Journal of Information Systems and Informatics

Vol. 6, No. 3, September 2024 e-ISSN: **2656-4882** p-ISSN: **2656-5935**

DOI: 10.51519/journalisi.v6i3.828 Published By DRPM-UBD

Machine Learning Algorithms to Defend Against Routing Attacks on the Internet of Things: A Systematic Literature Review

Lanka Chris Sejaphala[1], Vusimuzi Malele[2], Francis Lugayizi[3]

[1,2]Department of Computer Science and Information Systems, North West University, Vanderbijlpark, South Africa
[3] Department of Computer Science and Information Systems, North West University, Mmabatho, South Africa
Email: [1]chris.sejaphala@nwu.ac.za, [2]vusi.malele@nwu.ac.za, [3]francis.lugayizi@nwu.ac.za

Abstract

The Internet of Things (IoT) has become increasingly popular, opening vast application possibilities in different fields including smart cities, healthcare, manufacturing, agriculture, etc. IoT comprises resource-constrained devices deployed in Low Power and Lossy Networks (LLNs). To satisfy the routing requirements of these networks, the Internet Engineering Task Force (IETF) created a standardised Routing Protocol for low-power and Lossy Networks (RPL). However, this routing protocol is vulnerable to routing attacks, prompting researchers to propose several techniques to defend the network against such attacks. Machine learning approaches demonstrate effective ways to detect such attacks in large quantities. Therefore, this paper systematically synthesised 17 publications to compare the performance of traditional and advanced machine learning algorithms to identify the best algorithm for detecting RPL-based IoT routing attacks. The findings of this paper show that machine learning algorithms are capable of effective detection of many routing attacks with high accuracy and a low False Positive Rate. Furthermore, the results demonstrate that on average, advanced machine learning algorithms can achieve an accuracy of 96.03% compared to traditional machine learning algorithms which achieved 91.67%. Traditional machine learning algorithms demonstrated the best performance on average False Positive Rate by achieving 2.75% compared to their counterparts which gained 4.79%. However, Random Forest showed the best performance and outperformed all the algorithms in the selected publications by achieving over 99% accuracy, precision and recall.

Keywords: RPL, IoT, LNNs, Machine learning, routing attacks

1. INTRODUCTION

The IoT is a paradigm of interconnected devices which collect and exchange data with each other from an environment of deployment and share the data over the internet to achieve a particular goal [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, etc.

Due to its characteristics and nature, IoT has limitations regarding energy, memory, and computational capabilities, which traditional routing protocols cannot satisfy[2]. The Internet Engineering Task Force (IETF) working group designed and standardised Routing protocol for low-power and Lossy networks (RPL) to satisfy the routing needs of Low Power and Lossy Networks (LLNS) and to enable the resource-constrained devices to communicate their routing information among themselves and route their observed data to the root node[3, 4]. However, RPL as the DE facto routing protocol in IoT is susceptible to different routing attacks (i.e. flooding, sinkhole, worst parent attacks, etc) [5]. Routing attacks pose a great threat to the RPL-based IoT and can affect its performance and functionalities [4].

Different defence techniques against routing attacks in RPL-based IoT have been studied in the recent past, including the secure protocol, IDS and machine learning-based [6-8]. Machine learning techniques are currently new and more effective techniques used to deal with routing attacks in RPL as compared to traditional approaches [9]. Machine learning helps to analyse the IoT attack data and make accurate predictions in detecting routing attacks. This paper presents the findings of the Systematic Literature Review (SLR) method which is employed to identify the best-performing machine-learning algorithm to detect routing attacks in RPL-based IoT. Several SLR studies have been conducted in the past to try and find gaps in the machine learning-based detection techniques in RPL-based IoT[10-12]. Unlike in [13] in which authors highlighted strengths and limitations of machine learning algorithms, our study's primary objective is to use the SLR method to identify the best-performing machine learning algorithms. However, authors in [14] highlighted that most studies use private or self-generated datasets, which is one of the fundamental drives of our study. The selected studies used network simulation tools to generate their training and testing datasets, because of lack of publicly available datasets[13] .

