Computers, Materials & Continua
DOI: 10.32604/cmc.2023.032207
Article

Tech Science Press

Secure and Optimal LOADng Routing for IoT with Composite Routing Metric

Divya Sharma[1,*], Sanjay Jain[2] and Vivek Maik[3]

[1]Department of Electronics and Communication, New Horizon College of Engineering, Bengaluru, 560103, India
[2]CMR Institute of Technology, Bengaluru, 560037, India
[3]Department of Electronics and Communication, SRM Institute of Science and Technology, Kattankulathur, Chennai, 603203, India
*Corresponding Author: Divya Sharma. Email: divyasharmaphd69@gmail.com
Received: 10 May 2022; Accepted: 12 June 2022

Abstract: Security is the one of the major challenges for routing the data between the source and destination in an Internet of Things (IoT) network. To overcome this challenge, a secure **L**ightweight **O**n-demand **A**d hoc **D**istance-vector—Next Generation (LOADng) Routing Protocol is proposed in this paper. As the LOADng protocol is the second version of Ad Hoc On-Demand Distance Vector (AODV) protocol, it retains most of the basic functionality and characteristics of AODV. During the route discovery process, the cyclic shift transposition algorithm (CSTA) is used to encrypt the control packets of the LOADng protocol to improve its security. CSTA approach only derives transposition and substitution without product cipher with respect to input data. Besides this, for choosing the best probable path between the source and destination, routing metrics such as link quality Indicator (LQI), hop count (HC) and queue length (QL) are included in the control packets. The data is then securely sent using CSTA using the optimal secure path selected. Experimental Results depict that the proposed secure and optimal LOADng (SO-LOADng) using CSTA encryption obtains better throughput, delivery ratio encryption time and decryption time than the existing state-of-art approaches.

Keywords: IoT; LOADng; CSTA; link quality indicator; queue length

1 Introduction

The IoT is a broad concept that has recently gained much attention from the research community. The term IoT refers to a pervasive and ubiquitous network in which devices exchange information between each other without the need for human intervention [1,2]. This network can be deployed for wide range of applications with varying objectives, such as, smart homes and metropolitan networks [3], smart agriculture [4], modern automation [5], adroit business areas [6], and clinical care structures [7]. IoT technology allows us to solve certain existing unique problem statements which were hindering the wide spread connectivity of devices.

In Wireless Sensor Networks (WSN), energy effectiveness is enhanced by ideal clustering, routing, and aggregation of data alongside the adaptable sink node [8]. Many works [9,10] have focused on altering the cluster information to improve energy productivity. In cluster-based network, the sensor nodes are segregated into smaller clusters with certain model assumptions which uphold energy effectiveness and Quality of Service (QoS) through information total. For routing the traffic, the main routing metric employed is based on distance between a given node and a sink [11]. Other parameters like quality of links and the energy at node can be taken into account to improve the network efficiency. Further, optimal routing is used in WSN-IoT for the purpose of improving energy productivity and QoS [12,13]. Without any efficient routing plan, the loss of data and the energy consumption will be high which happens mainly due to the expansion in transmission distance. As a result, the WSN-IoT's can achieve energy efficiency only with optimal routing plan and it can benefit in large scaled application areas such as forest area monitoring, smart city, etc. [14].

Security is an important part of any network's QoS operations and in recently numerous security related researches have focused on integrating WSN and IoT for improvement in security features. As expressed before, WSN-IoT nodes are resource constrained which implies lightweight security scheme is critical [15,16]. A lightweight cryptography design mitigates the problem of complex encryption process, resulting in increased energy efficiency. [17,18]. Particularly, the traditional cryptography algorithms are designed with the aim to work with work stations and PCs (i.e.,) which are gadgets with higher energy requirements. On the other hand, the lightweight codes are intended to deal with the resource obliged gadgets like sensors and RFID. In WSN-IoT applications these light weight gadgets have become the building blocks to further facilitate energy efficiency, QoS and security. Most of the times the individual work centres around improvement of single parameter in either energy, QoS or security. The proposed algorithm in this paper also works to establish a novel WSN-IoT network plan to accomplish better execution and to achieve the above mentioned goals, with the following contributions.

- Optimal LOADng routing protocol is used to find the best path between the source and the destination. For efficient path selection, LQI, QL and HC are all considered in this paper. Based on the approach, link quality, queue length at each node, hop count, the path is estimated. This will give stable, shortest path with reduced delay.
- To enhance the security of data transmission, the data/control packets LOADng protocol are encrypted using keyless cryptography algorithm called as CSTA which will ensure discovery of an optimal secure path.
- The performance of the proposed scheme is evaluated in terms of delivery ratio, throughput, control overhead, encryption time and decryption time.

The rest of the paper is organized as follows. Section 2 reviews some recent studies on secure routing in IoT networks. Section 3 proposes Secure LOADng Routing Protocol with Composite Routing Metric for IoT. Section 4 examines the performance of SO-LOADng protocol. Section 5 concludes the paper.

