Received: April 28, 2024. Revised: June 8, 2024.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

Blocollab: A Blockchain-aided Deep Learning Model for Hybrid and Collaborative Routing Attack Detection and Mitigation in RPL

Omar A. Abdulkareem[1,2]* Raja Kumar Kontham[1] Israa T. Aziz[3]

[1]*Department of Computer Science and Systems Engineering, Andhra University, Visakhapatnam, India*
[2]*Directorate of Research and Development, Ministry of Higher Education and Scientific Research, Iraq*
[3]*Computer Center, University of Mosul, Mosul, Iraq*
* Corresponding author's Email: omarasalam.rs@andhrauniversity.edu.in

Abstract: As Internet of Things (IoT) is a realism that variations in numerous aspects of our everyday life, from smart monitoring to the management of life-threatening infrastructure. In the modern world, secure communication is vital, and it is accomplished by routing protocol. The routing protocol for low power and lossy networks (RPL) is the only defector-consistent routing protocol in IoT systems and is thus deployed for many IoT applications. In the literature, we can bargain several attacks pointing to affect and interrupt RPL-based networks. Therefore, it is essential to develop security apparatuses that detect and mitigate any probable attack in RPL-based networks. Current state-of-the-art security solutions deal with very few attacks while proposing heavy mechanisms at the expense of IoT systems and overall network performance. In this paper, we proposed secure hybrid and collaborative intrusion detection in RPL based on blockchain (Block-RPL) to overcome these issues. The propounded work has wrapped out with four phases as symbolized as follows: network fabrication and node authentication, ideal parent node election, and Deep Learning-assisted collaborative and hybrid intrusion detection. Initially, we perform network fabrication in order to ideally place the Mr. Fixits and to cope with the network dynamics using the Bettered Remora Algorithm (Be-Remo). Then, the RPL topology is urged to register at the Dutiful Advisor (DA) by charitable parameters, and the DA offers the secret key to the nodes using the Boosted CHACHA algorithm (B-CHACHA). Subsequently, the root node in the RPL disseminates the DODAG Information Object (DIO) messages and each node selects its parent by considering several optimal features using the Be-Remo algorithm. Finally, collaborative and hybrid (i.e., specification and anomaly) intrusion detection is performed based on network behaviors using the Light residual attention mechanism aided by the VGG16 algorithm (LightVGG16). In our work, we have employed blockchain for data privacy and enhancing security during message dissemination. The proposed work was conducted using the Cooja simulator available in Contiki OS, and the performance of the proposed Block-RPL model is itemized based on various performance metrics in terms of number of the DIOs received, downward latency, energy consumption and attack detection accuracy.

Keywords: IoT, RPL protocol, Security, Low power and lossy network, Blockchain, RPL attacks, Deep learning, Routing and intrusion detection.

1. Introduction

With the rapid proliferation of IoT devices, communication technology plays a pivotal role in enhancing daily life [1, 2]. Such a cutting-edge technology is pampered and embedded by resource-constrained sensors, and Radio Frequency Identity (RFID), which are limited to energy, memory, computation, and so on because they are belonging to the low power and lossy networks (LLNs) [3, 4]. Such devices are widely adopted in smart industries, smart homes, smart transportation, smart environments, and the military. Varied communication protocol is adopted in IoT, such as IEEE 802.15.4, Wi-Fi, Bluetooth, and RFID. According to the device specification, the range required for communication and the surrounding atmosphere, protocols can be determined. However, the group of Internet Engineering Task Force (IETF) has standardized the IPv6 Routing Protocol for low

power and lossy network (RPL) to achieve dynamicity, scalability, and robust information exchange in low power and lossy network LLNs [5]. information exchange is becoming flexible and resource consumption is optimized by the RPL as it creates steadfast routing topologies with susceptible packet loss and connectivity. The RPL facilitates having alternate routes when the actual route's access fails. Yet, a significant hardship in terms of security is widely exploited by cyber crooks during routing functions [6]. As LLNs are resource-constrained, security breaches are effortlessly performed to deplete the entire network performance by means of routing attacks. Routing attacks include rank attack, version number attacks, DIS flooding attacks, DAO attacks, selective forwarding attacks, and black hole attacks. [7]. The motto of performing routing attacks is to consume the resources of already resource-constrained IoT devices by sending a huge amount of control messages [8]. The RPL topology is pillared as Destination Oriented Directed Acyclic Graph (DODAG) with the help of several control message exchanging like DIO (DODAG Information Object), DAO (DODAG Advertisement Object) [9, 10], DAO-ACK (DODAG Advertisement Object Acknowledgement), DIS (DODAG Information Solicitation) [11]. Attackers manipulate control message information, altering version numbers and ranks, or inundating parent nodes with excessive control messages [12, 13]. While past research has explored methods for detecting malicious nodes in RPL topologies, challenges such as security vulnerabilities, performance degradation, inaccurate attack detection, improper intrusion detection system placement, and ineffective countermeasures persist [14]. Addressing these gaps, we propose a novel framework integrating blockchain technology to prevent data manipulation and lightweight deep learning and optimization algorithms for efficient routing attack detection (both specification and anomaly) [15].

A. Motivation and Objectives

The foremost aim of this research work is to identify and isolate malicious nodes in the RPL topology to provide high security to the RPL nodes. In addition, the proposed research work addresses several interesting problems that exist in RPL attack detection and mitigation in terms of topological inconsistency, poor accuracy, and inappropriate security practices.

B. *Research Contribution*

The proposed novel points for secure and hybrid intrusion detection in the RPL are mentioned. The major contributions of this research are as follows:

- The network is segregated into numerous layers for the ideal placement of Mr. Fixits in demand to handle network subtleties using the Be-Remo optimization algorithm, which has a high convergence rate and better accuracy.
- Ideal parent node voting is performed using Be-Remo by considering mobility, ELT, trust value, ETX, and rank to improve and residual energy ratio, reduce latency, and increase network reliability to avoid recurrent global and local repair mechanisms.
- Hybrid and collaborative IDS are accomplished to precisely detect and detach the malicious nodes from the network without problems using the LightVGG16 algorithm. To thwart the network from cooperative attacks, collaborative IDS is executed.

The performance of the proposed approach was validated and found to outperform other approaches in terms of the number of DIO received, downward latency, energy consumption, and attack detection accuracy.

C. *Paper Organization*

The remaining sections of this work are ordered as follows: section 2 provides information about the existing works in attack detection and mitigation in RPL and research gaps; section 3 emphasizes the overall problem statement of the existing works and its corresponding solutions; section 4 provides a the detailed explanation of the proposed, including equations and suitable diagrams; section 5 describes the simulation setup of the proposed work, simulation tool of their simulation parameters are explained, comparative analysis of various evaluation metrics with existing works, and an overall summary of the proposed work; and section 6 presents the conclusion of the proposed work. Notation list presents the notation forms for the proposed work.

2. Literature survey

This section presents a survey of the literature on routing attack detection and mitigation in RPL. The authors of this research paper proposed a scheme to detect RPL attacks occurring in the IoT environment [16]. This study encompassed four subprocesses: control message (routing information) acquisition, feature selection, attack identification, and classification. To acquire control messages, the authors employed several sniffing entities. These entities periodically disseminate the control message and other node's basic information to an external server. Then feature selection was performed on the basis of several features such as DIO received/transmitted, DODAG version, and so on. further attack detection was performed based on extracted features. Finally, using the autoregressive