The primary objective of this paper is to use a systematic literature review method to identify the best machine learning algorithm for the detection of routing attacks in RPL-based IoT. Contributions of this paper are that the study uses the SLR method to select and screen publications for inclusion and exclusion, Furthermore, provides a compressive summarised review of studies which proposed machine learning algorithms to act against routing attacks in IoT, Lastly, the study identifies the best-performing machine learning algorithm from the included publications

The rest of the paper is organised as follows: Section 2 presents a critical review literature in this area. Section 3 we propose our robust SLR methodology including inclusion and exclusion criteria followed to achieve relevant publications. Section 4 gives insight into the findings and analysis. Last, Section 5 concludes this paper by highlighting a summary of findings, limitations of the study, recommendations and scope of future work.

2. METHODS

This paper adopts the Systematic Literature Review (SLR) methodology to systematically source, analyze, and synthesize data into insightful information, with the aim of addressing the research question and presenting the findings in a comprehensive manner. The research design followed for the SLR is illustrated in Figure 1, outlining the structured process undertaken to achieve the objectives of this study. The design encompasses stages 2-5, which are essential for the selection and inclusion of relevant publications for the review.

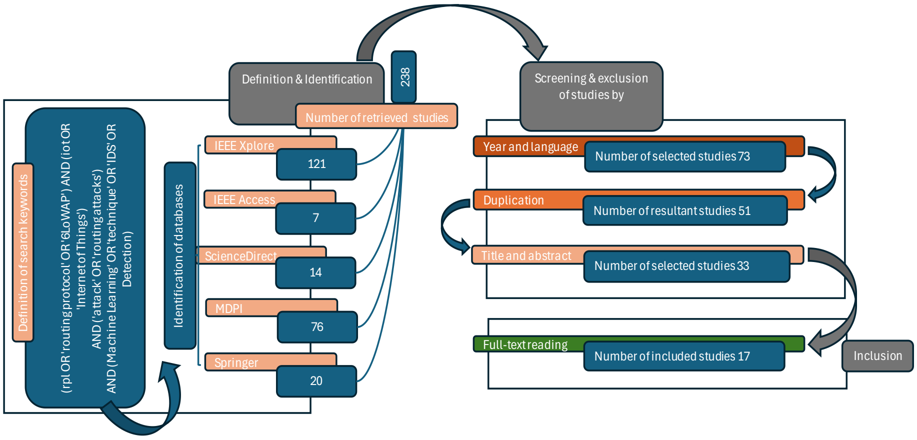
Definition of search keywords
(rpl OR 'routing protocol' OR '6LoWAP') AND (iot OR 'Internet of Things') AND ('attack' OR 'routing attacks') AND (Machine Learning' OR 'technique' OR 'IDS' OR Detection)
Identification of databases
IEEE Xplore
121
IEEE Access
7
ScienceDirect
14
MDPI
76
Springer
20
Definition & Identification
238
Number of retrieved studies
Screening & exclusion of studies by
Year and language
Number of selected studies 73
Duplication
Number of resultant studies 51
Title and abstract
Number of selected studies 33
Full-text reading
Number of included studies 17
Inclusion

Figure 1. The adopted SRL research design.

The SLR approach employed in this paper consists of six critical stages. These stages ensure a rigorous review process, allowing for a systematic collection and evaluation of relevant literature. The stages are as follows:

1. **Stage 1**: Formulating the key research question. The research question that guides this study is: *Which machine learning algorithm, based on the synthesized publications, demonstrates the best performance in terms of accuracy, precision, and recall?*
2. **Stage 2**: Defining search keywords. This stage involves selecting specific keywords to narrow down relevant studies within the scope of machine learning in RPL (Routing Protocol for Low-power and Lossy Networks) and IoT (Internet of Things).

3. **Stage 3**: Identifying academic databases. Relevant academic libraries were identified to source publications, including reputable databases such as IEEE Xplore**,** ScienceDirect**,** MDPI, and Springer. These sources provide a wide range of high-quality peer-reviewed articles.
4. **Stage 4**: Screening and inclusion of studies (as detailed in Table 1). This stage involved the selection process, where studies were screened based on predefined criteria. A total of 73 studies initially met the year and language criteria, but after screening, 22 duplicate studies were excluded, 18 studies were dismissed due to irrelevant titles or abstracts, and 16 were excluded due to the unavailability of full texts. As a result, 17 studies were ultimately included for analysis.
5. **Stage 5**: Data extraction and synthesis. In this stage, data were meticulously extracted from the selected studies, and the relevant information was synthesized to ensure meaningful insights were drawn.
6. **Stage 6**: Presentation of findings. The final stage involves presenting the synthesized findings derived from the SLR process, which will be discussed in detail in the subsequent section of this paper.

