International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7034
***Article Received**: 04 April 2023 **Revised:** 29 May 2023 **Accepted:** 10 June 2023*

A Novel Cryptography-Based Multipath Routing Protocol for Wireless Communications

S. Venkatramulu[1,*],V. Chandra Shekar Rao[2] , K. Vinay Kumar[3] , C. Srinivas[4] ,B. Raghuram[5] and Shaik Rasool[6]
[1,2,3,4,5&6]Department of Computer Science and Engineering, Kakatiya Institute of Technology and Science, Warangal.
Corresponding Author: svr.cse@kitsw.ac.in

Abstract

Communication in a heterogeneous, dynamic, low-power, and lossy network is dependable and seamless thanks to Mobile Ad-hoc Networks (MANETs). Low power and Lossy Networks (LLN) Routing Protocol (RPL) has been designed to make MANET routing more efficient. For different types of traffic, RPL routing can experience problems with packet transmission rates and latency. RPL is an optimal routing protocol for low power lossy networks (LLN) having the capacity to establish a path between resource constraints nodes by using standard objective functions: OF0 and MRHOF. The standard objective functions lead to a decrease in the network lifetime due to increasing the computations for establishing routing between nodes in the heterogeneous network (LLN) due to poor decision problems. Currently, conventional Mobile Ad-hoc Network (MANET) is subjected to different security issues. Weathering those storms would help if you struck a good speed-memory-storage equilibrium. This article presents a security algorithm for MANET networks that employ the Rapid Packet Loss (RPL) routing protocol. The constructed network uses optimization-based deep learning reinforcement learning for MANET route creation. An improved network security algorithm is applied after a route has been set up using (ClonQlearn). The suggested method relies on a lightweight encryption scheme that can be used for both encryption and decryption. The suggested security method uses Elliptic-curve cryptography (ClonQlearn+ECC) for a random key generation based on reinforcement learning (ClonQlearn). The simulation study showed that the proposed ClonQlearn+ECC method improved network performance over the status quo. Secure data transmission is demonstrated by the proposed ClonQlearn + ECC, which also improves network speed. The proposed ClonQlearn + ECC increased network efficiency by 8-10% in terms of packet delivery ratio, 7-13% in terms of throughput, 5-10% in terms of end-to-end delay, and 3-7% in terms of power usage variation.

Keywords*:* Lightweight, security, optimal path, routing, reinforcement learning.

I. INTRODUCTION

Objects in a Mobile Ad-hoc Network (MANET) are those that (1) exist in the real world or cyberspace, (2) make their own decisions and perform their tasks, (3) can communicate with other devices, (4) function interactively due to their integration with heterogeneous devices, and (5) can be used to provide any service at any time and in any place [1]. They are, technically speaking. However, MANET is now a vast heterogeneous network [2] due to the integration of various networking technologies such as WSN, RFID, VANET, Wireless Personal Area Networks (WPAN), Smart ad hoc networks, WIreless FIdelity Networks (WIFI), and many others.

MANET has experienced a meteoric expansion in the recent past. Many different types of MANET devices are interconnected for uses as diverse as environmental and health tracking, automated building systems, smart city infrastructure, and military operations. This handle and smarten up daily tasks to a remarkable degree. However, this creates a cyber-space where cybercriminals can operate freely. Researchers are inspired to create security and safety measures in response to attacks like the Mirai botnet and the hacking of smart televisions [3]. Users are vulnerable to various attacks because of the devices' lack of protection [4]. Often, monetary loss or even worse results from these assaults [5]. Attestation can be performed cheaply, allowing for the detection of these malevolent devices. Naive device-to-device remote attestation is cheap but needs help in attestation latency and communication overhead. In addition, there is no scaling for systems that employ a network of dynamic topology tools, such as computers and robots used in oil and gas exploration. Secure MANET network activities necessitate novel, scalable, dependable attestation solutions [6] [7].

Researchers were prompted to create various protection methods that offered network security [8] because attackers target devices linked to the MANET infrastructure, where the protection mechanism can be easily broken [9]. The MANET environment is subjected to other challenges rather than security. In instances, MANET requires an effective security scheme to attain security reliably to incur security in terms of complexity and computational overheads. This

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7034
***Article Received**: 04 April 2023 **Revised:** 29 May 2023 **Accepted:** 10 June 2023*

demands an effective and secure lightweight scheme for a dynamic network environment [10].

In this article, we create a probabilistic attestation scheme (ClonQlearn +ECC) to strengthen the safety of MANET data transmissions. Also, this research utilizes a trust mechanism to route data effectively within the network.

Contribution to the work

- The proposed method incorporates reinforcement learning based (ClonQlearn) integrated with Elliptic-curve cryptography (ClonQlearn+ECC) for random key generation.
- Each node in the suggested model generates its attestation and sends it to other nodes in the network. After the attestation, the proposed method estimates the different paths and carries out data transmission within the network.
- Network data transmission is contingent upon nodes responding to tickle times with proper attestation; otherwise, transmission is halted.
- Finally, a trust mechanism is applied for effective data routing within the network.
- The simulation findings show that the proposed method (ClonQlearn+ECC) significantly outperforms the state-of-the-art methods.

The sections of this document are as follows: The current methods and their related works are discussed in Section 2. The Proposed (ClonQlearn+ECC) scheme is shown in Section 3. Section 4 shows the Q-learning-based Reinforcement algorithm. Simulation results and analysis are shown in section 5. Section 6 provides the conclusion of the work.

II. RELATED WORKS

Due to an initial assumption of responsible conduct among MANET nodes, the security of MANET routing protocols must be considered during protocol development. Additionally, it was desired that the routing methods remain lean and effective. With more and more uses in military and police work, however, security has risen to the forefront as a necessity. Several proposals have been made to improve the security of already-existing protocols and to introduce new, safe routing protocols.

Veeraiah, N et.al [11] proposed a trust-based security model for a MANET environment with a cat slap single-player algorithm (C-SSA). The developed C-SSA model focused on the routing scheme in the MANET environment. Additionally, the developed model comprises fuzzy clustering with the cluster head prediction scheme. The developed scheme estimates the direct, indirect, and recent trust mechanisms with the computation of the trust value. With trust value computation, effective routes in the network are computed with the hybrid protocol and identify the effective route based on throughput, delay, and network connectivity. The developed model concentrated on considering the different attacks in the MANET environment.

