AN EFFICIENT SECURE CRYPTOGRAPHY SCHEME FOR NEW ML-BASED RPL ROUTING PROTOCOL IN MOBILE IOT ENVIRONMENT

Kishore Golla[1] and S. PallamSetty[2]

[1]Research Scholar, Dept. of CSE, Andhra University, Visakhapatnam, Andhra Pradesh, India
[2]Dept. of CSE, Andhra University, Visakhapatnam, Andhra Pradesh, India

ABSTRACT

Internet of Things (IoT) offers reliable and seamless communication for the heterogeneous dynamic low-power and lossy network (LLNs). To perform effective routing in IoT communication, LLN Routing Protocol (RPL) is developed for the tiny nodes to establish connection by using deflaut objective functions: OF0, MRHOF, for which resources are constraints like battery power, computation capacity, memory communication link impacts on varying traffic scenarios in terms of QoS metrics like packet delivery ratio, delay, secure communication channel. At present, conventional Internet of Things (IoT) are having secure communication channels issue for transmission of data between nodes. To withstand those issues, it is necessary to balance resource constraints of nodes in the network. In this paper, we developed a security algorithm for IoT networks with RPL routing. Initially, the constructed network in corporates optimization-based deep learning (reinforcement learning) for route establishment in IoT. Upon the establishment of the route, the ClonQlearn based security algorithm is implemented for improving security which is based onaECC scheme for encryption and decryption of data. The proposed security technique incorporates reinforcement learning-based ClonQlearnintegrated with ECC (ClonQlearn+ECC) for random key generation. The proposed ClonQlearn+ECCexhibits secure data transmission with improved network performance when compared with the earlier works in simulation. The performance of network expressed that the proposed ClonQlearn+ECC increased the PDR of approximately 8% - 10%, throughput of 7% - 13%, end-to-end delay of 5% - 10% and power consumption variation of 3% - 7%.

KEYWORDS

ECC, security, Optimal path, Routing, Reinforcement learning.

1. INTRODUCTION

Internet of Things (IoT) is a network that connects some significant number of objects where an object is characterized as (1) physical or virtual, (2) decisions and functioning are independent, (3) capable of communicating with other devices, (4) operates interactively since integrated with heterogeneous devices, and (5) flexibly interacts with objects for any type of service anytime and anywhere[1]. However, recently, from a technical point of view, IoT fuses several networking technologies like Radio Frequency Identification (RFID), Wireless Sensor Networks (WSN), Vehicular Ad hoc Networks (VANET), Smart ad hoc networks, WIrelessFIdelity Networks (WIFI), Wireless Personal Area Network (WPAN), and many others; thus IoT is a vast heterogeneous network [2].

In present era, there is tremendous growth in usage of IoT devices by deploying them in unmanned areas for surveliance with mobility feature. Numerous heterogeneous IoT devices are

DOI: 10.5121/ijnsa.2022.14201

connected for various applications like monitoring environment and health, automated buildings, smart cities, and the military applications. These make life very easier and smart as well as automated. But threats are introduced and open a cyber-space for hackers. Attacks like Mirai-botnet and smart-tv hack [3] motivate the researchers to develop security and safety mechanisms. Devices lack security and thus expose the users to numerous attacks [4]. Frequently, these attacks cause financial loss or sometimes even worse [5]. These malicious devices are identified by performing attestation at a lowcost. However, a cost-effective naive device-to-device remote attestation relates to high attestation time and communication overhead challenges. Moreover, there exists no scalability for systems with a group of dynamic topology devices like ITS and robots utilized for oil and gas search. Therefore, novel, scalable and reliable attestation solutions are required for secure network operations of IoT devices [6] [7]. The devices connected to the infrastructure of IoT are attacked by the attackers where the protection mechanism is easily broken [8]; these circumstances motivated the researchers to develop various protecting methods which provided network security [9]. Additionally, IoT security needs to provide scalable features with consideration of the complexity and computational overhead. Thus, the design of a secure and lightweight scale is compatible to withstand demand in the dynamic network [10].

In this research, a probability-based attestation scheme (ClonQlearn+ECC) is developed for improving security in IoT communication. In the proposed CLONQLEARN+ECC scheme, the node creates its attestation and transmits it within the network. After, the creation of attestation the proposed ClonQlearn - ECC estimates the various path and perform data transmission within the network. Based on the tickle time if the node replies with appropriate attestation, then data is transmitted in the network else transmission will be terminated. Simulation results illustrated that the proposed ClonQlearn+ECC exhibits significant performance than existing techniques. The organization of the paper is as follows. In Section II, the related works of the proposed rouing protocol is discussed. In Section III, system model is described. In Section IV, the concept of optimal path selection and the encryption process based on clonQlearn ECC are explained. In Section V, Genetic Qlearn based trickle timer estimation is illustrated. Section VI shows the performance analysis of proposed work and comparison with other earlier works as well as in the Section VII the conclusion of the paper is given.