Table 1. List of Publications selection criteria

No	Inclusion	Exclusion
1	Published between 2018 & 2023	A study is a duplicate
2	Written in the English language	Published in a language other than English
3	A study remains within the borders of machine learning in RPL and/or IoT	Not relevant to the scope of this article
4	A study is a journal article, a book chapter and a conference proceeding	Is a grey literature
5	Full-text reading is available	Full-text reading is not available

3. RESULTS AND DISCUSSION

3.1 SLR Results

This section presents the findings of the Systematic Literature Review conducted in this paper. The main objective of this paper is to compare the performance results of machine learning algorithms from different studies in detecting routing attacks in RPL-based IoT. The selected studies used self-generated datasets from different simulation tools (e.g., Cooja, MATLAB, NetSim and OMNeT++) to develop and fit their selected machine-learning algorithms. However, some of the findings of this paper are that most studies that try to defend IoT using machine learning algorithms do not:

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

1. Demonstrate the impact of the observed attacks
2. Energy consumption of the proposed models is not well addressed
3. The placement strategy of the detection model is not presented
4. The proposed techniques only classify or detect the attacks, they do not identify intruders nor mitigate the attacks.

In this paper, we have summarised the findings of different studies comparing traditional and advanced machine learning algorithms in Tables 2 and Table 3 respectively. Table 3 displays a comparison results of different traditional machine learning algorithms from synthesised studies. Only one study from the selected studies had fitted Random Forest (RF) in their generated dataset.

Table 2. Performance metrics of traditional machine learning algorithms

	RF	**DT**	**KNN**	**Naïve Bayes**	**Google AutoML**	**SVM**
Accuracy	99.30	92.69	95.12	75.95	-	95.30
Precision	99.20	88.03	90.90	96.40	93.30	92.91
Recall	99.30	80.10	86.60	89.35	93.30	94.31
F1-Score	99.30	84.75	87.15	96.10	93.30	94.13
FPR	-	1.82	5.40	0.87	-	2.91

From the results, it appears that RF outperformed all the selected algorithms achieving an accuracy of 99.30% followed by SVM which achieved an accuracy of 95.30%. However, Naïve Bayes outperformed both RF and SVM in terms of precision and FPR achieving 96.40% and 0.87% respectively; followed by DT which achieved an FPR of 1.82%. Though Naïve Bayes' accuracy is the lowest it displayed exceptional results following RF though its FPR is not known. Figure 2 presents a graphical representation of Table 2. It displays averages of the evaluated performance metrics of traditional machine-learning algorithms.

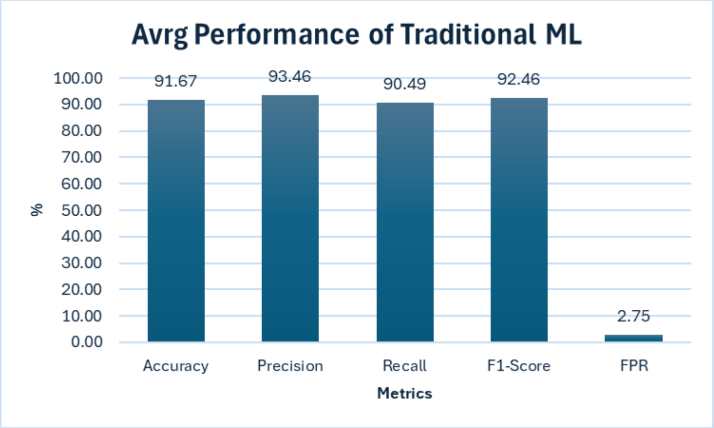

Figure 2. Performance metrics of traditional machine learning algorithms

On average the traditional machine learning algorithms achieved an accuracy of 91.67% and an FPR of 2.75%. This is however acceptable given their ability to produce such a low FRP and a precision of 93.46%.

Table 3 presents the results of advanced machine learning algorithms. As presented below Reinforcement learning algorithms outperformed all the algorithms in terms of accuracy, precision, Recall and F1-Score; in its performance, it achieved more than 98% in all the performance metrics but incurred a higher FPR of 8% which is still good but not acceptable. Followed by Neural Network (NN) which achieved an accuracy of 97.88% but ensembled achieved a higher precision and recall of 96.70% and 96.52% respectively. Moreover, Multi-Layer Perceptron (MLP) achieved the lowest FPR and second highest F1-Score of 98%.