A MANET multi-level security scheme with a suitable encoding mechanism was devised by Ahmad, S. J. et al. [12]. For MANET protection, the suggested model combines the Weighted Hex Code Division Method with the Hamming bit. In the MANET setting, the developed scheme employs the security code via cyclic code while also considering the tach hop count via enhanced hamming bits. The MANET's cyclic code is estimated and calculated with each hop count calculation to provide an overall cyclic code evaluation. In a MANET setting, threats are calculated at the application, network, and transport layers. According to the results of the experimental study, the developed scheme significantly increases security in a MANET setting.

Jim, L. E. et al. [13] used the optimization model to develop a MANET security method. The created model utilizes a bio-inspired artificial Immune System Based Algorithm (AISBA) to identify selfish nodes in MANETs. Moreover, the suggested model incorporates Artificial Immune Systems (AIS) into its trust-based framework. The suggested model has a weighted and reliable threshold detection rate of 93.41 per cent. Traditional secured Ad-hoc On-demand Distance Vector (SAODV) displays a detection rate of 86%, and its performance is compared with that of the suggested model. Based on the estimated false-positive probability, the comparative analysis found that the suggested security scheme provides a high level of security.

Khan, B. U. I et al., [14] evaluated the MANET network for real-time data streaming in multimedia data applications. The security analysis is based on the consideration of the security scenario in terms of the secure data packet and the unpredictable characteristics of the attacker. The security in the MANET environment is evaluated in a sophisticated environment with an evaluation of the attacker nodes. With the optimization model, each node identity is estimated based on considering the attack environment through modelling statistics. Additionally, the developed model uses a game theory model considering multiple-collision attacker evaluation. The optimization model comprises the modelling strategies for computation of the node capability with computation of the attacker nodes.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7034
***Article Received**: 04 April 2023 **Revised:** 29 May 2023 **Accepted:** 10 June 2023*

The analysis of the results stated that the proposed optimization-based game theory model exhibits significant performance in detecting and classifying attacks in MANET.

In 2022, Ahmed Ahmed [15] set up a SA for the IoT networks used by WSNs. At first, the constructed network utilizes deep learning techniques associated with path optimization. After that, the ClonQlearn-related SA will be implemented to beef up the security already established by an ECC algorithm that mixes data encryption and decryption, primarily for generating random keys. ClonQlearn, built on reinforcement learning, is integrated with ECC (ClonQlearn+ECC) in the proposed security method. This proposed method correlates well with prior works in simulation, demonstrating secure data transfer and improved network execution.

An efficient and secure routing algorithm for the MANET environment was developed by Veeraiah, N., et al. [16]. A trust-based secure energy efficiency model is created using a hybrid algorithm to improve MANET security. Multi-path routing in a MANET setting is a key component of the created algorithm based on the cat slap single-player algorithm (C-SSA). Considering the trust mechanism, a fuzzy clustering scheme is developed and used to create the clustering. The constructed routing strategy considers throughput, delay, and connectivity as it computes network routes using a multi-hop and hybrid routing method. The built C-SSA has a throughput of 0.74bps, a packet delivery rate of 0.99%, and a detection rate of 90% with a minimum energy consumption of 0.11m joules. The suggested C-SSA performs admirably for the packet-dropping attack in a MANET setting.

Srilakshmi, U et al., [17] developed a Genetic Algorithm for Hill Climbing (GAHC) with optimal routing in the MANET environment. The clustering in the MANET network is performed with the Improved fuzzy with C-means clustering scheme to compute the density and energy level of the nodes in the MANET environment. Through computation of the threshold energy level of the nodes, prediction of the network is performed for aggregation of the optimal route in the network. The proposed GAHC is evaluated based on connection, latency, and throughput estimation. The developed scheme exhibits a minimal energy level of 0.10m joules and a delay time value of 0.004 msec. The suggested GAHC also displays a detection rate of 91%, a packet delivery ratio of 89%, and a throughput value of 0.85bps. In cases of selective packet-dropping attacks, the suggested scheme performs admirably.

Simpson, S. V., and Nagarajan, G [18] created a Secure method for the IoT-MANET setting. Smart city Environment by Accusation-based List management (Secure SEAL) describes the developed model, which includes investigating a cooperative assault at the network's periphery. To create a reliable environment and lessen security threats in MANET-IoT networks, we use a fuzzy-grained technique to evaluate nodes in the IoT environment during a coordinated attack. The end-device performance in the MANET environment is the focus of the fuzzy method to identify malicious entities enabled by edge computing. The experimental evaluation showed that the created method significantly reduces network latency and bandwidth consumption. In addition, the IoT devices are removed from the MANET network using the developed scheme. According to the experimental evaluation results, the MANET significantly boosts efficacy by 90%. This section serves as a synopsis of the entire literary search.

Active Routing and Security Protocol [19] was created by Tu, J. et al. for use in MANETs. An active-routing authentication scheme is a term used to describe the suggested model. (AAS). The focus of the developed method for identifying malicious nodes in MANET was on assessing forwarding attacks, false routing attacks, route spoofing attacks, and byzantine attacks. An increased packet delivery rate of 33.9% in detecting the malicious node is demonstrated by experimental analysis of the suggested AAS scheme. However, the average network duration for collision attacks is 1.6, and 79.2% of the time is spent detecting malicious nodes. Sowjanya developed a lightweight Ciphertext Policy-Attribute Based Encryption, K. et al. [20]. (CP-ABE). In order to encrypt and decrypt data, the team created lightweight key management that incorporated the escrow problem. Elliptical Curve Cryptography (ECC) is used to lessen the load on the network during decryption in the suggested key management mechanism. The summary of the literature is shown in Table 1.

Bondada P. [21] proposes a secure, low-energy routing algorithm that relies on shared cryptographic keys. Two nodes, the Calculator Key (CK) and the Distribution Key (DK), are used with asymmetric key encryption. (DK). Keys are generated, validated, and disseminated between these two hubs. Consequently, the computation required to generate the private keys by other nodes is eliminated. These nodes are chosen based on low energy use and high confidence scores. More energy is wasted because, in most current routing algorithms, every node must generate and disperse its secret keys. As an added note, security holes should appear if even a single server is breached. The integrity of the network as a whole is not endangered if nodes apart from the CK and DK are compromised.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7034
***Article Received**: 04 April 2023 **Revised:** 29 May 2023 **Accepted:** 10 June 2023*

Extensive experiments are conducted while considering the current and suggested protocols. Analyses of the suggested protocol's performance show that it is superior to competing protocols.

