Computer Systems Science & Engineering
DOI: 10.32604/csse.2023.031605
Article

Logistic Regression with Elliptical Curve Cryptography to Establish Secure IoT

J. R. Arunkumar[1,*], S. Velmurugan[2], Balarengadurai Chinnaiah[3], G. Charulatha[4], M. Ramkumar Prabhu[4] and A. Prabhu Chakkaravarthy[5]

[1]Department of Information Technology, Sree Vidyanikethan Engineering College (Autonomous), Tirupati, Andhra Pradesh, India
[2]Department of Electronics and Communication Engineering, TJS Engineering College, Kavaraipettai, Chennai, Tamil Nadu, India
[3]Department of Computer Science and Engineering, Vidyavardhaka College of Engineering, Mysuru, Karnataka, India
[4]Department of Electronics and Communication Engineering, Peri Institute of Technology, Chennai, Tamil Nadu, India
[5]Department of Computer Science and Engineering, Saveetha School of Engineering, Saveetha Institute of Medical and Technical Science, Chennai, Tamil Nadu, India
*Corresponding Author: J. R. Arunkumar. Email: arunkumarjr@yandex.com
Received: 22 April 2022; Accepted: 08 June 2022

Abstract: Nowadays, Wireless Sensor Network (WSN) is a modern technology with a wide range of applications and greatly attractive benefits, for example, self-governing, low expenditure on execution and data communication, long-term function, and unsupervised access to the network. The Internet of Things (IoT) is an attractive, exciting paradigm. By applying communication technologies in sensors and supervising features, WSNs have initiated communication between the IoT devices. Though IoT offers access to the highest amount of information collected through WSNs, it leads to privacy management problems. Hence, this paper provides a Logistic Regression machine learning with the Elliptical Curve Cryptography technique (LRECC) to establish a secure IoT structure for preventing, detecting, and mitigating threats. This approach uses the Elliptical Curve Cryptography (ECC) algorithm to generate and distribute security keys. ECC algorithm is a light weight key; thus, it minimizes the routing overhead. Furthermore, the Logistic Regression machine learning technique selects the transmitter based on intelligent results. The main application of this approach is smart cities. This approach provides continuing reliable routing paths with small overheads. In addition, route nodes cooperate with IoT, and it handles the resources proficiently and minimizes the 29.95% delay.

Keywords: Wireless sensor network; internet of things; security; elliptical curve cryptography; machine learning; regression analysis

1 Introduction

WSN is the leading technology necessary for the execution of the IoT structure. IoT's operational ability and energy established the network communication, cost-effectiveness, dependability, stability, and dynamic function [1]. IoT is talented naturally from the internet. The things associated with the internet differ significantly in terms of characteristics. IoT is promising as a dynamic cyber-physical network that

facilitates smart devices to supervise and modify the world [2]. The existence of a large network of interrelated objects leads to serious problems about security which limit the wider utilization of IoT [3]. Integrating expertise in several sensible fields of function offers the remuneration of additional efficient action and quick reply to the necessary alteration. The approaches utilized for transmission and messaging are the key necessities of an IoT system [4]. Machine learning technique for precise and optimized IoT and it utilizes different efficient features extracted from IoT [5]. But, IoT with WSN is vulnerable to a diversity of attacks which could create convincing damage to the security. Security interrelated attacks can be classified into two types: active and passive attacks [6]. Furthermore, it is feasible to classify passive attacks promoted as disruption, eavesdropping, failure of server, deprivation, and traffic analysis. In active attacks, an attacker cooperates with the roles and actions of the WSN [7]. The attacker offers obvious damage which cannot be simply identified through the security systems. Active attacks contain flooding, jamming, denial-of-service, wormhole, black hole, sinkhole, also Sybil types [8].

Logistic regression (LR) is a type of machine learning algorithm for continuous variables. Though, LR is a classification algorithm, not a constant variable forecasting algorithm [9]. LR is a binary classifier, and it is utilized to evaluate discrete values like 0/1 from a set of independent variables. LR is easy to understand, and it implements easily [10].

The ECC algorithm is public key cryptography established on the algebraic structure of elliptic curves through finite fields. ECC is the best algorithm since it is a smaller key size. As a result, it is a power-efficient cryptosystem. The field utilized for the elliptic curve is defined over a prime number [11]. ECC method can efficiently encrypt and decrypt the information by digital signatures. It contains both public and private keys. This method ensures efficient privacy and security while related to other algorithms [12].