Table 3. Performance metrics of different advanced machine learning

Metrics	NN	MLP	Ensembled	Log Regression	Reinforcement
Accuracy	97.88	91.11	96.50	96.18	98.50
Precision	92.00	96.00	96.70	95.65	98.60
Recall	92.00	93.85	96.25	93.44	98.00
F1-Score	92.00	98.00	-	90.80	98.50
FPR	-	1.16	-	5.20	8.00

Advanced machine learning algorithms appear to have achieved over 94% on all the performance metrics i.e., accuracy, precision, recall, and f1-score and below 5% of FPR as displayed in Figure 3.

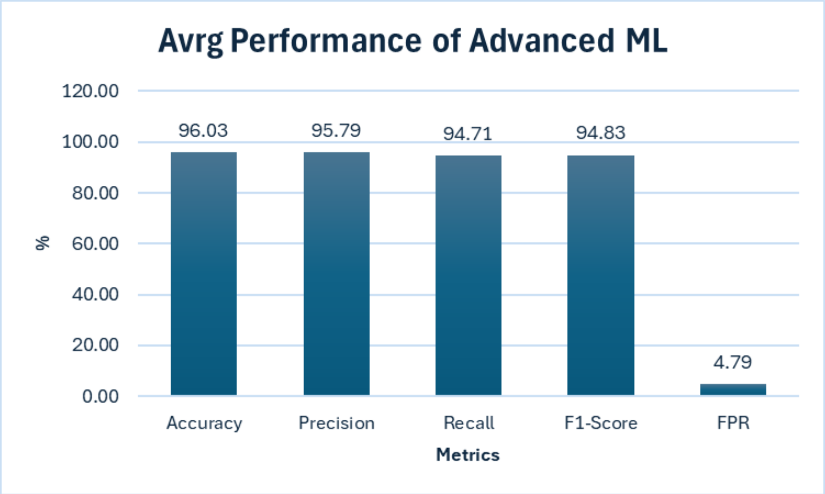

Figure 3. Performance metrics of advanced machine learning algorithms

From the results in Figure 2 and Figure 3, it is evident that advanced machine learning algorithms yield significant performance in detecting routing attacks. However, they turn out to incur a higher false alarm as compared to traditional machine learning algorithms. However, results in Table 3 and Table 4 demonstrate that Random Forest achieves significantly higher accuracy and precision, Recall and F1-Score. However, Naïve Bayes demonstrated a very low False alarm percentage of 0.87%. Furthermore, Reinforcement learning achieved higher accuracy, precision and recall percentages followed by ensembled learning then MLP coming second in F1-Score. From the presented results, on average, it can be concluded that traditional machine learning algorithms seem to excel in maintaining a very low FPR while advanced machine learning algorithms are good at producing higher accuracy and precision. However, individual algorithms demonstrate that Random Forest yields the best result as compared to all the algorithms presented in this paper.

3.2 Discussion

As recent works suggest, intelligence defense techniques are prominent solutions to defend against attacks in IoT [14, 15], particularly machine learning as it improves the attack detection rate using efficient learning techniques [16]. In their study [16], the authors proposed a machine learning-based technique to detect version number, rank, and DoS attacks. The technique employs a Support Vector Machine (SVM) integrated into each node of an RPL-based IoT.

In 2021, a Random Forest classifier [17] was proposed to defend IoT against five types of attacks. Although the proposed technique achieves a high detection rate, it does not mitigate the attacks. The authors in [18] proposed a reinforcement learning model for Software-Defined IoT networks to combat rank attacks. Their experimental results demonstrated that a State Action Reward State Action (SARSA) model is more effective in facilitating the implementation of Intrusion Prevention Systems.

The study [19] compared the performance of four supervised-learning algorithms, namely Logistic Regression, SVM, Gaussian Naive Bayes, and Neural Networks, to detect version number attacks. The Neural Network outperformed traditional machine learning algorithms and achieved an accuracy of 97.76%. Another study [20] proposed a distributed One-Class SVM (OCSVM) to detect outliers related to 10 types of attacks. The results of the OCSVM are communicated to a hybrid centralized IDS. However, the OCSVM adds energy consumption overhead.