2 Related Works

Sujanthi et al. [8] had introduced a dynamic cluster depend routing in WSN-IoT for quality of service aware using secure deep learning approach. The authors used this approach to create a dynamic cluster of WSN-IoTs along with bi-concentric hexagons and Mobile Sinks to enhance the energy efficiency of the network. The cluster heads were chosen by quality prediction phenomenon and the dynamic clusters were created in Bi-Hex network following which at one time-PRESENT

cryptography algorithm was used to attain efficient protection. After this, it was confirmed that mobile sinks provided high level QoS. The crossover between optimal routing path selection and deep neural network facilitated improvement in network life, performance, packet distribution rate, delay and encryption time.

Mujeeb et al. [9] had introduced big data classification on IoT network using Energy-Efficient and Trust Aware Secure Routing Algorithm. Using this approach, the authors proposed adaptive energy harvesting and trust aware routing using the cost metric function for the optimal secure routing path selection. Next, the classification of big data was done using the auto encoder stacked on the MapReduce framework whilst the data sets were trained using the proposed adaptive E2-Bat algorithm which gave an optimal energy gain of 0.948 J compared to other proposed methods.

Sahraoui et al. [10] had introduced improved security and reliability on heterogeneous IoT low power and loss network based secure and multipath RPL (IPv6 Routing Protocol for Low power and Lossy Networks). The authors had used an effective design that improves both communication reliability and security in heterogeneous IoT enabled low power and loss networks. Three different types of adaptive and secure multipath routing were proposed that controls multipath routing security and using a Contiki OS Cooja simulator the performance was evaluated and shown to be outperform the competition.

Kavitha [12] had introduced security privacy in the IoT environment using the multi-hop dynamic clustering routing protocol and elliptic curve crypto system for the WSN. In this approach, the authors used optimal privacy-multihop dynamic clustering routing protocol which reduced sensor terminal power consumption and also increased the lifetime of the WSN. The algorithm also proposed use of elliptic curve Integrated Encryption-Key Provisioning Method for data privacy which enabled the protection of sensitivity data with minimal computational overheads and provided superior performances.

Shende et al. [13] proposed an energy-aware routing protocol based Crow Whale optimization algorithm for WSN in IoT. In the proposed approach the authors combined CSA (Crow Search Algorithm) and WOA (Whale Optimization Algorithm) optimization algorithms which worked based on energy aware multicast routing protocol. Initially, the authors evaluated trust and energy of the nodes using the optimization algorithm for path selection. Following that, each node's energy and trust are replenished at the end of each transmission, resulting in more secure network connection. This approach was evaluated using various performance tests and detection rate for Crow Whale – ETR was found to be enhanced than other methods.

Jain [14] had introduced a model for route adjustment in IoT that was both secure and energy efficient by utilizing genetic algorithm for optimal value search and the sensor nodes. Subsequently, threshold based timeslots were allocated by TDMA and energy consumption was reduced by ESRA (full form if used first time) before selecting the optimal routing path from the current location of the sink node. MATLAB R-2016a was used to measure performance from various angles, and the suggested system's performance was assessed.

Kothandaraman et al. [15] proposed a secured routing algorithm based on sequence number based secure routing algorithm (SNSR) for IoT networks. The network performance was improved by maximizing the packet delivery ratio and the network lifetime. For IoT simulation test was carried out NS-3 and the SNSR method implemented with random mobility point.

Deebak et al. [16] had introduced hybrid secure routing and monitoring method in WSN-IoT which improved the secure data transmission using selective sensor monitor nodes and multi variant

tuples with MARS, RC6, Serpent and Two fish approaches. Subsequently, this hybrid approach would detect and block enemies in the global sensor network using authentication and ATE along with eligibility weighted node selection method for sensor guard node selection. The experimental results suggested better rate of monitor and detection ratio.

To improve the delivery ratio and extend lifetime of network authors [17] have designed composite metric based on energy left and active routes. This helps in resolving issues related to congestion by checking the number of connections that are active at a particular node. Additionally, the energy remaining at node helps in increasing the network life.

Tilwari et al. [18] proposed a routing approach based on multiple criteria for selecting routes. The decision making was done by estimating mobility and queue length. The performance of the proposed work was compared with the traditional Multipath-Optimized Link State Routing (MP-OLSR). The results depicted improved throughput, delay with reduction in packet drops.

A comparison of link quality estimators followed by a hybrid link quality estimation-based routing was suggested by authors in [19]. In order to enhance link stability, a probe packet was included to assess the link quality. Furthermore, the proposed Hybrid Reliable Routing Algorithm Based on LQI and PRR in Industrial Wireless Networks (HLQEBRR) included an effective recovery of route failures.

Charles et al. [20] have suggested a new objective function for RPL routing based on link quality for accurate link estimation values as compared to ETX method. This estimation is carried out with the support of a metric called Packet Reception Rate (PRR). The LQL is ranked from 1 to 7, reflecting the quality of the link. The default ETX along with this estimated LQL value is used deciding best path.

Bapu et al. [21] proposed a novel link quality based opportunistic routing method. Assessment of the link quality using link quality to detect and avert the broadcast faults in the network. Opportunistic routing (OR) algorithm will choose the relay nodes based on OR theory to boost the lifetime of network. Finally, it evaluates the performance of the proposed method in the working platform of MATLAB simulation.

