Intensive Investigation of RPL Attacks Based on Artificial Neural Network in Internet of Things (IoT)

Faisal Ghazi Abdiwi [1] **Yasamin Hhamza abdulammer**[2] **Reyadh Hazim Mahdi** [3]

Faisal.ghazi@muc.edu.iq Yhamza@uomustansiriyah.edu.iq reyadh.hazim@uomustansiriyah.edu.iq

Abstract: The restricted Internet of Things (IoT) devices are well-suited to the energy-efficient processes and accessible, confined, secure modes of operation of the Routing Protocol for Low Power and Lossy Networks. Nevertheless, we feel compelled to investigate, evaluate, and provide probable explanations for routing vulnerabilities due to the pressing need for security in RPL-based IoT networks. In order to study, evaluate, and quantify network topology assaults in RPL, also known as rank and local repair, this research introduces a lightweight model of an artificial neural network. This study builds a small artificial neural network (ANN) model with a low false positive rate, high accuracy (up to 0.99), and a significant effect by merging two datasets of attack scenarios. The suggested anomalous method is based on this strategy, which involves researching, evaluating, and capitalizing on the most crucial aspects of the RPL protocol.

Keywords: IoT Security, ANN learning, RPL attacks, Rank attack, Local Repair attack.

1. Introduction

changer. As the Internet (of computers) has progressed, it has naturally given rise to embedded and cyber-physical systems—"things" that aren't computers but do contain computers. With a distributed system of low-cost sensors and networked objects, we may gather data about our world and environment at a finer scale than ever. This specificity level will allow for greater efficiency and the provision of cutting-edge services in many application areas, such as ubiquitous healthcare and smart city infrastructure. Serious security and privacy issues have been raised since collecting, processing, and sharing information about individuals is becoming

[1] Ph.D., Department of Computer Science and Information Systems, Al-Mansour University College, Baghdad, Iraq
[2] Ph.D., Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, Iraq
[3] M.Sc., Department of Computer Science, College of Science, Mustansiriyah University, Baghdad, Iraq

increasingly covert, dense, and pervasive [1]. Many security issues have been found in connected devices like smart locks [2] and cars [3]. Some of the features of the IoT that raise security and privacy concerns include its decentralized structure, heterogeneity in device resources, an abundance of attack surfaces, context-aware and situation-specific nature of threats, and scalability[4].

In the IoT, there are no limits on the processing and communication capabilities of the devices that can be connected wirelessly, in contrast to sensor networks or other wireless communication networks. IoT security issues directly impact the significance of device security because, as a result, IoT systems are susceptible to several threats [5]. In order to protect the privacy of all sent and received data, secure communication in an IoT system is essential. In other words, the connection between secrecy and veracity must be protected. Due to the utilization of open authentication, ensuring the security and integrity of the system, establishing a secure connection, maintaining confidentiality, and ensuring data veracity become inherently challenging. The system is still susceptible to a multitude of threats. RPL is a real routing protocol for IoT systems. However, it has many security problems regarding data flow, topology, and node resources [6][7].

Problem Statement: The primary difficulty arises from the fact that Internet of Things (IoT) systems are highly susceptible to cyber-attacks due to the fact that they handle and control real-time events that produce a large amount of aggregated data from dispersed network nodes that are processed by a centralized curator.

handle events as they happen, which produce massive amounts of aggregated data from dispersed network nodes that are handled by a single curator and are very susceptible to cyber-attacks.

A novel RPL-based IDS design method addressed in recent papers uses Machine Learning and Deep Learning algorithms to detect attacks and mitigate risks intelligently. Researchers are increasingly focused on learning-based models to detect and respond to complex and unidentified attacks due to the challenges given by scenario-based methodologies and cyber-attack detection datasets. [8][9][10]. This paper introduces a model to identify and classify RPL attacks using an ANN learning algorithm. A lightweight ANN approach is proposed for IOT network resources. The key contributions are given as follows:

1- The emphasis of this paper is on attacks based on the topology of RPL networks. The analysis and investigation of attacks is the primary focus of our work.

2- As a case study on network topology attacks, design a lightweight ANN model to conduct in-depth research on, analyze, and classify RPL attacks in terms of rank and local repair.

3- Use the DARA public dataset to generate fresh examples of rank attacks and local rapiers by combining two attack scenarios [11].

PAPER ORGANIZATION: The RPL topology and a sample of the most typical attacks are covered in the section after. The present study being done to address RPL security issues is explained in Section 3, the proposed system is covered in Section 4, the results and analysis are covered in Section 5, and the conclusion and future work are covered in Section 6.