To address blackhole, sinkhole, decreased rank, and selective forwarding attacks, the study [21] proposed a fuzzy KNN classifier. The authors in [22] proposed an ensembled classifier consisting of SVM, Naïve Bayes, and a Decision Tree to detect blackhole, hello flooding, and version number attacks. The results show that using the ensembled method yields higher performance than a single classifier. The authors in [23] compared the performance of Microsoft Azure SVM, Decision Tree, and Google AutoML to detect rank and blackhole attacks. Google AutoML achieved a higher precision of 93.3% and outperformed Microsoft Azure's SVM and Decision Tree based on other evaluation metrics. In [24], the authors proposed an Artificial Neural Network using Multi-Layer Perceptron (MLP) to detect rank attacks in RPL-based IoT. The proposed technique produced a precision of 100% and an accuracy of 96%. However, the technique does not mitigate the attack, and no placement strategy was provided.

The study [25] compared the performance of SVM and Binary Logistic Regression (BLR) to detect sinkhole attacks in IoT. The results indicated that BLR outperformed SVM, and it was implemented for detection. However, the energy consumption of the proposed BLR was not presented, though it is reported to be lightweight. The study [26] proposed an ensembled method to detect seven routing attacks in RPL-based IoT. This study utilized the RPL-NNIDS17 dataset to train and test the proposed technique.

The authors in [27] proposed a Reinforcement-learning technique to defend against eight routing attacks in RPL-based IoT. The technique combines homogeneous machine learning algorithms, such as SVM, Decision Tree (DT), KNN, K-Means, and Logistic Regression. To achieve optimum performance, they used Deep Q-Network (DQN) and Double DQN (DDQN) to approximate the Q function for value-action selection.

The work in [28] investigated the performance of SVM, Logistic Regression (LR), and Gated Recurrent Unit (GRU)-based Deep Learning to defend against hello flooding attacks in RPL-based IoT. Their results indicated that GRU outperformed both SVM and LR, yielding higher accuracy and PDR. The proposed technique, implemented with Recurrent Neural Networks architecture, is used to classify malicious nodes and mitigate hello flooding attacks.

The authors in [29] proposed a hybrid Deep Learning Artificial Neural Network (DANN) to classify network traffic. The performance of the proposed technique was compared with J48, SVM, KNN, and Long Short-Term Memory (LSTM), with DANN achieving 98% accuracy and a 92% F1-Score. To detect rank and wormhole attacks, the authors in [30] proposed a Machine Learning Lightweight Gradient Boost Machine Model (ML-LGBM) to classify rank, wormhole, and normal attacks. In their study, they compared the performance of GRU-DL, SVM, Gradient Boost (GB), and Extended Gradient Boost (XGB), with the proposed technique showing better performance in terms of accuracy and precision.

The study [9] proposed a stacking ensembled method that combines the results of C4.5 and SVM. This technique was integrated into a Hybrid IDS to detect seven routing attacks in IoT. The study compared C4.5, MLP, SVM, and Naïve Bayes, with the experimental results showing that the ensemble of C4.5 and SVM outperformed other individual techniques in terms of accuracy and false alarms. The study [31] proposed the ProSenAD model to detect rank and wormhole attacks. The proposed technique optimizes LGBM for multiclass classification to detect protocol-specific and sensor network attacks. The authors compared several machine learning algorithms, but the ProSenAD model outperformed them in terms of classification accuracy.

Table 4 summarises the findings of this paper, outlining the strengths and limitations of the study and proposed defence technique, names and number of attacks addressed, and whether the study demonstrates the impact of the studied attacks or not; furthermore, demonstrates if the proposed technique mitigates the attacks or not. Lastly, the machine learning algorithms were investigated, and the size of the dataset used in the study.

Table 4. Summarised findings from the included publications

Study	ML-algorithms	Dataset	No of Attacks	Strength	Limitation	Attacks	Impact of attacks
[17]	SVM	Generated - NA	4	the proposed technique achieves more than 90% accuracy and consumes less energy as compared to base RPL	Though the proposed technique achieves acceptable performance results, the number of malicious nodes is not mentioned	Version Number, Rank, DoS Attack	Yes
[16]	Random Forest Classifier	Generated - NA	6	Achieves 99.46% detection rate	The technique does not mitigate the attacks	UDP Flooding, Selective Forwarding, Blackhole, DIS Flooding, ICMPv6 Flooding	Yes
[18]	State Action Reward State Action	Generated - NA	1	It is said the proposed technique	Only one malicious	Rank	No

