Indonesian Journal of Computer Science
ISSN 2549-7286 (*online*)
Jln. Khatib Sulaiman Dalam No. 1, Padang, Indonesia
Website: ijcs.stmikindonesia.ac.id | E-mail: ijcs@stmikindonesia.ac.id

High-Level Defence Model against Routing Attacks on the Internet-of-Things

Lanka Chris Sejaphala[1], Vusumuzi Malele[2] , Francis Lugayizi[3]
chris.sejaphala@nwu.ac.za, vusi.malele@nwu.ac.za, francis.Lugayizi@nwu.ac.za
North-West University, South Africa

Article Information

Submitted : 1 Feb 2024
Reviewed: 11 Feb 2024
Accepted : 27 Feb 2024

Keywords

Internet of Things, RPL, Machine learning,

Abstract

This paper aims to answer the following research question: "To what extent can an intelligent security model effectively defend against routing attacks in RPL-based Internet of Things (IoT) with a demonstration of less network resource consumption, high detection rate, and minimal false negatives?" To answer this question, this paper proposes a high-level conceptual framework to defend the IoT against routing attacks. In recent works, mitigation techniques have been proposed to act against routing attacks, however conceptual defence or mitigation framework is not presented as a set of steps to follow to develop an effective and robust intelligent security model. This paper aims to present a high-level conceptual defence framework against routing attacks; specifically, sinkhole, rank, DIS-Flooding, and worst parent. The four mentioned routing attacks are capable of disturbing IoT network functions and operations, and consuming network resources such as memory and power.

A. Introduction

In recent years, technology has evolved significantly, leading to distinct generations characterised by major advancements and innovations. The current generation of technology is characterised by the proliferation of the internet users, IoT, Artificial Intelligence (AI), cloud computing, etc. It encompasses the third and fourth industrial revolutions [1]. The third industrial is referred to as the digital revolution characterised by the advent of the internet and digital technology. This revolution gave rise to the integration of Information Technology into various industries and transformed how people communicate, work, and access information.

The current phase of the industrial revolution, the 4th Industrial Revolution (4IR) is characterised by the convergence of physical, digital, and biological technologies, involving advancements in Internet-of-Things (IoT), Machine Learning, Three-Dimensional (3D) printing, Nanotechnology, and Biotechnology to name a few. The 4th Industrial Revolution aims to create "smart" and interconnected systems that can enhance efficiency and productivity across various sectors, including transportation, manufacturing, mining, agriculture, health, and energy [2].

The IoT is a paradigm of interconnected devices that collect and exchange data with each other from the environment of deployment and share the data over the Internet to achieve a particular goal (see Figure 1). This paradigm is used in a wide range of applications including home security management, industrial automation, smart energy monitoring and management, surveillance and military, smart cities, and farming, to name a few.

The IoT applications are growing rapidly, bringing significant differences in human lives, and helping industries like manufacturing, logistics, and health make critical decisions. The IoT market is estimated to grow over $2.4 trillion annually by 2027. This includes the growth of IoT devices from 8 billion in 2019 to 41 billion in 2027 [3]. The IoT has brought very significant benefits to our lives, society, and industries. Given the applications of IoT, most of the IoT devices are resource-constrained (small on-board memory, less energy, and low computation capabilities) and are expected to operate for a long period; thus, low power-consuming protocols are desired. Due to its resource constraint (energy, memory, computation) nature, IoT devices use standardised Routing Protocol for Low-power and Lossy networks (RPL) to communicate their routing information among themselves and route their observed data to the sink node.

