$

$$V_{n+1}^{p}\left(\frac{-0.3-0.7S_{p} \times M_{n}^{p}}{0.7(1-S_{p} \times M_{n}^{p})}\right) = \frac{-S_{p} \times M_{n}^{p} \times W_{\boldsymbol{n}}^{\boldsymbol{u}}}{0.7(1-S_{p} \times M_{n}^{p})} \tag{30}$$

$$V_{n+1}^{p} = \frac{S_{p} \times M_{n}^{p} \times W_{n}^{u}}{0.3+0.7S_{p} \times M_{n}^{p}} \tag{31}$$

The second equation of CWOA is given as,

$$V_{n+1}^{p} = \frac{10}{3}(1-V_{n}^{p}) \tag{32}$$

After substituting equation (25) in above equation, the obtained equation is expressed as,

$$V_{n+1}^{p} = \frac{10}{3}\left(1-\frac{V_{n+1}^{p}-S_{p} \times M_{n}^{p} \times W_{n}^{u}}{(1-S_{p} \times M_{n}^{p})}\right) \tag{33}$$

$$V_{n+1}^{p} = \frac{10}{3}\left(1-\frac{V_{n+1}^{p}}{(1-S_{p} \times M_{n}^{p})}+\frac{S_{p} \times M_{n}^{p} \times W_{n}^{u}}{(1-S_{p} \times M_{n}^{p})}\right) \tag{34}$$

$$V_{n+1}^{p} = \frac{10}{3}-\frac{10}{3}\frac{V_{n+1}^{p}}{1-S_{p} \times M_{n}^{p}}+\frac{10}{3}\frac{S_{p} \times M_{n}^{p} \times W_{n}^{u}}{1-S_{p} \times M_{n}^{p}} \tag{35}$$

$$V_{n+1}^{p}+\frac{10}{3}\frac{V_{n+1}^{p}}{1-S_{p} \times M_{n}^{p}} = \frac{10}{3}+\frac{10}{3}\frac{S_{p} \times M_{n}^{p} \times W_{n}^{u}}{1-S_{p} \times M_{n}^{p}} \tag{36}$$

$$V_{n+1}^{p}\left(1+\frac{10}{3(1-S_{p} \times M_{n}^{p})}\right) = \frac{10}{3}\left(1+\frac{S_{p} \times M_{n}^{p} \times W_{n}^{u}}{1-S_{p} \times M_{n}^{\boldsymbol{p}}}\right) \tag{37}$$

$$V_{n+1}^{p}\left(1+\frac{10}{3(1-S_{p} \times M_{n}^{p})}\right) = \frac{10}{3}\left(1+\frac{S_{p} \times M_{n}^{p} \times W_{n}^{u}}{1-S_{p} \times M_{n}^{\boldsymbol{p}}}\right) \tag{38}$$

$$V_{n+1}^{p}\left(13-3S_{p}M_{n}^{p}\right) = 10\left(1-S_{p}M_{n}^{p}\left(1-W_{n}^{u}\right)\right) \tag{39}$$

$$V_{n+1}^{p} = \frac{10\left(1 - S_{p} M_{n}^{p}\left(1 - W_{n}^{u}\right)\right)}{13 - 3S_{p} M_{n}^{p}} \tag{40}$$

Both equation (31) and (40) obtained by integrating CWOA and CSA is substituted in equation (21), for acquiring the final equation for secure routing, which is given as,

$$V_{n+1}^{p} = \begin{cases} \dfrac{S_{p} \times M_{n}^{p} \times W_{n}^{u}}{0.3 + 0.7 S_{p} \times M_{n}^{p}} & ;V_{n}^{p} < 0.7 \\ \dfrac{10\left(1 - S_{p} M_{n}^{p}\left(1 - W_{n}^{u}\right)\right)}{13 - 3S_{p} M_{n}^{p}} & ;V_{n}^{p} \geq 0.7 \end{cases} \tag{41}$$

Step4: Determine the fitness of the solutions: After updating the whale's position, the fitness of the updated solutions is evaluated. Accordingly, the solution referring to the best solution is denoted as, V_{best} . The fitness function is based on the objective function defined in equation (19), which should be maximal for selecting the effective solution. Thus, the effective solution is nothing but the optimal trusted nodes involved in the routing process.

Step5: Validate the stopping condition: The stopping criterion is verified to mark the end of the optimization process. The stopping criterion is defined for better convergence of the algorithm, comprising maximal iterations, improvement percentage, and time-taken for execution. Then, the optimal or intermediate nodes for continuing the routing between the source and destination nodes are performed using the proposed CWC algorithm. The pseudo-code for the proposed CWC algorithm is given below in Algorithm 1

5. RESULTS AND DISCUSSION

This section illustrates the proposed method's comparison with conventional methods by simulating the IoT network with 100 and 150 nodes. The analysis is done by varying the time from 1 sec to 10 sec.