Study	ML-algorithms	Dataset	No of Attacks	Strength	Limitation	Attacks	Impact of attacks
				effectively prevents rank attack's harmful effects	node is considered		
[19]	Logistic Regression, SVM, Gaussian Naïve Bayes, Neural Network	Generated -103839	1	The proposed technique achieves 97.76% accuracy	The placement strategy of the proposed technique is not presented	Version number attack	No
[20]	SVM	Generated - NA	10	The proposed technique can detect malicious activities with a 99.74% TPR	The proposed technique adds energy consumption overhead	Sinkhole, Blackhole, Grayhole, DIS Flooding, Increase Rank, Wormhole, DIO Suppression, Worst Parent, Version Number, Neighbour Attack	No
[21]	Fuzzy KNN Classifier	Generated - NA	4	The proposed technique achieves an accuracy of more than 98%	The proposed technique cannot mitigate the detected attacks	Decreased Rank, Blackhole, Sinkhole, Selective Forwarding	No
[22]	SVM, Naïve Bayes, Decision Tree	Generated - NA	3	The proposed technique achieves more than 98% accuracy, precision, recall, TPR, F-measure and MCC.	The proposed technique cannot mitigate the detected attacks. only one malicious	Blackhole, Hello Flooding, Version Number	No

Study	ML-algorithms	Dataset	No of Attacks	Strength	Limitation	Attacks	Impact of attacks
					was considered.		
[23]	Azure SVM, Azure Decision Tree, Google AutoML.	Generated - NA	2	The evaluation show that ML techniques can be effective in detecting rank and blackhole attacks achieving a precision of 93.3%	The proposed technique cannot mitigate the detected attacks.	Rank, Blackhole	No
[24]	MLP ANN	Generated - NA	1	Achieves 100% precision	The study considered a small network size with only 2 malicious nodes	Rank	No
[25]	BLR & SVM	Generated - NA	1	The proposed Binary Logistic Regression achieves higher accuracy and precision	The energy consumption of the proposed technique is not presented	Sinkhole	No
[26]	Boosted Trees, Bagged Trees, Subspace Discriminant, & RUS Boosted Trees.	Generated -175077	7	The proposed ensembled achieved 94.5% and 93.4% accuracy and AUC respectively.	The proposed technique cannot mitigate the detected attacks.	Sinkhole, blackhole, Sybil, Clone ID, Selective Forwarding, Hello Flooding, & Local Repair	No

p-ISSN: **2656-5935** http://journal-isi.org/index.php/isi e-ISSN: **2656-4882**

Study	ML-algorithms	Dataset	No of Attacks	Strength	Limitation	Attacks	Impact of attacks
[27]	Decision Tree, K-NN, K-means, SVM, & Logistic Regression	Generated -80000	8	The proposed RL technique achieves 96.6% and 96.7% accuracy and precision respectively	The proposed technique cannot mitigate the detected attacks.	Sinkhole, Blackhole, Grayhole, DIS Flooding, Increased Rank, Wormhole, DIO Suppression, Replay	No
[28]	GRU, SVM, LR	Generated -10519	1	The proposed GRU produces an accuracy of 99.95% with higher PDR	The energy consumption of the proposed GRU-based DL is not presented	Hello-Flooding	Yes
[29]	DANN, J48, KNN, SVM, LSTM	Generated -380732	3	The proposed DL technique shows exceptional results performance against supervised learning algorithms achieving 98% and 92% accuracy and F1-score respectively	The proposed technique cannot mitigate the detected attacks.	DIS-Flooding, Rank & Wormhole	No
[30]	LGBM, GRU-DL, SVM, GB, XGBoost	Generated -31062	2	The proposed technique achieved an accuracy of 99.8% which is higher than all other algorithms in the study	The proposed technique cannot mitigate the detected attacks.	Rank & Wormhole	No

Study	ML-algorithms	Dataset	No of Attacks	Strength	Limitation	Attacks	Impact of attacks
[31]	C4.5, SVM, MLP, & Naïve Bayes	Generated -3190	8	The proposed technique produces a high TP of 97.1% and FP of almost 1%	Only one malicious node is considered in the study	Flooding, Dos, Wormhole, Rank, blackhole, Version number, & Sinkhole	No
[9]	GAN-C, ML-LGBM, LGBM, GB, XGBoost	Generated - NA	2	The proposed technique demonstrated a high level of accuracy and precision in detecting rank and wormhole attacks	The number of attacking nodes is not mentioned and the model can only classify, it does not identify nor mitigation	Rank & Wormhole	No

From Table 4 presented the evident that machine learning algorithms are capable of addressing several routing attacks where we see over only 5 studies out of 17 addresses only one attack. However, most of the studies we synthesised did not disclose their dataset size which also affect the performance of the machine learning algorithms.