III. PROPOSED (ClonQlearn+ECC) SCHEME

To improve the security in the MANET environment, propose the multipath routing method based on reinforcement learning.RPL routing with OFO and MRHOF integrated with reinforcement learning. The distance between the node's hope count is computed and estimated in the reinforcement learning energy as the path transmits the secure data transmission. We used Clonal optimization with ECC cryptography to provide secure routing. However, ECC is subjected to higher computation and complexity due to random fields. To overcome these drawbacks, using a clonal algorithm to select points in the curve effectively increases security and minimizes complexity. Once done, routing is performed using a trickle timer for effective routing and security. Figure 1 shows the proposed method architecture diagram.

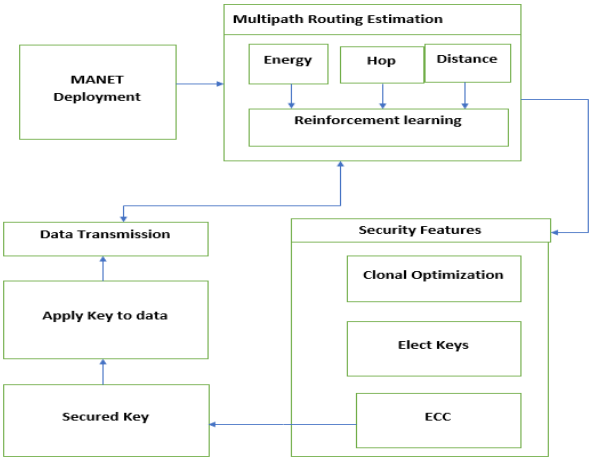

Figure 1. Proposed method architecture diagram

3.1 Conventional Objective Functions in RPL routing

The Routing Protocol for Low-Power and Lossy Networks is characterized by distance vector proactive routing with topology destination-oriented directed acyclic graph construction. RPL is the standard Internet algorithm version (IPv6) routing algorithm in an IoT setting. It is used to create a topology in the shape of a tree by considering several optimization procedures. IoT's node-forming network is referred to as 6LoWPAN. Regarding Internet-based open protocols in 6LoWPAN. However, the RPL routing protocol suffers from increased packet loss for limited power and lossy networks. As a result, there will be constraints on network longevity, an abundance of power sources, and dependability. The Objective Function-based routing route of a DODAG is calculated in RPL. Metrics for transportation, objective function optimization, and other uses form the basis of the OF. The traditional OF is based on two classes, including Objective Function Zero (OF0) and Minimum Rank Hysteresis Objective Function (MRHOF) [20]. (IETF). While MRHOF uses the minimal hop count to find the best route, both OF0 and MRHOF use route optimization based on the Expected Transmission Count (ETX).

Metrics like the number of hops estimated (multiplicative, additive, minimum, maximum), connection quality, node energy, and other similar factors are considered by OF in the DODAG. The design method considers three factors: i) the node's network operation, ii) the objective functions, and iii) the message options. The suggested WOABC considers the node energy (NE), the hop count (HC), and the distance between nodes as additional aspects. (D). SDIS, SDIO, SDAO, SDAO-ACK, and CC are not considered in this article because they are rarely used. RPL routing relies on the computation of prefix information, Route information, and Target Descriptors based on the message choices [12]. The developed RPL OF0 employs a compute rank technique to determine route rank for node metrics. This article implements the RPL routing in the NS3 environment using the ns3::rpl4dc::Routing Protocol and ns3::Ipv6RoutingProtocol packages, respectively, for OF0 and MRHOF. Table 1 shows the operation frequency (OF) used by the 6LoWPAN for RPL routing. Figure 2 illustrates OF route selection.

Table 1. Characteristics of Objective Function

Objective Function	File Name	Control Messages
OF0	ns3::rpl4dc::Routing Protocol	ns3::Icmpv6Header
MRHOF	ns3::Ipv6RoutingProtocol	IcmpvOptionHeader

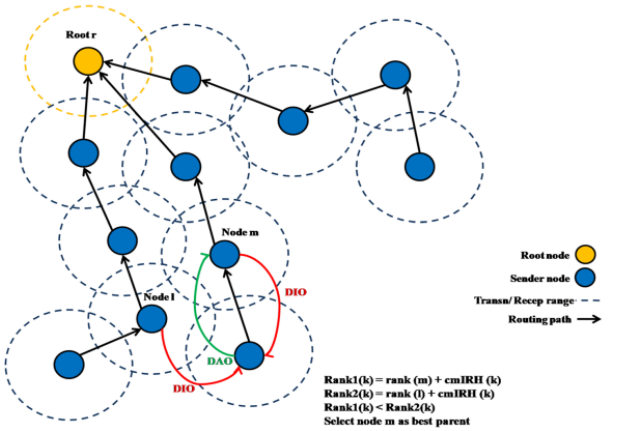

Figure 2. Path Selection with OF

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7034
Article Received: 04 April 2023 Revised: 29 May 2023 Accepted: 10 June 2023

3.2 Developed Clonal Selection Algorithm

In 2002, De Castro and Von Zuben [15] developed a biological-inspired artificial immunology model based on a clonal selection algorithm for combinatorial optimization. Also, the developed model performance is based on optimizing the multimodal principle. The procedures for clone selection in an Internet of Things setting are as follows:

Step 1: Set the network's initial conditions, including the number of nodes, number of iterations, distance of data transfer, and other variables. Select antigens and produce antibodies in the node, including residual and memory cells, following network implementation.

Step 2: Estimate the greatest affinity of each node in the network by calculating the affinities between them.

Step 3: Positive association between antigen nodes can be calculated by copying their respective distance or link information.

Step 4: The less likely an antibody will undergo a mutation due to duplication, the more information can be transmitted between the Internet of Things nodes.

Step 5: Extrapolate the conditions under which the nodes with more specific mutation information are linked from the data at hand.

Step 6: Select a replacement node randomly to minimize the residual set's energy and network traffic.

Step 7: If the iteration requirements are met, set 2 can be skipped.

Researchers found that the clonal selection method cared a lot about the connectivity and traffic levels between nodes. Cloning and modification of data between nodes are central to this process. As long as the data hits the node with the highest affinity, it does not matter whether the least active link belongs to that node. Memory estimates are made at each clonal selection step so that the expected lifetime of each node can be calculated and a threshold estimated.

3.2.1 Affinity Calculation

For convenience, we can express the computation of node affinity as an equation (1) considering function values in terms of the test function.

$$Aff_{cs} = f(x_1, x_2, \dots \dots x_D) \quad (1)$$

Where Node characteristics are indicated by $\{x_i | \, i = 1,2, \dots \dots, \}$ D and node dimensionality is represented by D.