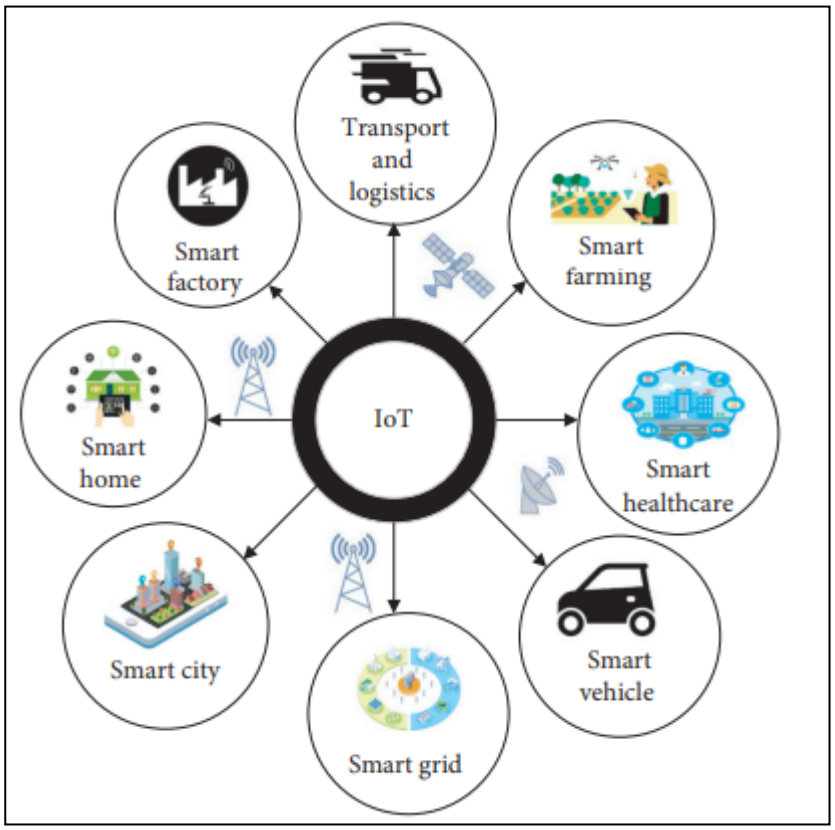

Figure 1. Applications of the Internet of Things [4]

RPL is the only DeFacto standardised network layer routing protocol for Low-power and Lossy Network (LLN) IoT [5]. Standardised in 2012 as RFC 6550 by Routing Over Low Power and Lossy Networks (ROLL) which is a working group of the Internet Engineering Task Force (IETF) [6]. The RPL has gained much popularity in the industry and academia because of its capability to provide efficient routing among resource-constrained smart IPv6-enabled IoT nodes, Quality of Services (QoS) support, and flexibility in adapting to different network topologies. The RPL uses low energy-consuming techniques to support self-organisation and self-healing for handling frequent node failure. Furthermore, providing efficient routing for IPv6 packets, these capabilities of RPL favours its usage in the IoT applications running on LLN infrastructure.

While IoT opens doors to the realisation of the connected world and new networking possibilities, it is vulnerable to routing attacks. The most common types of attacks in IoT running RPL are routing attacks since all nodes in the network partake in packet forwarding for the whole network [7]. These attacks cause massive data theft and system susceptibility [8]. Moreover, an increase in connected IoT devices and their insecure nature gives adversaries more options to gain access to the devices and use them to launch further large-scale catastrophic attacks like DDoS [9]. The popularity of RPL in IoT applications renders the security of this protocol of paramount importance. In other words, the deployment of RPL-based IoT has caused critical security vulnerabilities simultaneously, as such it has become crucial to address these vulnerabilities in RPL-based IoT [10]. The RPL as a widely deployed routing protocol in IoT is susceptible to routing attacks such as DIS-

flooding, sinkhole, rank, and worst parent attacks to name a few. Routing attacks pose a great threat to IoT running RPL as a routing protocol; and may affect its performance and functionalities [11].

In recent years, traditional techniques have been proposed; however, in literature, it is reported that Machine Learning techniques are more effective in terms of analysing IoT network traffic and making accurate predictions [12]. As such Machine Learning algorithms are utilised to monitor the behaviour of the network, classify network traffic, detect and mitigate network attacks, etc. However, these intelligent security models impose memory and computational power challenges in the IoT network, they require large memory and computational power to carry out their functions. In this study, edge computing is realised as a suitable solution to the challenges faced by intelligent model deployments.