3 A Secure and Optimal LOADng Routing Protocol with Composite Routing Metric

3.1 Overview

To solve the security issues during the process of route discovery, secure LOADng protocol is proposed where the control packets of LOADng such as route reply (RREP) and route request (RREQ) are encrypted using CSTA which includes both encryption and decryption which leads to an optical secure routing path selection Besides, to choose the efficient path between the source and destination, the control packets are updated with the routing metrics such as LQI, HC and QL and with threshold dependence, the shortest routing path with maximum link quality, minimum queue length is selected as an optimal path to communicate the data. Fig. 1 depicts the work flow diagram of the proposed scheme.

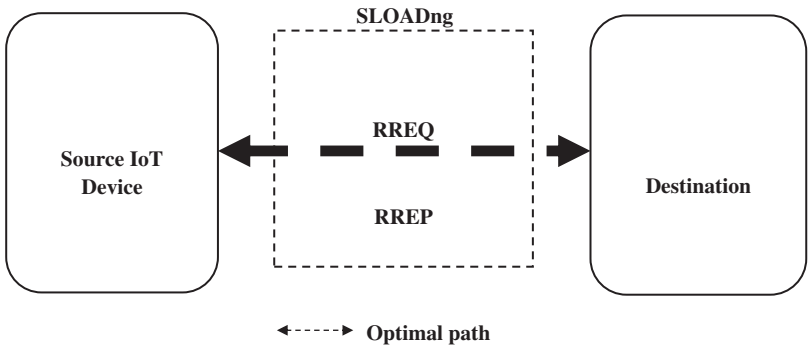

Figure 1: Overall workflow diagram of the proposed scheme

3.2 Optimal LOADng Protocol

As the LOADng protocol is the second version of AODV protocol, it retains most of the basic functionality and characteristics of AODV. The routing process includes the route discovery packets such as RREQs which originates from the source device and RREPs which originates from the destination. Also, LOADng includes the uni-cast hop-by-hop forwarding of RREPs to the source. In this protocol, if the route between source and destination is failed to connect the communication, a local route repair message i.e., Route Error denoted as RERR message will be forwarded to the source. In LOADng protocol, intermediate nodes between source and destination are not permitted to reply to the RREQ. Only destination nodes are allowed to reply to the RREQ. Gratuitous RREPs can be eliminated while confirming loop freedom as RREQ or RREPs a single unique, monotonically increasing sequence number but this protocol never updates precursor list. Thus, RERR is only forwarded to the source if the data packet fails to reach the next hop on route.

Fig. 2 highlights the standard format of control packets. In the control packets, <tlv-block> denotes the type length value elements. <message> includes the elements of RREQ, RREP. <metric> includes the composite routing metrics LQ_w (weak link quality) and Q_v (Queue length) and hop count (HC) to select the optimal path. Route metric represents the information of routing paths between source and destination by adding metrics of all interfaces that it has crossed. The link metric represents weight of link. The additional parameters chosen for link metric are LQ_w and Q_v namely indicating the number of weak links and large queue length respectively at each hop.

Route Discovery–In LOADng routing in addition to the default metric hop count, to distribute the load uniformly and reduce the delay along with sufficient bandwidth, additional information about node's queue length and link quality has been incorporated using the proposed design. When the intermediate node receives the RREQ, it sums up their queue length value (Q_v) and frail link count (LQ_w) in supplement to hop count and broadcast it further. Eventually, at the destination node, RREQ contains the sum of frail links and total number of nodes with smaller queue lengths.

Hop Count (HC): Hop count is the significant factor to discover the routing path in the LOADng protocol. It is also used to find the longer paths with more reliability than to choose the shorter paths without reliability. Besides, the routing path with minimum hop count is considered as good routing path.

<packet> := <type>

<tlv-block>

<message>

(a) Format of LOADng packet

<message> := <flag>

<addr-length>

<seq-num>

<metric>

<LQ_W>

<Q_V>

<HC>

<destination>

<originator>

(b) Message format of RREQ and RREP

Figure 2: (a) Format of LOADng packet (b) Message format of RREQ and RREP

Queue Length (QL): For real-time traffic transmission latency is a crucial metric. Intermediated IoT nodes receive and store packet in their buffers and later depending on availability of output link, forwards it. However, if the link is occupied then the packet is kept in buffer queue till link becomes available. Thus, minimum QL or queue size of the node supports to deliver with reduced latency. The QL is calculated every time a new RREQ is received at the node. The average QL can be calculated as follows,

$$QL = \phi * QL_{Current} + (1 - \phi) * QL \tag{1}$$

Here, $QL_{Current}$ denotes the current length of the queue at node N and ϕ denotes the smoothing time constant. The maximum possible queue length Q_{imax} at node i is equivalent to its buffer size. When RREQ is received at an intermediate node then it checks its current queue length and if it is greater than the threshold value Q_{Th} then queue length factor Q_v is incremented by 1 indicating higher queueing delay at this node. The intermediate node forwards control packet after updating the value of Q_v accordingly. Q_{Th} is given by

$$Q_{Th} = \beta Q_{\max} \tag{2}$$

The value of β is chosen as 0.75 for our work.