3.2.2 Cloning Method

Antigen and antibody binding at the node level play an integral role in cloning. A greater affinity indicates more energetic connections for data transfer. Equation 2 represents the precise cloning algorithm.

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

Population size is represented by the number of antibodies in the preceding formulae. Each antibody pair's affinity is indicated by ab_ij, and the population's clone number by Aff_cs.

3.2.3 Variation Method

The mutation process includes both the replication of the antibody or nodes and the assessment of the degree of change based on the affinity of the nodes. The lower the likelihood of mutation, the greater the affinity.

The equation gives the formula for the particular variation. (3)

$$ab = \{x_i | \, i = 1,2, \dots \dots, D\}$$

$$x_i = \begin{cases} x_i + random\,(-a, a), random\,(0,1) < e^{-\left(\frac{r*aff}{\max\_aff}\right)} \\ x_i, random\,(0,1) > e^{-\left(\frac{r*aff}{\max\_aff}\right)} \end{cases} \quad (3)$$

where *r* is denoted as the mutation rate, the variation range is represented as *a*, and the maximum affinity of the antibody is denoted as $a > 0$.

IV. Q-learning-based Reinforcement algorithm

The analysis considers traditional LLN mode in IoT applications such as industrial automation. In the developed model, the sensor nodes are distributed as LLN through the DODAG. The established DODAG provides connections based on private IP-based or Public Internet connections. The nodes use the communication link of IEEE 802.15.4 for route establishment between each node and use RPL for route construction.

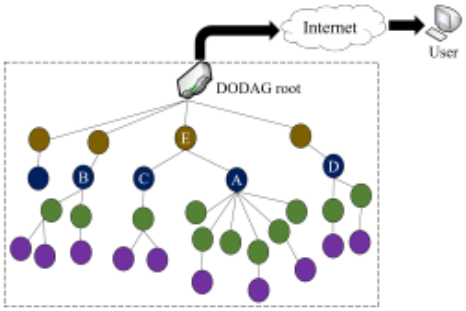

Figure 3. RPL model

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7034
***Article Received**: 04 April 2023 **Revised:** 29 May 2023 **Accepted:** 10 June 2023*

Figure 3 presents the RPL routing-based data transmission in the MANET environment. Through the constructed model, varying the number of nodes' performance of the proposed model is computed.

4.1 Optimal Path Design

MANET devices are subjected to limited resource utilization with data transmission for confidentiality and information security with an appropriate lightweight cryptographic system. The performance needs to be evaluated in speed, power consumption and size for flexible information. The MANET devices are implemented in different platforms but fail to provide appropriate data security.

Currently, the de facto routing protocol for MANETs is the RPL protocol, which is applied in existing MANET infrastructures. In this article, we present a design for (ClonQlearn+ECC) that allows the desired functionalities to provide secure communication in a time-effective manner. The multipath routing strategy requires discovering a backup path to every network node's final destination. As the number of nodes in a network increases, so does the energy expense of transmitting data between them.

Following is a breakdown of how clonal selection works in a MANET setting:

Step 1: Set the network's initial conditions, including the number of nodes, number of iterations, distance of data transfer, and other variables. After implementing the network, select antigens and make antibodies in the node containing residual and memory cells.

Step 2: Determine the strongest connections between each component in the network and make an educated guess as to how strongly they are connected.

Step 3: Positive association between antigen nodes can be calculated by copying their respective distance or link information.

Step 4: Due to high-affinity cloning and reduced mutation rates in the antibodies, MANET nodes can exchange information with one another.

Step 5: Extrapolate the conditions under which the nodes with more specific mutation information are linked from the data at hand.

Step 6: Select a replacement node randomly to minimize the residual set's energy and network traffic.

Step 7: If the iteration requirements are met, set 2 can be skipped.

Researchers found that the clonal selection method greatly concerned the connectivity and traffic levels between nodes. Cloning and modification of data between nodes are central to this process. As long as the data hits the node with the highest affinity, it does not matter whether the least active link belongs to that node. Memory estimates are made at each clonal selection step so that the expected lifetime of each node can be calculated and a threshold estimated.

Equation 4 represents the computation of node affinity using the test function regarding function values.

$$Aff_{cs} = f(x_1, x_2, \dots \dots x_D) \tag{4}$$

Where Node traits are represented by $\{x_i | \ i = 1,2, \dots \dots ,\}$ D and node dimensionality is represented by D.

Antigen and antibody binding at the node level play an integral role in cloning. A greater affinity indicates more energetic connections for data transfer. Equation 5 represents the precise cloning algorithm.

$$Abc = \left\{ ab_{ij} \begin{cases} i \in [0, population\ size - 1] \\ j = \max(1, int\left(\frac{Aff_{cs}+a}{a}\right) * \max clone \end{cases} \right\} \tag{5}$$

The number of antibodies is represented by $population\ size$ in the preceding formulae. Antibody binding affinity is represented as ab_{ij}, population clone count denoted by the symbol Aff_{cs} and the clone number of the antibodies.

The replication of the antibody or nodes and the evaluation of the degree of mutation based on the affinity of the nodes constitutes the mutation process. The lower the likelihood of mutation, the greater the affinity.

Equation 6 provides the formula for the particular variation.

$$ab = \{x_i | \ i = 1,2, \dots \dots , D\}$$

$$x_i = \begin{cases} x_i + random\ (-a, a), random\ (0,1) < e^{-\left(\frac{r*aff}{\max\_aff}\right)} \\ x_i, random\ (0,1) > \ e^{-\left(\frac{r*aff}{\max\_aff}\right)} \end{cases} \tag{6}$$

Where r is the mutation rate, a is the variation range, $a > 0$, and the concentrated antibody's maximum affinity.

4.2 Encryption Using (ClonQlearn + ECC)

Data transmission in the cloud relies on cryptography as a protection mechanism. This study set out to create attributes-based cryptography for a key generation because a number of current security schemes are vulnerable to specific threats. Key creation using the ECC cryptographic method was chosen. This Elliptical idea

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7034
***Article Received**: 04 April 2023 **Revised:** 29 May 2023 **Accepted:** 10 June 2023*

considers several positive points on an Elliptical plane between two fixed nodes in the network to choose a public key for cryptography. Elliptical fixed points, or foci, are divisible into smaller points of focus or distinct calls as the security parameters comprise the domain-specific parameters in the elliptic curve with the public and system parameters estimation. Here, the CS has collaborated with the KGC to estimate random numbers $a_i \in Z_q^*$ with attribute authorization $i \in \omega$. In this, ω is denoted as the authorized attributes set $PP = \{a_1, a_2, a_3, \ldots\ldots, a_n\}$, i = 1 to m and $i \in \omega$.