This paper aims to propose a high-level conceptual framework that will contribute towards the development of a defence model that will effectively defend against routing attacks in RPL-based IoT with a demonstration of less network resource consumption, high detection rate, and minimal false negative. Taking advantage of the memory and computational capability of edge computing, as its use in model deployment to defend against routing attacks in IoT remains limited. Despite this introduction, this paper comprises of the following sections: literature review, methodology, proposed model, and conclusion and future studies.

B. Research Method

In this section, experimental setup and methods of data collection and analysis are presented. However, prior to the latter, this section will discuss both network and adversary modelling as a subsection of the experimental setup.

- **Experimental setup**

To run different simulation scenarios, the study utilises NetSim V13.2 installed on an HP laptop running a 64-bit Windows 10 Pro Operating System and 16GB RAM. MATLAB R2023 is utilised for performance metrics visualisation, the edge computing device is simulated as an HP PC running Linux OS with 16 GB memory.

- **Network Modelling**

We conduct extensive simulation experiments using NetSim to model IoT running RPL. Where IoT nodes are uniformly distributed in a defined network area, with a single DODAG root. The communication range of each node is 50m with a normal data rate of 250Kbps, and 802.15.1 MAC/PHY operates with a default configuration.

- **Adversary Model**

The attack model is followed to capture the performance of the network under different numbers of attacking nodes defined as percentages and to evaluate the robustness of the proposed scheme. The paper defines 5%,10%, and 15% for each network size (e.g., 25,36, and 64) as attacking nodes as a mechanism to evaluate the performance of the proposed scheme. As presented in Table 3 below, a network size of 25 IoT devices provides 1 attacking node at 5% attack, and a network size of 36 IoT devices provides 5 devices attacking nodes, and so on.

Table 1. Attack percentage distribution

	Attack %		
Network Size	5%	10%	15%
25	1	3	4
36	2	4	5
64	3	6	10

- **Evaluate performance**

To evaluate the performance of the proposed model, the paper considers the following performance metrics accuracy, precision recall, and area under ROC. These metrics are most used to evaluate the performance of Machine Learning algorithms. Furthermore, the paper utilises network performance metrics to evaluate the performance of the network during a network attack, no attack, and after the mitigation of the attack. Metrics that are considered are packet delivery ratio, energy consumption, detection rate, false negative, control message overhead, and end-to-end delay.

- **Assumptions and Limitations**

The network can only maintain one DODAG instance. The security of edge device is not the scope of this work, as such, the paper assumes that the edge device is secured.

- **Data Collection and Analysis**

Wireshark as a packet sniffing application is utilised as a data collection tool. Wireshark has the capability to capture network packets and display them at a granular level [25]. It can be used for real-time or offline analysis to assist with network analysis and ultimately network security. Collected data is analysed using a graphical representation. Both MATLAB and/or Microsoft Excel applications are utilised for the presentation of data.

C. Result and Discussion

This paper proposes a high-level conceptual framework to defend against routing attacks in IoT running RPL routing protocol. The framework utilises edge computing technology to deploy the Intelligent Security Model at the edge of the network. The high-level conceptual framework is depicted in Figure 2 and details of each component are described in the following subsections.

- **High-level conceptual framework**

The proposed framework implements ensemble learning, where multiple supervised machine learning algorithms are integrated into one model for the classification of network traffic data, detection of attacks, and identification of malicious nodes. A list of malicious nodes list is forwarded to the 6LowPWAN Border Gateway (6BG), which then multicast the malicious node list to the legitimate nodes with an instruction of selective-forwarding. As depicted in Figure 2, a proposed conceptual defence framework is presented. Edge computing technology is utilised to deploy the Intelligence Security Model, the framework uses packet

sniffing devices to forward the network traffic as a pcap file to the model deployed at ML-enabled edge device for analysis.

The output from the ML-enabled edge device is a list of malicious nodes identified in the network and is sent to the 6BG for mitigation. During mitigation, legitimate IoT nodes are instructed to drop control message packets from the malicious node list as a mitigation mechanism. While MATLAB is used to capture and display the performance of the network and the Intelligent Security Model.

