ML-Driven Attack Detection in RPL Networks: Exploring Attacker Position's Significance

Baraq Ghaleb, Ahmed Al-Dubai, Imed Romdhani, Jawad Ahmad, Talal Aldhaheri* and Sonali Kulkarni*
School of Computing, Edinburgh Napier University, UK
{b.ghaleb, a.al-dubai, I.romdhani, j.ahmad}@napier.ac.uk
*Department of Computer Science and Information Technology, Ambedkar Marathwada University, India
*{talalalthahri, sonalibkul}@bamu.ac.in

***Abstract*—The Routing Protocol for Low Power and Lossy Networks (RPL) plays a pivotal role in IoT communication, employing a rank-based topology to guide routing decisions. However, RPL is vulnerable to Decreased Rank Attacks, where malicious nodes illegitimately lower their ranks to manipulate routing paths. While exploring the applicability of machine learning (ML) techniques for attack detection holds promise, their effectiveness is often overlooked in the context of attacker position within the network. This study bridges this gap and delve into investigating the impact of attacker position on Decreased Rank attack detection using ML-based approaches. Our findings reveal that the success of attack detection is highly contingent on the attacker's proximity to the network root, highlighting the importance of considering network topology in attack mitigation strategies.**

Keywords— Internet of Things (IoT), IoT Security, RPL Standard, Decreased Rank Attack

I. INTRODUCTION

Recently the Low-power and Lossy Networks (LLNs), a collection of interconnected tiny sensor nodes, have been considered one of the key enabling blocks of the ever-growing Internet of Things (IoT) paradigm [1], [2]. The communication between LLNs devices is subject to restrictions on the performance as they utilize limited resources in relation to memory footprint, processing, and power [1]. To cater for such limited resources, the Internet Engineering Task Force (IETF) has specified the IPv6 Routing Protocol for LLNs (RPL) [3] as the routing standard for such networks. Indeed, and since it was a proposal, the RPL's security aspects have been analyzed by several research efforts. It has been reported that the existence of multiple security attacks needs to be addressed to facilitate the adoption of the protocol in a wide range of applications [4][5][6][7]. RPL proposes optional cryptography modes to secure its communication aiming to provide communication integrity, confidentiality, and authenticity. However, the LLNs devices are not usually tamper-resistant so malicious actors can still easily get control of and extract security primitives to mount several types of attacks. In addition, implementing security modes of RPL can greatly degrade the network performance as many of these security primitives, such as digital signatures, are power-hungry and require an abundant of processing and storage resources that cannot be met by resource-constrained devices [6] [7]. While some of attacks against RPL are already well-studied in the literature as they are inherited from WSNs such as the blackhole attack which drops received packets, some others are unique to RPL and have not yet been well-studied [8][9]. The Decreased Rank Attack is one of these attacks unique to the RPL standard. The Rank is a property in RPL which relatively represents the path quality to the Destination-oriented Directed Acyclic Graphs (DODAGs) root and based on routing decisions are made. Each RPL's node calculates its own rank based on a specific objective function and the rank of its preferred next hop (parent) to the root which is then communicated to immediate neighbor to calculate in turn their ranks [10][11]. A node receiving multiple rank values from multiple neighbors should opt to select the neighbors with the lowest rank value as its preferred parent. Hence, the rank property can be exploited by a malicious actor, internal or external, to announce a fake lower value of the rank compared to other nodes in the network so misleading such nodes into selecting the attacker as their preferred parent towards the DODAG root. The Decreased Rank attack can be combined with other attacks to further damage the network including, for instance, selective forwarding or blackhole attacks which can now be made more effective as the attacker is locating itself in a more strategic position where it receives all traffic from neighboring nodes [12][13][14][15][16].

Several research studies have been proposed to develop solutions for detecting or mitigating the attacks against RPL including the Decreased Rank Attack reporting some encouraging results [17][18][19][20]. However, these studies were carried out under restricted scenarios that do not account for the position of the attacker in the network which we considered in this study. Contrary to the previous literature, we found that the successful detection of the Decreased Rank attack greatly relies on the position of the attacking node. Hence, a ML-based solution will be only effective under scenarios where the attacker is located more than two hops away from the root of the network, otherwise it fails. The rest of the paper is organized as follows. Section II briefly reviews the basic operations of RPL protocol and its security issues highlighting the decreased rank attack. An overview of related work around the attack is provided in Section III. The ML-based developed solution is presented in Section IV highlighting the obtained results. Finally, conclusion and future work are reported in Section V.