5.1 Experimental Setup

The execution of the proposed method is done in NS2 using 150 and 100 nodes. The proposed method is executed on a PC with Windows 10 OS, 2GB RAM, and Intel i3 core processor. The detailed setup is depicted in Table 2 given below:

5.1.1. Simulation Results

Figure 4 elaborates the simulation results of the proposed CWC based on 100 nodes and 150 nodes. Figure 4 a) portrays the analysis based on 100 nodes, whereas figure 4 b) represents the analysis based on 150 nodes. Here, the dark blue nodes represent the source, and the greenish node represents the destination. The source nodes send the data packet to the destination nodes by selecting a specific path wherein the path with the nodes is represented in yellowish colors. Thus, secure transmission is attained in the IoT network.

Table 1. Algorithm 1: Pseudo-code for CWC algorithm

Input: Solution V
Output: Best solution V_{n+1}^{p}
Begin:
$z = 0$;
Initialize the population randomly;
while stopping criterion is not satisfied do
Evaluate error using equation (19);
if ($n <$ maximum number of iterations)
Update the position using equation (25)
else
Update the position using the equation (41)
End if
Re-evaluate the fitness
$n = n + 1$
End while
Return V_{n+1}^{p}

5.2 Evaluation Metrics

The metrics employed for analyzing the methods include delay, energy, and throughput.

i) Throughput

The throughput refers to the total data rates transmitted over the network at a specific time.

$$Throughput = \frac{Number\ of\ packets\ received}{Time} \tag{42}$$

ii) Delay

The delay parameter describes the total time taken for transmitting the data irrespective of the attacker. The formula for the delay is modeled as,

$$Delay = \frac{N_b}{R} \tag{43}$$

Table 2. Experimental setup

Parameter	Value
channel type	Channel/WirelessChannel
radio-propagation model	Propagation/TwoRayGround
network interface type	Phy/WirelessPhy
MAC type	Mac/802_11
interface queue type	Queue/DropTail/PriQueue
link layer type	LL
antenna model	Antenna/OmniAntenna
max packet in ifq	50
routing protocol	DSDV
X dimension of topography	1501
Y dimension of topography	600
time of simulation end	15
Energy Model	
Initial Energy	3.4
Transmitter Power	0.33
Received Power	0.1
Idle Power	0.05
Sleep Power	0.03

where, N_b indicate the number of bits and R represent the rate of transmission.

iii) Energy

The energy of the node is elaborated in section 3.1.1

5.3 Comparative Methods

The methods employed for the analysis include: LaSeR (Mick, *et al.,* 2017), PM Ipv6 (Shin, *et al.,* 2017), secTrust-RPL (Airehrour, *et al.,* 2019), RISA (Jazebi and Ghaffari, 2020), LSDAR (Haseeba,*et al*., 2020), and proposed CWC algorithm.

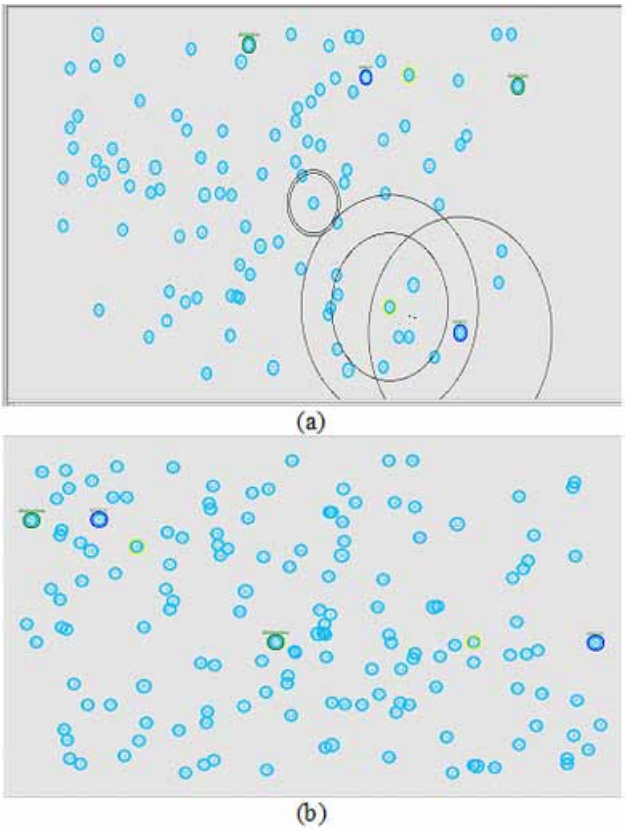
5.4. Performance Analysis

The performance analysis of the proposed CWC algorithm based on delay, energy and throughput parameters is evaluated in this section. The analysis is carried out by varying rounds 0 to 1000. Moreover, the population size of the proposed CWC is varied for proving the effectiveness of the proposed method. Furthermore, the analysis is performed with 400 and 500 nodes, respectively.