2. RPL Protocol Topology

Distance vector-based proactive routing technique, the RPL protocol design for low-power and lossy networks (LNN), is primarily recommended for LLN networks [12]. RPL is widely used in various Internet of Things (IoT) applications due to its adaptability to various technological restrictions.

RPL Topology: In an LLN network, when given an Objective Function, RPL will generate a DODAG (Destination-Oriented Directed Acyclic Graph) that will be used to connect the nodes (OF). The OF improves the DODAG's route generation with more desirable metrics like the Expected Transmission Count (ETX). Regarding communication, RPL allows for one-way traffic (smart devices talking to the DODAG root) and two-way traffic (the root talking to the smart devices). The IPv6 address of a node is its permanent digital fingerprint. Except for the root, all other nodes have at least one parent and a directory of direct adjacency graph (DAG) neighbors. Further, an RPL node's rank specifies how close it is to the root node; the lowest-ranked nodes are at the absolute bottom of the tree. One can think of the downward direction as the path that leaves the root and travels to other nodes and the upward direction as the road that leaves other nodes and returns to the root[13]. Figure [1] depicts the systematic DODAG network example.

Although the restrictions of RPL are designed to increase network efficiency, attackers can use them in several cunning ways. Attacks like Rank, local repair, and resource depletion are all potential scenarios. [14].

This study focuses on two categories of network topology attacks, namely local repair and rank.

Rank attack. The Rank assault is a style of coordinated threat. According to the RPL routing rule, "rank strictly increases in the downstream direction and strictly drops in the upstream way" [15]. This rule is designed to stop the nodes from taking a circuitous or inefficient route.

In the RPL topology, the rank property is a potential entry point for attackers as it is the primary factor for selecting parents. Because every given node's value might fluctuate at any time, even a small shift in the rank value can significantly impact the network's efficiency[16].

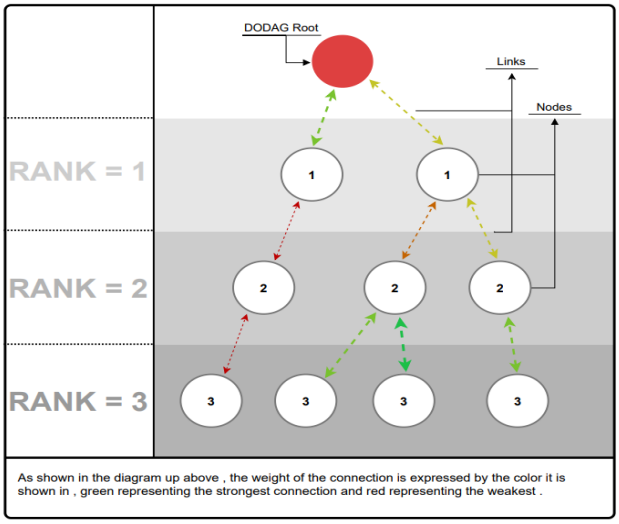


Figure 1. Example of DODAG network.

Local repair attack: Whenever a node in RPL loses contact with its preferred parent, it initiates a local repair procedure in order to restore the connection. Changing the DODAG ID value in DIO or updating the node's rank to infinite enables it to multicast DIO to all of its neighbors, kicking off a local repair procedure. Both strategies motivate surrounding nodes to look for a new parental figure. A converged RPL network can be quickly restored by local maintenance. This technique is meant to be invoked only when a child node can no longer communicate with its parent. An attacker can use both approaches maliciously to force unneeded local repairs while the child is still linked to its parent [17]. This is feasible because RPL does not describe a mechanism by which a node can ensure that a local repair undertaken by its neighbours is genuine[18]. The network's topology must be reorganized everywhere that a local repair is triggered. Aside from disrupting the routing process, this also causes the affected nodes to consume more energy.

3. Related Work

Recent research provides an useful in the IoT setting [19]. A thorough analysis was conducted by closely examining security attacks, RPL composition, components, and control messages [20]. They have also provided a taxonomy for classifying attacks and offered the organized classification of defenses developed by other researchers. One sort of attack against a protocol is addressed by Osman et al. [21], where a machine learning-based binary classification algorithm is given. Due to the

lack of a suitable dataset, the researchers created their own by developing a version number assault network model and simulating the attack using the Cooja network simulator. There are many methods for doing the crucial tasks of feature scaling and selection required for success in machine learning.

Yavuz et al. [22] proposed a deep neural network method to defend against RPL attacks, such as the rank attack. The dataset was produced with the help of the Contiki system's Cooja simulator. Using accuracy and other common performance criteria, they determined that the model fared well against a "hello flood" attack. Similar to competing approaches in this space, this one requires extensive training time and is vulnerable to a wide range of attacks on the model layers.