2. RELATED WORKS

Security is a major concern for all the layer of the IoT architecture in the case of research point of view. Hence, security is considered as a major conctraint for increasing the application design and eeffective usage of the IoT network [11]. In [12] reviewed the generic approach for increasing the challenges associated with twofold manner. The primary challenge is associated with the estimation of identification of principles with generic techniques compared with IoT protocol. The construction of an IoT attack describes the performance of the fundamental protocol stack. However, those approaches explored similar attackswith consideration of various IoT protocols under three categories. The consideration of IoT attacks under three categories such as packet transmitted environment under cryptographic attacks either passive and active environment. The protocol focused on the attacks such as MITM, flooding, Sybil, and wormhole attacks and consideration of attack in whole system sinkhole and selective forwarding attacks.

In [13] presented efficient solutions to address the challenges associated with changes in IoT security. In this scenario, the evaluation is based on consideration of security associated with the lifecycle of IoT products, taxonomy for IoT lifecycle, phases of the lifecycle for estimation of changes to derive security solutions, and evaluation of issues with computation of changes in the network. Similarly, [14] aimed to evaluate the taxonomy thoroughly for classification with the estimation of energy-saving techniqueswith conventional constrained networks in IoT. It is based on the consideration of changes in the taxonomy for improved security aspects.

In [15] comparatively examined the IoT attacks with the estimation of different solutions in the network. primarily, the network security architecture is developed with consideration of 3 layers of 6LOWPAN such as perception layer, network layer, and application layer for low power lossy networks. Every layer on the network is performed with hierarchical architecture with improved security in terms of authenticity, data acquisition, confidentiality, and integrity. In [16] developed a technique Survivability Aware Channel Allocation (SACA) integrated with a fuzzy-based mechanism. The proposed SACA is involved in the estimation of network components for effective access in the channel. The proposed SACA comprises of cross-layer design with computation of upper layer with the design of medium access technique. Simulation results expressed that the proposed model exhibits increased network throughput and PDR with a reliable network. In [17] constructed a protocol termed as Cluster-Tree based Energy-Efficient Data Gathering (CTEEDG) to improve the lifetime and performance of the IoT network. The developed CTEEDG uses Fuzzy logic to select Cluster Head (CH) for information gathering in the network. The comparative analysis of results expressed that proposed CTEEDG exhibits superior performance than conventional FAMACROW and DL-LEACH with improved performance 28.81% and 38.28% respectively. Also, the developed model exhibits improved performance with FAMACROW and DL-LEACH energy consumption levels of 29.26% and 49.29% respectively.

In [18] developed a transformation technique for evaluation of K-center problem with formulated multi-objective optimization technique with consideration of multiple constraints. Subsequently, to withstand the vulnerabilities in the security UAV-aided data collection is performed for authority authentication through a lightweight model with a set of specific procedures to enforce data collection by trusted sensors in UAVs with acceptable delay authentication. Finally, through numerical analysis demonstration is performed for evaluation results with efficient performance characteristics.

3. SYSTEM MODEL

The RPL routing protocol is used in our research work WOABC (Multi-Objective RPL) routing model. The basic concentration of this protocol is optimal path selection by calculating the hop count. By calculating the optimal path to certain level the bandwidth of the network is increased and the packet drop is reduced. This protocol achieves minimium overhead and better route maintenance. The packet header of our protocol consists of information such as distance, cost, latency, traffic and network reliability. And the message types are Route Request (RREQ), Route Reply (RREP), Route Errors (ERR), and Hello Message. For optimal path selection and route establishment, whale optimization with encircling prey is used. The information of our routing protocol is based the Directed Acyclic Graph (DAG) as well as the packet distribution is done using trickle algorithms with Destination Oriented Directed Acyclic Graph (DODAG).