5.4.1. Analysis Based on 400 Nodes

Figure 5) illustrates the analysis of the proposed CWC using 400 nodes by varying the population size from 10 to 40. The analysis of the proposed CWC based on the delay parameter is illustrated in figure 5a). For round=200, the delay values computed by proposed CWC with population size =10, 20, 30, and 40 are 91.734ms, 91.382ms, 88.986ms, and 85.633ms, respectively. The analysis of the

Figure 4. Simulation results of proposed CWC using a) 100 nodes b) 150 nodes

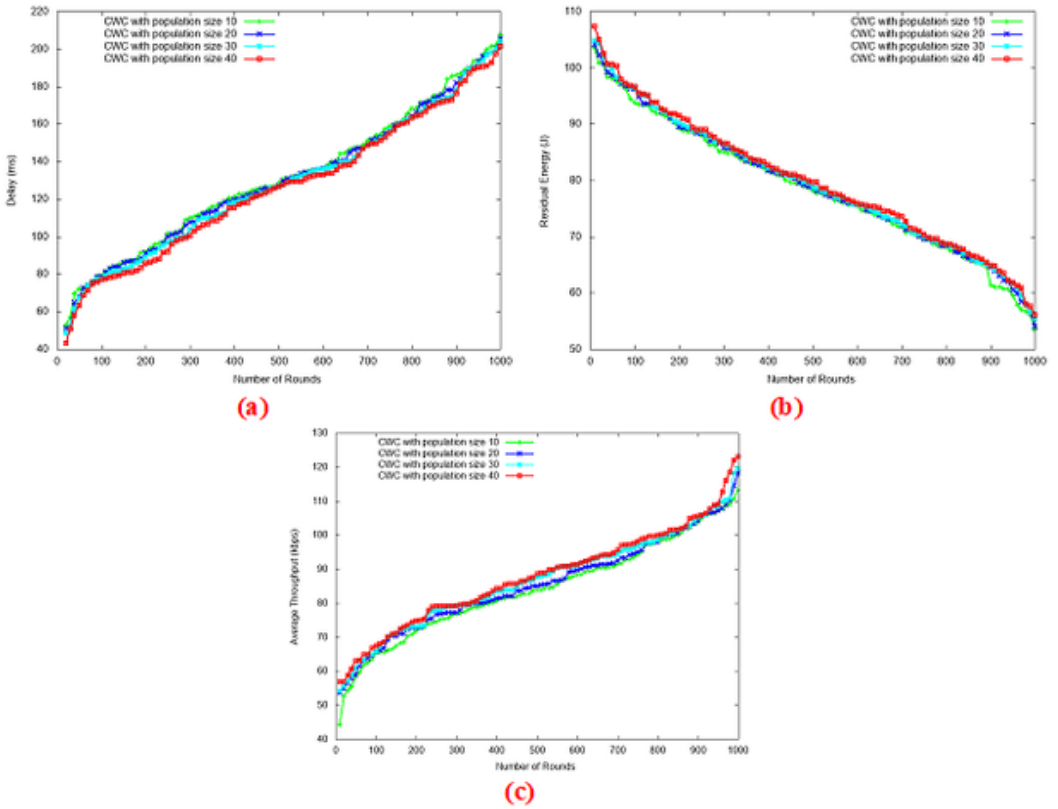


proposed CWC based on energy parameters is illustrated in figure 5b). For round=600, the energy values computed by proposed CWC with population size =10, proposed CWC with population size =20, proposed CWC with population size =30, proposed CWC with population size =40 are 75.506J, 75.56J, 75.669J and 75.807J, respectively. The analysis of the proposed CWC based on throughput parameter is illustrated in figure 5c). For round=800, the throughput values computed by proposed CWC with population size =10, proposed CWC with population size =20, proposed CWC with population size =30, proposed CWC with population size =40 are 97.936kbps, 98.065kbps, 98.572kbps, and 99.884kbps, respectively.

5.4.2. Analysis Based on 500 Nodes

Figure 6) illustrates the analysis of the proposed CWC using 500 nodes by varying the population size from 10 to 40. The analysis of the proposed CWC based on the delay parameter is illustrated in figure 6a). For round=300, the delay values computed by proposed CWC with population size =10, proposed CWC with population size =20, proposed CWC with population size =30, proposed CWC with population size =40 are 126.763ms, 125.82ms, 125.136ms, and 122.142ms, respectively. The analysis of the proposed CWC based on energy parameters is illustrated in figure 6b). For round=700, the energy values computed by proposed CWC with population size =10, proposed CWC with population size =20, proposed CWC with population size =30, proposed CWC with population size =40 are 86.254J, 86.593J, 86.818J, and 87.062J, respectively. The analysis of proposed CWC based on throughput parameter is illustrated in figure 6c). For round=100, the throughput values

Figure 5. Analysis of proposed CWC using 400 nodes a) Delay b) Energy c) Throughput



computed by proposed CWC with population size =10, proposed CWC with population size =20, proposed CWC with population size =30, proposed CWC with population size =40 are 66.299kbps, 71.048kbps, 72.063kbps, and 72.346kbps, respectively.