IoT security is attracting an increasing concentration from both the industry and academic fields. IoT devices are prone to several security attacks and leakage of information. This can potentially offer a broad attack surface for an attacker. IoT devices with weak authentication necessities can be simply compromised and controlled as part of an attack; as the number of connected devices increases, this attack surface continuous to grow. Though, Hybrid Secure Routing and Monitoring (HSRM) with IoT approach using multi-variant tuples using Two-Fish symmetric key approach to determine and avoid the adversary. This approach is preferred to be built through success to the assets of both multipath optimized link-state routing with *ad hoc* on-demand distance vector. It is planned by the Authentication and Encryption Model, which utilizes Eligibility Weight Function for choosing the sensor guard nodes. However, this approach increases the complexity. In addition, it can't be able to provide strong security in WSN [13].

To solve this problem, the Secure IoT structure established a WSN using the Machine Learning concept is introduced. This paper objective is to forward the information through intelligent transmitter thus, minimizes the packet losses in the WSN. In addition, the receiver received the secured information from sender to receive by ECC algorithm.

This approach has the following contribution.

- The Logistic Regression machine learning technique selects the optimal transmitter based on intelligent results. Logistic Regression machine learning objective is to establish a secure IoT structure for preventing, detecting, and mitigating threats.
- The Elliptical Curve Cryptography algorithm is a light weight key, and it distributes the security keys. It minimizes the routing overhead.
- This optimal transmitter improves energy efficiency and minimizes the delay in the WSN.

2 Related Works

ECC is lengthily utilized in several multifactor authentication approaches. The threat model deliberates several kinds of attacks comprising Man in the Middle (MIM), denial of service, and weak authentication. Countermeasures to decrease or otherwise evade these attacks are advised. An Intrusion detection system is used to prevent the MIM attack. The Intrusion detection system occasionally catechizes nodes one hop away [14]. Energy-Efficient and Secure IoT structure applies supervised machine learning techniques to enhance precision. Signal communication from several biosensors to utilizes the greatest amount of energy. The structure considerably improves energy efficiency and durability [15]. Elliptic Curve Diffie Hellman key interchange is investigated by applying the pyCryptodome package and the integrated encryption method of an elliptic curve. Authentication is also required for node-to-node transmission. The elliptic Curve Digital Signature method offers a suitable mechanism for evaluating key generation time, packet size, and hello message count. This approach assists in obtaining the complete network in a better and more effective method. This approach minimizes the cost risk and threats of security on authentication. However, this approach can't select an optimal forwarder [16].

ECC is an efficient key because it is a smaller key. Hence, it minimizes unwanted energy utilization. ECC is a faster transmission, rising for a severe operation. Thus enormous injuries are triggered through intrusion attacks. But, it has not improved the routing efficiency. [17]. The Extended Identity Based Encryption (EIBE) approach ensures authentication and confidentiality. The Kerberos authentication approaches and identity based encryption to confirm authentication and privacy [18]. The WSN is prepared to allot continuous observing of ecological security and ecological problems, the risk of probable fire otherwise, and crime in the situation [19].The Diffie-Hellman convention utilizes Elliptic Curve Cryptography (DHECC), both elliptic open and sealed key, to construct a mutual secret key over an indeterminate channel. Advanced encryption standard algorithm for encrypting and decrypting the information also ensures security. So ECC is the best applicant for offering secure communication between WSN. Though, this approach does not utilize the machine learning algorithm [20].

An energy-efficient method established public-key cryptography method attains instant authentication, and it avoids Denial of Service attacks [21]. Enhanced ECDH key interchange method with the Digital Signature of Elliptic Curve method is utilized to interchange the secured shared key between multiple nodes and remove the MIM attacks to provide less computation complexity [22]. Neighbor Co-ordination-based Fault Node Detection approach (NCFD) focuses on fault node credentials. In this approach, the neighboring nodes attempt to recognize the faulty sensor by equating their observed data with other neighbors' information. This approach notices faulty sensor nodes applying a neighbor coordination method [23]. The Time Based Reliable Link is proposed to support the smart city that determines the topography of every node by applying the topography discovery technique. The reliability of every node recognized link is decided when using the two nodes' consistent model. This dependability model minimizes the probability of horizontal and greater depth level transmission between nodes and chooses the next dependable transmitters. However, it does not enhance network security [24].