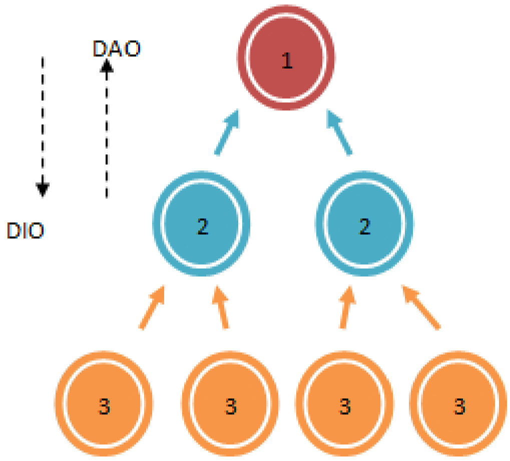

Figure 1. Multi Objective RPL Illustration of DODAG

4. PROPOSED CLONQLEARN - ECC SCHEME

4.1. Construction of Optimal Path

IoT devices are having having limited resources constraints as there is a huge number of applications are developed for monitoring realtime activities like humidity, temperature, smart meters, border surveliance.etc.In all applications, IoT devices are transmitting confidential data, which leads develop effective and lightweight cryptographic systems to protect transmitted data even in mobile environment of IoT nodes. Innovation and implementation of a lightweight cryptographic system face a lot of challenges due to impact on performance metrics of QoS.i.e, throughput, packet delivery ratio, powerconsumption, computation capacity as well as speed of nodes in the network; in addition to the flexibility to implement the lightweight cryptographic system ondifferent kinds IoT devices with atmostdatasecurity.

Existing IoT infrastructures are implemented using RPL protocol for implementation, which is a de-facto routing protocol for these networks. ClonQlearn+ECC design is presented which enables desired functionalities to provide secure communication efficiently. The routing approach with multipath is involved in the identification of alternate paths for each destination node of the network. The transmissionpowerof the nodes in the network involved in the transmission size of data packets needs to have a higher energy level with higher frequency of nodes in the network with more computation capacity.

The steps involved in clonal selection for IoT environment are presented as follows:

Step 1: Initialize the network with the number of nodes, iteration, data transmission distance, and other parameters. Upon the deployment of the network select antigen and generate antibodies in the node which comprises residual energy and memory
Step 2: Calculate the affinity between each node and estimate the highest affinity of every node in the network
Step 3: Clone the distance or link information between the nodes and compute the positive correlation between the nodes of antigen.
Step 4: Performa mutual information transmission between the IoT node generated through cloning and high-affinity values, the lower probability of mutation in the antibodies.
Step 5: Estimate the link condition between the nodes with mutation information with higher affinity from the present set of memory.

Step 6: Randomly elects the new node for the node which reduces the energy and traffic in the remaining set
Step 7: Skip the set 2 involved in iteration with appropriate termination conditions.

It has been observed that the clonal selection algorithm highly concentrated on the link or traffic condition between the nodes. This algorithm involved in the process of cloning and the mutation of the information between the nodes. The node with minimal link traffic is not involved in the data transmission as long as it reaches the highest affinity. In each stage of clonal selection, appropriate memory estimation is performed for computation of the lifetime of each node with the estimation of the threshold.

Node affinity is calculated with test function concerning function values, which is represented in equation (1)

$$Aff_{cs} = f(x_1, x_2, \ldots \ldots x_D) \tag{1}$$

Where, $\{x_i |\, i = 1,2, \ldots \ldots, D\}$ is denoted as characteristics of nodes and the dimensionality of the nodes is denoted as D.

The node affinity concerning antigen and antibody are actively involved in a cloning operation. The increase in the affinity exhibits the higher energy of links for data transmission. The specific cloning formula is denoted in equation (2)

$$Abc = \left\{ ab_{ij} \begin{cases} i \in [0, population\, size - 1] \\ j = \max(1, int\left(\frac{Aff_{cs}+a}{a}\right) * \max clone \end{cases} \right\} \tag{2}$$

In the above equations, the count of antibodies is denoted as $population\, size$. The affinity between the antibodies is denoted as ab_{ij}, the clone number of the population is represented as Aff_{cs} and the clone number of the antibodies is represented as a.

The mutation process involved in the cloning of the antibody or nodes and evaluating the degree of mutation based on the affinity of the nodes. The higher the affinity, the minimal the possibility of the mutation.

The specific variation formula is presented in equation (3)

$$\begin{gathered} ab = \{x_i |\, i = 1,2, \ldots \ldots, D\} \\ x_i = \begin{cases} x_i + random\,(-a, a), random\,(0,1) < e^{-\left(\frac{r*aff}{\max\_aff}\right)} \\ x_i, random\,(0,1) > e^{-\left(\frac{r*aff}{\max\_aff}\right)} \end{cases} \end{gathered} \tag{3}$$

where *r* is the mutation rate, *a* is the variation range, *a* > 0, andmax_affis the maximum affinity of the concentrated antibody.