A trust-based approach mitigates security concerns about protocol-specific rank assaults in RPL networks. This approach involves simulating the impact of the predicted transmission count metric-based strategy on various network performance metrics, including power consumption, packet delivery speed, throughput, and network stability [23].

Table 1 Related Work Summary

RF	Approach	Algorithm
19	A survey of the current Internet of Things (IoT) communication and networking technologies	NA
20	They also supply a taxonomy for attack categorization and the systematic classification of defenses created by other researchers.	NA
21	A binary classification approach based on machine learning is provided to handle one kind of attack against a protocol. building an updated model of the number assault network and running the attack simulation in the Cooja simulator.	Light Gradient Boosting
22	a deep neural network method to defend against RPL attacks, such as the rank attack	ANN
23	This method reduces the risk of protocol-specific rank attacks in RPL networks. Power consumption, packet delivery speed, throughput, and network stability are some of the network performance metrics that may be affected by a strategy based on the anticipated transmission count measure. This strategy can be tested using simulations.	System for Metric-Based RPL Credibility Model (MRTS)

However, the problem of accessibility was ignored. Each node must also have a hardware security chip installed. Numerous studies investigating various strategies for fending off security assaults in IoT and RPL-based IoT have been conducted, both systematically reviewed and survey-based methods. Table 1 summarizes the related work.

4. Proposed System

In terms of Internet of Things security, this paper introduces an ANN learning model that analyzes and deeply investigates the RPL attacks based on network topology attacks, specifically rank and local repair attacks. This approach proposes the dataset by combining rank attack scenarios and local repair, publicly known as RADAR. Figure [2] depicts our proposed solution, which is composed of the following phases:

- Initial dataset phase.
- Preprocessing Phase.
- Deep learning model phase.
- Evaluation phase.

A. Initial data set phase

The RADAR dataset extracts RPL traffic attacks, As we discussed obviously, our concern is the local repair attack scenario and rank attack, which are explained in this data set. We proposed an approach to extract these specific attacks with an 18-node dataset by combing and shuffling all data and preparing to be fetched in the next phase raw by raw with much care of not missing any value or features before the preprocessing stage. The produced dataset includes 23 features.

B. Preprocessing Phase

Since our new dataset is ready to be clean and complete, we removed all null values. Clean replicated data and normalized all values.

C. Artificial Neural Network Model

This paper aims to analyze rank and local repair node traffic attack patterns deeply and then invest more features in identifying attacks. Our solution relies on a deep learning approach. This solution introduces a distinctive sense of network topology attacks by learning rank and local repair attacks and later analyzing those attacks. In our approach, we build a deep learning model, which tracks attack features in known and unknown cases, and it reports that case as unknown. In this situation, it

is possible to be a new attack, most importantly, a new feature that could be a new version of a known attack.

To present a model in simplified structure, proposed a Multi-Layer (MLRPL) model by employing an ANN approach for analysis of Rank and local repair in RPL. We've constructed a condensed, multi-layered ANN. The suggested ANN diagram for the proposed system for the selected data set is depicted in Figure 3.

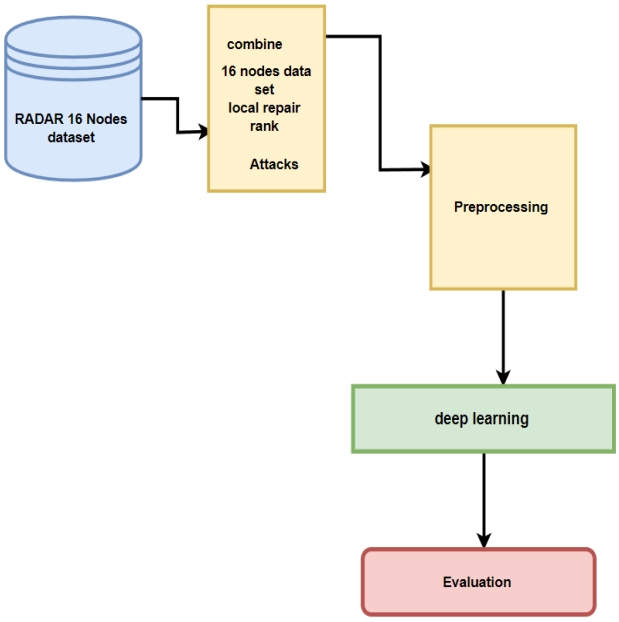


Figure 2. The proposed ANN learning model.