Link Quality Indicator (LQI): LQI is the most efficient metric for estimating the LQ of the routing path. The value of LQI is varied within the range [0, 255] where 0 denotes the worst link and 255 denotes the strong link. The LQI is computed based on the value of SNR (Signal to Noise Ratio) and RSSI

(Received Signal Strength Indicator). The mathematical form of LQI is defined as follows,

$$LQI = \omega_1 * RSSI + (1 - \omega_1) * SNR \tag{3}$$

Here, ω_1 denotes the random variable within the range [0, 1].

Each node determines the LQI for the RREQ received. Then it is compared with the threshold LQI (LQI_{Th}). If the LQI is less than the LQI_{Th}, the quality of the link is considered as frail else the quality of the link is considered as strong. If the RREQ is received over a frail link, then the node waits for a random amount of time to receive duplicate RREQs from other nodes else it will forward it if received over strong link. It will assess the link quality for duplicate RREQs. It compares all RREQs of same sequence number for better link quality. Whichever RREQ is received over a strong link is then forwarded further. If none of the RREQ is received over strong link, then the RREQ which was received over the highest link quality value amongst all will be forwarded. While forwarding the RREQ, it updates the count of weak links in RREQ (LQ_W) field accordingly and forwards it further.

3.3 Optimal Path Selection Based on Composite Metric (LQH)

The destination generates RREPs for each RREQ received containing the aggregate of these metrics. The source that had initiated RREQ after receiving all the RREP packets computes the cost for each possible path. The cost for the entire path is the sum of these composite metric values (LQH) of each node along that path. The path with minimum cost (min LQH) value is selected by the source node. The LQH metric is updated at each node using Eq. (4).

$$LQ_n = \alpha * (LQ_{wn} + Q_{vn}) + (1 - \alpha) * (HC) \tag{4}$$

where α indicates the weight between 0 and 1.

The route cost is the sum of the costs over all nodes along the path and is given by Eq. (5).

$$C_p = \sum_{n=1}^{m} LQ_n \tag{5}$$

After choosing the optimal path, the source node forwards the data securely using CSTA algorithm to the destination through the optimally selected path. Fig. 3 depicts the flowchart of optimal route selection.

By including these messages, LOADng protocol executes the RREQ packets for route discovery between the source and destination. Unfortunately, during the process of route discovery, the control packets such as RREQs as well as RREPs are misused by the third parties. To overcome this issue, the control packets should be encrypted during the route discovery process. To achieve this goal, CSTA is used in the propose approach. The following section describes the operation of CSTA algorithm.

3.4 Cyclic Shift Transposition Algorithm (CSTA) Based Optimal LOADng

CSTA is a keyless cryptography as it does not depend on any key management system. And it focuses on achieving the protocol design of data ownership. Moreover, most of the existing encryption algorithms uses transposition, substitution and product cipher in their implementation, but CSTA approach only derives transposition and substitution without product cipher with respect to input data. The proposed CSTA algorithm mainly consists of two stages, namely, encryption and decryption.

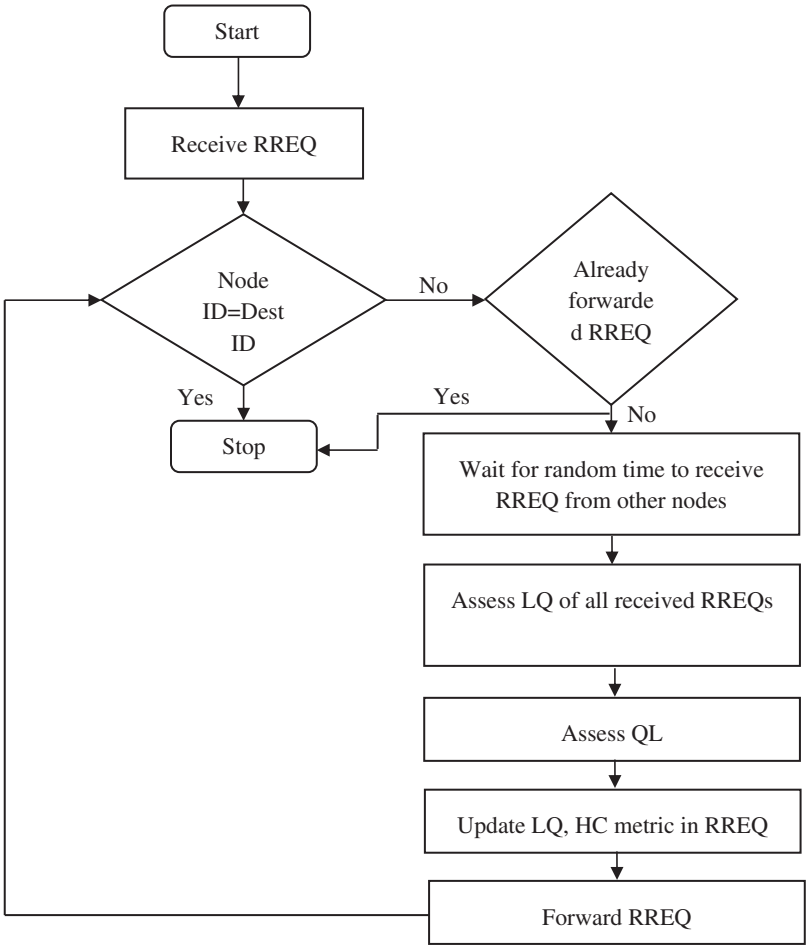

Figure 3: Flowchart of optimal route selection

3.4.1 Encryption Process

The process of encryption is applied to convert the original information into ciphertext. Fig. 4 depicts the encryption process. As depicted in the figure, the proposed CSTA performs the partitioning and shifting function, such as row transition, column transition, primary diagonal transformation, and secondary diagonal transformation.