model, attackers were classified into null attacks and attacks. This work lack with intrusion detection is performed in this work. However, the absence of considering network dynamicity during attack detection limit to have effective performance. DODAG information solicitation attack mitigation was performed in this work by introducing a load balancing scheme [17]. The purpose of this research work was to improve the network lifetime of the node by sharing the workload. They assumed that a malicious node periodically propagates DIS messages. To mitigate DIS flooding attacks, they have considered three thresholds which include residual energy, solicitation sending interval, and allowed DIS sending counts. Eventually, mentioned that thresholds can have deviations according to the implementation scenarios. This work lack with mitigated the DIS flooding attack by limiting the DIS messages based on the threshold. However, the consideration behind the DIS sending is unfocused in this work. Hence, legitimate nodes may suffer in such a scenario. Version number and rank attacks were detected and mitigated in this paper [18]. Here, the root node was assumed not to be exploited under cyber-attacks as its identity was encrypted using an elliptic cryptographic algorithm. This work identified attacks in several working progressions. In the first progression, they set a threshold value for DIO exchanged; if it exceeded the threshold then it was discarded. Otherwise, it was forwarded to the second progression in which the sender node's identity was cross-verified. Further, third progression rank and version number attacks were determined on the basis of the version changes. In addition, the rank deviation of the child node from its parent node is used to label a malicious node. Eventually, the malicious nodes were added to the blacklist. This work lacks with control messages that are exchanged among nodes unencrypted. This encourages cyber attackers to perform MIMA, spoofing, and other attacks. The authors of this research work introduced a DL-based model which was supported by a gated recurrent unit for identifying the malicious nodes that perform hello flooding attacks [19]. Here, simulation, cleansing, feature extraction, and attack classification was performed. Primarily, network was determined by entities such as root node, illegitimate nodes, and legitimate nodes. In addition, the energy, radio transmission/reception, and idle state of the node and processing unit were estimated, filtered, and extracted. Finally, IoT nodes were classified as malicious (packets dropped) or normal using GRU. At last, they evaluated their work using other regression and support vector machine algorithms. This work lack with prevention is done by dropping the malicious node's control messages. However, educating legitimate nodes about malicious nodes limits future attack detection at earlier stages. In this research paper, the authors introduced a game model that combines both evolutionary and stochastic models for accurate anomaly detection [20]. The first game model, i.e. stochastic identifies the anomaly that is presented in the network, whereas the second model, i.e., evolutionary approves the maliciousness of a node. Primarily, the control message-exchanging states were formulated as game rules in the stochastic game model as well as giving reward based on states. Because a malicious node affects the state of normal nodes, thus normal nodes will be classified as malicious. Therefore, an evolutionary game was used to ensure malicious activities. This work lack with attack detection is performed. However, it is ineffective in identifying co-operative attacks performed by intellectual assaulters. Hence, it affects the security. In this research work, the authors introduced an intrusion detection model which was based on RPL CPS [21]. The RPL attacks detected in this work were the DIS attack, Hello flooding attack, decreased rank attack, and increased rank attack. This work encompassed with three processes such as data gathering, data analysis, and prediction. The first process captures the routing traffic when the network is under attack. In addition, feature engineering was performed to generate features and eliminate unwanted data reduction to improve classification accuracy. At last, IDS (deployed at the router) was performed using five different ML algorithms: SVM, random forest, logistic regression, naïve Bayes, and decision tree. This work lack with intrusion detection and is deployed at the border router. However, poor security over that router has the chance to be exploited by highly potential attackers. Hence, it affects the security of the system. Two different attacks that affect the RPL protocol i.e., blackhole attacks and rank attacks were identified in this work [22]. In addition, they investigated the consequences of this combination of attacks by introducing a new working mechanism. Here, routing-based IDS, threshold-centered IDS, threshold-centered objective functions, and were incorporated. Initially, information was gathered by routing the IDS. With the help of this IDS, each node estimates the trust of a node in selecting an optimal parent node using mathematical formulas. When trust values diminish from the expected value and deviations on packet forwarding, it is labeled as malicious and added to the blacklist. This work lack with an external entity is used as the intrusion detection system. However,

inappropriate placement of IDS limits its ability to adapt to network dynamic changes with effective intrusion detection and mitigation. The consequences such as network performance degradation and high usage of resources raised by the DODAG information solicitation attack were mitigated in this study [23]. As the motives of the DIS flooding attacks were achieved by the needless trickle timer resets, the authors of this research have set a threshold value for controlling the control message exchange. Here, DIS flooding attacks were tackled and mitigated based on the expiration of the DIS interval and the number of DIS messages that had to be transmitted. Eventually, they evaluated that their framework limits energy consumption and improves network performance. This study lacks attack detection and mitigation. However, the identity of the malicious nodes was uneducated to the benign nodes. Thus, future attack detection during the initial phases becomes challenging because it needs to be investigated by IDS. This leads to energy consumption and security vulnerabilities. In this paper, the authors proposed a lightweight routing protocol for triggering attacks in an RPL network [24]. In this research work, a lightweight and effective attack detection and mitigation solution against the network addresses. This paper proposed a cooperative scheme for security improvement to RPL network and this work has an aimed to understand the effective detection and vindication of VN attacks in fluctuating scale networks deployed for any IoT submission. It provides a well-organized security solution by ranging the RPL functionality. In this paper, multilayer RPL was proposed for the energy-aware cluster for the network cluster that forms a cluster and chooses the Cluster Head CH node [25]. The full node capable of downloading and verifying the current nature of the network. Energy consumption is a key in low power networks. The research of the reduced quantitative network to choose the most best grid low power consumption of the energy and performance aided in the nature of the proposed work in the environment. In this paper, sensor network-based specific rank detection accuracy and modification of the network model [26]. The RPL specific rank attack on a self-generated dataset. The attack detection was performed based on the optimal features of attack detection and mitigation especially for wormhole attack and also considered optimal parameters and are characterized by accuracy, performance, and detection rate which is weighed through typical ML evaluation metrics as fine as multilevel classification of features for attack detection. In this RPL with de-facto IoT routing protocol for numerous internal attack detection and mitigation [27]. The proposed techniques used the intrusion detection and mitigation in a trust-based hybrid collaborative RPL protocol to detect the malicious sybil nodes to determine the proposed work performance and the correction of the network that determine the average energy consumption protocol for the attack detection and maintenance of the energy consumption at each node selection and determination of message exchange and network lifetime.

3. Problem statement

The foremost problem statement considered in this work is the blockchain enabled hybrid attack detection and mitigation in RPL. some specific problems in the existing work are provided as follows,

In this research paper, version number attacks performed in the resource-constrained network were identified using an improved ML model named gradient boosting [28]. To detect version number attacks, the work encompasses four subprocesses such as information acquisition, cleansing, feature selection, and intrusion detection. Initially, control messages are collected using a tool in a PCAP file format and then analysed by Wireshark and saved in a JSON file format. Then, normal and abnormal features were extracted using a python model and kept in a CSV file format. After that, data cleansing was performed in terms of duplicate and unwanted data removal. At the end, the nodes were classified as benign and malign using the ML model by considering several features like rank, version, packet length, source/destination IP, DAO sequence etc.ws,

- In this research work, intrusion detection is performed based on several features. However, accurate malicious node detection requires more specified features. Thereupon, it influences the version number attack detection accuracy.
- Besides, gradient boosting is utilized for version number attack detection in this work which is a machine learning-based algorithm. As the ML algorithms have less capacity to learn from their own errors and their limited self-learning capability confines the accuracy of RPL attack detection.
- Along with this, ML-based model is used in this work for attack detection which is placed in a centralized manner. So that, proficient assaulters can bypass the intrusion detection system effortlessly hence resulting in security vulnerabilities.

In this research paper, the authors have proposed a framework to mitigate DAO attacks held in the RPL topology [29]. The insider DAO attack presence was addressed and mitigated using two working progressions in this work. In the initial progression, the number of DAO message transmissions was limited per child under a specific timeslot. When the child node exceeds its predefined threshold for forwarding DAO messages, the parent node stops the packets. On the other hand, in the second phase, the DAO message sent by other nodes was restricted other than which child node had actually originated.

- DAO attack mitigation is done in this research work. However, the restriction over the DAO message forwarding affects the nodes' lifetime as it is actually resource- constrained. Hence, it results in network inconsistency as it paves to frequent local and global repair mechanisms.
- On the other hand, the reason behind receiving DAO messages is ineffectively investigated (cross-validation) hence it affects the overall scope of the mitigation. The malicious nodes' presence in the network is uneducated to the benign nodes. Hence, it diminishes future attack detection at the earlier stages.