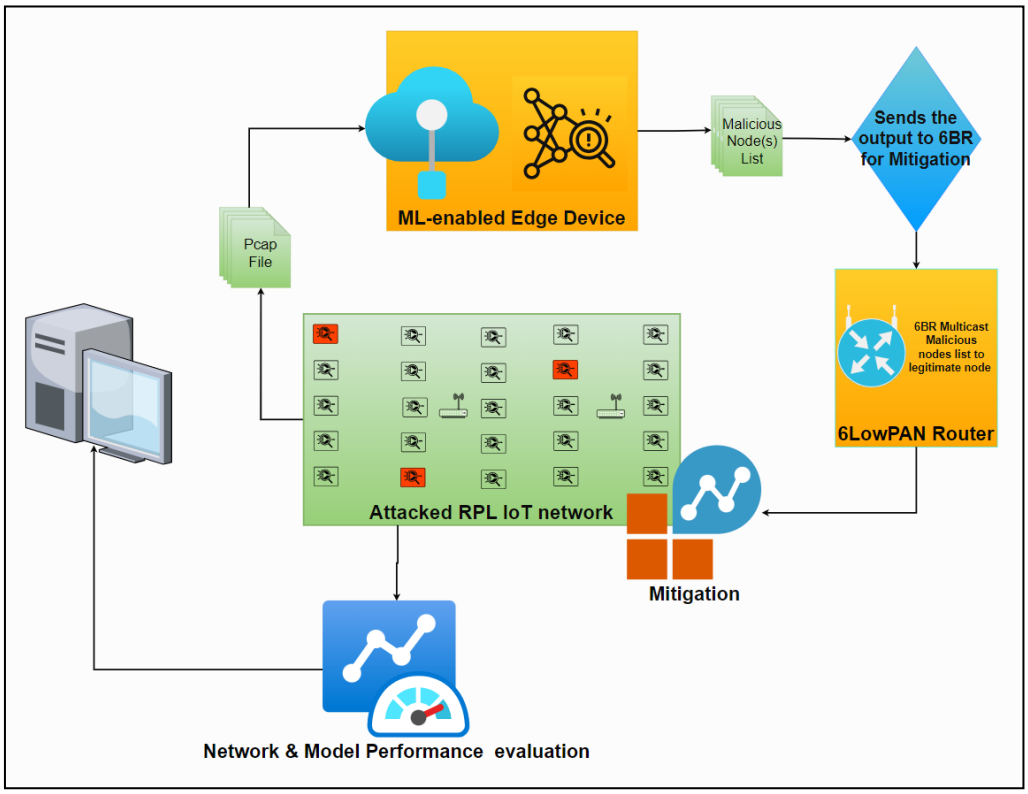

Figure 1. Proposed conceptual defence framework.

- **High-level conceptual framework: Literature Contribution**

It is fundamental to develop security techniques that detect and mitigate routing attacks with less or close to zero network overhead. Current state-of-art security solutions use traditional techniques (e.g., trust-based, rule-based, signature-based, encryption, and key-management, etc.) trying to ensure the security of the RPL-based IoT [13]. While securing the network, these techniques introduce heavy mechanisms at the expense of IoT devices and the overall network performance. To launch an attack, cybercriminals generally modify an existing attack code to replicate an attack. This is where the power of edge-enabled intelligent mitigation techniques proves to be an ideal solution because they rely on past learning rather than signature and rules which can be changed easily [14] while the computations are done on the edge of the network instead of at the IoT device level.