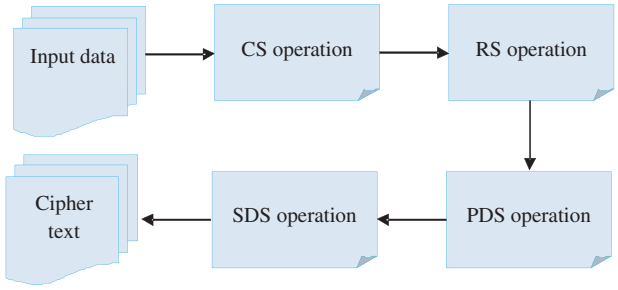

Figure 4: CSTA encryption process

Step 1: To start the process, the input data or control messages of LOADng protocol denoted as D_iD_i is partitioned into M words or characters. Then the partitioned M words are converted into $N \times N$ matrix format. Here, N varies depending upon the size of the input data. The input plaintext is eventually scattered into rows and columns for $N \times N$ matrix as given in Eq. (6).

$$D = \begin{pmatrix} M_{00} & M_{01} & M_{02} & \ldots & M_{0n} \\ M_{10} & M_{11} & M_{12} & \ldots & M_{1n} \\ \ldots & & & & \\ M_{n0} & M_{n1} & M_{n2} & \ldots & M_{nn} \end{pmatrix} \tag{6}$$

where M_{00} represent the 1st element of the original data D, M_{01} represent the 2nd element of the original data, likewise M_{nn} represent the last element of the original data.

Step 2: In this step, operation of shift column (SC) is performed on the $N \times N$ matrix. In a SC, each element of the $N \times N$ matrix is converted based on the order representation. Each column rotates cyclically from bottom to top. The SC computation is defined in Eq. (7).

$$D'_{SC} = D_{((R+shift\ (C,N_b)\%N_b),C)} \tag{7}$$

where, R represent the row number, C represent the column number, N_b represent the block size and D'_{SC} refer the encryption output of SC operation. Here, $shift\,(C, N_b)$ depend only on the the certain number of order of elements that are to be shifted and the mod denotes the arithmetic function.

Step 3: Then, operation of shift row (SR) is used. Here, each row is rotated from right to left based on the certain number of order. The SR computation is defined in Eq. (8).

$$D'_{SR} = D_{R,\ (((shift(R,N_b)+C)\%N_b))} \tag{8}$$

where, R refer the Row number, C refer the column number, N_b refer the block size, D'_{SR} defined as encryption process in row shift operation.

Step 4*:* Then, we perform primary diagonal shift (PDS) operation. In PDS operation, the diagonal elements are shifted from top to right bottom based on the shift order configuration. The function of PDS is defined as follows

$$D'_{PDS} = D_{(R+Shift\,(R,N_b)\%N_b),\,(C+shift\,(R,N_b)\%N_b)} \tag{9}$$

In the above equation, for each row, the shifting position of the diagonal elements can be represented as 'R'.

Step 5: Then, we perform secondary diagonal shift (SDS) operation. In SDS operation, the diagonal element of $N \times N$ matrices is shifted from left bottom to right top based on the certain number of order. The function can be written as follows;

$$D'_{SDS} = D_{(R+Shift\,(R,N_b)\%N_b),\,(((C+N_b)-shift(R,N_b))\%N_b)} \tag{10}$$

Step 6: Finally, we obtain the encrypted output which is given in Eq. (11).

$$E = C\left[D'_{SDS}\ \ \left(D'_{PDS}\ \ \left(D'_{SR}\ \ \left(D'_{SC}\ \ (D)\right)\right)\right)\right] \tag{11}$$

where; C represents the cyclic process of encryption. D'_{SC}, D'_{SR}, D'_{PDS} and D'_{SDS} denote the output of SC, SR, PDS and SDS respectively.

Step 7: After that, we convert the output to ASCII format to get the encrypted text.

3.4.2 Decryption Process

Fig. 5 depicts the process of CSTA decryption. The process of decryption is the reverse of the process of encryption. After receiving the encrypted control messages, the neighbour node decrypts the data by doing the operations like shifting and partition. The process of decryption is described as follows:

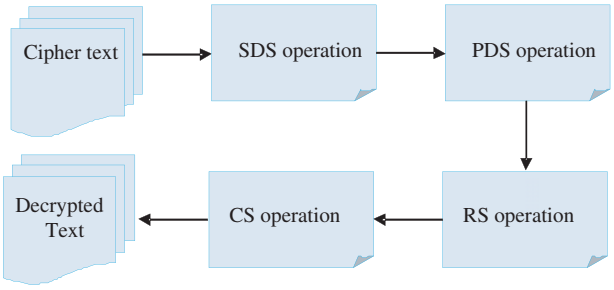

Figure 5: CSTA decryption process

Step 1: At first, the encrypted control message is converted into ASCII format.