D. Evaluation phase

The solution efficiency is evaluated based on the confusion matrix. From the modeling view, our concern is that the confusion matrix is used to measure the remedy's effectiveness. The next section provides evaluation criteria for measuring the efficiency of this solution, intending to reach a low positive rate in the event of the study of these types of attacks from a modeling perspective.to reach a low positive rate in case of analysis of these types of attacks, evaluation criteria for measuring this solution's efficiency are given in the next section.

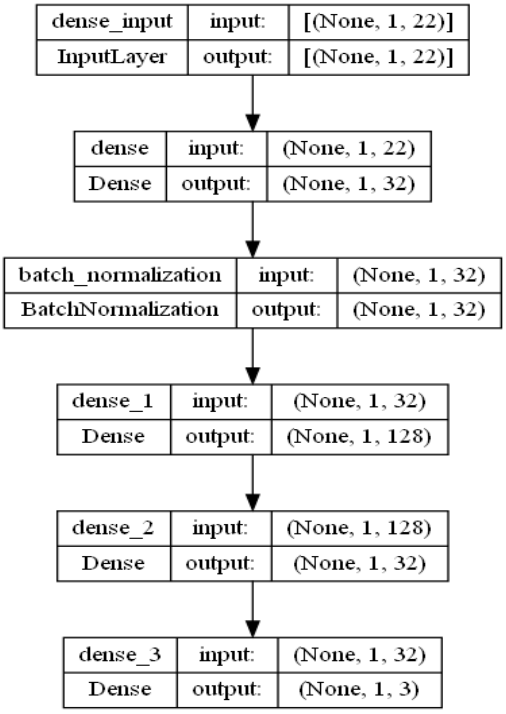


Figure 3. Proposed ANN structure.

E. Testing and Validation

Evaluation of our proposed model to analyze and deeply investigate two types of attack topology in RPL.

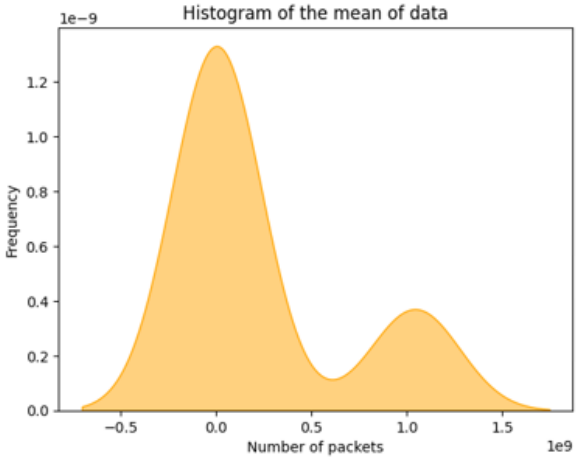
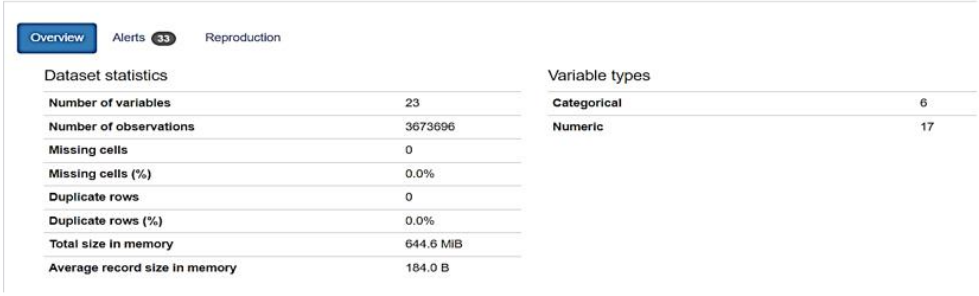


Figure 4. Mean of packet numbers.

Assuming these attacks happen in a systematics scenario that is applied simply to capture and extract the RADAR dataset. We merge two dataset folders named Rank and Local Repair; we produce a new dataset. Figure (4) shows the maximum data value—the size of reach to 3673696 frames, as indicated in Figure (5).