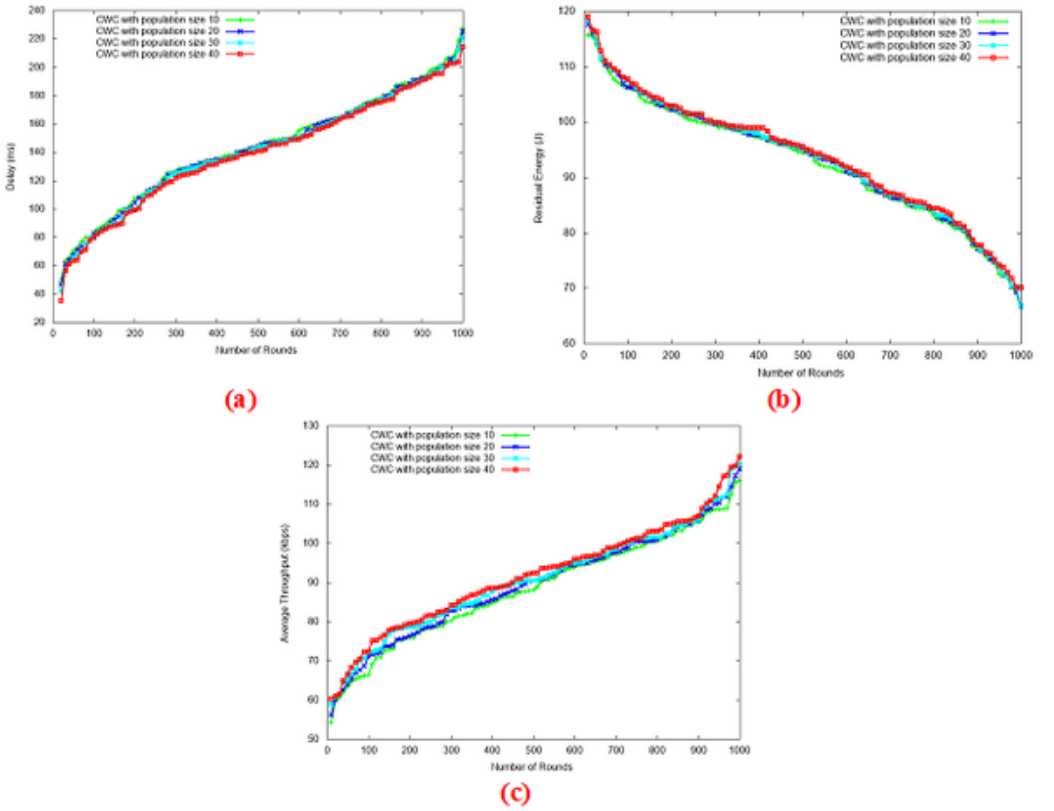
5.5. Comparative Analysis

The comparative analysis of the proposed CWC algorithm with the existing methods based on delay, energy and throughput parameters is evaluated in this section. The analysis is performed using 400 and 500 nodes, respectively.

5.5.1. Analysis Based on 400 Nodes

Figure 7) illustrates the analysis of methods using 400 nodes by varying round from 0 to 100 rounds. The analysis of methods based on delay parameter is illustrated in figure 7a). For 500 round, the delay values computed by LaSeR, PM Ipv6, secTrust-RPL, RISA, LSDAR, and proposed CWC are 141.354ms, 131.382ms, 129.934ms, 120.350ms, 128.167ms, and 118.621ms, respectively. The analysis of methods based on energy parameter is illustrated in figure 7b). For 600 round, the energy values computed by LaSeR, PM Ipv6, secTrust-RPL, RISA, LSDAR, and proposed CWC are 65.402J, 66.326J, 66.456J, 72.627J, 66.873J, and 78.407J, respectively. The analysis of methods based on throughput parameter is illustrated in figure 7c). For round=700, the throughput values computed by LaSeR, PM Ipv6, secTrust-RPL, RISA, LSDAR, and proposed CWC are 97.558kbps, 99.763kbps, 100.965kbps, 101.201kbps, 105.993kbps, 106.966kbps, respectively.