The fact that a large amount of data is acquired from IoT devices with limited resources such as computing, has rendered conventional techniques ineffective leading to the emergence of intelligent systems [12]. In recent years, research work

in the integration of artificial intelligence particularly machine learning as a security solution has been conducted [15]. It is evident that machine learning-based methods promise to be a viable solution against routing attacks, but little attention has been given to IoT [16]. It is expected that machine learning algorithms promise to produce desired results in efficient and effective mitigation approaches to address some of routing attacks in RPL-based IoT networks [17]. In the context of networks, the most used machine learning techniques from literature are supervised learning [18], they achieve high-performance metrics percentage in classifying several attacks. However, most of the proposed machine learning-based security techniques in RPL-based IoT only classify attacks without mitigation. It is known that RPL-based IoT has adopted some spectrum of wireless sensor network attacks [19]. In their study, they proposed a machine learning class, ensemble learning-based intrusion detection system for RPL-based IoT to detect against selected seven network layer attacks which use four different classifiers. The four classifiers e.g., boosted trees, subspace discriminant, RUS boost tree and bagged tree were trained and tested. Boosted tree achieved the highest accuracy of 94.5% and RUS boosted tree achieved a better area under ROC of 98%. However, their proposed system only classifies normal and attack traffic it does not neither identify malicious nodes nor mitigate them. Their system model does not offer an end-to-end mitigation mechanism.

Although in the recent past, some works have been done on traditional techniques aiming at securing RPL, showing acceptable results [20]. However, although these conventional techniques promise to mitigate routing attacks in RPL-based IoT, most of them do not evaluate resource utilization and communication overhead during detection and mitigation [21]. Furthermore, with conventional techniques, it is also not feasible to address multiple attacks with only one technique [22]. Moreover, these conventional techniques either introduce communication overhead, computation performance issues, and/or energy consumption in these LLNs. A conventional end-to-end mitigation technique to act against Network Isolation Attacks in defending RPL [23]. Unlike [19] and [23], [24] not only employed an intelligent security model to identify anomalies in the IoT but also realised and utilised fog computing for model deployment. In ensuring that the proposed model does not contribute much to IoT device resource consumption. They allowed expensive computation of the detection model to be handled by a fog device equipped with computational power and memory. However, as far as [19] realised the power of the intelligent model, they could only identify attacks, without mitigation. But [23] implemented end-to-end detection and mitigation technique. Whereas [24] integrated methods in [19] and [23] into fog computing to realise an end-to-end defence against one type of attack, DDoS, by classifying network traffic. This paper then proposes the integration of an intelligent security model into an edge device to defend against multiple routing attacks. Furthermore, evaluate both the performance of the model and network under different performance metrics.

In the IoT environment given its large-scale deployment, applications, and wide uses it is vital to develop an intelligent security model against routing attacks aiming at disrupting network functionality. The security model must be able to achieve a high detection rate, and almost close to zero false negative while mitigating the attacks with close to zero network overhead. Furthermore, the model

must consider the resource-limitation nature of the RPL-based IoT networks. To the best of our knowledge through literature, such an intelligent security model has not yet been developed. The work illustrated in Table 2 presents the theoretical contribution that our proposed model promises to close the gap.

Table 2. Theoretical gap contribution

Studies		Open issues				
		Effects of attacks on the network	**Proposed technique Resource consumption**	**Spectrum of attacks**	**Mitigation**	**Network performance metrics**
Existing Research work	**Conventional based**	Not addressed	Addrresed	Difficult to address multiple attacks	Techniques are able to mitigate and isolate malicious nodes from the network	Presented
	Intelligent Security based	Not addressed	Partially addressed	Able to address mutliple attacks at once	Techniques only attacks they do not provide mitigation mechanism	Not addressed, only machine learning metrics evaluation are presented
Proposed Study	**Intelligent security Model**	Will be addressed	Will be addressed, computations to be done on edge device	Mutliple attacks will be addressed	Malicious nodes will be identified, isolated and attacks will be mitigated	Both machine learning and network performance metrics will be presented

This paper attempts to close the gap of the need for a supervised machine learning mitigation model to act against routing attacks, to secure the network, and maximise its performance. As such, the paper contributes an intelligent security model as a defence mechanism against routing attacks in IoT running RPL as a routing protocol. The model will integrate best-performing supervised algorithms for the classification of network traffic, detection of attacks, and identification of malicious nodes. The model will take advantage of the edge computing technology and have all the computations done on the edge device, not the IoT device level.