Overview Alerts 33 Reproduction

Dataset statistics

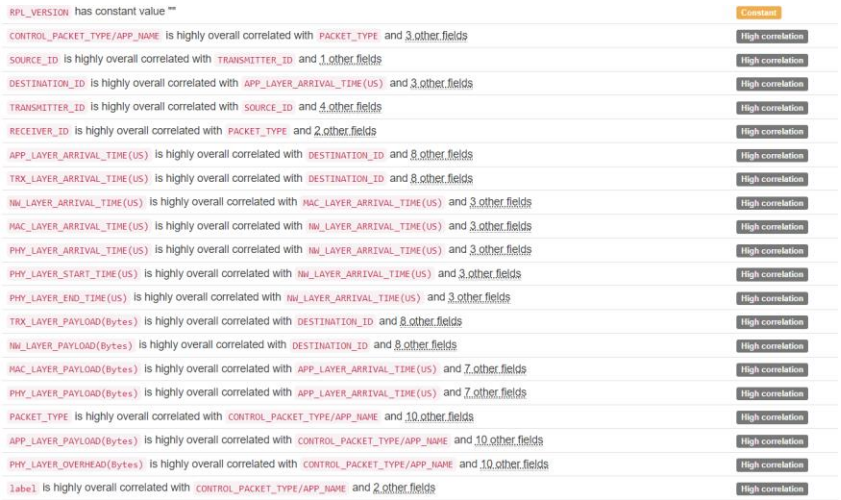
Number of variables	23
Number of observations	3673696
Missing cells	0
Missing cells (%)	0.0%
Duplicate rows	0
Duplicate rows (%)	0.0%
Total size in memory	644.6 MiB
Average record size in memory	184.0 B

Variable types

Categorical	6
Numeric	17

Figure 5. Statistical information of the dataset.

Since the preprocessing phase is applied to clean data, the total number of high-correlation features will be trained through our model, and the number of features will reach 23. Figure (6) Displays feature names and numbers.



RPL_VERSION has constant value ""	Constant
CONTROL_PACKET_TYPE/APP_NAME is highly overall correlated with PACKET_TYPE and 3 other fields	High correlation
SOURCE_ID is highly overall correlated with TRANSMITTER_ID and 1 other fields	High correlation
DESTINATION_ID is highly overall correlated with APP_LAYER_ARRIVAL_TIME(US) and 3 other fields	High correlation
TRANSMITTER_ID is highly overall correlated with SOURCE_ID and 4 other fields	High correlation
RECEIVER_ID is highly overall correlated with PACKET_TYPE and 2 other fields	High correlation
APP_LAYER_ARRIVAL_TIME(US) is highly overall correlated with DESTINATION_ID and 8 other fields	High correlation
TRX_LAYER_ARRIVAL_TIME(US) is highly overall correlated with DESTINATION_ID and 8 other fields	High correlation
NW_LAYER_ARRIVAL_TIME(US) is highly overall correlated with MAC_LAYER_ARRIVAL_TIME(US) and 3 other fields	High correlation
MAC_LAYER_ARRIVAL_TIME(US) is highly overall correlated with NW_LAYER_ARRIVAL_TIME(US) and 3 other fields	High correlation
PHY_LAYER_ARRIVAL_TIME(US) is highly overall correlated with NW_LAYER_ARRIVAL_TIME(US) and 3 other fields	High correlation
PHY_LAYER_START_TIME(US) is highly overall correlated with NW_LAYER_ARRIVAL_TIME(US) and 3 other fields	High correlation
PHY_LAYER_END_TIME(US) is highly overall correlated with NW_LAYER_ARRIVAL_TIME(US) and 3 other fields	High correlation
TRX_LAYER_PAYLOAD(Bytes) is highly overall correlated with DESTINATION_ID and 8 other fields	High correlation
NW_LAYER_PAYLOAD(Bytes) is highly overall correlated with DESTINATION_ID and 8 other fields	High correlation
MAC_LAYER_PAYLOAD(Bytes) is highly overall correlated with APP_LAYER_ARRIVAL_TIME(US) and 7 other fields	High correlation
PHY_LAYER_PAYLOAD(Bytes) is highly overall correlated with APP_LAYER_ARRIVAL_TIME(US) and 7 other fields	High correlation
PACKET_TYPE is highly overall correlated with CONTROL_PACKET_TYPE/APP_NAME and 10 other fields	High correlation
APP_LAYER_PAYLOAD(Bytes) is highly overall correlated with CONTROL_PACKET_TYPE/APP_NAME and 10 other fields	High correlation
PHY_LAYER_OVERHEAD(Bytes) is highly overall correlated with CONTROL_PACKET_TYPE/APP_NAME and 10 other fields	High correlation
label is highly overall correlated with CONTROL_PACKET_TYPE/APP_NAME and 2 other fields	High correlation

Figure 6. The high correlation features are implied in our model.

Following extensive testing, we settled on a training data proportion of 80% and a testing data percentage of 20%. Figure (7) shows the train samples that are labeled.