The authors of this research work identified an attack (divide and conquer) in which a malicious node falsifies the rank and manipulates the optimal path to reach the root node [30]. As the RPL topology exchanges several control messages to construct the network, initially the root disseminates DIO messages. After receiving the DIO messages, each node in the network estimates its location in terms of minimum rank and maximum rank based on its neighbouring node's rank value. Here, the minimum and maximum rank (threshold) were calculated using a mathematical equation. Each node in the RPL detects the malicious node based on the threshold. If a node has any deviation from its actual rank value, it was labelled as malicious and added to the blacklist.

- In this work, malicious nodes were blocked once they deviate from the threshold value. However, several nodes' rank may change if their mobility speed increases. Hence, blocking the malicious nodes without proper cross-validation limits the IDS accuracy.
- On the other hand, rank attacks were identified based on a threshold value. However, it is insufficient to differentiate a malicious node from a legitimate node, hence it affects effective classification.
- Here, DIO messages are plainly exchanged in the network. Such a scenario welcomes the assaulters to perform other attacks in terms of spoofing, man in the middle attack and so on. Henceforth, it affects the overall security of the network.
- In addition to that, malicious node detection is done by the node itself. As it is already belonging to the power, memory, energy, and computation constraints, results in reduced node lifetime and increases the consumption of resources.

In this research work, the authors have introduced a mechanism to ensure high security against routing attacks that arise in low power lossy networks using blockchain and improved gradient boosting [31]. The attacks detected in this work were rank attacks and version number attacks. Here, the Ethereum blockchain was acting as the medium between low-power lossy network and an intrusion detection system. Initially, the node estimates its rank based on the expected transmission count from DIO messages whereas malicious nodes increment their rank than the expected threshold. Using blockchain smart contract functions such as rows addition (routing info is stored in the blockchain), rank estimation (gives alerts on rank changes), and version checking (gives alerts on version changes), alerts were triggered for improving security.

- Rank of a node is determined by the expected transmission count. However, it is insufficient for effective rank determination. Thus, it results in end-to-end delay, high packet loss rates, security issues, and communication overhead.
- Along with this, intellectual attackers can perform cooperative attacks. In such a scenario this research work would yield less attack detection and mitigation efficiency. So that it affects the well-being of low power lossy network.
- In addition to that, optimal IDS placement is unconsidered in this work. By doing so, monitoring the exchange of control messages and adapting to the network dynamics becomes more complex.
- The authors of this research work have assumed that all the nodes are legitimate. However, limiting the access of unauthorized nodes was given the least importance. Hence, it results in computational complexity and poor network performance.

To overcome the problem faced by the existing works, network fabrication is performed in order to

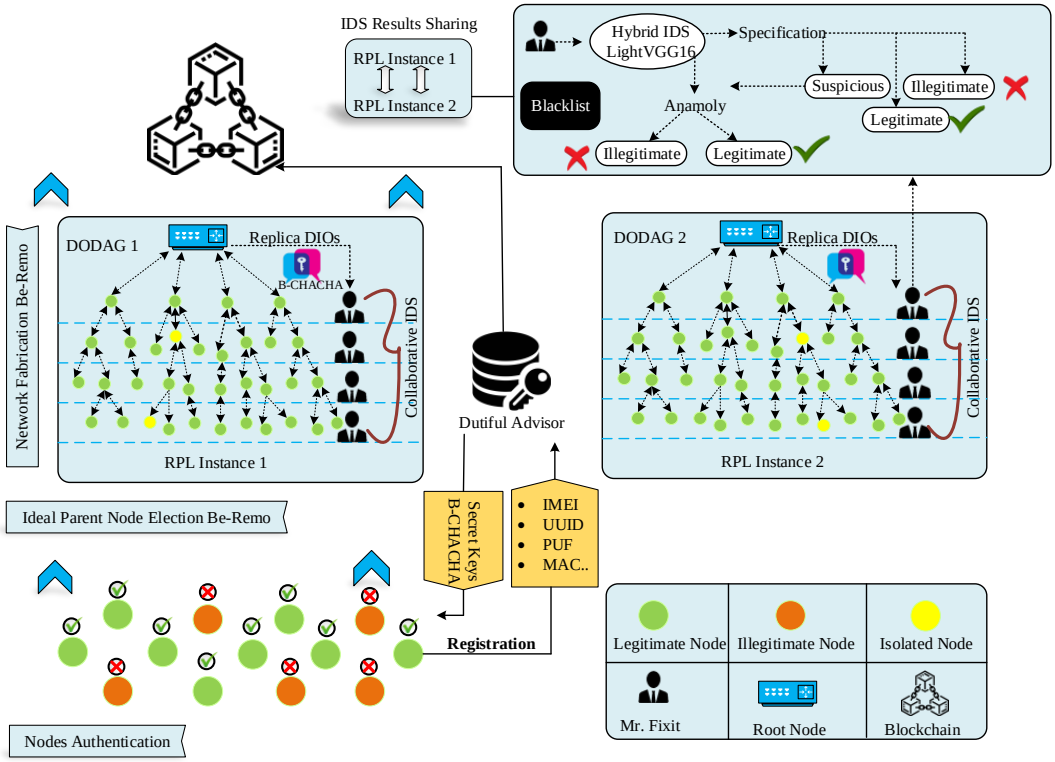

Figure. 1 Overall Architecture of the Proposed Secure RPL

ideally place MR. Fixits and to cope with network dynamic using Be-Remo approach. The node in the RPL topology is urged to registration at dutiful advisor by the parameters and dutiful advisor offers a secret key using B-CHACHA algorithm. Then, the root node in the RPL topology disseminates DIO information objects control messages contains the RPL instances and each node selects the parent node by considering the features using Be-Remo. Here, hybrid IDS (i.e., specification-based IDS and anomaly-based IDS) are performed using the LightVGG16 algorithm. The mentioned algorithm reduces the computational complexity.

4. Proposed work

The proposed work mainly focuses on hybrid and collaborative routing attack detection and mitigation in RPL, which are stored in the blockchain. The overall architecture of the proposed work is shown in Fig.1.

A. System model

The major theme of the proposed work is to offer high security to the RPL nodes by performing both specification and anomaly-based intrusion detection in a low-power and lossy network using a lightweight deep learning (DL) algorithm. By utilizing DL, we can achieve more robust classification results. The research work has several key entities named, the root node, parent node, child node, dutiful advisor, and several Mr. Fixits, which are mentioned as below,

*(i)**Nodes***

The node determines the order in which the terminals are driven and acts as the connection point among network devices. In the proposed consists of several nodes such as child node, parent node and the root node.

*(ii)**Dutiful advisor***

The advisor plays a role by registering the nodes in the RPL topology and also offers the secret key to the node for secure routing.

*(iii)**Mr. Fixits***

Mr. Fixits which are juxtaposed with digital ledger technology (blockchain) and deployed by the blockchain so that information security is assured and bypassing the intrusion detection system is suppressed.

*(iv)**Blockchain***

The blockchain incorporates with lightweight which adopts secure routing for minimizing computational burden and allows storing transaction securely.

B. Network Fabrication & Nodes Authentication

In this first phase, we perform network fabrication to ideally place Mr. Fixits and to cope with the network dynamics using a Be-Remo algorithm. The mentioned optimization algorithm has improved in terms of high convergence and supreme accuracy by means of adding adaptive probability (to decide whether to explore or exploit),

stochastic (for augmenting exploration capacity), and reboot (to foil population from stagged states) strategies. This progression actually divides the Destination Oriented Directed Acyclic Graph (DODAG) topology into multiple layers and allocates 3 child nodes per parent to avoid the parent node burden, high energy consumption, degradation of node lifespan, delay, etc. From Eqs. (7) to (12), the DODAG topology is obtained. In each layer, Mr. Fixit is responsible for monitoring the exchange of control messages. This layer-wise fabrication eases the processing of parent nodes by reducing the packet loss rate and offers robust workability.