4.2. Encryption Using ClonQLearn – ECC

Cryptography act as a security scheme for data transmission in the cloud environment. At present there are several network security schemesare available with certain issues, depends on resource constraints of IoT devices, leads to minimizing the network lifetime, as well as decreasing the performance of QoS metrics, which leads to develop attributes-based cryptography for key generation in this paper. The selected cryptography technique is involved in the generation of keys ECC. The propsedElliptical Curve Cryptography includes several points in the plane of Elliptical curve by considering two fixed points existing in the network with consideration of positive points for selecting a public key for applying security for transmission data. The fixed point in the Elliptical is defined as foci that can be separated into branches known as separate calls. The point where two points in Elliptical intersect are utilized for the generation of the secret key in the encryption and decryption techniques to definevertices in Elliptical curve. Elliptical utilizes general equation which is presented in equation (4),

$$X^2\text{-}Dy^2=1 \tag{4}$$

Where D denotes the non-square integer, this is used for the generation of a public key with consideration of coordinates x and y. Some researchers stated that D is also a perfect square.

Consider the convergent point in hyperbole as $h_i/k_i$for selecting an integer at the point of intersection for the generation of the public key. The coordinates value in the Elliptical are utilized for hashing and it will be always integers those are represented as in equation (5):

$$x_k + y_k\sqrt{D} = \pm\left(x_0 + y_0\sqrt{D}\right)^k ; k > 1 \tag{5}$$

The above equation is utilized for performing the generation of public and private keys based on the Elliptical point coordinates in the cloud platform.

4.2.1. Encryption and Decryption using ECC

This research utilizes ECC for the generation of keys for securing files in the cloud. The algorithm utilized for encryption and decryption of ECC keys are presented as follows:

Algorithm 1: The encryption algorithm

```
Input: ECC points in the coordinates
Output: Generated keys H and T
1. Chooses coefficients to define hyperbolic curve $x^2$-$Dy^2$=1 over finite field Fn.
2. Picks a based point G=(x0,y0) with a large order r and this gives us $G^r$=E.
3. Selects an integer m and m<r.
4. Computes B=$G^m$ mod q.
The public keys of the system are formed by (G,B) and can be publicly in an open channel
while the private key of ECC is represented as m.
To encrypt any message w to Alice, Bob does the following:
1. Randomly chooses the secret integer k.
2. Computes H=$G^k$ mod n and T=$B^k$w mod n.
3. Produces the ciphertext (H,T).
4. Sends (H,T) to Alice.
1. Computes R=$H^m$ mod n.
2. Recovers w=T/R mod n.
```

5. Trickle–Timer Estimation with Developed Genetic Q-Learning

Q-learning belongs to the class of reinforcement learning technique in which agents perform the best action through the establishment of a Q-table. In the proposed approach Q-table offers information about the routing table of each node with the selection of preferred destination node for information transmission. In a dynamic network,the optimal selection of the parent with optimal selection policy is done to maintain congestion and link quality. In the proposed model each node x within the network comprises N(x) nodes for computation of communication exchange range. The Q-values of the periodic process is presented in equation (6) as follows:

$$Q_{table}^{new}(x) = Q_{table}^{old}(x) + \alpha\left[S(x) - Q_{table}^{old}(x)\right] \tag{6}$$

In the above equation (6) the present and previous Q-values within the interval is denoted as $Q_{table}^{new}(x)$ and $Q_{table}^{old}(x)$ respectively. The learning rate of the deep learning model is defined as α and the feedback function model is stated as $S(x)$. The duration between the interval is computed with trickle timer as with network deployment Q-values are computed as zero initial values. The routing path between the nodes for data transmission $Q_{table}\,(y)$ between the coordinates x and y. The proposed ClonQlearn concentrated on maintenance of congestion level between the neighboring nodes through the feedback $S(x)$. Through the selection of efficient neighboring nodes, parents can perform the load balancing between the nodes. The routing path for data transmission between the node in position is computed as $BF(x)$, which provides the ratio between present queue length and total size of the queue. The position of the nodes in the network is exponentially computed with the weighted moving average filter calculated with $BF(x)$. To achieve the optimal performance of the network computed with clone selection algorithm in high traffic mode. In those scenarios, the node learns the identification of the parent node for congestion detection and avoidance under minimal traffic scenarios. The nodes elect the optimal path with the computation of node neighbor, link quality, and hopping distance. Thus the $S(x)$ metrics for the RPL routing is defined as follows in equation (7)

$$S(x) = \gamma(x)BF(y) + ETX(x,y) + H(x) \tag{7}$$

Where, in above equation $H(x)$ denoted the DODAG hop-count node in the direction of x, $ETX(x,y)$is the deployment of nodes between x and y. In the RPL routing network the energy $ETX(x,y)$ are data deployment periodically. The deployed periodic information is represented as (8)

$$ETX(x,y) = \frac{\#total\ transmission\ in\ the\ direction\ x\ and\ y}{\#\ successful\ information\ transmission\ in\ both\ x\ and\ y\ direction} \tag{8}$$