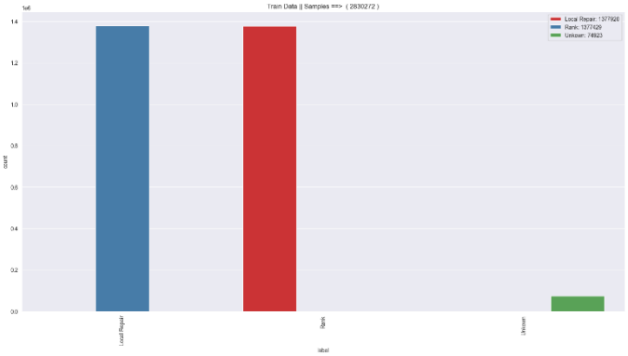


Figure 7. Train data samples.

Figure (8) shows the test data samples and Figure (9) shows sample data in the validation.

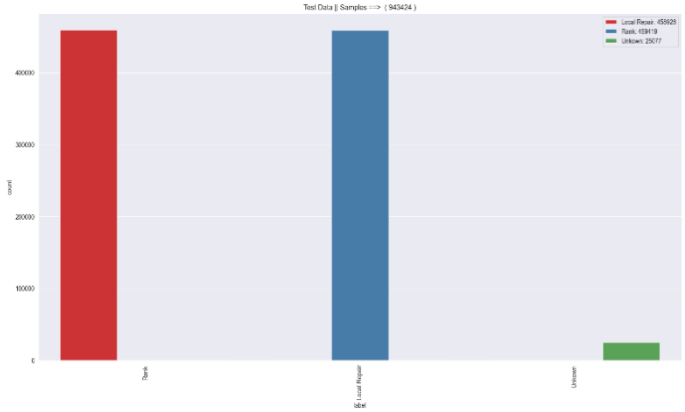


Figure 8. Testing data samples.

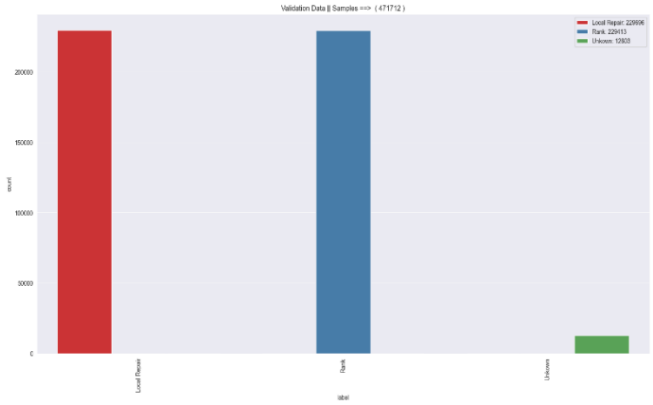


Figure 9. Testing data samples.

The model reaches 0.98 accuracy in the analysis of the RPL attack: rank, local repair, and unknown. Figure (10) shows the accuracy of the proposed model. Figure (11) indicates the low rate of loss value .

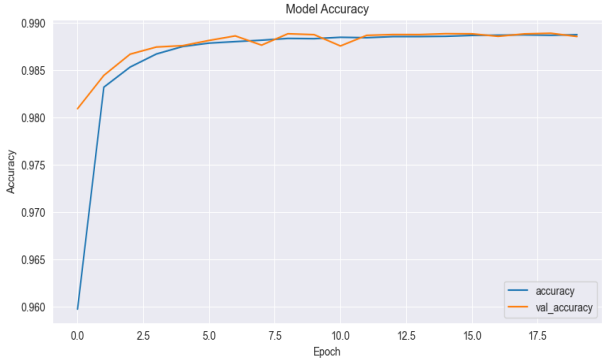


Figure 10. proposed system accuracy.

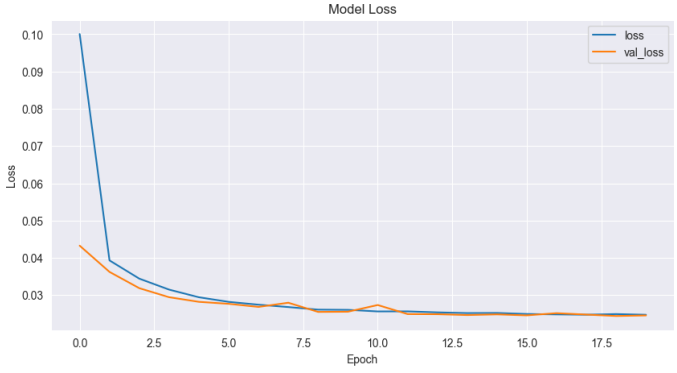


Figure 11. Loss value.

To evaluate our solution, as we discussed earlier, a proposed model reaches multiclass investigating including rank, local repair, and unknown. Our goal of this work is to reach accurate results with a low positive rate, Figure (12) shows the effective low positive between 1-39, which is the promising range of results in a contract with big-size data.