After network fabrication, the nodes in the RPL topology are urged to do registration at Dutiful Advisor by giving parameters like IMEI (International Mobile Equipment Identity, UUID (Universally Unique Identifier), PUF (Physical Unclonable Function), MAC address (Media Access Control), and the location. The Dutiful Advisor offers secret keys to the nodes using the B-CHACHA algorithm. The stated algorithm overcomes the drawbacks of conventional CHACHA by incorporating ASCII values which are resistance against random nonce value cracking. By performing authentication, unauthorized access is revoked; thus, this process acts as front-tier security.

The nonce values are adopted randomly in the conventional Cha-cha 20. The plain text can be retrieved easily if the attacker detects a random value. Thus, prior to encryption, the plain text is transmitted to its value to prevent this and improve the algorithm's security level.

The 4×4 matrix input of size 512 bits is taken by the Cha-cha20 in this matrix, the first row is a 128-bit relentless string, and the second collected with the third row is filled with a total size of the 256-bit key. In the last row, the initial element is a 32-bit hunk message pawn. Similarly, the last rows remaining rudiments are filled through the after of 96 bits. Thus, the Cha-cha20's initial state with the effort values is formed as

$$R_{o\times p} = \begin{bmatrix} b[0] & b[1] & b[2] & b[3] \\ l[0] & l[1] & l[2] & l[3] \\ l[4] & l[5] & l[6] & l[7] \\ ctr & p[0] & p[1] & p[2] \end{bmatrix} \rightarrow \begin{bmatrix} r[0] & r[1] & r[2] & r[3] \\ r[4] & r[5] & r[6] & r[7] \\ r[8] & r[9] & r[10] & r[11] \\ r[12] & r[13] & r[14] & r[15] \end{bmatrix} \quad (1)$$

where the input medium comprises constants $(b[0], \ldots . b[3])$, which are the hex notation of the nonce, is depicted as $R_{o\times p}$, keys for encoding sideways with decryption are $(l[0], \ldots . l[7])$, to locate the key brooks position, the hostage ctr is applied, and the number applied once is called a nonce. Odd besides even remain the 2 ways fashionable in which the quarter smooth-edged function is realized. The even smooth-edged is positioned on the diagnosis of the state matrix $R_{o\times p}$.

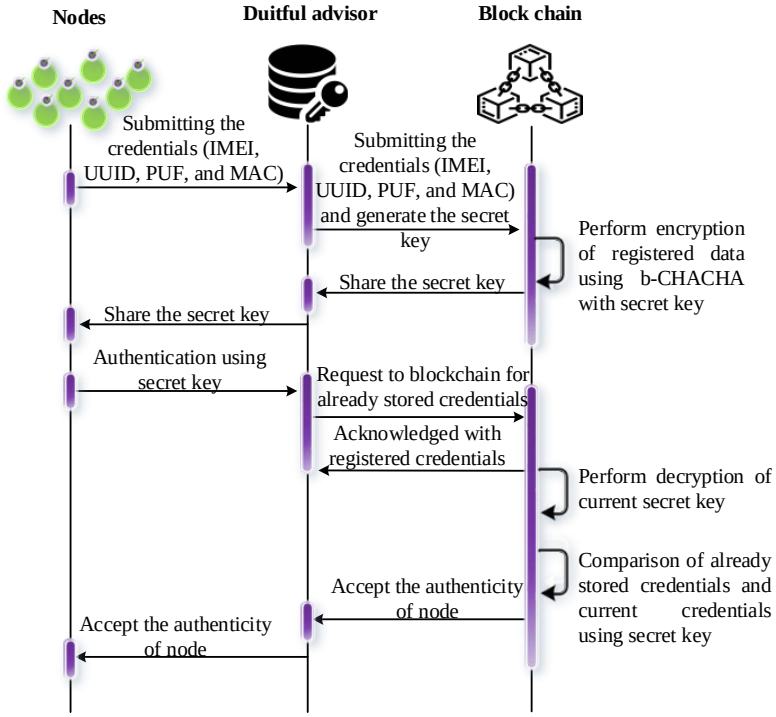

Figure. 2 Authentication of nodes using B-CHACHA

$$FG(odd)_{R_{o\times p}} = FG\begin{cases}(r[0], r[4], r[8], r[12])\\(r[1], r[5], r[9], r[13])\\(r[2], r[6], r[10], r[14])\\(r[3], r[7], r[11], r[15])\end{cases} \quad (2)$$

$$FG(even)_{R_{o\times p}} = FG\begin{cases}(r[0], r[5], r[10], r[15])\\(r[1], r[6], r[11], r[12])\\(r[2], r[7], r[8], r[13])\\(r[3], r[4], r[9], r[14])\end{cases} \quad (3)$$

Every single sector round implements the following purpose as, where the four 32-bit column of $R_{o\times p}$ are described as $r[0], r[4], r[8], r[12]$.

$$FGE = \begin{cases} r[0] = r[0] + r[4] \to r[12] = (r[12] \emptyset\, r[0]) << v\\ r[8] = r[8] + r[12] \to r[4] = (r[4] \emptyset\, r[8]) << v - 4\\ r[0] = r[0] + r[4] \to r[12] = (r[12] \emptyset\, r[0]) << v - 4\\ r[8] = r[8] + r[12] \to r[4] = (r[4] \emptyset\, r[8]) << v - 1 \end{cases} \quad (4)$$

The addition procedure is quantified as \$, the XOR operation is signified as $\emptyset$, the rotation procedure is displayed as $<<$, and the amount bits to be alternated is stated as $\Re$. Therefore, to attain the key cohort, the updated matrix is attached to the initial public, which is uttered as $R_{o\times p}^{key}$ as,

$$CGI = W_{inp(ASCII)} \emptyset\, R_{o\times p}^{key} \quad (5)$$

where the input data transmogrified to its ASCII value is extended as $W_{inp(ASCII)}$, the cipher text developed succeeding to encryption is extended as CG, the input plain text to be scrambled is noted as input. The data decoding is performed when the user gets admittance to the data, it is formulated as,

$$W_{inp(ASCII)} = CGI\, \emptyset\, R_{o\times p}^{key} \quad (6)$$

Consequently, the data $W_{inp(ASCII)}$ obtained, which is in this ASCII value, is communicated to the plain text, which is then applied for further dispensation.

C. Ideal Parent Node Election

After authentication, the root node in the RPL topology disseminates DIO (DODAG Information Object) control messages to build the network for effective communication. Here, the border router acts as the root node. The DIO control message contains the RPL instance ID, version number, rank information, and objective functions. Subsequently, each node selects its parent by considering several features in terms of ELT (Expected Lifetime), ETX (Expected Transmission Count), mobility, trust value, residual energy, and rank using the Be-Remo algorithm. The ideal parent selection process yields fruitful benefits in terms of reduced end-to-end delay, low packet loss rate, and better network consistency. Then, the child node sends DAO (DODAG Advertisement Object) control messages to the parent node for levying down the downward routes.

On the other hand, the nodes which are out of the DODAG range, and which are under local repair send DIS (DODAG Information Solicitation) control messages. Upon receiving DIS, the available node shares DIO messages with the child nodes. In the RPL, global and local repair mechanisms are included. In the global repair mechanism, the entire topology is reconstructed, whereas in the local repair mechanism, the energy-constrained node poison outs its own routes from its children by indicating the need to find alternate parents.