Step 2: Using shift order configuration, SDS operation is applied to the attained matrix.

Step 3: Then, PDS operation is applied as per the shift order configuration.

Step 4: SR operation is initiated on the output matrix of PDS operation.

Step 5: Then, SC operation is again applied as per shift order configuration.

Step 6: At final, the decrypted message is obtained.

Due to the operation of CSTA algorithm, the control packets are exchanged between the source and destination securely during the process of route discovery. This CSTA algorithm secures the transmitting data from the attackers. After exchanging the control messages, optimal path selection takes place between source and destination depending on the data LQI, HC and QL which are included in the control messages.

4 Results and Discussion

The effectiveness of the proposed approach is analyzed in this section. The proposed approach is implemented using the MATLAB simulator Version 20a. Tab. 1 shows the simulation setting of the proposed scheme. In this implementation, 250 nodes are used. Data packets are sent at a rate of 500 kbps and the size of each packet is 512 bytes. For routing the data packet, the LOADng routing protocol is used. Simulation time for each approach is 100 s. For secure transmission of control packets and data, CSTA algorithm is applied.

Table 1: Simulation parameters configuration

Parameters	Assumptions
Number of nodes	50–250
MAC	802.11

(Continued)

Table 1: Continued

Parameters	Assumptions
Rate	500 Kbps
Traffic source	CBR
Simulation time	100 s
Propagation	TwoRayGround
Packet size	512 byte
Antenna	Omni antenna
Routing protocol	LOADng
Cryptography	CSTA

Performance Analysis

In this section, the performance of the CSTA based LOADng (CSTA-SO-LOADng) is analyzed in terms of energy efficiency, delivery ratio, control overhead, throughput, encryption time and decryption time. Besides, the performance of CSTA-SO-LOADng is compared with that of the RSA-SO-LOADng and LOADng.

Performance Analysis In Terms Of Varying Number of Nodes

In this section, the performance metrics of the CSTA-SO-LOADng is analyzed in terms of varying number of nodes 50, 100, 150, 200 and 250. The comparison of delivery ratio of different schemes is illustrated in Fig. 6. Because of the optimal path selection with the routing metrics, delivery ratio of CSTA-SO-LOADng is improved. In comparison to RSA-LOADng and LOADng without encryption, delivery ratio of CSTA-SO-LOADng is increased by 6.8% and 23% respectively.

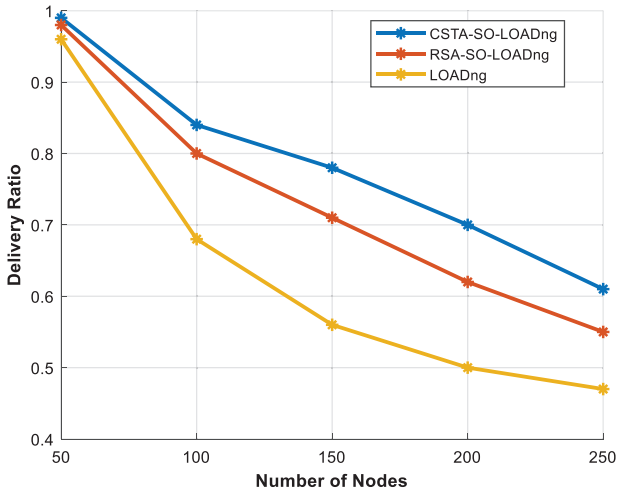

Figure 6: No. of nodes *vs.* delivery ratio

Fig. 7 depicts the analysis of the control overhead of CSTA-SO-LOADng. Because of the inclusion of routing metrics in the control packets, the control overhead of CSTA-SO-LOADng is increased than the existing models. Namely, control overhead of CSTA-SO-LOADng is decreased by 9.7% and 21% than that of RSA-SO-LOADng and LOADng. The comparison of throughput of the different

schemes is shown in Fig. 8. As depicted in the figure, compared to RSA-SO-LOADng and LOADng, throughput of CSTA-SO-LOADng is increased by 9.2% and 39% respectively. Fig. 9 depicts the comparison of delay of different schemes. As the computational complexity of CSTA algorithm is less, delay of CSTA-SO-LOADng is reduced by 22% and 30% than that of RSA-SO-LOADng and LOADng.