Figure 6. Analysis of proposed CWC using 500 nodes a) Delay b) Energy c) Throughput



5.5.2. Analysis Based on 500 Nodes

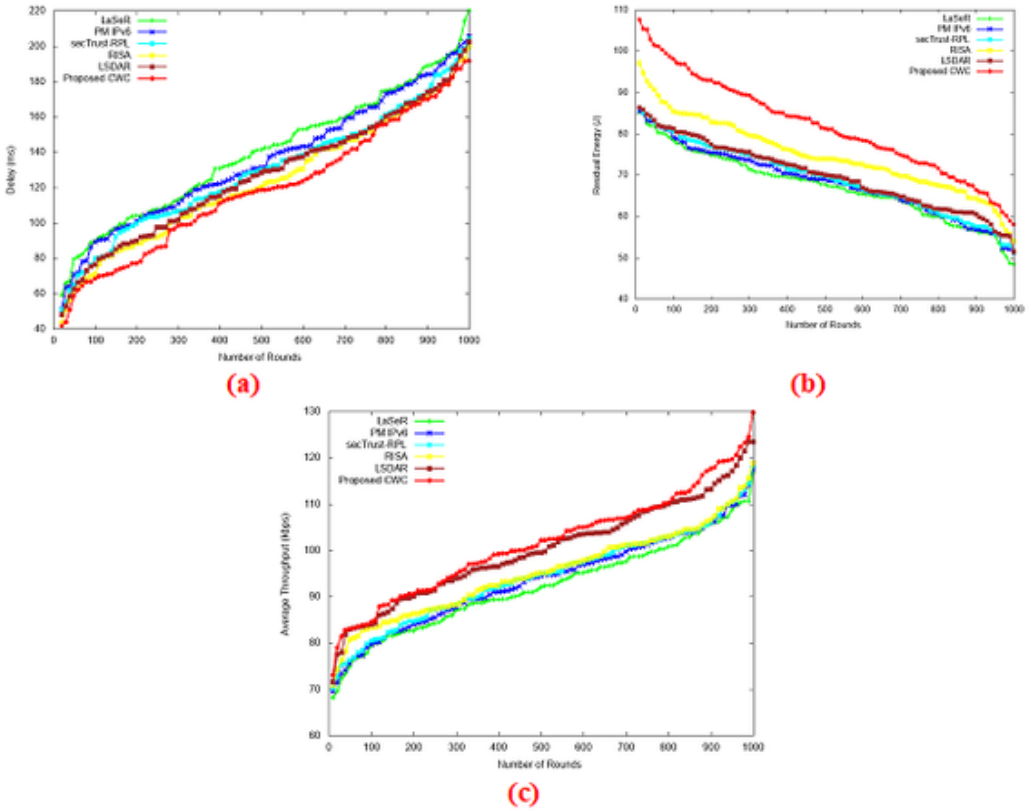
Figure 8) illustrates the analysis of methods using 500 nodes by varying round from 0 to 1000. The analysis of methods based on delay parameter is illustrated in figure 8a). For round=100, the delay values computed by LaSeR, PM Ipv6, secTrust-RPL, RISA, LSDAR, and proposed CWC are 98.787ms, 96.555ms, 86.178ms, 76.228ms, 82.988ms, and 72.927ms, respectively. The analysis of methods based on energy parameter is illustrated in figure 8b). For round=200, the energy values computed by LaSeR, PM Ipv6, secTrust-RPL, RISA, LSDAR, and proposed CWC are 88.680J, 89.142J, 89.775J, 98.623J, 90.467J, and 104.705J, respectively. The analysis of methods based on throughput parameter is illustrated in figure 8c. For round=300, the throughput values computed by LaSeR, PM Ipv6, secTrust-RPL, RISA, LSDAR, and proposed CWC are 89.083kbps, 89.280kbps, 89.630kbps, 91.581kbps, 95.039kbps, 99.165kbps, respectively.

5.6. Comparative Discussion

Table 3 elaborates the comparative analysis of methods based on delay, energy and throughput parameters using 400 and 500 nodes.

In case of 400 nodes, the best performance is showed by proposed CWC with minimal delay of 191.468ms, whereas the delay of existing LaSeR, PM Ipv6, secTrust-RPL RISA, LSDAR, are 219.9451ms, 205.547107ms, 204.5171ms, 199.4916ms, and 202.4595ms, respectively. The maximal performance is showed by proposed CWC with maximal energy of 58.059J, whereas the energy of existing LaSeR, PM Ipv6, secTrust-RPL RISA, LSDAR, are 48.320J, 51.171J, 51.323J, 54.060J, and