A Trust-based Formal Model describes the fault recognition procedure and verifies faults lacking simulating and running. This algorithm is introduced to organized detection models. Though, the trust method does not provide better security [25]. A fault-containment discovers the restraining the pollution of faults inside a small region; this approach attains healing inside time and works proportionate to the alarm size and autonomous size. Specification-based design of self-healing addresses the next issues. Since specifications are more succinct than implementations, this method produces a well-organized plan of self-healing even for large executions [26]. More secure and efficient access control allows an Internet user in certificate-less cryptography to transmit with a sensor node in identity-based cryptography surroundings with dissimilar system parameters. Furthermore, this approach attains specific temporary information security, which is the most of access control approaches [27]. ECC method is used for

improving sensor node authentication [28]. Secure and efficient audit service approach for improving data integrity. However, this approach can't provide secure IoT [29].

3 Logistic Regression with Elliptical Curve Cryptography to Establish Secure IoT

The objective supervises the IoT surroundings sporadically and forwards the information toward the Base Station (BS), applying multi-hop. Then the destination node cooperates with servers over the internet to store the information. The information is forwarded through the untrustworthy wireless transmission links in the existence of malfunctioning nodes. The malfunctioning nodes produce and distribute the fake Route Request (R_{REQ}) packets; as a result, links are congested in the network. In this approach, we consider several IoT-based sensors which can exchange the information and forward the supervised information to the BS by applying intelligent boundaries nodes. These boundary nodes have an extra aptitude for information processing and taking an intelligent result to transmit the information toward servers for storage.

The stored information on servers can be transmitted to the smart devices of the end-users via the internet. The IoT devices are established during the authentication phase to be coordinated with companionable devices that are noticeable as suitable entities for the information routing table. Initially, the BS broadcasts the sensor identities (IDs), boundary nodes Ni in the network. All nodes obtainthese broadcast messages; all IoT nodes keep the edge node's IDs in their table. In this approach, we use the ECC that forward secure information.

ECC is a public key cryptography algorithm, and this model detects several kinds of attacks comprising man in the middle, denial of service, and weak authentication. The ECC model utilizes two keys: the public key and the private key. The public key encrypts the real information; the private key decrypts the original information. Thus, the attackers can't read and modify the original information. ECC method provides secure information transmission and improves node Reliability.

The Procedure for LRECC approach is given below.

Input: Sender, Receiver, Public key, private key,

Output: Transmitter nodes, Secure information

Begin Procedure {

BS Broadcasts sensor node Identity and Edge nodes

Store these information to table

While Sender does not reach the information to receiver do {

Sender selects Transmitter

Logistic Regression do {

Foreach neighbor node {

check transmission time

check packet sent

check packet response

Update table }}

Select minimum loss rate node as a Transmitter

Sender forward information to receiver

ECC {
Sender encrypts the real information
Sender Forward the encrypted information through Transmitter
Receiver gets the encrypted information
Receiver Decrypts the original information
Receiver gets the secured information }}
End Procedure }

Fig. 1 explains the block diagram of LRECC. It presents four main parts. Initially, the IoT launched sensors to cooperate and swap their identities. They validate and confirm their ID; then, the ECC algorithm is applied by the LRECC to generate and distribute security keys. Furthermore, the Logistic Regression machine learning technique is utilized by the LRECC for the transmitter election and continuing reliable routing paths with small overheads. In addition, route nodes cooperate with IoT and BS to handle the resources proficiently and minimize the delay.

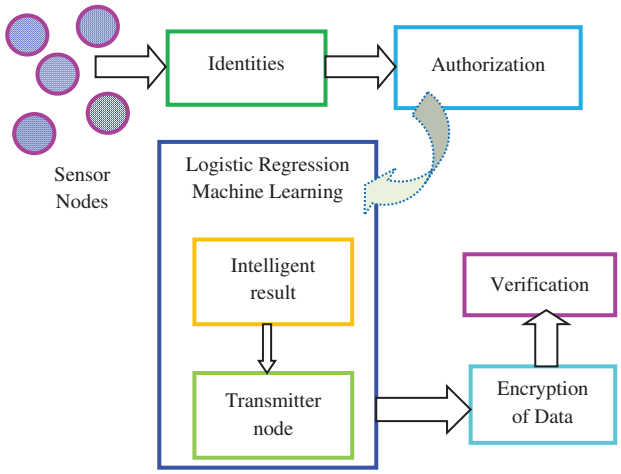

Figure 1: Block Diagram of LRECC

4 Regression Analysis

In the LRECC, the IoT sensor nodes gather the information and forward it to the transmitter node chosen by the regression analysis machine learning technique. This technique provides an intelligent result. The regression analysis is necessary through the information that the election of forwarder nodes established on the transmission time, the packet sent, and the response of the packet through obtaining node. In this process, the regression analysis is aimed to determine the effects of independent variables over the dependent variable.