In the ECC setup, the master secret key is generated $k \in Z * q$ based on the ECC in which the public key is computed as $PP_{KGC} = k.G$i.e., $\{MK_{KGC} = k, PP_{KGC} = k.G\}$.

CS Setup: The master secret key is elected based on $c \in Z * q$, and the public key is estimated as $PP_{CS} = c.G.$; $\{MK_{CS} = c, PP_{CS} = c.G\}$. In this, the output phase public parameters are stated as $params = \{PP, P_{KGS}, PP_{CS}\}$

Even though the intersection of two Ellipsoidal points is not a vertex, it is still used to generate the hidden key in the encryption and decryption processes. Equation 7 shows the basic equation used by the elliptical.

$$X^2\text{-}Dy^2=1 \quad (7)$$

Where D is a non-square number, it generates a public key considering the given x and y coordinates. One or more studies have claimed that D is also a perfect cube.

To generate a public key, use the hi/ki convergent point of two hyperbolas as the number. Elliptical coordinate values are always written as integers for hashing purposes, as shown in equation 8.

$$x_k + y_k\sqrt{D} = \pm\left(x_0 + y_0\sqrt{D}\right)^k; k > 1 \quad (8)$$

The above equation is used in the cloud to generate public and private passwords based on the coordinates of elliptical points.

4.2.1 Encryption and Decryption using ECC

In this study, we show an algorithm for encrypting and decrypting ECC keys, which we use to generate keys for securing cloud-stored data.

Algorithm 1: The encryption algorithm

Input: ECC points in the coordinates

Output: Generated keys H and T

1. Select the coefficients in the hyperbolic curve in the finite field x^2-Dy^2=1 for Fn.

2. Compute the points G=(x0,y0) for the higher order r represented as G^r=E.

3. Estimate the integer value between m and m<r

4. Compute the value in the ECC range of $B=G^m$ mod q.

The framed public key is represented as (G, B). Those are available in the public channel with the ECC private key denoted as m.

The encryption of the message is evaluated in the MANET environment

1. Randomly select the secret integer k.
2. Evaluate the $H=G^k$ mod n and $T=B^k w$ mod n
3. Generate the cypher text *(H, T).*
4. *Compute the value $R=H^m$ mod n.*
5. *Recover w=T/R mod n*

4.3 Trickle–timer estimation with developed genetic Q-learning

As a reinforcement learning method, Q-learning helps agents take the most beneficial course of action by creating a "Q-table" [23]. Each node's routing table and the node chosen as the most preferred data recipient are available via Q-table in the suggested method. In order to sustain congestion and link quality in a dynamic network, the learning objectives are adjusted for the optimal selection of the parent with an optimal selection policy. According to the suggested model, the number of network nodes needed to calculate the communication exchange range is N(x). Equation 9 gives the following presentation of the Q-values of the cyclic process:

$$Q_{table}^{new}(x) = Q_{table}^{old}(x) + \alpha\left[S(x) - Q_{table}^{old}(x)\right] \quad (9)$$

In the above equation (9), the present and previous Q-values within the interval are denoted as $Q_{table}^{new}(x)$ and $Q_{table}^{old}(x)$, respectively. The model's feedback function, S, is specified as the learning rate and is the mathematical formula for deep learning. (x). As in network distribution, the interval is calculated using a trickle timer. The Q-values used in calculations begin at zero. The route between x and y in the Q_(table) (y) that nodes take to send and receive data. The proposed (ClonQlearn) aimed to keep congestion levels consistent among nearby nodes using input from those nodes. (x). Parents can distribute workloads between their children's nodes by choosing productive neighbours. The routing path for data transmission between the positioned nodes can be determined by calculating BF(x), which provides the ratio between the current and total queue

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7034
***Article Received**: 04 April 2023 **Revised:** 29 May 2023 **Accepted:** 10 June 2023*

lengths. A weighted moving average filter is computed using BF, and its exponential calculation is applied to the network component positions. In order to compute the best possible network efficiency under heavy load, clone selection is used. To identify and avoid congestion in such low-traffic situations, a node learns the identifier of its parent node. The nodes determine the best route by weighing neighbouring nodes, link strength, and hopping distance. Equation 10 defines the S(x) measures used in RPL routing.

$$S(x) = \gamma(x)BF(y) + ETX(x,y) + H(x) \quad (10)$$

When H(x) above depicts the DODAG hop-count node in the direction of x, then ETX(x,y) indicates the placement of nodes between x and y. Energy ETX(x,y) info is broadcast periodically throughout the RPL routing system. Equation 11 depicts the distributed periodic data.

$$ETX(x,y) = \frac{\#total\ transmission\ in\ the\ direction\ x\ and\ y}{\#\ successful\ information\ transmission\ in\ both\ x\ and\ y\ direction} \quad (11)$$

The overcrowding between nodes in direction x is given by the weighted sum of BF(y) in the above equation. The proposed ClonQlearn specifies γ(x) as equation 12, where x is a real number between 0 and BF(x)-1.

$$\gamma(x) = max\left(\frac{BF(x)}{BF_{th}}, 1 - \frac{BF(x)}{BF_{th}}\right) \quad (12)$$

The above equation threshold design parameters are denoted as BF_{th}, which computes 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). The parent node's value is calculated using its neighbours' minimal Q-value, according to a greedy selection strategy. Routing and load balancing within the network are affected by the position and mobility of nodes. The suggested method (ClonQlearn) takes a probabilistic stance in selecting candidate nodes from the network to estimate their locations. As shown in equation 13, a node's probability is denoted by P_x (y), where y is the favoured parent.

$$P_x(y) = 1 - \frac{e^{\frac{Q_x(y)}{\theta}}}{\sum_{k\in N(y)} e^{\frac{Q_x(y)}{\theta}}} \quad (13)$$

The determination of experimental parameters is denoted by the aforementioned equation. The above equation also shows the minimal Q-value that is the most probable parent of a node with a high Q-value and a low probability of being the parent of the node in question. According to the RPL routing protocol, RANK-based DIO messages are regularly passed from node to node. Here, we define (ClonQlearn) RANK as H.(x). Equation 14 shows how the implicit BF(y) is converted to the RANK value during DIO message transmission in the suggested (ClonQlearn) method.

$$RANK^{new}(y) = \gamma(H(y) + 1) + (\gamma - 1)BF(y) \quad (14)$$

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 (15) and (16)

$$BF(y) = \frac{mod(RANK^{new}(y),\gamma)}{\gamma - 1} \quad (15)$$

$$H(y) = \left[\frac{RANK^{new}(y)}{\gamma}\right] - 1 \quad (16)$$

The symbol for the modular procedure is "mod." (). This suggested method (ClonQlearn) uses existing DIO messages without modification to disseminate traffic data to nearby nodes. The Trickle timer regulates the frequency with which DIO communications are sent and received. Typically, a Trickle Timer would restart the timer after sensing a structure shift. DIO communication intervals are maximized under the assumption of a reliable network. The nodes' understanding of when to update traffic data between themselves may be incorrect and out-of-date if they follow such approaches. However, the suggested solution takes into account the increased routing overhead caused by the Trickle Timer's frequency modification.