In the above equation $\gamma(x)$ for weight control of $BF(y)$ which provides the congestion level between the node in direction x. It lies between the value of $0 \leq BF(x) \leq 1$, the proposed ClonQlearn defines the $\gamma(x)$as in equation (9)

$$\gamma(x) = max\left(\frac{BF(x)}{BF_{th}}, 1 - \frac{BF(x)}{BF_{th}}\right) \tag{9}$$

Where the above equation threshold design parameters are denoted as BF_{th} which compute the congestion on the network. In the congestion scenario $BF(x) \geq BF_{th}, BF(x)$ exhibits the effective impact over the $ETX(x,y)$ and $S(x)$ compared with $BF(x)$. Concerning received feedback $H(x)$ with the updated node value of $Q_{table}\,(x)$ as stated in equation (1). Based on the greedy selection policy neighboring nodes are the value of parent are computed with minimal Q-value of neighbor nodes. The network is subjected to changes in location and mobility of nodes which impacts the routing and load balancing within the network. To estimate the position of nodes in the network the proposed ClonQlearn uses a probability approach for node selection. The probability of nodes is defined as $P_x(y)$ for the node position x with the preferred parent y represented as in equation (10)

$$P_x(y) = 1 - \frac{e^{\frac{Q_x(y)}{\theta}}}{\sum_{k\in N(y)} e^{\frac{Q_x(y)}{\theta}}} \tag{10}$$

In the above equation, exploration parameter determination is represented as $\theta.$ Also, the above equation illustrates the minimal Q-value that is likely to be the preferred parent with a neighboring node that has a high Q-value with minimal probabilistic value. As per the RPL routing protocol, DIO messages are exchanged periodically between the node between nodes based on RANK. In this, the proposed ClonQlean RANK is defined as $H(x)$. In the proposed ClonQlearn implicit $BF(y)$ converted to the RANK value with the transmission of the DIO messages represented as follows in equation (11)

$$RANK^{new}(y) = \gamma(H(y) + 1) + (\gamma - 1)BF(y) \tag{11}$$

Where γ denoted as the positive integer which involved in decoding of $BF(y)$ and $H(y)$ in the numeric field $RANK^{new}$. In this, the value of γ is within the limit of $RANK^{new}(y)$ with its 16-bit boundary range. Specifically, the neighboring node those receives DIO messages extract the two values such as $BF(y)$ and $H(y)$ from the $RANK^{new}(y)$ in equation (12) and (13)

$$BF(y) = \frac{mod(RANK^{new}(y),\gamma)}{\gamma - 1} \tag{12}$$

$$H(y) = \left\lceil \frac{RANK^{new}(y)}{\gamma} \right\rceil - 1 \tag{13}$$

The modular operation is denoted as mod $(RANK^{new}(y), \gamma$). In this proposed ClonQlearn information about the traffic is distributed between the neighboring nodes without any alteration in the DIO messages without any message overhead. The information transmission interval of DIO messages is controlled by the Trickle timer. Conventionally, Trickle Timer reset the interval in the time when the change in topology is detected. In the case of a consistent network scenario, the interval of DIO messages is doubled to the maximal values. Based on those strategies, the nodes may be inaccurate and outdated about the update of the traffic information between nodes. On other hand, frequency modification in the Trickle Timer increases the routing overhead. To balance this, a modified strategy is incorporated in the proposed ClonQlearn.

The trickle timer reset value to I_{min} with the certain number of consecutive losses of queue defined as φ. Specifically, in the minimal LLN queues node are occupied temporarily without any traffic which leads to false positives, which causes an unnecessary overhead of DIO messages. To overcome this, the proposed ClonQlearn uses consecutive loss reset of Trickle timer. Upon the reset of the trickle I_{min} the value of the queue is increased as $\emptyset_0$ as the frequency limit for reset and DIO message overhead scenario.

6. SIMULATION ANALYSIS

In this study, the simulation of a smart IoT sensor is localized to create a highly-secured smart environment. The simulation is done and it illustrates the performance of the proposed ClonQlearn+ECC algorithm. In the simulation the region is constraucted for 200 m *200 m with the topology consists of various number of nodes linke 20, 40, 60 and 80 notes and the number of attacker will increase if the nodes increases. Each and every nodes consists of its buffer size of 50 packets with the packet size of 127 bytes. The initial energy is equally distributed to all the nodes in the network. During the process of communication in the network, the number of attacker nodes may increase according to the topography.

For node deployment the locations are predefined and the transmissions are done according to the time slots. The performance of the network is computed for varying the network environment under 4 scenarios such as small, medium, high, and very high. In table 1 presented a simulation setup for the proposed ClonQlearn+ECC algorithm.