Because of, the sensor node loss rate in the communication procedure as a dependent variable and forwarding information, along with its instant time as independent variables, any node can forward information packets p_a at time t_a toward the neighboring node by loss rate LR_a. These details are kept in the table during the information forwarding and receiving to perform the regression analysis, applying Eq. (1).

$$LR_a = \gamma_0 + \gamma_1 p_a + \gamma_2 t_a + \in \tag{1}$$

Here, LR_a indicates the loss rate, γ_0 represents the y-intercept; $\gamma_1 p_a$ indicates the initial regression coefficient together with the forwarded information packet; $\gamma_2 t_a$ indicates the coefficient of 2nd regression, t_a denotes the time instant variable, and $\in$ denotes the residual error. This method aim is to discover the lowest loss rate for selecting the transmitter nodes. The coefficients γ_1 and γ_2 are calculated using Eqs. (2) and (3).

$$\gamma_1 = \frac{(\sum t_a{}^2)(\sum p_a LR_a) - \sum p_a t_a)(\sum p_a LR_a)}{(\sum p_a{}^2)(t_a{}^2) - (\sum p_a t_a)^2} \tag{2}$$

$$\gamma_2 = \frac{(\sum t_a{}^2)(\sum t_a LR_a) - \sum p_a t_a)(\sum p_a LR_a)}{(\sum p_a{}^2)(t_a{}^2) - (\sum p_a t_a)^2} \tag{3}$$

In the same way, the values' y-intercept γ_0 can be computed through the set values of γ_1 and γ_2 in Eq. (4).

$$\gamma_0 = LR_a - \gamma_1 \overline{p_a} + \gamma_2 \overline{t_a} \tag{4}$$

The adjacent node with the minimum packet loss nodes are selected as a transmitter for transmitting the information to the BS. In the next part, the LRECC model forwards the gathered information to the BS via route nodes. These route nodes execute the encryption function, applying the ECC technique. ECC is public-key cryptography, and it contains a public key and a private key. Regard as two sensor nodes are communicated among them, they agree to generate an ECC key R. Assume A and B sensor node's private keys are

$$PRK_a = nA \tag{5}$$

$$PRK_b = nB \tag{6}$$

nA and nB correspondingly. sensor nodes A and B public keys are specified below.

$$PUK_a = nAR \tag{7}$$

$$PUK_b = nBR \tag{8}$$

If A sensor desires to forward a message m to B, A applies B sensor public key to encrypt the message. The ciphertext is specified below.

$$C = \{KR, M, KPUK_b\} \tag{9}$$

Here 'k' represents the arbitrary number. The arbitrary k ensures that the ciphertext produced is diverse each time, even for an identical message. This provides a hard time for attackers illegitimately demanding to decrypt the message. B decrypts the message by subtracting the organize of kR multiplied via nB from

$$M + KPUK_b$$

$$M = \{M + KPUK_B - nBKR\} \tag{10}$$

Here, nB is the private key of sensor B, and it can decrypt the message of sensor A. Here, the sensor nodes are authentic and regression analysis is executed to choose the optimal transmitter. It guides to low transmission and overhead computing overhead. The integration of route nodes minimizes the communication distance with IoT devices and the consumption of resources at minimum expenses. As a

result, regression analysis chooses the node with minimum loss rate as a transmitter. Furthermore, the security of LRECC raises reliability.

5 Simulation Analysis

In this paper, we use the network simulator ns-2.35 to measure the network performance of the HSRM and LRECC approaches. Here, we use 100 sensor nodes, and these sensor node's transmission range is 200 m. 10 unreliable sensor nodes are arbitrarily distributed in the field. The parameters applied for the investigation are described in Tab. 1.

Table 1: Simulation Parameters of HSRM and LRECC

Parameters	Values
Sensor nodes count	100
Unreliable sensor node count	10
WSN traffic	Constant bit rate
Node distribution	Arbitrarily way
Simulation time	100 s
Sensor node medium access control	802.15.4
Sensor node queue	Priority queue
Transmission range	200 m

The function of the LRECC is measured by delay, remaining energy, throughput, the ratio of packet losses, and overhead of routing. Fig. 2 explains the execution of the HSRM and LRECC approaches for the throughput ratio.