Node assortment for the DODAG range is a stochastic strategy extensively used in optimization algorithms. It has large interpretations in the high probability of accidental walking for cumulative the chance of the system construction. After that, the method can combine the levy aeronautical into the formula Stochastic Fitness Optimization strategy, which is described as follows,

$$Y(n+1) = Y_{bst}(n) - \left(rnd \cdot \left(\frac{Y_{bst}(n)+Y_{rnd}(n)}{2}\right) - Y_{rnd}(n)\right) \cdot Lvy(n) \quad (7)$$

$$lvy(G) = 0.01 \times \frac{s\times\varrho}{|w|^{\frac{1}{\gamma}}} \quad (8)$$

$$\varrho = \left(\frac{\varpi(1+\gamma)\times sin\left(\frac{\Psi\gamma}{2}\right)}{\varpi\left(\frac{1+\gamma}{2}\right)\times\gamma\times 2^{\left(\frac{\gamma-1}{2}\right)}}\right)^{\frac{1}{\gamma}} \quad (9)$$

where lvy represents the flight function, and D is the measurement size of the problems, S and W are chance values assigned between 0 and 1, and γ is an endless number equal to 1.5. The restart systems give a worse separate jump out of the home-grown optimum, so they are used to prevent the population from deteriorating. If the trail values are not abridged beyond the predefined lmt , the position will be substituted by choosing the place with a better fitness value from Eq. (7).

$$Y(n+1) = fe + rnd \cdot (se - fe) \quad (10)$$

$$Y(n+1) = rnd \cdot (se + fe) - y(n) \quad (11)$$

where fe and se are the inferior and upper sure of the problematic, respectively. From Eq. (6), the chance opposition-based learning policy is used to obtain a contradictory site. A better solution produced from Eqs. (4) and (5) is adopted if the experimental value is not less than the limit.

$$Y(n+1) = (se + fe) - rnd \cdot Y(n) \quad (12)$$

D. DL Assisted Collaborative and Hybrid Intrusion Detection

After selecting the ideal parent, collaborative and hybrid intrusion detection is performed with the help of Mr. Fixits, who is positioned in each layer of the RPL topology. Mr. Fixits closely watches the exchange of control messages in a nonstop manner. In hybrid IDS, specification-based IDS and anomaly-based IDS are performed respectively using the LightVGG16 algorithm. The mentioned algorithm reduces computation cost and trainable parameters by replacing the actual convolution layers with depth-wise separable layers and dual attention modules channel (which is need to be surfed and spatial (where it needs to be plotted)).

Then anomaly detection is done to investigate the suspicious nodes. For anomaly detection, we considered version number attacks, DAO attacks, and rank attacks in which each attack severely affects the network performance. To be more specific, version number attack results in network inconsistency. A DAO attack consumes the energy of the nodes and results in a low network lifetime. Rank attack forces child nodes to join under the malicious nodes which also results in an unstable network.

Whenever the root node disseminates DIO messages, its replica copies are securely given to each Mr. Fixit for intrusion detection. As they are continuously monitoring the nodes, they quickly identify which node is abnormal or malicious. For that, we have trained Mr. Fixits with several features such as the number of DAO messages a node has received and transmitted (version & rank), the number of DIO messages a node has received and transmitted (version & rank), the range of a node from the root node and the state of the route poisoned node (DIS flooding), rank changes Vs mobility and timestamp (rank). At last, they classify the suspicious into illegitimate and legitimate.

Primarily, specification-based IDS is performed based on network behaviours in both local repair mechanisms and global repair mechanism cases and classifies the nodes as legitimate, illegitimate, and suspicious. We've considered some of the network behaviours as mentioned are Local repair mechanism and Global repair mechanism. The local repair mechanism involves poison message, processing DIO, sending DAO, receiving DAO, sending DIO, receiving DIO, sending DIS, sending no change DIO, sending new changed DIO, and sending DAO-ACK. Then global repair mechanism involves sending DIO, receiving DIO, sending DAO, receiving DA, sending DAO-ACK.

To thwart the co-operative attack performed by cyber assaulters, we effectively perform collaborative intrusion detection by communicating with different Mr. Fixit. When receiving intrusion detection results from other Mr. Fixit, each Mr. Fixit at other layers cognitively do cross-verification to detect whether the malicious node has a relationship (based on communication history) with other nodes or not. If such connectivity is found, isolation of those nodes is done. At last, illegitimate nodes are blocked and added to the blacklist in order to intimate the nodes presented in the network. All the control messages are securely exchanged throughout the network as it is encrypted using the B-CHACHA algorithm which acts as a shield for tackling Man in the Middle Attack (MIMA), Spoofing, and so on. Eventually, each instance's IDS results are shared to strengthen security practices. Fig. 3 represents the hybrid and collaborative intrusion detection. Consider network behaviours and spells $J_y \in I^{T\times R\times D}$ is input into the model. The attention module will infer a 1D channel wise consideration map $N_D \in I^{1\times 1\times D}$. The spatial attention module will infer a 2D longitudinal wise attention map $N_y \in I^{T\times R\times 1}$. The complete attention mechanism process can be abridged as follows:

$$J'_y = T_d(O_y) \uplus J_{y'} \quad (13)$$

$$J''_y = T_y(O'_y) \uplus J'_{y'} \quad (14)$$

where $\uplus$ denotes the element astute cot produce. The construction of channel-wise attention is stimulated by the inverted remaining module

The process of a normal remaining module can be decided as "compression-convolution-expansion". Comparatively, the process of an inverted lingering module can be settled as "Expansion-convolution-compression". Aimed at the channel attention module, the participation feature assortment will first knowledge a global regular pooling. The pooling value of each channel can be observed with a worldwide region of attention. Its calculation process is shown as:

$$V_d = GAP(l_d) = \frac{1}{T \times R} \sum_{i=1}^{T} \sum_{j=1}^{R} l_d(i,j) \quad (15)$$

where V_d is the pooling rate of the d th intrusion discovery and $l_d(i,j)$ is the value at position (i,j) of the d th finding in the input structures.

Pointwise convolution is accomplished after GAP to increase the exposure rate. It can be represented as:

$$V'_d = \sum_{i=1}^{D} R_d \times V_i \quad (16)$$

where V'_d is the pooling rate of the d th attack discovery, d is the enlarge ratio, R_d is the weight of the d th filter, and V_i is the assembling value of the ith attack.

Depth wise convolutional is accomplished after the first pointwise convolutional to citation the attack recognition and assortment. The spatial attention module is associated after the exposure attention module. It deeds the attack astute weighted structures as its given input. Its demeanour's the convolution with a normal convolutional layer. We select a 3×3 convolution kernel here to decrease the computational cost. It is verified that a 7×7 convolution kernel produces a somewhat higher accuracy for attack discovery. However, considering the rise model difficulty, we still use a 3×3 kernel for high accuracy of the discovery of module.

$$N_y(O'_y) = \text{ð}\left(O^{3\times3}\left([avgpool(O'_y); maxpool(O'_y)]\right)\right) \quad (17)$$

where ð signifies a sigmoid role. The attention module can be organized in three different conformations concerning the series or parallel fitting together.

5. Experimental results

In this section, we present the proposed Block-RPL based deep learning model-based hybrid routing attack detection and mitigation in RPL. This experimental research comprises three subsections explicitly simulation setup, comparative analysis, and research summary. The result section illustrates that the proposed work achieves superior performance compared to previous work.