Table 1. Simulation Setup

Parameters	Value
Number of nodes	20,40, 60 and 80
Mote type	skymote
Packet length	100B
Propagation Model	Log – normal
PHY and MAC protocol	IEEE 802.15.4 with CSMA/CA
Time slot	10ms
Trickle Timer X	100ms
Slot length	500 slots
Message	DIO,DAO,DIS,DAO+ACK
Routing Protocol	RPL
Security protocol	ClonQlearn+ECC
RPL Objective Function	WOABC,MRHOF
Network Topology	Random
Simulation Duration	1000s
Network Size	200 meters
Mobility model	Uniform mobility(10m/sec)

The performance of the proposed ClonQlearn+ECCare comparatively examined with conventional RPL-MRHOF and iCPLA - IoT. In table 2 presented about packet delivery function.

Table 2. Comparison of Packet delivery Ratio between default RPL and Proposed Model (%)

Number of Nodes	ClonQlearn+ECC	ClonQlearn	iCPLA [19]	RPL – MRHOF [10]
20	94.56	93.4	92	86
40	92.67	89	87	72
60	88.23	83	63	56
80	84.56	77	46	39

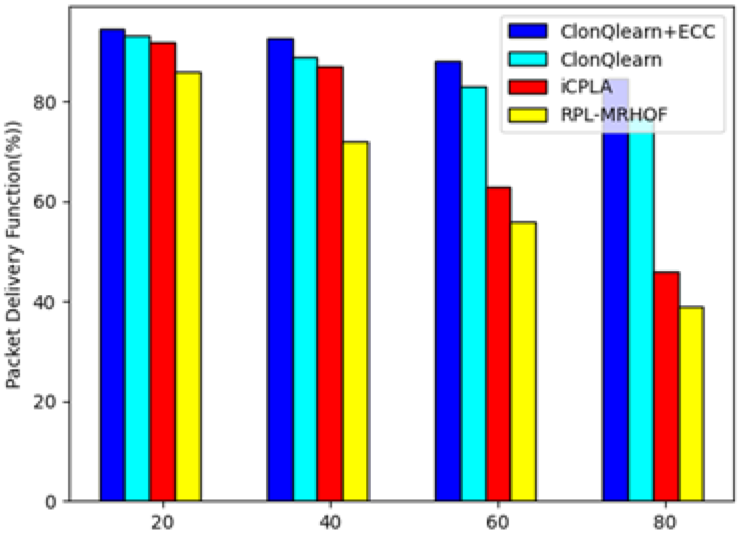

Figure 2. Comparison of PDR values between Default RPL and Proposed RPL with security features

With reference to the results available in graphical comparison of the proposed model with the earlier works in terms of PDR,x-axis represents the number of motes in the network and the y-axis represents the packet delivery ratio (PDR). The experimental reults are obtained for different sizes of network with 20, 40, 60, and 80 nodes under constant area only. The proposed ClonQlearn with ECC process greatly increases the PDF which leads to improving the overall QoS of the network.

Table 3. Avge.End - to End Delay of various methods(in msec)

Number of Nodes	**ClonQlearn + ECC**	**ClonQlearn**	**iCPLA [19]**	**RPL – MRHOF [10]**
20	1.07	1.2	1.4	1.8
40	1.89	2.4	2.8	2.9
60	2.56	3.2	3.6	3.8
80	3.36	3.9	4.3	4.6

The graphical representation of the Avge.E2E delay calculation represents on x-axis contains number of motes in the network along with avge.E2E delay values on y-axis. From these results, it’s understood that our proposed model produces great results in terms of PDR and E2E delay.

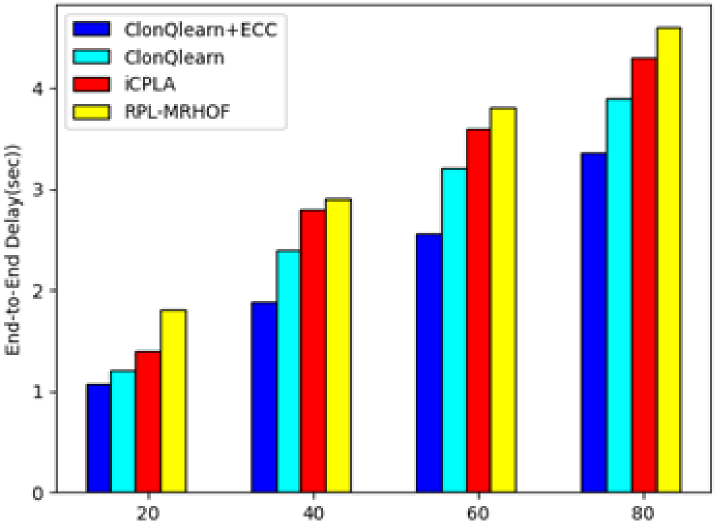

Figure 3. Average End_to_End Delay of proposed techniques

Network power consumption is defined as the energy utilized during the process of communication in the network. The graphical comparison of the proposed ClonQlearn+ECC with ClonQlearn, iCPLA, and RPL–MRHOF is shown in Figure 4and the values are given in table 4. The network power consumption (NPC) is calculated in node sizes of 20, 40, 60, and 80.the obtained results proven that the proposed model plays a significant role to provide a data security by keeping in view of avge network power consumption.