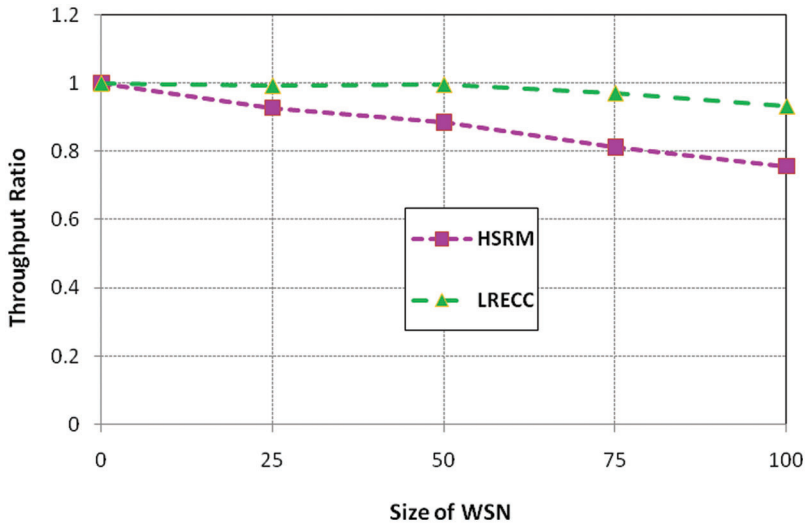

Figure 2: HSRM and LRECC approaches for throughput ratio

From Fig. 2, the LRECC approach selects the transmitter node selection by logistic regression analysis. This technique makes an intelligent decision for selecting the transmitter node based on the transmission time, the packet sent, and the response of the packet through obtaining the node. Thus, the network congestion is minimized by forwarding the information through optimal routing. But, the HSRM approach can't select the intelligent transmitter in the network. As a result, the network throughput in the network is minimized. Fig. 3 explains the HSRM and LRECC approaches for the remaining energy ratio.

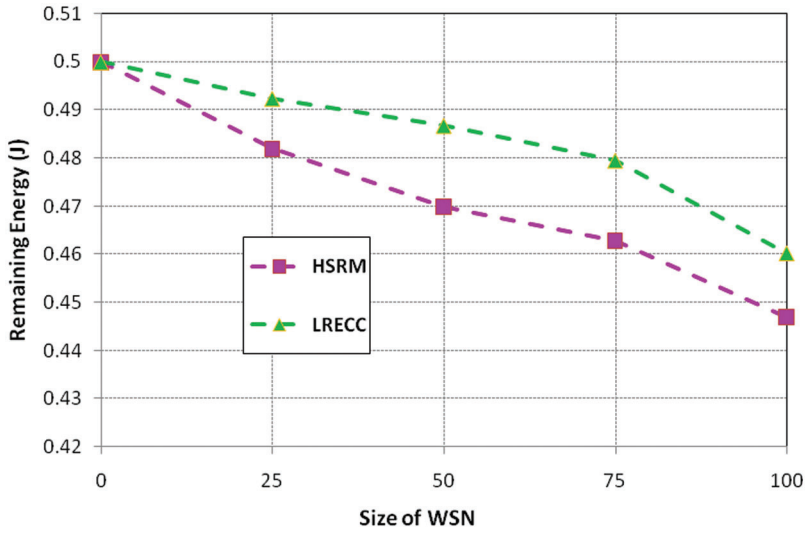

Figure 3: HSRM and LRECC approaches for Remaining Energy

Fig. 3 illustrates that the HSRM approach has the highest Remaining Energy than the LRECC approach. Since this approach using the ECC method improves network security and regression analysis method, selecting the optimal nodes to improve the energy efficiency in the network. Fig. 4 demonstrates the delay of HSRM and LRECC approaches.