D. Conclusion

In this paper, we proposed a high-level conceptual framework to defend against routing attacks in IoT running RPL. The framework displays the use of edge computing technology to store and execute the defence model, as edge computing technology is capable of integrating high-performing (in terms of memory storage and computational power) devices closer to the IoT end-devices. The framework demonstrates high-level end-to-end mitigation.

This paper aims to contribute towards the development of an effective and efficient Intelligent Security Model to defend against routing attacks in IoT networks running RPL. As such, the primary contribution of this paper is to propose a high-level conceptual framework for defence against routing attacks. The secondary contribution of the paper is the identification of a theoretical gap in the literature to utilise edge computing integrated intelligent security model to defend IoT against routing attacks. Limitations of the study are that the simulation tool can only simulate homogeneous IoT device networks.

In future work, routing attacks defence is intended to be addressed by developing an intelligent security model to defend IoT against routing attacks. Furthermore, future work will enhance the performance of the Intelligent Security Model by providing feedback on its performance and suggestions to improve its performance metrics. In such a way that the model will not only defend against the routing attacks, but its poor performing metrics will be improved from performance feedback.

E. References

[1] P. Ross, and K. Maynard, "Towards a 4th industrial revolution", Intelligent Buildings International, 13, (3), pp. 159-161, 2021.

[2] A.O. Adebayo, M.S. Chaubey, and L.P. Numbu, "Industry 4.0: The fourth industrial revolution and how it relates to the application of internet of things (IoT)", Journal of Multidisciplinary Engineering Science Studies (JMESS), 5, (2), pp. 2477-2482, 2019.

[3] R. Ahmad, and I. Alsmadi, "Machine learning approaches to IoT security: A systematic literature review", Internet of Things, 14, pp. 100365, 2021.

[4] M.Y. Mehmood, A. Oad, M. Abrar, H.M. Munir, S.F. Hasan, H.A.U. Muqeet, and N.A. Golilarz, "Edge Computing for IoT-Enabled Smart Grid", Security and Communication Networks, pp. 5524025, 2021.

[5] F.E. Hachemi, M. Mana, and B.A. Bensaber, "Study of the Impact of Sinkhole Attack in IoT Using Shewhart Control Charts", in Editor (Ed.)^(Eds.): 'Book Study of the Impact of Sinkhole Attack in IoT Using Shewhart Control Charts' (edn), pp. 1-5, 2020.

[6] A. Verma, and V. Ranga, "Analysis of routing attacks on RPL based 6LoWPAN networks", International Journal of Grid and Distributed Computing, 11, pp. 43-56, 2018.

[7] M. Koosha, B. Farzaneh, and S. Farzaneh, "A Classification of RPL Specific Attacks and Countermeasures in the Internet of Things", in Editor (Ed.)^(Eds.): 'Book A Classification of RPL Specific Attacks and Countermeasures in the Internet of Things' (edn.), pp. 1-7, 2022.

[8] R. Raman, B. Mandaloju, D. Singh, V. Tripathi, U.H. Maginmani, and J.L.A. Gonzáles, "An Experimental Study of Sink Hole Attacks and Distributed

Denial of Service (DDS) on IoT network-based Healthcare Applications", in Editor (Ed.)^(Eds.): 'Book An Experimental Study of Sink Hole Attacks and Distributed Denial of Service (DDS) on IoT network based Healthcare Applications' (edn.), pp. 990-993, 2023.

[9] A.K. Bediya, and R. Kumar, "Real Time DDoS Intrusion Detection and Monitoring Framework in 6LoWPAN for Internet of Things", in Editor (Ed.)^(Eds.): 'Book Real Time DDoS Intrusion Detection and Monitoring Framework in 6LoWPAN for Internet of Things' (edn.), pp. 824-828, 2020.

[10] Z. Fatima, N. Jhanjhi, S.N., Brohi, and N.A. Malik, "Proposing a Rank and Wormhole Attack Detection Framework using Machine Learning", in Editor (Ed.)^(Eds.): 'Book Proposing a Rank and Wormhole Attack Detection Framework using Machine Learning' (edn.), pp. 1-9, 2019.