4. CONCLUSION

In conclusion, machine learning algorithms display an effective and efficient way to detect routing attacks. From the studies that were synthesised, it is evident that machine learning algorithms can detect many routing attacks with high accuracy and precision while also displaying a significantly low False Positive Rate. This paper investigated the performance of different machine-learning algorithms from 17 publications that met the inclusion criteria of this paper, and it was discovered that between traditional machine learning and advanced machine-learning algorithms, on average advanced machine learning demonstrated the best performance over traditional machine-learning algorithms. However, this paper aims to identify the best machine learning algorithm from the synthesises publications. It was then discovered that Random Forested demonstrated the best results in terms of accuracy, precision, Recall and F1-Score. Although dataset size, feature engineering techniques used, number of features selected, number of attacks, and training time are some of the factors that are to be considered, however, they are not within the scope of this paper but are to be considered. In future, the authors intend to generate datasets of different attacks and legitimate traffic using one of the simulation tools described in the literature to compare the performance of machine learning algorithms. The authors will train and test the algorithms on the same dataset and consider all factors mentioned, furthermore, propose the best-performing model for implementation to defend IoT against routing attacks.

REFERENCES

[1] 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)*, vol. 5, no. 2, pp. 2477-2482, 2019.

[2] A. J. Witwit and A. K. Idrees, "A comprehensive review for RPL routing protocol in low power and lossy networks," in *Proc. Int. Conf. New Trends Inf. Commun. Technol. Appl.*, Cham, Switzerland: Springer International Publishing, Sep. 2018, pp. 50-66.

[3] F. Garba, "A Comprehensive Review of Routing for Low Power and Lossy Network (RPL) Protocol Challenges and Proposed Improvements," 2022.

[4] 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*, vol. 11, pp. 71073-71087, 2023.

[5] J. Rani, A. Dhingra, and V. Sindhu, "A Detailed Review of the IoT with Detection of Sinkhole Attacks in RPL based network," in *Proc. A Detailed Review of the IoT with Detection of Sinkhole Attacks in RPL based network*, 2022, pp. 1-6.

[6] A. Agiollo, M. Conti, P. Kaliyar, T. N. Lin, and L. Pajola, "DETONAR: Detection of Routing Attacks in RPL-Based IoT," *IEEE Transactions on Network and Service Management*, vol. 18, no. 2, pp. 1178-1190, 2021.

[7] H. Alam, M. S. Yaqub, and I. Nadir, "Detecting IoT Attacks using Multi-Layer Data Through Machine Learning," in *Proc. Detecting IoT Attacks using Multi-Layer Data Through Machine Learning*, 2022, pp. 52-59.

[8] A. U. Gawade and N. M. Shekokar, "Lightweight Secure RPL: A Need in IoT," in *Proc. Lightweight Secure RPL: A Need in IoT*, 2017, pp. 214-219.

[9] A. Alazab, A. Khraisat, S. Singh, S. Bevinakoppa, and O. A. Mahdi, "Routing Attacks Detection in 6LoWPAN-Based Internet of Things," in *Proc. Routing Attacks Detection in 6LoWPAN-Based Internet of Things*, 2023.

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

[11] T. A. Al-Amiedy, 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," in *Proc. A Systematic Literature Review on Machine and Deep Learning Approaches for Detecting Attacks in RPL-Based 6LoWPAN of Internet of Things*, 2022.

[12] 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*, vol. 21, no. 11, pp. 12940-12968, 2021.

[13] T. A. Al-Amiedy, M. Anbar, B. Belaton, A. A. Bahashwan, I. H. Hasbullah, M. A. Aladaileh, and G. A. L. Mukhaini, "A systematic literature review on attacks defense mechanisms in RPL-based 6LoWPAN of Internet of Things," *Internet of Things*, vol. 22, pp. 100741, 2023.

[14] G. A. L. Mukhaini, M. Anbar, S. Manickam, T. A. Al-Amiedy, and A. A. Momani, "A systematic literature review of recent lightweight detection approaches leveraging machine and deep learning mechanisms in Internet of Things networks," *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 1, pp. 101866, 2024.