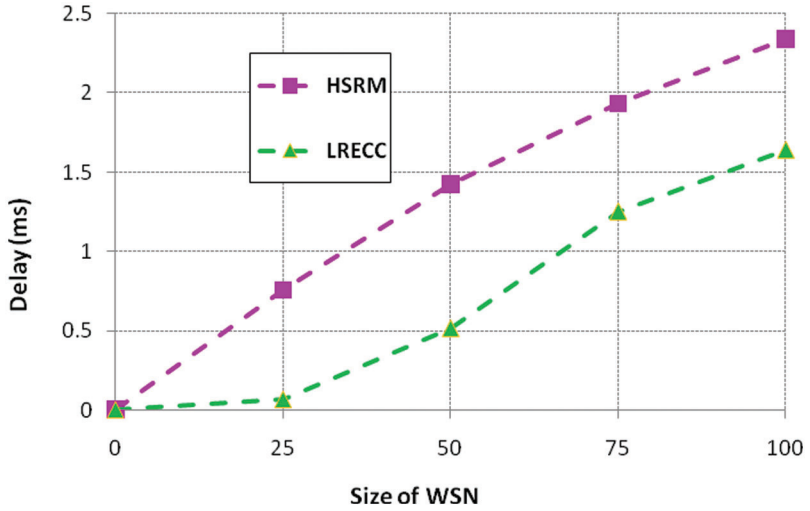

Figure 4: HSRM and LRECC approaches for delay

From Fig. 4, the LRECC approach minimizes the delay in the network. In LRECC, we select the optimal route by regression analysis since this approach forms the route by multi-hop route. In addition, the LRECC enhances the load of information allotment through transmitters and optimizes the function of the links in network traffic. Though, the HSRM approach increases the delay compared to the LRECC approach. Fig. 5 explains the routing overhead of HSRM and LRECC approaches.

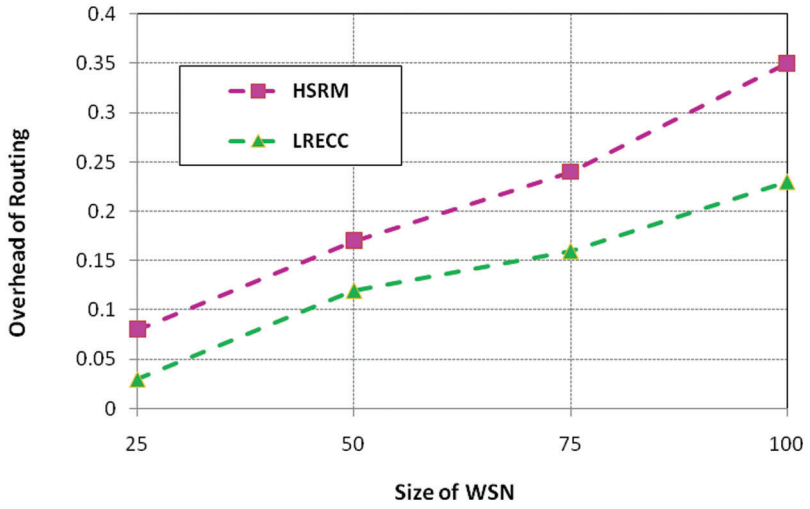

Figure 5: Routing overhead of HSRM and LRECC approaches

It is clear that the LRECC approach minimizes the routing overhead compared to the LRECC approaches. This approach uses the ECC method for security. It reduces the routing overhead. It is due to the regression-based machine learning technique for transmitter node selection which allows efficient communication between the neighboring nodes. The node chosen procedure is established by the stored information concerning the packet loss rate of every neighboring node. Fig. 6 explains the network's HSRM and LRECC approaches packet losses.

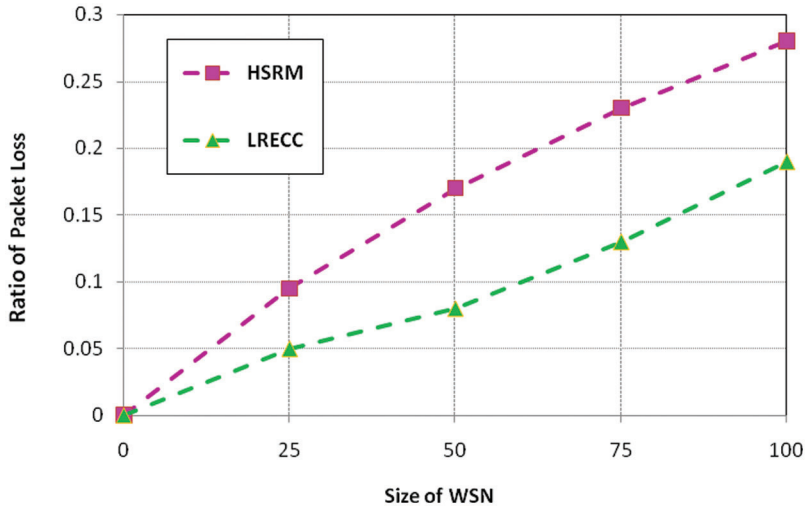

Figure 6: Ratio of packet losses of HSRM and LRECC approaches

Fig. 6 indicates that the LRECC approach minimizes the packet loss ratio in the network. Since the LRECC approach selects the optimal route by the regression analysis. This approach improves network security. As a result, minimizes the packet loss ratio in the network.