After a predetermined amount of queue losses, denoted by, the trickle timer will reset to I_min. In the case of the minimal LLN, false positives arise when a node is briefly occupied without any traffic, leading to an unnecessary overhead of DIO messages. The suggested method (ClonQlearn) gets around this problem by resetting the Trickle timer after each successive loss. The queue's value is incremented by _0 as the upper bound for the reset and DIO message overhead situation whenever the trickle I_min is reset.

V. SIMULATION ANALYSIS

This research uses a localized sensor simulation of a smart MANET to produce a smart setting with the highest possible level of security. There are a total of 30 motes across this terrain, and approximately 3–4 of them are hostile. The topology of the network affects how many attacker motes there will be during the communication procedure. Motes are deployed at predetermined places, and transmissions are

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7034
***Article Received**: 04 April 2023 **Revised:** 29 May 2023 **Accepted:** 10 June 2023*

scheduled at regular intervals. Four different situations, including low, medium, high, and very high traffic loads, are used to calculate the network's performance. It is shown in table 2 how the suggested (ClonQlearn+ECC) algorithm would run in a simulation environment.

Table 2. Simulation Setup

Parameters	Value
PHY and MAC protocol	IEEE 802.15.4 with CSMA/CA
Packet length	100B
Propagation Model	Log – normal
Message	DIO
Time slot	10ms
Network Size	20,40, 60 and 80
Slot length	500 slots
Trickle Timer X	100ms
α	0.3
BF_{th}	0.5
γ	100
$\emptyset_0$	2
I_{min}	3s

Packet delivery Function (%)

The performance of the proposed (ClonQlearn+ECC) is comparatively examined with Secure SEAL and C-SSA - MANET. In table 3 presented about packet delivery function.

Table 3. Comparison of Packet delivery Function (%)

Number of Nodes	(ClonQlearn+ECC)	(ClonQlearn)	C-SSA [16]	Secure SEAL [18]
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

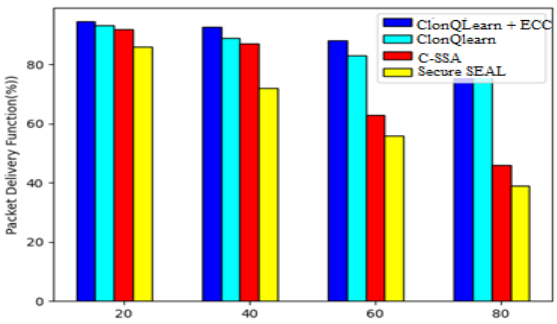

Figure 4. Comparison of PDF

Figure 4 is a bar chart contrasting the proposed model's packet distribution function (PDF) with that of prior works; the x-axis shows the total number of modes in the network, and the y-axis shows the PDF as a percentage. The PDF is calculated using a time period of 20, 40, 60, or 80 nodes. At the outset of the game, the learning automata play a crucial role in protecting ETX from external threats. Table 3 shows how this procedure improves the network's total QoS by significantly increasing the PDF.

End - to End Delay (in sec)

The node value in the network is estimated based on the computation of the delay values in the network. The table 4 shows the end-to-end delay of the proposed method.

Table 4. Comparison of End - to End Delay (in sec)

Number of Nodes	(ClonQlearn + ECC)	(ClonQlearn)	C-SSA [16]	Secure SEAL [18]
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

In figure 5 the computed End-to-end delay measured for the MANET environment is presented. Figure 4 and table 4 provide a visual and numerical comparison of the suggested (ClonQlearn +ECC) method to its predecessor (ClonQlearn), as well as to C-SSA and Secure SEAL. Network latency is measured in increments of 20 nodes, 40 nodes, 60 nodes, and 80 nodes. From the simulation results, the proposed method (ClonQlearn +ECC) provides a minimum delay of 3.36 msec when compared to (ClonQlearn) is 3.9 msec,C-SSA is 4.3 msec and Secure SEAL is 4.6 msec. The proposed (ClonQlearn+ECC) exhibits minimal delay compared with the conventional technique.

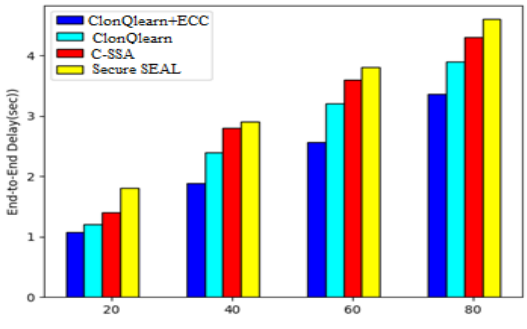

Figure 5. Comparison of End-to-End Delay

Network power consumption (Mbit/J)

Power consumption in a network is the amount of electricity used for data transmission. Figure 6 and table 5 demonstrate

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7034
***Article Received**: 04 April 2023 **Revised:** 29 May 2023 **Accepted:** 10 June 2023*

a graphical comparison of the proposed (ClonQlearn +ECC) to (ClonQlearn), C-SSA, and Secure SEAL, respectively. Node counts of 20, 40, 60, and 80 are used to determine the total network power usage (NPC). Early on, the biological system is seen utilizing the learning automata to enhance ETX's functionality. The network is currently prepared to deal with its inherent improbabilities. When compared to earlier models, the process significantly aids in decreasing the network's power consumption. Another way in which whale optimization helps save power is by decreasing network latency, or the extra work done by the system when sending and receiving data. The values and graph show that our suggested model performs well in comparison to the previous works.