[15] H. Xu, Z. Sun, Y. Cao, and H. Bilal, "A data-driven approach for intrusion and anomaly detection using automated machine learning for the Internet of Things," *Soft Computing*, vol. 27, no. 19, pp. 14469-14481, 2023.

[16] M. D. Momand, M. K. Mohsin, and Ihsanulhaq, "Machine Learning-based Multiple Attack Detection in RPL over IoT," in *Proc. Machine Learning-based Multiple Attack Detection in RPL over IoT*, 2021, pp. 1-8.

[17] Kamaldeep, M. Malik, M. Dutta, and J. Granjal, "IoT-Sentry: A Cross-Layer-Based Intrusion Detection System in Standardized Internet of Things," *IEEE Sensors Journal*, vol. 21, no. 24, pp. 28066-28076, 2021.

[18] C. M. Moreira and G. Kaddoum, "QL vs. SARSA: Performance Evaluation for Intrusion Prevention Systems in Software-Defined IoT Networks," in *Proc. QL vs. SARSA: Performance Evaluation for Intrusion Prevention Systems in Software-Defined IoT Networks*, 2023, pp. 500-504.

[19] A. R. L., B. S., and C. S. G., "An Effective Detection of Version Number Attacks in the IoT using Neural Networks," in *Proc. An Effective Detection of Version Number Attacks in the IoT using Neural Networks*, 2022, pp. 1-7.

[20] A. M. Pasikhani, J. A. Clark, and P. Gope, "Incremental hybrid intrusion detection for 6LoWPAN," *Computers & Security*, vol. 135, pp. 103447, 2023.

[21] T. Raghavendra, M. Anand, M. Selvi, K. Thangaramya, S. V. N. Santhosh Kumar, and A. Kannan, "An Intelligent RPL attack detection using Machine Learning-Based Intrusion Detection System for Internet of Things," *Procedia Computer Science*, vol. 215, pp. 61-70, 2022.

[22] S. Rabhi, T. Abbes, and F. Zarai, "IoT Routing Attacks Detection Using Machine Learning Algorithms," *Wireless Personal Communications*, vol. 128, no. 3, pp. 1839-1857, 2022.

[23] P. P. Ioulianou, V. G. Vassilakis, and S. F. Shahandashti, "ML-based Detection of Rank and Blackhole Attacks in RPL Networks," in *Proc. ML-based Detection of Rank and Blackhole Attacks in RPL Networks*, 2022, pp. 338-343.

[24] W. Choukri, H. Lamaazi, and N. Benamar, "RPL rank attack detection using Deep Learning," in *Proc. RPL rank attack detection using Deep Learning*, 2020, pp. 1-6.

[25] C. Ioannou and V. Vassiliou, "Accurate Detection of Sinkhole Attacks in IoT Networks Using Local Agents," in *Proc. Accurate Detection of Sinkhole Attacks in IoT Networks Using Local Agents*, 2020, pp. 1-8.

[26] A. Verma and V. Ranga, "ELNIDS: Ensemble Learning based Network Intrusion Detection System for RPL based Internet of Things," in *Proc. ELNIDS: Ensemble Learning based Network Intrusion Detection System for RPL based Internet of Things*, 2019, pp. 1-6.

[27] A. M. Pasikhani, J. A. Clark, and P. Gope, "Reinforcement-Learning-based IDS for 6LoWPAN," in *Proc. Reinforcement-Learning-based IDS for 6LoWPAN*, 2021, pp. 1049-1060.

[28] 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*, vol. 8, pp. 183678-183689, 2020.

[29] Y. Al Sawafi, A. Touzene, and R. Hedjam, "Hybrid Deep Learning-Based Intrusion Detection System for RPL IoT Networks," in *Proc. Hybrid Deep Learning-Based Intrusion Detection System for RPL IoT Networks*, 2023.

[30] 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," in *Proc. Rank and Wormhole Attack Detection Model for RPL-Based Internet of Things Using Machine Learning*, 2022.

[31] F. Zahra, N. Z. Jhanjhi, N. A. Khan, S. N. Brohi, M. Masud, and S. Aljahdali, "Protocol-Specific and Sensor Network-Inherited Attack Detection in IoT Using Machine Learning," in *Proc. Protocol-Specific and Sensor Network-Inherited Attack Detection in IoT Using Machine Learning*, 2022.