6 Conclusions

This paper presents Logistic Regression machine learning with the ECC technique to enhance the performance to prevent, detect, and mitigate threats. This paper objective is to forward the information through intelligent transmitter thus, minimizes the packet losses and receiver received secured information in the WSN. This approach uses the ECC algorithm to generate and distribute security keys. ECC is a light weight key; thus, it minimizes the routing overhead. This cryptography technique verifies the sensor nodes and provides better security in the network. Furthermore, the Logistic Regression machine learning technique selects the optimal transmitter based on intelligent results. This optimal transmitter improves energy efficiency and minimizes the delay in the WSN. An extensive simulation illustrates that the proposed LRECC reaches better throughput and it provides continuing reliable routing paths with small overheads. In addition, route nodes cooperate with IoT, and it minimizes the delay. The future enhancement of this approach is to include node mobility. Furthermore, it will be employed in IoT-established WSNs to secure the application environment, for example, smart cities.

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

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

References

[1] V. Chinnalagi, R. Murugeswari, T. Priyadharshni, K. Rajalakshmi and J. V. Ananthi, "Dynamic performance of smart sensor network using IoT," in *Int. Conf. on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)*, Palladam, India, pp. 49–53, 2017.

[2] S. M. He, K. Xie, K. X. Xie, C. Xu and J. Wang, "Interference-aware multisource transmission in multiradio and multichannel wireless network," *IEEE Systems Journal*, vol. 13, no. 3, pp. 2507–2518, 2019.

[3] Z. Xu, W. Liang, K. C. Li, J. Xu and H. Jin, "A blockchain-based roadside unit-assisted authentication and key agreement protocol for internet of vehicles," *Journal of Parallel and Distributed Computing*, vol. 149, no. 6, pp. 29–39, 2021.

[4] Z. Xu, X. Li, J. Xu, W. Liang and K. K. R. Choo, "A secure and computationally efficient authentication and key agreement scheme for internet of vehicles," *Computers & Electrical Engineering*, vol. 95, no. 2, pp. 1–14, 2021.

[5] Y. Yue, S. Li, P. Legg and F. Li, "Deep learning-based security behaviour analysis in IoT environments: A survey," *Security and Communication Networks*, vol. 2021, no. 1, pp. 1–13, 2021.

[6] R. Kumar, M. Swarnkar, G. Singal and N. Kumar, "IoT network traffic classification using machine learning algorithms: An experimental analysis," *IEEE Internet of Things Journal*, vol. 9, no. 2, pp. 989– 1008, 2021.

[7] F. Jeelani, D. S. Rai, A. Maithani and S. Gupta, "The detection of IoT botnet using machine learning on IoT-23 dataset," *IEEE 2nd Int. Conf. on Innovative Practices in Technology and Management*, vol. 2, pp. 634–639, 2022.

[8] B. D. Deebak and F. Al-Turjman, "A hybrid secure routing and monitoring mechanism in IoT-based wireless sensor networks," *Ad Hoc Networks*, vol. 97, pp. 1–35, 2020.

[9] K. V. K. Mahalaxmi and K. S. Rekha, "Comparison of logistic regression and artificial neural network for modelling credit card data set with the identification of precise fraudulent," in *Int. Conf. on Business Analytics for Technology and Security*, Dubai, United Arab Emirates, pp. 1–5, 2022.

[10] K. V. Bhavitha and S. J. J. Thangaraj, "Novel detection of accurate spam content using logistic regression algorithm compared with gaussian algorithm," in *Int. Conf. on Business Analytics for Technology and Security*, Dubai, United Arab Emirates, pp. 1–5, 2022.

[11] M. Anas, R. Imam and F. Anwer, "Elliptic curve cryptography in cloud security: A survey," in *IEEE 12th Int. Conf. on Cloud Computing, Data Science & Engineering (Confluence)*, Noida, India, pp. 112–117, 2022.