II. RPL CONCEPTS AND OPERATIONS

RPL [3] is basically an IPv6 proactive distance-vector routing protocol designed by the IETF community specifically

979-8-3503-3094-6/24/$31.00 ©2024 IEEE

to fulfill the unique requirements of a wide range of low-power applications. It organizes its physical network into a form of DODAGs where each DODAG is rooted at a single destination, referred to as the LBR (LLNs Border Router) [3][5] as shown in Figure 1. The term "upward routes" is used to refer to routes that carry the traffic from normal nodes to the root (i.e., LBR) whereas routes that carry the traffic from the DODAG root to other nodes are called the downward routes [3]. The term Objective Function (OF) is used to describe the set of rules and policies that governs the process of route selection and optimization, in a way that meets the different requirements of various IoT applications [3]. In technical terms, the objective function is used for two primary goals: first, it specifies how one or more routing metrics, such as energy or latency, can be converted into a Rank, a value that reflects the node's relative position in the network; second, it defines how the Rank should be used for selecting the next hop (preferred parent) to the DODAG root. Currently, two objective functions have been standardized for RPL namely, the Objective Function Zero (OF0) [10] and the Minimum Rank with Hysteresis Objective Function (MRHOF) [11]. The OF0 is designed to select the nearest next hop to the DODAG root with no attempt to perform any load balancing. The Rank of a node is calculated by adding a strictly positive scalar value (rank-increase) to the Rank of a selected preferred parent utilizing a specific routing metric such as hop count or the expected transmission cost (ETX). For the parent selection, a node running OF0 always considers the parent with the least possible rank as its preferred parent. OF0 considers also selecting another parent as a backup in case the connectivity with its preferred parent is lost. Unlike OF0, the MRHOF is designed to prevent excessive churn (i.e., frequent parent change due to lower rank values) in the network topology and a node will not always replace change its current preferred parent to a parent with a lower rank value unless a significant change in the cost has been discovered (i.e., the Rank has changed by more than a pre-defined threshold called the Hysteresis value).

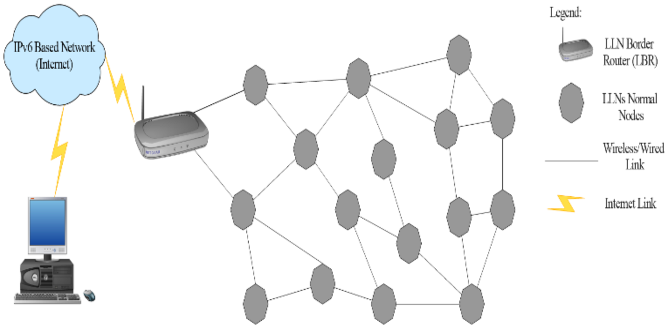

Figure 1. A typical LLNs

To facilitate the upward traffic pattern, a DODAG topology centered at the network root must be constructed. In such a topology, each non-root node willing to participate in upward communication must select one of its neighbors to act as that node default route (DODAG parent) towards the root [3]. The construction of the DODAG starts with the root multi-casting control messages called DODAG Information Objects (DIOs) to its RPLs neighbors. The DIOs carry the necessary routing information and configuration parameters required to build the DODAG including the rank property [3] [4]. An RPL node receiving a multicast DIO message will: (1) add the sender address to its candidate parent set; (2) calculate its distance (rank) with respect to the DODAG root based on the rank of that candidate parent, routing information advertised; (3) setup its default route (preferred parent); and (4) update the received DIO with its own rank and multicast it to other neighboring nodes, enabling them, in turn, to perform the previous operations [3][4].

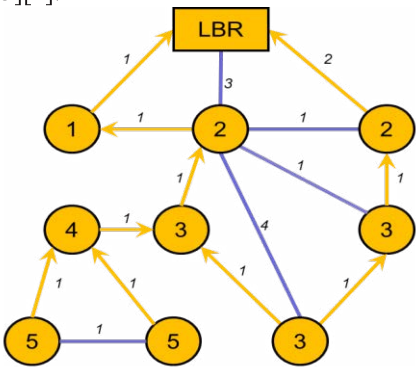

Figure 2: DODAG topology. Arrows represent child-parent relationships, lines represent alternative connections, numbers inside circles represent the ***ranks*** *values of nodes while other numbers refer to the quality of connections.*

A. The Decreased Rank Attack

The RPL routing standard is vulnerable to a wide range of attacks, which can be roughly categorized into three classes [12] [13]. In the first class (resources), the attackers aim to deplete network constrained resources such as power, bandwidth, and memory. For instance, an attack targeting the energy resources can be particularly damaging as it can greatly shorten the network lifetime and indirectly damage the network's reliability. In the second class (topology), the attackers target the network topology usually by forcing the protocol to build sub-optimized topology or isolating some nodes from communicating with the rest of the network. In the third class (traffic), the attackers target the traffic of the network through traditional traffic analysis or eavesdropping attacks with the main aim to gather information that can help in launching the previous two classes.