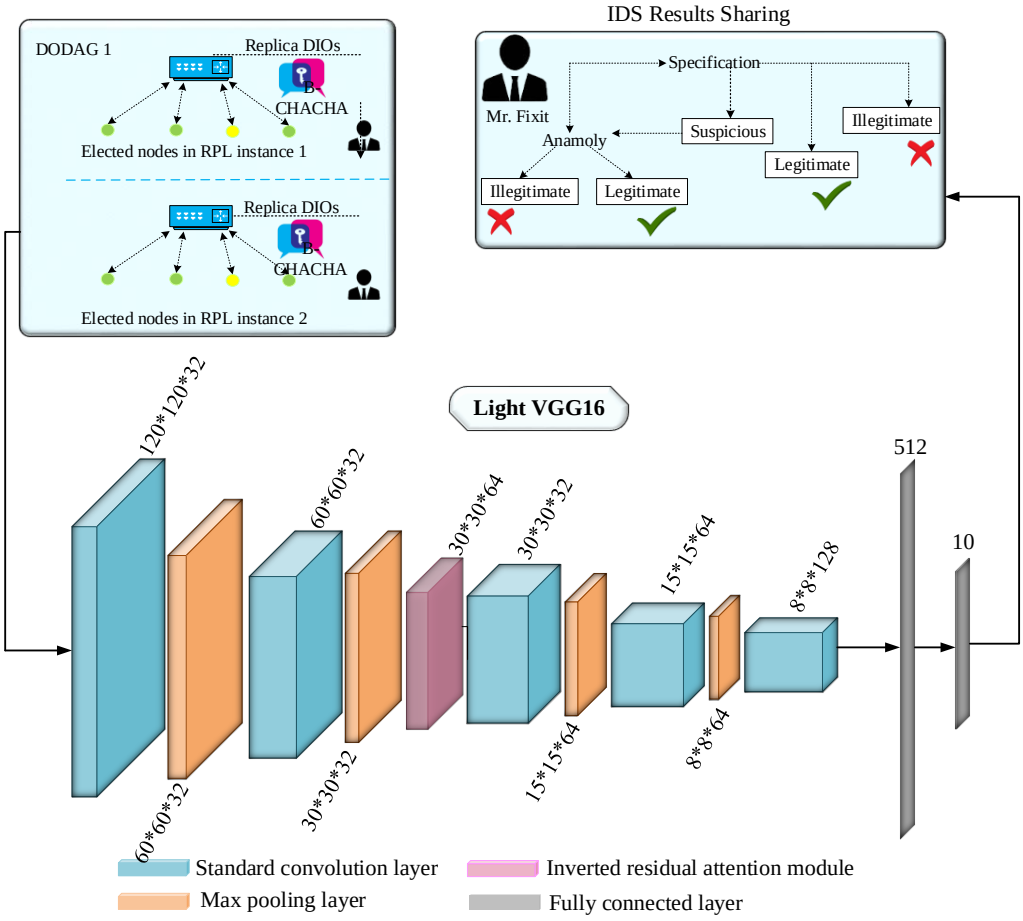

Figure. 3 Hybrid intrusion detection using Light VGG16

A. Simulation Setup

The simulation result of this proposed work is implemented by Cooja simulator available in Contiki operating system which improves the performance of this research. The proposed framework compared with several performance metrics and proven that our work achieves superior performance. Table 1 describes the system configuration and Table 2 describes the network parameters configuration.

Table 1. System Parameters

Hardware configuration	Hard disk	62 GB
	RAM	8 GB
	Processor	Pentium dual core and above
Software configuration	Simulation tool	Cooja simulator
	Operating system	Ubuntu 14.04 LTS

Table 2. Simulation Parameters

Parameter	**Value**
No. of nodes	150 nodes
No. of dutiful advisors	3
Root node	1
Sink node	1
Block chain	1
Network topologies	DODAG
Experiment duration(s)	1200
Operating system	Contiki
Frequency	IEEE 802.15.6 radio
Mac protocol	Contiki MAC
Setup delay(s)	62
Transmission of data rate	190-byte payload every 30 s
DIO minimum interval (ms)	11
DIO doublings interval (ms)	9
Operation of mode in RPL	Storing mode
Validation	Y
Control size path	0
DIO constant redundancy	9
Increase max rank	1200
Increase hop rank	250

B. Comparative Analysis

In this section, we epitomized the evaluation analysis between the proposed Block-RPL framework and existing works where we consider two existing works such as IoT-LLNS [3], [4] and ML-LGBM [28]. The main objective of this research is to provide accurate attack detection and mitigation based on blockchain. The proposed work achieved better performance in terms of number of DIO received, downward latency, energy consumption and attack detection accuracy.

a. Impression of DIO received.

This metric is utilized to estimate the DIO received of the proposed Block-RPL framework. The RPL message DIO is of ultimate importance in set up and amending the DODAG. DIO is constantly the primary log message that apiece node sends to all adjoining nodes proximately after startup.

$$DIORNK(R) = FLR\left(\frac{R}{increase\ mini\ hop}\right) \quad (18)$$

If the FLR are the floor messages of the DIO for calculating the received messages in the decision-making process. Fig. 4 represents the comparison of no of DIO received and time. The comparison result describes that the proposed work achieves lower DIO messages dissemination by adopting various features when compared to the other two previous work such as IoT-LLNS and ML-LGBM. The existing works are performed time with DIO by with anomaly detection by considering limited number of features for disseminates the DIO messages and the less attention in maintaining the discontinuous features of the obtained model of the work and the several factors are considered it also leads to massive amount of DIO messages.

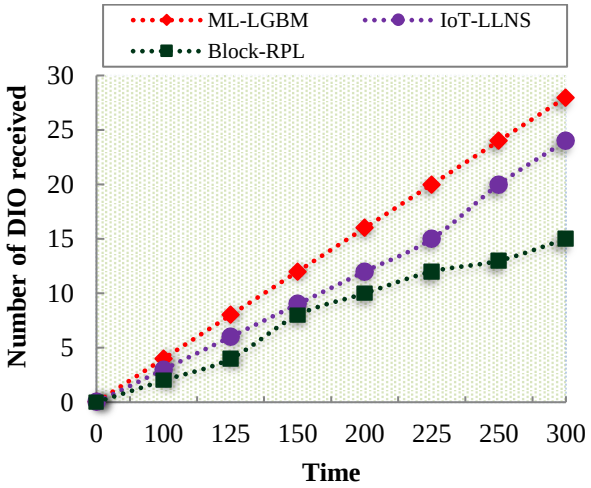

Figure. 4 Time Vs number of DIO received

The proposed Block-RPL approach performs number of DIO message received reduces the message abridged 2 where the exiting works performs IoT-LLNS is 3 and ML-LGBM is 8 received messages. The average DIO message received of the proposed work for 300 time is 15 which shows that we perform better than existing work such as IoT-LLNS is 24 and ML-LGBM is 28. From these numerical results shown in the graph indicates that out proposed work performs better than existing work.

b. Impression of downward latency

This metric is exploited to estimate the downward latency of the proposed Block-RPL framework. latency is the delay between a nodes action and web application response to the node activities, often referred to in networking terms as the total round-trip time it takes for a data packet to transmission.

$$\zeta = \frac{\varphi}{\varpi} \tag{19}$$

where ζ is the latency of the delay of the packets, φ is the link media delay and ϖ queueing delay of the node processing unit for delay serialization of the link data rate and the series. Fig. 5 represents the comparison of number of attack and downward latency. The comparison result describes that the proposed work accomplishes lower downward latency by parent node selection process yields with benefits when compared to the other two previous work such as IoT-LLNS and ML-LGBM. The existing works are performed number of attacks with downward latency by with parent node selection remaining levying down the downward routes and intrusion detection is performed based on several features. However, accurate malicious node detection requires more specified features.

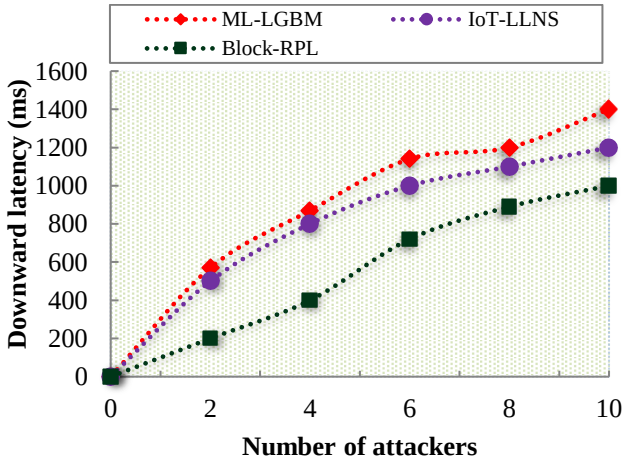

Figure. 5 No. of attackers Vs downward latency

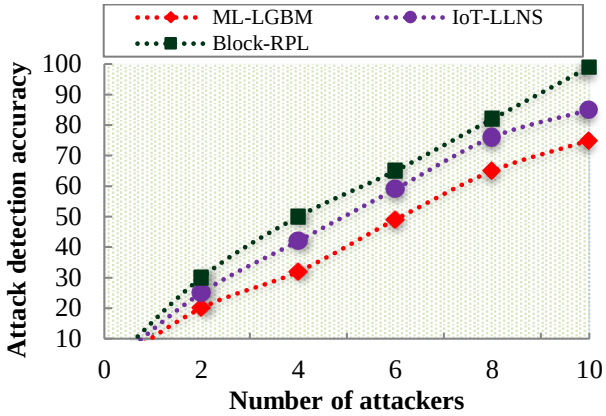

Figure. 6 No of attackers Vs accuracy

Thereupon, it influences the version number attack detection accuracy.