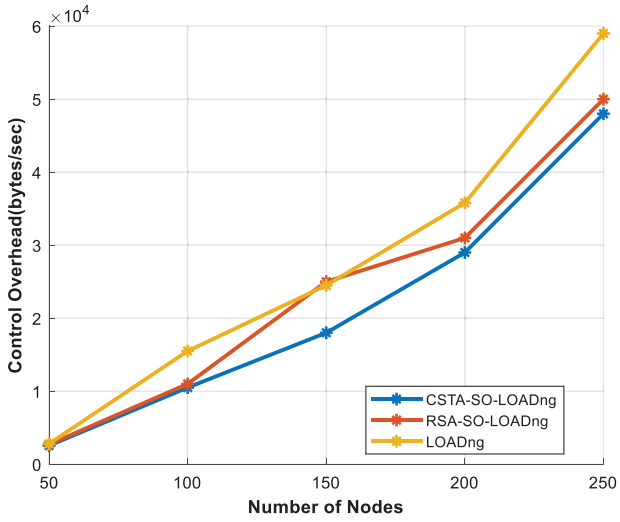

Figure 7: No. of nodes *vs.* control overhead

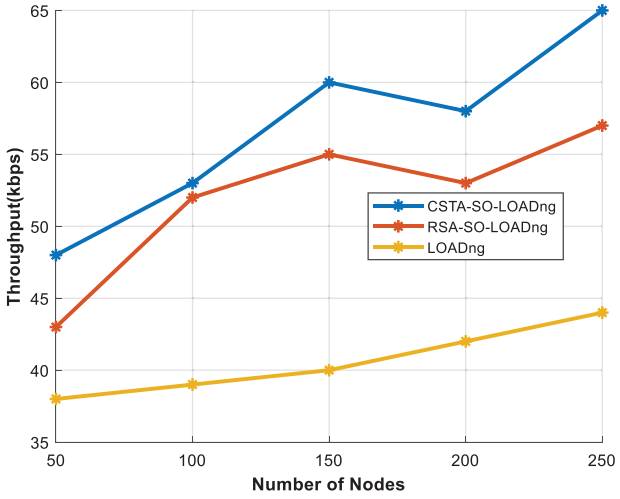

Figure 8: No. of nodes *vs.* throughput

Security strength of the proposed CSTA-SO-LOADng is analysed in terms of encryption time and decryption time. Fig. 10 illustrates the evaluation of encryption time and decryption time of CSTA-SO-LOADng. As the computational complexity of CSTA is better than the RSA, encryption time of CSTA-SO-LOADng is decreased by 77% than that of RSA-SO-LOADng. As depicted in the figure, compared to RSA-SO-LOADng, decryption time of CSTA-SO-LOADng is deceased by 73%.

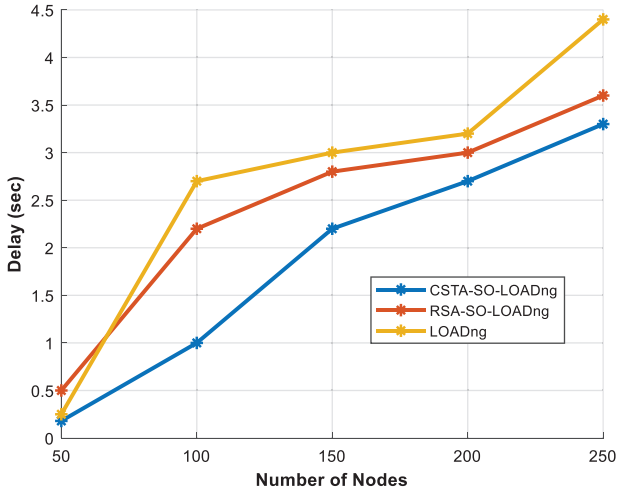

Figure 9: No. of nodes *vs.* delay

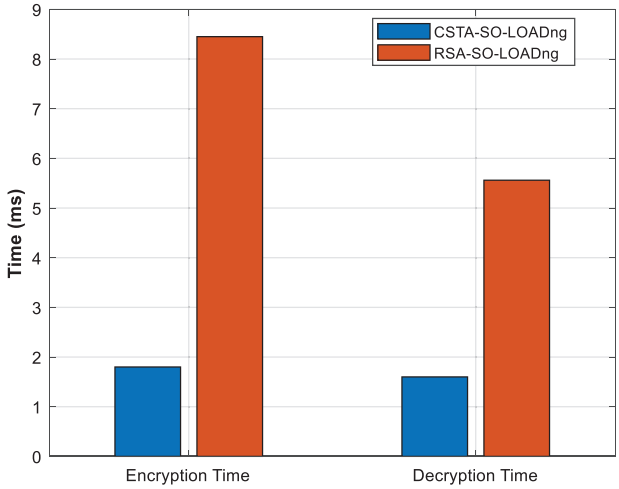

Figure 10: Encryption time and decryption time

5 Conclusion

To enhance the security of IoT, a secure LOADng routing protocol with routing metrics has been presented in this paper. The control packets of LOADng protocol such as RREQ and RREP are encrypted using CSTA algorithm. These control packets contained the routing metrics such as LQI, QL and hop-count. By using these routing metrics, optimal path has been selected between the source and destination. Through the optimal path the data has been forwarded securely using CSTA algorithm. The performance of the proposed CSTA-LOADng has been evaluated in terms of delivery ratio, throughput, control overhead, encryption time and decryption time. Besides, the performance of CSTA-LOADng has been compared with that of RSA-LOADng. As depicted in the results, the encryption and decryption time of CSTA-LOADng are decreased by 53% and 46% respectively.

Acknowledgement: The author with a deep sense of gratitude would thank the supervisor for his guidance and constant support rendered during this research.

Funding Statement: The authors received no specific funding for this study.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] S. Chaudhary, R. Johari, R. Bhatia, K. Gupta and A. Bhatnagar, "Craiot: Concept, review and application (s) of iot," in *2019 4th Int. Conf. on Internet of Things: Smart Innovation and Usages (Iot-SIU)*, Ghaziabad, India, IEEE, pp. 1–4, 2019.