[11] A. Jahangeer, S.U. Bazai, S. Aslam, S., Marjan, M., Anas, and S.H. Hashemi, "A Review on the Security of IoT Networks: From Network Layer's Perspective", IEEE Access, 11, pp. 71073-71087, 2023.

[12] S. Cakir, S., Toklu, and N. Yalcin, "RPL Attack Detection and Prevention in the Internet of Things Networks Using a GRU Based Deep Learning", IEEE Access, 8, pp. 183678-183689, 2020.

[13] M. Hasan, M.M., Islam, M.I.I. Zarif, and M.M.A. Hashem, "Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches", Internet of Things, 7, pp. 100059, 2019.

[14] I.F. Kilincer, F. Ertam, and A. Sengur, "Machine learning methods for cyber security intrusion detection: Datasets and comparative study", Computer Networks, 188, pp. 107840, 2021.

[15] A.M. Pasikhani, J.A. Clark, P. Gope, and A. Alshahrani, "Intrusion Detection Systems in RPL-Based 6LoWPAN: A Systematic Literature Review", IEEE Sensors Journal, 2021, 21, (11), pp. 12940-12968, 2021.

[16] M.D Momand, M.K. Mohsin, M.K., and I-ul-Haq: 'Machine Learning-based Multiple Attack Detection in RPL over IoT', in Editor (Ed.)^(Eds.): 'Book Machine Learning-based Multiple Attack Detection in RPL over IoT' (2021, edn.), pp. 1-8

[17] F. Zahra, N.Z. Jhanjhi, S. Brohi, N.A. Malik, and M. Humayun, "Proposing a hybrid RPL protocol for rank and wormhole attack mitigation using machine learning". Proceedings of the 2nd International Conference on Computer and Information Sciences (ICCIS). 2020. https://doi.org/10.1109/ICCIS49240.2020.9257607

[18] A, Jamalipour, and S. Murali, "A Taxonomy of Machine-Learning-Based Intrusion Detection Systems for the Internet of Things: A Survey", IEEE Internet of Things Journal, 9, (12), pp. 9444-9466, 2022.

[19] A. Verma, and V. Ranga, "ELNIDS: Ensemble Learning based Network Intrusion Detection System for RPL based Internet of Things", in Editor (Ed.)^(Eds.): 'Book ELNIDS: Ensemble Learning based Network Intrusion Detection System for RPL based Internet of Things' (edn.), pp. 1-6, 2019.

[20] B. Chen, Y. Li, and D. Mashima, "Analysis and enhancement of RPL under packet drop attacks", in Editor (Ed.)^(Eds.): 'Book Analysis and enhancement of RPL under packet drop attacks' (edn.), pp. 167-174, 2018.

[21] A. Raoof, A. Matrawy, and C.H. Lung, "Routing Attacks and Mitigation Methods for RPL-Based Internet of Things", IEEE Communications Surveys & Tutorials, 21, (2), pp. 1582-1606, 2019.

[22] K. Sanders, and S.S. Yau, "An Effective Approach to Protecting Low-Power and Lossy IoT Networks Against Blackhole Attacks", in Editor (Ed.)^(Eds.): 'Book An Effective Approach to Protecting Low-Power and Lossy IoT Networks Against Blackhole Attacks' (edn.), pp. 65-72, 2021.

[23] A.D. Seth, S. Biswas, and A.K. Dhar, "Mitigation Technique against Network Isolation Attack on RPL in 6LoWPAN Network", in Editor (Ed.)^(Eds.): 'Book Mitigation Technique against Network Isolation Attack on RPL in 6LoWPAN Network' (edn.), pp. 68-73, 2021.

[24] R.J. Alzahrani, and A. Alzahrani, "A Novel Multi Algorithm Approach to Identify Network Anomalies in the IoT Using Fog Computing and a Model to Distinguish between IoT and Non-IoT Devices", Journal of Sensor and Actuator Networks, 12 (2), pp. 19, 2023.

[25] U. Lamping, and E. Warnicke, "Wireshark user's guide", Interface, 4, (6), pp. 1, 2004.