Table 4. Comparison of Network Power Consumption (Mbit/J)

Number of Nodes	ClonQlearn + ECC	ClonQlearn	iCPLA [19]	RPL – MRHOF [10]
20	0.31	0.34	0.38	0.43
40	0.36	0.39	0.43	0.64
60	0.42	0.47	0.54	0.83
80	0.49	0.52	0.63	0.92

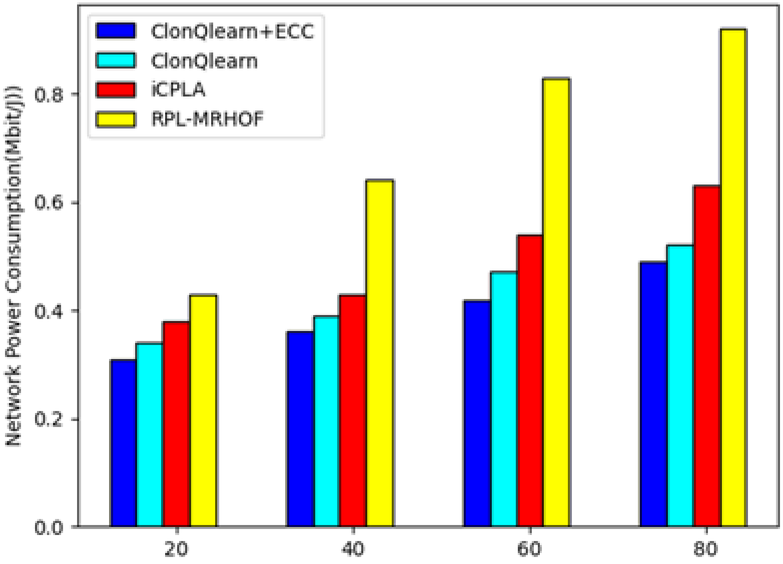

Figure 4. Comparison of NPC

Table 5. Comparison of Throughput (Mbps)

Number of Nodes	ClonQlearn + ECC	ClonQlearn	iCPLA [19]	RPL – MRHOF [10]
20	0.92	0.89	0.83	0.78
40	0.88	0.84	0.76	0.73
60	0.84	0.76	0.69	0.67
80	0.78	0.73	0.64	0.61

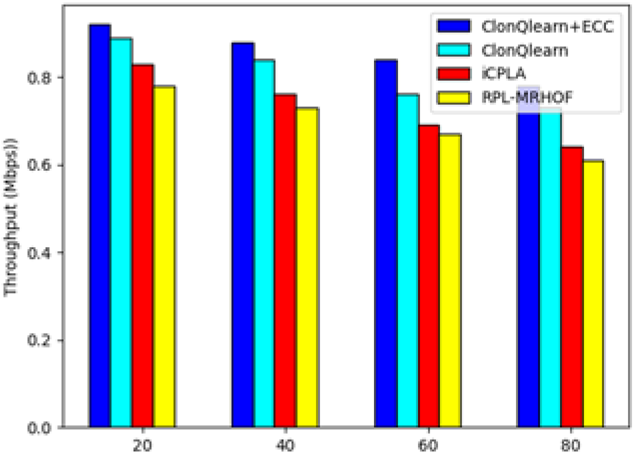

Figure 5. Comparison of Throughput

The comparative examination of throughput in figure 5 expressed that the proposed ClonQlearn+ECCexhibits higher performance than the other technique. The throughput of iCPLA and RPL-MRHOF is minimal where the values are mentioned in the Table 5. From the results it conclude that the proposed ClonQlearn+ECC RPL routing protocol shows the longitivity in network efficiency and it helps the network to increase the overall QoS.