Figure 7. Analysis of methods using 400 nodes a) Delay b) Energy c) Throughput



51.486J, respectively. The optimal performance is gained by proposed CWC with maximal throughput of 129.776kbps whereas the energy of existing LaSeR, PM Ipv6, secTrust-RPL RISA, LSDAR, are 116.6577kbps, 117.518983kbps, 118.1119kbps, 118.7895kbps, and 123.4659kbps, respectively. The computation time obtained by the proposed CWC method is 2.20min, whereas the energy of existing LaSeR, PM Ipv6, secTrust-RPL RISA, LSDAR, are 2.8993min, 2.484min, 2.891min, 2.3512min, and 2.3182min, respectively. In case of 500 nodes, the best performance is showed by proposed CWC with minimal delay of 210.047ms whereas the delay of existing LaSeR, PM Ipv6, secTrust-RPL RISA, LSDAR, are 231.555ms, 226.3674ms, 216.7031ms, 210.3318ms, and 211.32ms respectively. The maximal performance is showed by proposed CWC with maximal energy of 71.25J whereas the energy of existing LaSeR, PM Ipv6, secTrust-RPL RISA, LSDAR, are 61.988J, 65.042J, 65.877J, 67.896J, and 66.345J, respectively. The optimal performance is gained by proposed CWC with maximal throughput of 121.167kbps, whereas the energy of existing LaSeR, PM Ipv6, secTrust-RPL, RISA, LSDAR, are 115.8573kbps, 119.455292kbps, 120.5413kbps, 122.921kbps, and 125.440kbps, respectively. The computation time obtained by the proposed CWC method is 3.007min, whereas the energy of existing LaSeR, PM Ipv6, secTrust-RPL RISA, LSDAR, are 3.5073min, 3.7677min, 3.2938min, 3.1756min, and 3.1739min, respectively

6. CONCLUSIONS

This paper proposes a novel optimization algorithm named CWC algorithm to achieve secure routing in the IoT environment. Initially, the IoT nodes are simulated in the distributed environment and as a