[2] J. Fox, A. Donnellan and L. Doumen, "The deployment of an IoT network infrastructure, as a localised regional service," in *2019 IEEE 5th World Forum on Internet of Things (WF-IoT)*, Limerick, Ireland, IEEE, pp. 319–324, 2019.

[3] K. Agarwal, A. Agarwal and G. Misra, "Review and performance analysis on wireless smart home and home automation using IoT," in *2019 Third Int. Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*, Palladam, India, IEEE, pp. 629–633, 2019.

[4] J. Mannar, S. Kanimozhi, M. Dhivya and T. Parameswaran, "Smart scheduling on cloud for IoT-based sprinkler irrigation," *International Journal of Pervasive Computing and Communications*, vol. 17, no. 1, pp. 3–19, 2021.

[5] S. Rehan and R. Singh, "Industrial and home automation, control, safety and security system using bolt IoT platform," in *2020 Int. Conf. on Smart Electronics and Communication (ICOSEC)*, Trichy, India, IEEE, pp. 787–793, 2020.

[6] R. Angeline, T. Gaurav, P. Rampuriya and S. Dey, "Supermarket automation with chatbot and face recognition using IoT and AI," in *2018 3rd Int. Conf. on Communication and Electronics Systems (ICCES)*, Coimbatore, India, IEEE, pp. 1183–1186, 2018.

[7] F. Fernandez and G. C. Pallis, "Opportunities and challenges of the internet of things for healthcare: Systems engineering perspective," in *2014 4th Int. Conf. on Wireless Mobile Communication and Healthcare-Transforming Healthcare Through Innovations in Mobile and Wireless Technologies (MOBIHEALTH)*, Athens, Greece, IEEE, pp. 263–266, 2014.

[8] S. Sujanthi and S. N. Kalyani, "SecDL: QoS-aware secure deep learning approach for dynamic cluster-based routing in WSN assisted IoT," *Wireless Personal Communications*, vol. 114, no. 3, pp. 2135–2169, 2020.

[9] S. M. Mujeeb, R. P. Sam and K. Madhavi, "Adaptive EHTARA: An energy-efficient and trust aware secure routing algorithm for big data classification in IoT network," *Wireless Personal Communications*, vol. 121, no. 1, pp. 621–646, 2021.

[10] S. Sahraoui and N. Henni, "SAMP-RPL: Secure and adaptive multipath RPL for enhanced security and reliability in heterogeneous IoT-connected low power and lossy networks," *Journal of Ambient Intelligence and Humanized Computing*, pp. 1–21, 2021.

[11] J. V. V. Sobral, J. J. P. C. Rodrigues, K. Saleem, J. F. de Paz and J. M. Corchado, "A composite routing metric for wireless sensor networks in AAL-IoT," in *2016 9th IFIP Wireless and Mobile Networking Conf. (WMNC)*, Colmar, France, pp. 168–173, 2016.

[12] V. Kavitha, "Privacy preserving using multi-hop dynamic clustering routing protocol and elliptic curve cryptosystem for WSN in IoT environment," *Peer-to-Peer Networking and Applications*, vol. 14, no. 2, pp. 821–836, 2021.

[13] D. K. Shende and S. S. Sonavane, "CrowWhale-ETR: CrowWhale optimization algorithm for energy and trust aware multicast routing in WSN for IoT applications," *Wireless Networks*, vol. 26, no. 6, pp. 4011–4029, 2020.

[14] J. K. Jain, "Secure and energy-efficient route adjustment model for internet of things," *Wireless Personal Communications*, vol. 108, no. 1, pp. 633–657, 2019.

[15] D. Kothandaraman, S. N. Korra, A. Balasundaram and S. M. Kumar, "Sequence number based secure routing algorithm for IoT networks," in *Materials Today: Proc.*, pp. 1–7, 2021.
[16] B. D. Deebak and F. Al-Turjman, "A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks," *Ad Hoc Networks*, vol. 97, pp. 1–34, 2020.
[17] D. Sasidharan and L. Jacob, "Design of composite routing metrics in LOADng routing protocol for IoT applications," in *ICN: The Sixteenth Int. Conf. on Networks*, vol. 2017, pp. 1–153, 2017.
[18] V. Tilwari, A. Bani-Bakr, F. Qamar, M. N. Hindia, D. N. K. Jayakody *et al.,* "Mobility and queue length aware routing approach for network stability and load balancing in MANET," in *2021 Int. Conf. on Electrical Engineering and Informatics (ICEEI)*, Kuala Terengganu, Malaysia, pp. 1–5, 2021.
[19] L. Jie, Y. Pan, S. Ni and F. Wang, "A hybrid reliable routing algorithm based on LQI and PRR in industrial wireless networks," *Wireless Communications and Mobile Computing*, vol. 2021, pp. 1–15, 2021.
[20] A. S. Charles and P. Kalavathi, "A reliable link quality-based RPL routing for internet of things," *Soft Computing*, vol. 26, no. 1, pp. 123–135, 2022.
[21] B. R. Bapu and L. C. Gowd, "Link quality based opportunistic routing algorithm for QOS: Aware wireless sensor networks security," *Wireless Personal Communications*, vol. 97, no. 1, pp. 1563–1578, 2017.