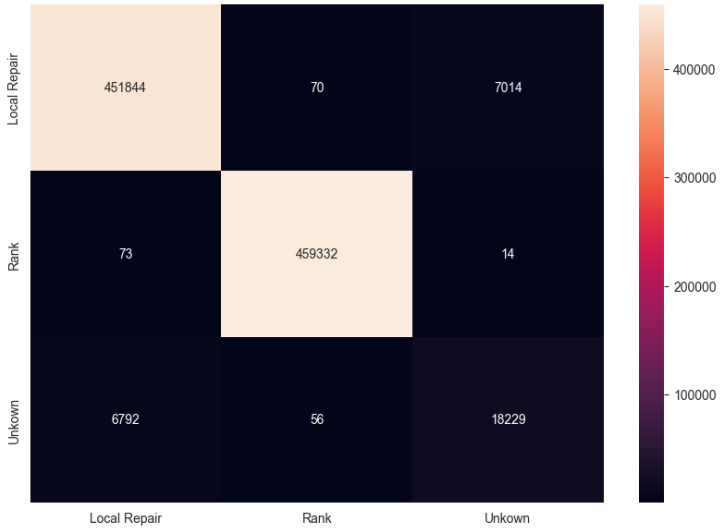


Figure 12. Validation results of the proposed system.

The suggested model varies from existing solutions for RLP attacks because it introduces an asset valuation model to examine both varieties of network topology attacks utilizing an anomaly method and a comprehensive picture of their characteristics and behaviors.

5. Conclusion and Future Work

This paper makes a number of discoveries that can examine RPL attack with two cases rank and local repair attack scenario. Our algorithm exhibits great accuracy when categorizing known samples; the bias scenario, however, calls for more research. This strategy highlights the great degree of similarity between two network topology attacks used in this paper. A lightweight ANN model that functions well in the LNN network has been investigated. Our model has a low false positive rate and an accuracy of 0.99 due to its in-depth analysis of attack behaviors. There is room for fresh analysis and investigation into the mysterious assault in upcoming developments. This study does not address the open topic of whether or not a previously unknown attack represents a new type of attack.

6. References

[1] Challenges: A Comprehensive Review, vol. 114, no. 2. Springer US, 2020. F. Mohammadi, "Emerging challenges in smart grid cybersecurity enhancement: A review," Energies, vol. 14, no. 5, 2021.

[2] D. Nawara and R. Kashef, "Context-Aware Recommendation Systems in the IoT Environment (IoT-CARS)-A Comprehensive Overview," IEEE Access, vol. 9, pp. 144270–144284, 2021.

[3] S. J. Muhamed, "Detection and Prevention WEB-Service for Fraudulent E-Transaction using APRIORI and SVM," Al-Mustansiriyah J. Sci., vol. 33, no. 4, pp. 72–79, 2022, doi: 10.23851/mjs.v33i4.1242.

[4] I. Lee, "Internet of Things (IoT) cybersecurity: Literature review and IoT cyber risk management," Futur. Internet, vol. 12, no. 9, 2020.

[5] R. K. Challa and K. S. Rao, "Resource Based Attacks Security Using RPL Protocol in Internet of Things," Ing. des Syst. d'Information, vol. 27, no. 1, pp. 165–170, 2022.

[6] M. A. Jabbar and R. Aluvalu, "Intrusion detection system for the internet of things: A review," IET Conf. Publ., vol. 2018, no. CP747, 2018.

[7] H. H. Ali, J. R. Naif, and W. R. Humood, "A New Smart Home Intruder Detection System Based on Deep Learning," Al-Mustansiriyah J. Sci., vol. 34, no. 2, pp. 60–69, 2023.

[8] Y. Al Sawafi, A. Touzene, and R. Hedjam, "Hybrid Deep Learning-Based Intrusion Detection System for RPL IoT Networks," J. Sens. Actuator Networks, vol. 12, no. 2, 2023.

[9] P. P. Ioulianou, V. G. Vassilakis, and S. F. Shahandashti, "ML-based Detection of Rank and Blackhole Attacks in RPL Networks," 2022 13th Int. Symp. Commun. Syst. Networks Digit. Signal Process. CSNDSP 2022, pp. 338–343, 2022.

[10] A. Agiollo, M. Conti, P. Kaliyar, T. N. Lin, and L. Pajola, "DETONAR: Detection of Routing Attacks in RPL-Based IoT," IEEE Trans. Netw. Serv. Manag., vol. 18, no. 2, pp. 1178–1190, 2021, doi: 10.1109/TNSM.2021.3075496.