The proposed Block-RPL approach performs number of attackers reduces the latency abbreviated 200 where the exiting works performs IoT-LLNS is 500 and ML-LGBM is 575 downward latencies. The average downward latency of the proposed work for 10 number of attackers is 1000 which shows that we perform better than existing work such as IoT-LLNS is 1200 and ML-LGBM is 1400. From these numerical results shown in the graph indicates that out proposed work performs better than existing work.

c. Impact of accuracy

Accuracy is one of the key metrics which is exploited for estimating the accuracy of intrusion detection. The intrusion detection with high accuracy in IoT environment enhances the network environment. Accuracy $\Re$ is denoted as the summation ratio of true positive (ψ) and true negative (ϑ) to the addition of true positive, true negative, false negative (ξ) and false positive ($\Im$) which is expressed as,

$$\Re = \frac{\psi+\vartheta}{\psi+\vartheta+\xi+\Im} \tag{20}$$

Fig. 6 represents the comparison of number of attack and accuracy. The comparison result designates that the proposed work realizes higher attack detection accuracy by hybrid intrusion detection using specification-based IDS and anomaly-based IDS by considering both local repair mechanism and global repair mechanism when compared to the other two previous work such as IoT-LLNS and ML-LGBM. The existing works are performed number of attackers with attack detection accuracy by with considering only local repair mechanism to ensure the techniques of the features obtained process and maintenance of feature attack

detection and the gradient boosting is utilized for version number attack detection in this work which is a machine learning-based algorithm. As the ML algorithms have less capacity to learn from their own errors and their limited self-learning capability confines the accuracy of RPL attack detection.

The proposed Block-RPL approach performs number of attackers with high detection accuracy condensed 30 % where the exiting works performs IoT-LLNS is 25% and ML-LGBM is 20%. The attack detection accuracy of the proposed work for 10 number of attackers is 99% which shows that we perform better than existing work such as IoT-LLNS is 85 % and ML-LGBM is 75 %. From these numerical results shown in the graph indicates that out proposed work performs better than existing work.

d. Impression of energy consumption

This metric is applied to estimate the energy consumption of the proposed Block-RPL framework. the consumption of energy is measured by multiplying the number of power unit consumed in a given period of energy transmission. The formula for consumption of energy is given below,

$$\varsigma = {\varphi}/{(\frac{s}{100})} \tag{21}$$

In this formula, ς refers to the measured joules or kilowatt per hour and φ refers to power used per unit in watts. Fig. 7 represents the comparison of number of attackers and energy consumption. The comparison result designates that the proposed work realizes lower energy consumption for legitimate the node, node selection and intrusion detection based on many features for dissemination of DIO messages when compared to the other two previous work such as IoT-LLNS and ML-LGBM. The existing works are performed number of attackers with energy consumption by with considering node selection and intrusion detection with high energy without the network behaviors.

In the several processes such as authentication and network topology are not performed which makes high energy consumption.

The proposed Block-RPL approach performs number of attackers with low energy consumption summarized 15 where the exiting works performs IoT-LLNS is 20 and ML-LGBM is 23. The energy consumption of the proposed work for 10 number of attackers is 40 % which shows that we perform better than existing work such as IoT-LLNS is 65 % and ML-LGBM is 75 %. From these numerical results shown in the graph indicates that out proposed work performs better than existing work.

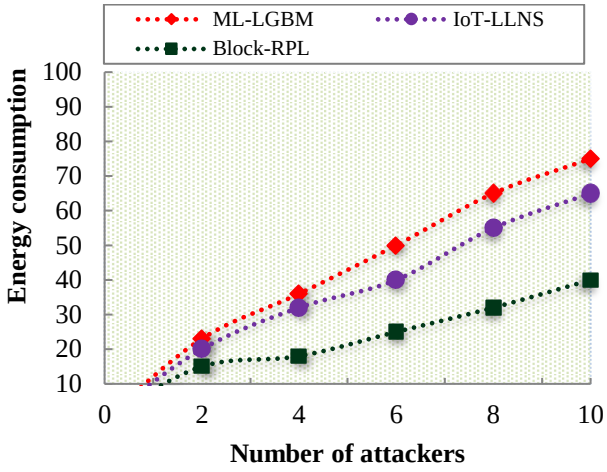

Figure. 7 No of attackers Vs energy consumption

C. Research Summary

In this section, we annotate the experimental results in summary which also proven that the proposed Block-RPL framework achieves superior performance through comparison result. The performance of proposed work is enumerated in terms of number of DIO received, downward latency, energy consumption and attack detection accuracy which are described in Figs. 4 to 7. Table 2 demonstrate the performance metrics in numerical analysis of proposed and existing works. Some of the highlights of this research are as follows,

- The network is segmented into several layers for the ideal placement of Mr. Fixits in order to cope with network dynamics using the Be-Remo optimization algorithm which has high convergence rate and better accuracy.
- Ideal parent node election is done using Be-Remo by considering ELT, ETX, mobility, trust value, residual energy, and rank to improve the reduce latency, and increase the network consistency to avoid frequent global and local repair mechanisms.
- At last, hybrid (specification and anomaly) and collaborative IDS are performed to accurately detect and isolate the malicious nodes from the network in an effortless manner using the LightVGG16 algorithm. To prevent the network from co-operative attacks, collaborative IDS is performed.

6. Conclusion

The major challenges in routing RPL are inaccurate detection and lack of security for attack detection is addressed by proposing a secure hybrid routing RPL. Initially, network fabrication is performed by ideally placing the MR. Fixits using Be-Remo and registration are urged at dutiful

advisor by giving parameters. Then, the dutiful advisor offers a secret key to the nodes using B-CHACHA approach. After that, each node selects their parents by considering features using Be-Remo algorithm and ideal parent node also be selected. Further, the collaborative and hybrid intrusion detection are performed with the help of Mr. Fixits using the LightVGG16 by considering network behaviours. Whenever the root node disseminates DIO messages, its replica copies are securely given to each Mr. fixit for intrusion detection. At last, blockchain is enabled for secure transmission of node and hybrid intrusion attack detection. The experimentation of the proposed approach is executed using cooja simulator available in Contiki operating system and the evaluation of proposed approach is carried out by comparing with the existing approaches in terms of no of DIO received, downward latency, attack detection accuracy and energy consumption. The performance of an approach is discussed with numerical analysis from which it can be proved that our approach outperforms the existing approaches in terms all the metrics.

Notation list

Notation	Description
$R_{o\times p}$	key for encoding sideway
$W_{inp(ASCII)}$	Cyber text
$R_{o\times p}^{key}$	Key cohort
lvy	Flight function
$\biguplus$	Astute code procedure
J_y	Network behavior's
V_d	Pooling rate
R_d	Assembling value of attack
V'_d	Discovery of attack
MIMA	Man in the Middle Attack
PDR	Packet delivery rate
DA	Dutiful Advisor
ζ	Latency
φ	Link media delay
ϖ	Queueing delay
$\Re$	Summation ratio
ψ	True positive
ϑ	True negative
ξ	False negative
$\Im$	False positive
$B\text{-}CHACHA$	Boosted CHACHA algorithm
DIO	DODAG Information Object
DAO	DODAG Advertisement Object
DIS	DODAG Information Solicitation
$Be\text{-}Remo$	Bettered Remora Algorithm
Pd	Probability of detection
Pfa	Probability of false alarm
ETX	Expected Transmission Count
ELT	Expected Lifetime

Conflicts of Interest

All authors affirm that there is no conflict of interest to disclose regarding the publication of this paper.

Author Contributions

Omar A. Abdulkareem was responsible for gathering needed the data, conceptual and methodology conducting the formal analysis, implementation the code, validation and writing the first draft of the article. Israa T. Aziz handled code validation, editing and supervising. Visualization project and supervision were done by Raja Kumar Kontham.

References

[1] R. Ruskone, *Big data analytics and computational intelligence for Cybersecurity*, Springer, 2022.