Table 5. Comparison of Network Power Consumption (Mbit/J)

Number of Nodes	(ClonQlearn + ECC)	(ClonQlearn)	C-SSA [16]	Secure SEAL [18]
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

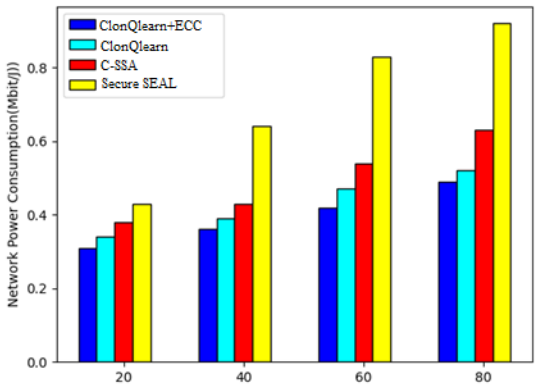

Figure 6. Comparison of NPC

Throughput (Mbps)

The network throughput is the quantity of data that can be sent in a given length of time. Table 6 provides numerical numbers, and Figure 7 provides a visual comparison of the proposed (ClonQlearn +ECC) to (ClonQlearn), C-SSA, and Secure SEAL. Node counts of 20, 40, 60, and 80 are used to determine the total network power usage (NPC).In comparison to (ClonQlearn) (0.73 Mbps), (C-SSA) (0.64 Mbps), and (Secure SEAL) (0.61 Mbps), the suggested method (ClonQlearn +ECC) offers maximum throughput of 0.78 Mbps in the simulations.

Table 6. Comparison of Throughput (Mbps)

Number of Nodes	(ClonQlearn + ECC)	(ClonQlearn)	C-SSA [16]	Secure SEAL [18]
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

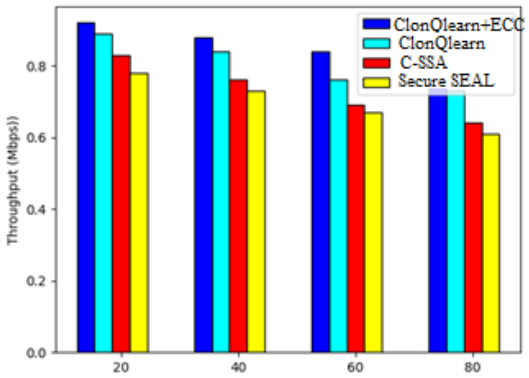

Figure 7. Comparison of Throughput

Throughput comparisons showed that the suggested ClonQlearn + ECC method outperforms the competing method. C-SSA and Secure SEAL both have lower throughput than the suggested ClonQlearn + ECC.

5.1 Security Features

The security features considered for analysis of the proposed (ClonQlearn + ECC) are evaluated with consideration of the security features. In table 7, the security features of the proposed (ClonQlearn + ECC) for analysis is presented.

Table 7. Security Features in (ClonQlearn + ECC)

Scheme	Key – escrow	Collusion Attack	Pairing – Free	Key Authority	ECC based	Provable Secured
GHZ [2]	Yes	Yes	No	Yes	No	Yes
J [3]	Yes	Yes	No	Yes	No	No
HZ [4]	No	No	Yes	No	No	Yes
XZY [5]	No	No	Yes	No	Yes	Yes
SCH [8]	No	Yes	Yes	No	Yes	Yes
Proposed (ClonQlearn + ECC)	Yes	Yes	Yes	Yes	Yes	Yes

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7034
***Article Received**: 04 April 2023 **Revised:** 29 May 2023 **Accepted:** 10 June 2023*

Table 7 presents the security features extraction for the processing of the cryptographic key management. The performance of the proposed (ClonQlearn + ECC) is comparatively examined with the bilinear pairing operations. Also, the existing scenario comprises the key-escrow problem through a lightweight CP-ABE scheme. The comparative analysis expressed that the proposed (ClonQlearn + ECC) approach uses the semi-trusted key authorities to achieve the key-escrow features.

5.2 Computation Overhead

As explained computation overhead comprises the sequence of operations that need to be performed in the encryption, decryption, key generation, and so on. The estimated balance comprises the bilinear pairing, exponential, point-has, and scalar multiplication based on the point. Additionally, it comprises other operations such as arithmetic and logical terms.

To perform authorization ECC-based operations for groups of the bilinear group

$\times G1 \rightarrow G2$ with basic modular operations. Table 8 presented the ECC-based modular operations for estimation of attributed scalar multiplications. As in the ECC-based technique, scalar multiplication is considered an effective parameter for the estimation of computation overhead. The attribute based ECC scheme is involved in the processing of the ECC scalar points with multiplication. The approaches with minimal computation overhead are effective for IoT-based healthcare data analysis. Table 8 shows overhead information.

Table 8. Computation Overhead

Scheme	Initialization	Encryption	Key generation	Decryption	Total
GHZ [20]	$P + 2E \approx 24S$	$P + (3 + l)E \approx 46S$	$(10 + 4u)E \approx 60S$	$3P \approx 60S$	190S
J [20]	$P + 3E \approx 26S$	$P + (3 + l)E \approx 46S$	$(4 + 2u)E \approx 28S$	$3P \approx 60S$	160S
XZY [20]	$(n + 1)S \approx 31S$	$(l + 1)S \approx 11S$	-	$(u + 1)S \approx 6S$	48S
SCH [20]	$(n + 1)S \approx 31S$	$(3l + 1)S \approx 31S$	-	$(3 + u)S \approx 8S$	70S
Proposed (ClonQlearn + ECC)	4S	$(4 + l)S \approx 12S$	8S	$(2 + u)S \approx 7S$	31S

(l = count of the access tree's terminal leaves, u = characteristics of the recipient, n = sum of all the data points that make up the system); $n = 30$, $l = 10$, $u = 5$. S stands for the scalar sum of points in the ECC system.

The computation of the scalar points in the ECC attributes the process of encryption and decryption is evaluated for the processing time. The examination is based on the consideration of the total number of computations overhead in the system. The estimation expressed that the proposed (ClonQlearn + ECC) technique exhibits minimal scalar operations compared with existing techniques. The cryptographic and encryption process exhibits significant performance compared with the existing technique in terms of the improved overall network performance. The performance of the cryptograph ad authorization is evaluated with the machine learning-based classifier model for processing the collected healthcare data. The (ClonQlearn + ECC) is involved in the computation of the healthcare data processing scenario based on the consideration of different key sizes. The evaluation is based on the consideration of healthcare data for processing. In figure 8 presented the under different attack scenario for varying medical dataset the performance is estimated.