Figure 8. Analysis of methods using 500 nodes a) Delay b) Energy c) Throughput

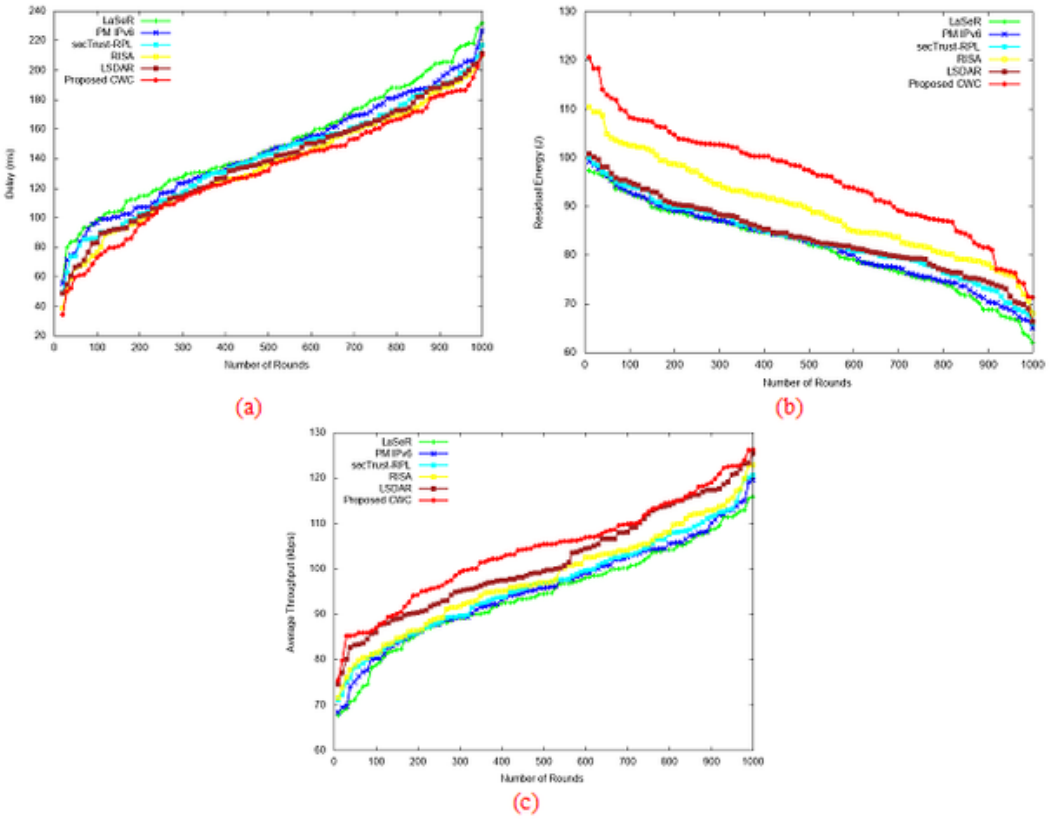


Table 3. Comparative Analysis

Nodes	Metrics	LaSeR	PM Ipv6	secTrust-RPL	RISA	LSDAR	Proposed CWC
Using 400 nodes	**Delay (ms)**	219.9451	205.547107	204.5171	199.4916	202.4595	**191.4668**
	Energy (J)	48.32099	51.1716921	51.3238	54.06091	51.48615	**58.05876**
	Throughput (kbps)	116.6577	117.518983	118.1119	118.7895	123.4659	**129.7769**
	Computation Time(min)	2.8993	2.484	2.891	2.3512	2.3182	**2.2094**
Using 500 nodes	**Delay (ms)**	231.5557	226.367457	216.7031	210.3318	211.32	**210.0478**
	Energy (J)	61.98853	65.0429877	65.8776	67.8966	66.34554	**71.2595**
	Throughput (kbps)	115.8573	119.455292	120.5413	122.921	125.4409	**126.1671**
	Computation Time(min)	3.5073	3.7677	3.2938	3.1756	3.1739	**3.007**

point of assuring security, the trust of the nodes is computed. The trust is computed for all the simulated IoT nodes in order to facilitate the secure communication in the network. The trust, namely direct trust, indirect trust, forwarding rate factor, integrity factor, availability factor, and energy is computed for all the simulated IoT nodes. Once the trust factor is computed, the secure routing framework is established using the secure IoT nodes. The selected trusted nodes are adapted for trust-based secure routing, which are optimally done through the proposed CWC, based on the fitness parameters trust,

and energy. The secure routing framework is progressed using the proposed CWC optimization algorithm, which is the integration of the CWO algorithm and the CSA. Moreover, the effectiveness of the proposed CWC algorithm is evaluated which shows optimal performance with minimal delay of 191.46ms, maximal energy of 71.25J, and maximal throughput of 129.77kbps, respectively. However, the proposed method is little time consuming and expensive to implement, which could be overcome in the future by developing a novel optimization algorithm with reduced time complexity.

FUNDING AGENCY

The publisher has waived the Open Access Processing fee for this article.

REFERENCES

Airehrour, D., Gutierrez, J., & Ray, S. K. (2016). Secure routing for internet of things: A survey. *Journal of Network and Computer Applications*, *66*, 198–213.

Airehrour, D., Gutierrez, J. A., & Ray, S. K. (2019). SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things. *Future Generation Computer Systems*, *93*, 860–876.

Altisen, K., Devismes, S., Jamet, R., & Lafourcade, P. (2013). SR3: secure resilient reputation-based routing. *Proceedings of IEEE International Conference on Distributed Computing in Sensor Systems*, 258-265.

AlZubi, A. A., Al-Maitah, M., & Alarifi, A. (2019). A best-fit routing algorithm for non-redundant communication in large-scale IoT based network. *Computer Networks*, *152*, 106–113.

Askarzadeh, A. (2016). A novel metaheuristic method for solving constrained engineering optimization problems: Crow search algorithm. *Computers & Structures*, *169*, 1–12.

Bellovin, S. M. (1989). Security problems in the TCP/IP protocol suite. *Computer Communication Review*, *19*(2), 32–48.

Bu, L., Isakov, M., & Kinsy, M. A. (2019). A secure and robust scheme for sharing confidential information in IoT systems. *Ad Hoc Networks*, *92*, 101762.

Chen, Z., He, M., Liang, W., & Chen, K. (2015). Trust-aware and low energy consumption security topology protocol of wireless sensor network. *Journal of Sensors*, *1*, 1–10.

Das, A., & Islam, M. M. (2011). Secured trust: A dynamic trust computation model for secured communication in multiagent systems. *IEEE Transactions on Dependable and Secure Computing*, *9*(2), 261–274.

Das, A. K., Wazid, M., Yannam, A. R., Rodrigues, J. J., & Park, Y. (2019). Provably Secure ECC-Based Device Access Control and Key Agreement Protocol for IoT Environment. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 55382–55397.

Esposito, C., Ficco, M., & Gupta, B. B. (2021). Blockchain-based authentication and authorization for smart city applications. *Information Processing & Management*, *58*(2), 2021.

Ganeriwal, S., Balzano, L. K., & Srivastava, M. B. (2008). Reputation-based framework for high integrity sensor networks. *ACM Transactions on Sensor Networks*, *4*(3), 15.

Harlamova, M., Kirikova, M., & Sandkuhl, K. (2017). A Survey on Challenges of Semantics Application in the Internet of Things Domain,*Applied*. *Computer Systems*, *21*, 13–21.

Haseeba, K., Islama, N., Sabab, T., Rehmanb, A., & Mehmoodc, Z. (2020). LSDAR: A light-weight structure based data aggregation routing protocol with secure internet of things integrated next-generation sensor networks. *Sustainable Cities and Society*, 54.