7. CONCLUSION

This paper proposed a ClonQlearn+ECC RPL routing protocol approach for the mitigation of node congestion and the establishment of links between nodes with RPL networks. The proposed technique concentrated on two aspects such as route establishment and security improvement. The proposed method is a Clonal selection algorithm used for establishing secure path by considering resource constraints of mobile motes in the IoT network. In the next stage, Q-learning is applied with feedback function for estimation of congestion level. To improve network security ECC based cryptography technique is adopted for data transmission between nodes. Upon the computation of congestion and traffic in the network RANK metrics are applied with a modified Trickle timer. The performance of the proposed ClonQlearn+ECC achieves effective improvement in the network performance in terms of packet delivery, average delay, power consumption, and throughput with provision of adequate security. In future, the Energy Harvesting technique can be introduced in order to improve the residual energy of the network.

REFERENCES

[1] Srilakshmi, A., Rakkini, J., Sekar, K. R., & Manikandan, R. (2018). A comparative study on Internet of Things (IoT) and its applications in smart agriculture. *Pharmacognosy Journal*, *10*(2).

[2] Samie, F., Bauer, L., & Henkel, J. (2019). From cloud down to things: An overview of machine learning in internet of things. *IEEE Internet of Things Journal*, *6*(3), 4921-4934.

[3] Shadroo, S., & Rahmani, A. M. (2018). Systematic survey of big data and data mining in internet of things. *Computer Networks*, *139*, 19-47.

[4] Accettura, N., Grieco, L. A., Boggia, G., & Camarda, P. (2011, April). Performance analysis of the RPL routing protocol. In *2011 IEEE International Conference on Mechatronics* (pp. 767-772). IEEE.

[5] Saad, L. B., Chauvenet, C., & Tourancheau, B. (2011, September). Simulation of the RPL Routing Protocol for IPv6 Sensor Networks: two cases studies. In *International Conference on Sensor Technologies and Applications SENSORCOMM 2011*. IARIA.

[6] 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.

[7] Tripathi, J., de Oliveira, J. C., & Vasseur, J. P. (2010, March). A performance evaluation study of rpl: Routing protocol for low power and lossy networks. In *2010 44th Annual Conference on Information Sciences and Systems (CISS)* (pp. 1-6). IEEE.

[8] Zhao, M., Ho, I. W. H., & Chong, P. H. J. (2016). An energy-efficient region-based RPL routing protocol for low-power and lossy networks. *IEEE Internet of Things Journal*, *3*(6), 1319-1333.

[9] Gaddour, O., Koubâa, A., Baccour, N., & Abid, M. (2014, May). OF-FL: QoS-aware fuzzy logic objective function for the RPL routing protocol. In *2014 12th International symposium on modeling and optimization in mobile, ad hoc, and wireless networks (WiOpt)* (pp. 365-372). IEEE.

[10] Kim, H. S., Kim, H., Paek, J., & Bahk, S. (2016). Load balancing under heavy traffic in RPL routing protocol for low power and lossy networks. *IEEE Transactions on Mobile Computing*, *16*(4), 964-979.

[11] Djedjig, N., Tandjaoui, D., Medjek, F., & Romdhani, I. (2017, April). New trust metric for the RPL routing protocol. In *2017 8th International Conference on Information and Communication Systems (ICICS)* (pp. 328-335). IEEE.

[12] Xie, H., Zhang, G., Su, D., Wang, P., & Zeng, F. (2014, June). Performance evaluation of RPL routing protocol in 6lowpan. In *2014 IEEE 5th International Conference on Software Engineering and Service Science* (pp. 625-628). IEEE.

[13] Abdel Hakeem, S. A., Hady, A. A., & Kim, H. (2019). RPL routing protocol performance in smart grid applications based wireless sensors: Experimental and simulated analysis. *Electronics*, *8*(2), 186.

[14] Conti, M., Kaliyar, P., Rabbani, M. M., & Ranise, S. (2018, October). SPLIT: A Secure and Scalable RPL routing protocol for Internet of Things. In *2018 14th International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob)* (pp. 1-8). IEEE.

[15] Alvi, S. A., ul Hassan, F., & Mian, A. N. (2017, June). On the energy efficiency and stability of RPL routing protocol. In *2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC)* (pp. 1927-1932). IEEE.

[16] Glissa, G., Rachedi, A., & Meddeb, A. (2016, December). A secure routing protocol based on RPL for Internet of Things. In *2016 IEEE Global Communications Conference (GLOBECOM)* (pp. 1-7). IEEE.

[17] Airehrour, D., Gutierrez, J., & Ray, S. K. (2017, November). A testbed implementation of a trust-aware RPL routing protocol. In *2017 27th International Telecommunication Networks and Applications Conference (ITNAC)* (pp. 1-6). IEEE.

[18] Airehrour, D., Gutierrez, J., & Ray, S. K. (2017). A trust-aware RPL routing protocol to detect blackhole and selective forwarding attacks. *Journal of Telecommunications and the Digital Economy*, *5*(1), 50-69.