[2] A. Seyfollahi, M. Moodi, and A. Ghaffari, "MFO-RPL: A secure RPL-based routing protocol utilizing moth-flame optimizer for the IoT applications", *Comput. Stand. Interfaces*, Vol. 82, p. 103622, 2022.

[3] Z. Ghanbari, N. J. Navimipour, M. Hosseinzadeh, H. Shakeri, and A. M. Darwesh, "The applications of the routing protocol for low-power and lossy networks (RPL) on the internet of mobile things", *Int. J. Commun. Syst.*, Vol. 35, No.12, p.e5253, 2022.

[4] S. Promchaiwattana, and D. Banjerdpongchai, "Design of supervisory model predictive control for building HVAC system subject to time-varying operating points", In: *Proc. of 22nd Int. Conf. Control, Automation and Systems (ICCAS)*, pp.1404-1409, 2022.

[5] S. Senthilkumar, and P. Poorana, "Review paper: RPL protocol load balancing schemes in low-power and lossy networks", *Int. J. Sci. Res. Comput. Sci. Eng.*, Vol. 11, No. 1, pp. 7-13, 2023.

[6] T. A. Alamiedy, M. Anbar, B. Belaton, A. H. Kabla, I. H. Hasbullah, and Z. R. Alashhab, "A systematic literature review on machine and deep learning approaches for detecting attacks

in RPL-based 6LoWPAN of internet of things", *Sensors (Basel, Switzerland)*, Vol. 22, No.9, 2022.

[7] A. Verma, and V. Ranga, "Security of RPL based 6LoWPAN networks in the internet of things: A review", *IEEE Sens. J.*, Vol. 20, No.11, pp. 5666-5690, 2020.

[8] A. Seyfollahi, M. Moodi, and A. Ghaffari, "MFO-RPL: A secure RPL-based routing protocol utilizing moth-flame optimizer for the IoT applications", *Comput. Stand. Interfaces*, Vol. 82, p. 103622, 2022.

[9] A. Alsirhani, M. A. Khan, A. Alomari, S. Maryam, A. Younas, M. Iqbal, M. H. Siqqidi, and A. Ali, "Securing Low-Power Blockchain-Enabled IoT Devices Against Energy Depletion Attack", *ACM Trans. Internet Technol. (TOIT)*, Vol.23, No.3, pp.1-17, 2023.

[10] A. J. H. Witwit, and A. K. Idrees, "A comprehensive review for RPL routing protocol in low power and lossy networks", In: *Proc. of Int. Conf. New Trends Inf. Commun. Technol. Appl*., Cham, Switzerland, pp. 1-10, 2018.

[11] C. Kean, B. Ghaleb, B. Mcclelland, J. Ahmad, I. Wadhaj, and C. Thomson, "The mobile attacks under Internet of Things networks", In: *Proc. of the International Conf on Emerging Technologies and Intelligent Systems*, pp. 523-532, 2022.

[12] S. M. Muzammal, R. Murugesan, N. Z. Jhanjhi, M. Humayun, A. O. Ibrahim, and A. Abdelmaboud, "A trust-based model for secure routing against RPL attacks in Internet of Things", *Sensors (Basel, Switzerland)*, Vol. 22, No.18, p.7052, 2022.

[13] C. Z. Doğan, S. Yılmaz, and S. Şen, "Analysis of RPL Objective Functions with Security Perspective", In: *Proc. of Int. Conf. Sens. Netw.*, pp. 71-80, 2022.

[14] A. B. Ordu, M. Bayar, and B. Örs, "RPL authenticated mode evaluation: authenticated key exchange and network behavioral", In: *Proc. of 13th Int. Conf. Ubiquitous Future Netw. (ICUFN*), pp. 167-173, 2022.

[15] I. S. Alsukayti, and M. Alreshoodi, "RPL-based IoT networks under simple and complex routing security attacks: An experimental Study", *Appl. Sci*., Vol.13. No.8, p.4878, 2023.

[16] A. Agiollo, M. Conti, P. Kaliyar, T. Lin, and L. Pajola, "DETONAR: detection of routing attacks in RPL-based IoT", *IEEE Trans. Netw. Serv. Manag*., Vol. 18, pp. 1178-1190, 2021.

[17] E. V. Abhinaya, and B. V. Sudhakar, "A secure routing protocol for low power and lossy networks based 6LoWPAN networks to mitigate DIS flooding attacks", *J. Ambient Intell. Humaniz. Comput*., pp. 1-12, 2021.

[18] Z. A. Almusaylim, N. Z. Jhanjhi, and A. Al-Humam, "Detection and mitigation of RPL rank and version number attacks in the internet of things: SRPL-RP", *Sensors (Basel, Switzerland)*, Vol. 20, No.21, p.5997, 2020.

[19] S. Çakır, S. Toklu, and N. Yalcin, "RPL attack detection and prevention in the internet of things networks using a GRU based deep learning", *IEEE Access*, Vol. 8, pp. 183678-183689, 2020.

[20] D. B. Gothawal, and S.V. Nagaraj, "Anomaly-based intrusion detection system in RPL by applying stochastic and evolutionary game models over IoT environment", *Wireless Pers. Commun.*, Vol. 110, No.3 pp. 1323-1344, 2020.

[21] M. Sharma, H. Elmiligi, and F. Gebali, "A novel intrusion detection system for RPL-based cyber-physical systems", *IEEE Can. J. Electr. Comput. Eng.*, Vol. 44, No.2 pp. 246-252, 2021.

[22] P. P. Ioulianou, V. G. Vassilakis, and S. F. Shahandashti, "A trust-based intrusion detection system for RPL networks: detecting a combination of rank and blackhole Attacks", *J. Cybersecurity Privacy*, Vol.2, No.1, 2022.

[23] A. Verma, and V. Ranga, "Mitigation of DIS flooding attacks in RPL-based 6LoWPAN networks", *Trans. Emerg. Telecommun. Technol*., Vol. 31, No.2, p. e3802, 2020.

[24] I. S. Alsukayti, and A. Singh, "A lightweight scheme for mitigating RPL version number attacks in IoT networks", *IEEE Access*, Vol. 10, pp. 111115-111133, 2022.

[25] A. Mehbodniya, J. L. Webber, R. J. Rani, S. S. Ahmad, I. Wattar, L. Ali, and S. J. Nuagah, "Energy-aware routing protocol with fuzzy logic in industrial internet of things with blockchain technology", *Wireless Commun. Mobile Comput*., Vol.2022, No.1, 2022.

[26] F. Zahra, N. Z. Jhanjhi, S. N. Brohi, N. A. Khan, M. Masud, and M.A. Alzain, "Rank and wormhole attack detection model for RPL-Based internet of things using machine learning", *Sensors (Basel, Switzerland)*, Vol. 22, No.18, p.6765, 2022.

[27] D. Arshad, M. Asim, N. Tariq, T. Baker, H. Tawfik, and D. Al-Jumeily Obe, "THC-RPL: A lightweight trust-enabled routing in RPL-based IoT networks against sybil attack", *PLoS ONE*, Vol. 17, No.7, p.e0271277, 2022.

[28] M. Osman, J. He, F. M. Mokbal, N. Zhu, and S. Qureshi, "ML-LGBM: A machine learning model based on light gradient boosting

machine for the detection of version number attacks in RPL-Based Networks", *IEEE Access*, Vol. 9, pp. 83654-83665, 2021.

[29] W. J. Buchanan, "Mitigation mechanisms against the DAO attack on the routing protocol for low power and lossy networks (RPL)", *IEEE Access*, Vol. 8, pp. 43665-43675, 2020.

[30] M. A. Boudouaia, A. Abouaissa, A. Ali-Pacha, A. Benayache, and P. Lorenz, "RPL rank based-attack mitigation scheme in IoT environment", *Int. J. Commun. Syst.*, Vol. 34, No.13, p. e4917, 2021.

[31] R. Sahay, G. Geethakumari, and B. Mitra, "A novel blockchain based framework to secure IoT-LLNs against routing attacks", *Computing*, Vol.102, No.11, pp.2445-2470 ,2020.