Hatzivasilis, G., Papaefstathiou, I., & Manifavas, C. (2017). SCOTRES: Secure routing for IoT and CPS. *IEEE Internet of Things Journal*, *4*(6), 2129–2141.

Jazebi, S. J., & Ghaffari, A. (2020). RISA: Routing scheme for Internet of Things using shuffled frog leaping optimization algorithm. *Journal of Ambient Intelligence and Humanized Computing*, *11*, 4273–4283.

Kalkan, K., & Zeadally, S. (2017). Securing internet of things (iot) with software defined networking (sdn). *IEEE Communications Magazine*, *99*, 1–7.

Kaur, G., & Arora, S. (2018). Chaotic whale optimization algorithm. *Journal of Computational Design and Engineering*, *5*(3), 275–284.

Kukreja, D., & Reddy, B. V. R. (2012). Trust based routing using Dominating Set Approach (TRDSA) in Wireless Ad-Hoc Networks. *IJCA Proceedings on National Conference on Communication Technologies and Its Impact on Next Generation Computing*, 1.

Li, D., Deng, L., Gupta, B. B., Wang, H., & Choi, C. (2019). A Novel CNN based Security Guaranteed Image Watermarking Generation Scenario for Smart City Applications. *Information Sciences*, *479*, 432–447.

Liu, Y., Kuang, Y., Xiao, Y., & Xu, G. (2017). SDN-based data transfer security for Internet of Things. *IEEE Internet of Things Journal*, *5*(1), 257–268.

Mick, T., Tourani, R., & Misra, S. (2017). Laser: Lightweight authentication and secured routing for ndn iot in smart cities. *IEEE Internet of Things Journal*, *5*(2), 755–764.

Miorandi, D., Sicari, S., De Pellegrini, F., & Chlamtac, I. (2012). Internet of things: Vision, applications and research challenges. *Ad Hoc Networks*, *10*(7), 1497–1516.

Over MANET, RBA. (2012). *Adhoc On-Demand Distance Vector Routing Reputation-Based (AODVRB) over MANET*. Academic Press.

Paris, S., Nita-Rotaru, C., Martignon, F., & Capone, A. (2013). Cross-layer metrics for reliable routing in wireless mesh networks. *IEEE/ACM Transactions on Networking*, *21*(3), 1003–1016.

Rathee, G., Sharma, A., Kumar, R., & Iqbal, R. (2019). A Secure Communicating Things Network Framework for Industrial IoT using Blockchain Technology. *Ad Hoc Networks*.

Shin, D., Sharma, V., Kim, J., Kwon, S., & You, I. (2017). Secure and efficient protocol for route optimization in PMIPv6-based smart home IoT networks. *IEEE Access: Practical Innovations, Open Solutions*, *5*, 11100–11117.

Stergiou, C.L., Psannis, K.E., & Gupta, B.B. (2021). IoT-Based Big Data Secure Management in the Fog Over a 6G Wireless Network. *IEEE Internet of Things Journal*, *8*(7).

Sun, Y., Tian, Z., Wang, Y., Li, M., Su, S., Wang, X., & Fan, D. (2019). Lightweight Anonymous Geometric Routing for Internet of Things. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 29754–29762.

Tewari, A., & Gupta, B. B. (2016). Cryptanalysis of a novel ultra-lightweight mutual authentication protocol for IoT devices using RFID tags. *The Journal of Supercomputing*, *73*(3).

Tewari, A., & Gupta, B. B. (2018). Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework. *Future Generation Computer Systems*, *108*(4).

Trivedi, A. K., Arora, R., Kapoor, R., Sanyal, S., & Sanyal, S. (2010). *A semi-distributed reputation based intrusion detection system for mobile adhoc networks*. arXiv preprint arXiv: 10061956.

Zhu, J. (2018). Wireless Sensor Network Technology Based on Security Trust Evaluation Model. *International Journal of Online Engineering*, *14*(04), 211–226.

Meghana G Raj is currently working as Assistant Professor in the School of Computer Engineering, KIIT Deemed to be University. She has over 7 years of experience in teaching under-graduate students in subjects ranging from Internet of Things, Database Management Systems, Data Structures and Design and Analysis of Algorithms. Prior to joining academia, she has worked for 2 years in the corporate sector as a System Analyst at IBM India, Bangalore. Her research interests include cloud-based security, algorithm design and internet of things. meghana.nitk@gmail.com

Santosh Kumar Pani is currently working as Professor in the School of Computer Engineering, KIIT Deemed to be University. He has over two decades of experience in teaching, research and administration. He has over twenty research publications indexed in global reputed databases and guided several Ph.D. Scholars and M.Tech students in School of Computer Engineering. He has served in various key administrative positions such as Controller of Examinations of KIIT, Deemed to be University over a period of four years. His recent research interests include program slicing, data flow analysis, internet of things and cloud services.