[11] J. V. V. Sobral, J. J. P. C. Rodrigues, R. A. L. Rabêlo, J. Al-Muhtadi, and V. Korotaev, "Routing protocols for low power and lossy networks in Internet of things applications," Sensors (Switzerland), vol. 19, no. 9, pp. 1–40, 2019.

[12] T. A. Al-Amiedy, M. Anbar, B. Belaton, A. H. 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, vol. 22, no. 9, 2022.

[13] 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.
[14] M. A. Boudouaia, A. Ali-Pacha, A. Abouaissa, and P. Lorenz, “Security against rank attack in RPL protocol,” IEEE Netw., vol. 34, no. 4, pp. 133–139, 2020.
[15] Z. A. Almusaylim, N. Z. Jhanjhi, and A. Alhumam, “Detection and mitigation of RPL rank and version number attacks in the internet of things: SRPL-RP,” Sensors (Switzerland), vol. 20, no. 21, pp. 1–25, 2020.
[16] N. A. Zabidi et al., “Jo ur na l P,” Int. J. Biol. Macromol., vol. 2, no. 2, pp. 33–47, 2022, [Online]. Available: https://doi.org/10.1016/j.ijbiomac.2022.05.116.
[17] B. Farzaneh, M. A. Montazeri, and S. Jamali, “An Anomaly-Based IDS for Detecting Attacks in RPL-Based Internet of Things,” 2019 5th Int. Conf. Web Res. ICWR 2019, pp. 61–66, 2019.
[18] A. Triantafyllou, P. Sarigiannidis, and T. D. Lagkas, “Network protocols, schemes, and mechanisms for Internet of things (IoT): Features, open challenges, and trends,” Wirel. Commun. Mob. Comput., vol. 2018, 2018.
[19] A. Raoof, A. Matrawy, and C. H. Lung, “Routing Attacks and Mitigation Methods for RPL-Based Internet of Things,” IEEE Commun. Surv. Tutorials, vol. 21, no. 2, pp. 1582–1606, 2019.
[20] M. Osman, J. He, F. M. 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.
[21] F. Y. Yavuz, D. Ünal, and E. Gül, “Deep learning for detection of routing attacks in the internet of things,” Int. J. Comput. Intell. Syst., vol. 12, no. 1, pp. 39–58, 2018.
[22] N. Djedjig, D. Tandjaoui, F. Medjek, and I. Romdhani, “Trust-aware and cooperative routing protocol for IoT security,” J. Inf. Secure. Appl., vol. 52, p. 102467, 2020.

دراسه مكثفه لهجمات RPL على أساس الشبكة العصبية الاصطناعية في إنترنت الأشياء (IoT)

رياض حازم مهدي[3] ياسمين حمزة عبدالامير[2] فيصل غازي بديوي[1]
reyadh.hazim@uomustansiriyah.edu.iq Yhamza @uomustansiriyah.edu.iq faisal.ghazi@muc.edu.iq

المستخلص: يعتبر بروتوكول التوجيه لشبكات الطاقة المنخفضة مناسبًا بشكل ممتاز لأجهزة إنترنت الأشياء المقيدة (IoT) نظرًا لإجراءاتها الموفرة للطاقة وأساليب التشغيل الآمنة والمقيدة والتي يمكن الوصول إليها. ومع ذلك، فإن الحاجة الملحة للأمن في شبكات إنترنت الأشياء القائمة على RPL تدفعنا إلى النظر في توجيه نقاط الضعف وتقييمها وتقديم مبررات محتملة. للتحقيق العميق وتحليل وقياس هجمات هيكليةالشبكة في RPL التي تسمى الرتبة والإصلاح المحلي، تقدم هذه الورقة نموذجًا للشبكة العصبية الاصطناعية خفيفة الوزن. نقوم بدمج مجموعتي بيانات من سيناريوهات الهجوم وإنشاء نموذج ANN خفيف الوزن يتسبب في تأثير ملحوظ، على وجه الدقة (إلى 0.99)، ومعدل إيجابي خاطئ منخفض. يعتمد هذا النهج على التحقيق والتحليل المتعمق والاستفادة من أهم سمات بروتوكول RPL لتشكيل أساس التقنية الشاذة المقترحة

الكلمات المفتاحية : امن انترنت الاشياء ، تعلم الشبكة العصبية الاصطناعية ، بروتوكول التوجيه ، اصلاح الهجوم المحلي

[1] م.د. قسم علم الحاسوب ونظم المعلومات - كلية المنصور الجامعة – بغداد - العراق
[2] م.د. قسم علوم الحاسبات - الجامعة المستنصرية - كلية العلوم – بغداد - العراق
[3] م. قسم علوم الحاسبات - الجامعة المستنصرية - كلية العلوم – بغداد - العراق