[12] S. A. Chaudhry, K. Yahya, S. Garg, G. Kaddoum, M. Hassan *et al.,* "LAS-SG: An elliptic curve based lightweight authentication scheme for smart grid environments," *IEEE Transactions on Industrial Informatics*, pp. 1, 2022.

[13] B. Nair and C. Mala, "Analysis of ECC for application specific WSN security," in *IEEE Int. Conf. on Computational Intelligence and Computing Research*, Madurai, India, pp. 1–6, 2015.

[14] D. Baskar, M. Arunsi and V. Kumar, "Energy-efficient and secure IoT architecture based on a wireless sensor network using machine learning to predict mortality risk of patients with COVID-19," in *6th Int. Conf. on Communication and Electronics Systems*, Coimbatre, India, pp. 1853–1861, 2021.

[15] M. F. Moghadam, M. Nikooghadam, M. A. B. Al Jabban, M. Alishahi, L. Mortazavi *et al.,* "An efficient authentication and key agreement scheme based on ECDH for wireless sensor network," *IEEE Access*, vol. 8, pp. 73182–73192, 2020.

[16] A. Hendra, E. Palantei, M. S. Hadis, N. Zulkarnaim and M. F. Mansyur, "Wireless sensor network implementation for IoT-based environmental security monitoring," *IOP Conference Series: Materials Science and Engineering*, vol. 875, no. 1, pp. 1–5, 2020.

[17] U. Iqbal and S. Shafi, "A provable and secure key exchange protocol based on the elliptical curve diffe-hellman for WSN," *Advances in Big Data and Cloud Computing*, vol. 750, pp. 363–372, 2019.

[18] A. Hendra, E. Palantei, M. S. Hadis, N. Zulkarnaim and M. F. Mansyur, "Wireless sensor network implementation for IoT-based environmental security monitoring," *IOP Conference Series: Materials Science and Engineering*, vol. 875, no. 1, pp. 1–5, 2020.

[19] K. Prabakaran and M. Prabu, "Secure and efficient data contribution using extended identity based encryption in cloud computing," *International Journal of MC Square Scientific Research*, vol. 9, no. 1, pp. 189–194, 2017.

[20] R. Qazi, K. N. Qureshi, F. Bashir, N. U. Islam, S. Iqbal *et al.,* "Security protocol using elliptic curve cryptography algorithm for wireless sensor networks," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 1, pp. 547–566, 2021.

[21] H. Ghasemzadeh, A. Payandeh and M. R. Aref, "Key management system for WSNs based on hash functions and elliptic curve cryptography," in *Int. Conf. on New Research Achievements in Electrical and Computer Engineering*, Tehran, Iran, pp. 1–9, 2017.

[22] P. Soni, A. K. Pal and S. H. Islam, "An improved three-factor authentication scheme for patient monitoring using WSN in remote health-care system," *Computer Methods and Programs in Biomedicine*, vol. 182, no. 1, pp. 1–19, 2019.

[23] T. Ali, M. Irfan, A. Shaf, A. Saeed Alwadie, A. Sajid *et al.,* "A secure communication in IoT enabled underwater and wireless sensor network for smart cities," *Sensors*, vol. 20, no. 15, pp. 1–24, 2020.

[24] P. Shukla and R. R. Panda, "Neighbor co-ordination based fault node detection algorithm for distributed wireless sensor networks," *International Journal of Engineering Research & Technology*, vol. 6, no. 9, pp. 261–265, 2017.

[25] P. Jiang, "A new method for node fault detection in wireless sensor networks," *Sensors*, vol. 9, no. 2, pp. 1282–1294, 2009.

[26] A. De Paola, G. Lo Re, F. Milazzo and M. Ortolani, "QoS-aware fault detection in wireless sensor networks," *International Journal of Distributed Sensor Networks*, vol. 2013, no. 9, pp. 1–12, 2013.

[27] M. Luo, Y. Luo, Y. Wan and Z. Wang, "Secure and efficient access control scheme for wireless sensor networks in the cross-domain context of the IoT," *Security and Communication Networks*, vol. 2018, no. 1, pp. 1–10, 2018.

[28] S. Lingeshwari, "Provisioning of efficient authentication technique for implementing in large scale networks (PEAT)," *International Journal of MC Square Scientific Research*, vol. 6, no. 1, pp. 34–42, 2014.

[29] G. Prakash, B. Vyas and V. R. Kethu, "Secure & efficient audit service outsourcing for data integrity in clouds," *International Journal of MC Square Scientific Research*, vol. 6, no. 1, pp. 5–60, 2014.