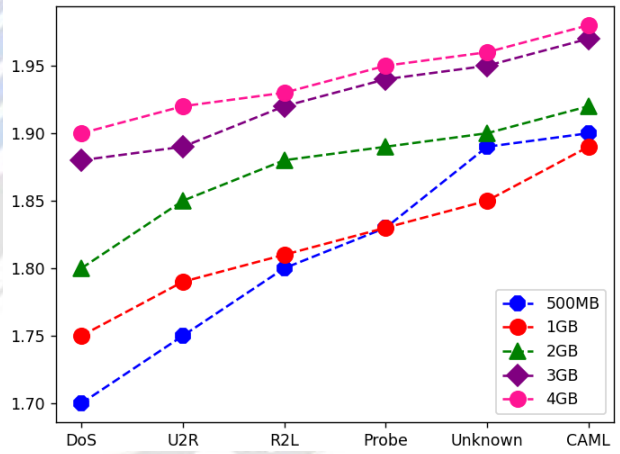

Figure 8. Comparison of different attack

The analysis of the results expressed that the proposed (ClonQlearn + ECC) evaluates the healthcare data for the varying file sizes. The healthcare data files sizes are varying from the size of 500MB to 4GB. Under different attack scenarios also the proposed (ClonQlearn + ECC) model exhibits superior performance. The comparative analysis of the proposed (ClonQlearn + ECC) with the consideration of sensitivity and specificity data expressed that the proposed (ClonQlearn + ECC) based regression classifier performance is effective compared with the conventional classifiers such as SVM, RF, and DT.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7034
***Article Received**: 04 April 2023 **Revised:** 29 May 2023 **Accepted:** 10 June 2023*

VI. Conclusion

With the goal of relieving node congestion and facilitating communication between RPL nodes, this article proposes a (ClonQlearn + ECC) RPL routing protocol approach. The suggested method prioritized route establishment and security enhancement. Clonal selection algorithm is used to optimize the network nodes in the suggested method. The next step involves estimating the degree of congestion by employing Q-learning with a feedback function. Data transfer between nodes in a secure network is now routinely encrypted using the Elliptic Curve Cryptography (ECC) method. Congestion and traffic in the network are calculated, and then RANK metrics are implemented using a modified Trickle timer. Improvements in packet delivery, average delay, power consumption, and throughput are achieved, and sufficient security is provided, thanks to the use of the suggested (ClonQlearn + ECC) solution.

References

[1] Srilakshmi, A., Rakkini, J., Sekar, K. R., & Manikandan, R. (2018). A comparative study on Mobile Ad-hoc Network (MANET) 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 Mobile Ad-hoc Network. IEEE Mobile Ad-hoc Network Journal, 6(3), 4921-4934.

[3] Shadroo, S., & Rahmani, A. M. (2018). Systematic survey of big data and data mining in Mobile Ad-hoc Network. 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] Dr. S. Praveen Chakkravarthy. (2020). Smart Monitoring of the Status of Driver Using the Dashboard Vehicle Camera. International Journal of New Practices in Management and Engineering, 9(01), 01 - 07. https://doi.org/10.17762/ijnpme.v9i01.81

[6] 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.

[7] Airehrour, D., Gutierrez, J. A., & Ray, S. K. (2019). SecTrust-RPL: A secure trust-aware RPL routing protocol for Mobile Ad-hoc Network. Future Generation Computer Systems, 93, 860-876.

[8] 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.

[9] 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 Mobile Ad-hoc Network Journal, 3(6), 1319-1333.

[10] 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.

[11] 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.

[12] Veeraiah, N., Khalaf, O. I., Prasad, C. V. P. R., Alotaibi, Y., Alsufyani, A., Alghamdi, S. A., & Alsufyani, N. (2021). Trust aware secure energy efficient hybrid protocol for manet. IEEE Access, 9, 120996-121005.

[13] Ahmad, S. J., Unissa, I., Ali, M. S., & Kumar, A. (2022). Enhanced security to MANETs using digital codes. Journal of Information Security and Applications, 66, 103147.

[14] Jim, L. E., Islam, N., & Gregory, M. A. (2022). Enhanced MANET security using artificial immune system based danger theory to detect selfish nodes. Computers & Security, 113, 102538.

[15] Khan, B. U. I., Anwar, F., Olanrewaju, R. F., Kiah, M. L. B. M., & Mir, R. N. (2021). Game Theory Analysis and Modeling of Sophisticated Multi-Collusion Attack in MANETs. IEEE Access, 9, 61778-61792.

[16] Sánchez, F., Đorđević, S., Georgiev, I., Jacobs, M., & Rosenberg, D. Exploring Generative Adversarial Networks for Image Generation. Kuwait Journal of Machine Learning, 1(4). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/147

[17] Ahmed, Ahmed & Rashid, Sami & Abbas, Ali & Abdulsattar, Nejood Faisal & Hassnen, Th & Mansour, Shakir & Mustafa, Th & Hassan, Mustafa & Habelalmateen, Mohammed. (2022). An Effectual Secure Cryptography Scheme for Multipath Routing in A Wsn-Based IoT Environment. 10.1109/IICETA54559.2022.9888604.

[18] Veeraiah, N., Khalaf, O. I., Prasad, C. V. P. R., Alotaibi, Y., Alsufyani, A., Alghamdi, S. A., & Alsufyani, N. (2021). Trust aware secure energy efficient hybrid protocol for manet. IEEE Access, 9, 120996-121005.

[19] Srilakshmi, U., Veeraiah, N., Alotaibi, Y., Alghamdi, S. A., Khalaf, O. I., & Subbayamma, B. V. (2021). An Improved Hybrid Secure Multipath Routing Protocol for MANET. IEEE Access, 9, 163043-163053.

[20] Simpson, S. V., & Nagarajan, G. (2021). A fuzzy based Co-Operative Blackmailing Attack detection scheme for Edge Computing nodes in MANET-IOT environment. Future Generation Computer Systems, 125, 544-563.

International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 7s
DOI: https://doi.org/10.17762/ijritcc.v11i7s.7034
***Article Received**: 04 April 2023 **Revised:** 29 May 2023 **Accepted:** 10 June 2023*

[21] Tu, J., Tian, D., & Wang, Y. (2021). An active-routing authentication scheme in MANET. IEEE Access, 9, 34276-34286.

[22] Sowjanya, K., Dasgupta, M., & Ray, S. (2021). A lightweight key management scheme for key-escrow-free ECC-based CP-ABE for IoT healthcare systems. Journal of Systems Architecture, 117, 102108.

[23] Bondada, P.; Samanta, D.; Kaur, M.; Lee, H.-N. Data SecurityBased Routing in MANETs Using Key Management Mechanism. Appl. Sci. 2022, 12, 1041