The Decreased Rank attack is one of the most serious attacks that could mounted against the RPL protocol within the IoT 6LowPAN communication standard [8]. As mentioned earlier, the Rank property plays a crucial role in building and optimizing the routing paths in RPL's networks and under both standardised objectives functions (i.e., OF0, MRHOF), a node with a lower rank would always be preferred to take upon the next hop role towards the DODAG root. In addition to optimizing the network topology, the rank property plays a fundamental role in building a loop-free topology.

In the Decreased Rank attack, a malicious actor illegitimately manipulates the rank property and broadcasts to its neighboring nodes a DIO with a fake decreased rank value. This may trigger the targeted nodes to change their preferred parents and select the attacker as their next hop to the root. A successful attack may have a devastating impact on the network topology with major issues including: (i) non-optimized route formation, (ii) and routing loop creation. The immediate outcome of that is damaging the reliability of the network as traffic now is not forwarded through optimal routes so packet delivery ratio may be decreased, and latency is increased which is worsened by the likely formation of loops. In addition, the formation of loops would trigger RPL's repair mechanisms which requires the protocol to speed up control messages transmission (i.e., DIOs) in a useless attempt to fix the created loops. Indeed, this only has the effect of depleting network limited resources with more energy consumption and less bandwidth available for the data plane traffic exacerbating further the issue of decreased reliability and increased latency.

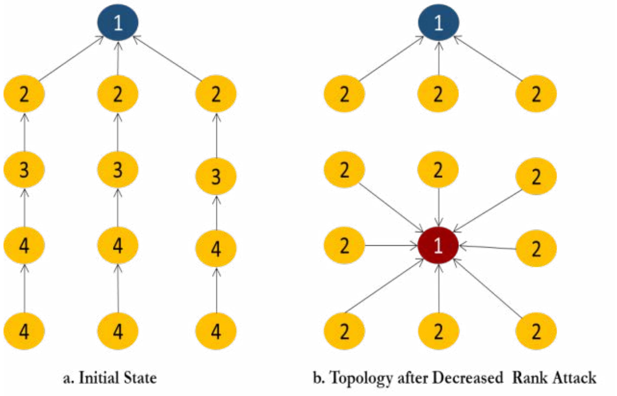

Figure 3. An example of the decreased rank attack. The initial state (a) represents the case before the attack where the topology is constructed assuming OF0 with the hop-count metric while (b) represents the case after the red node launched the decreased rank attack

III. Related Work

Several ML-based solutions have been proposed in the literature to detect the Decreased Rank attack. For instance, an ML-based anomaly-based rank attack detection solution is proposed in [15] utilizing Support Vector Machines (SVMs). The developed IDS is chosen to be deployed centrally on the border router as limited-resources normal nodes cannot tolerate the expensive operation of such a system. However, no details are provided on how the model is trained. In addition, the proposed system was not evaluated under different locations of the attacker node.

A second ML-based rank attack detection method is developed in [17] utilizing Multi-Layer Perceptron (MLP) neural network. The operation of the proposed solution is divided into three stages. In the first stage, the rank attack is simulated using Cooja with the results saved in pcap file. The pcap file is then converted in the second stage to CSV file where the data is extracted, filtered, and converted to a readable data. The MLP algorithm is applied in the third stage to detect the attack. The proposed IDS was showing to be effective in detecting the attack, however, it was unclear which features are extracted and used for classification purposes in addition to the absence of any analysis pertaining to the attacker location. Another framework named SVELTE is proposed in [20] for detecting routing attacks of the RPL protocol under the 6LowPAN standard. SVELTE employs a hybrid approach for intrusion detection where some modules are placed on the border router while some others are hosted on the constrained nodes of the RPL network. The framework was then evaluated by means of Contiki operating system and Cooja with a maximum number of nodes of 32. The proposed framework was shown to have a good capacity in detecting the respective attacks while not resulting in significant increase in the overhead in terms of energy consumption or memory footprint. One of the noticeable issues of SEVELTE is the unclarity regarding how to set the threshold value that governs the process of classifying nodes into malicious nodes. It also exhibits the same limitation of the previous two solutions pertaining to the location of the attacker.

The authors in [21] claimed that the existing IDSs consume too much resources, thus, they developed a sink-based intrusion detection system to address the sinkhole attack in 6LoWPAN networks. The process starts by having each node communicating to the sink some information including its IP address, preferred parent IP address, and rank encrypted with a key. The sink then compares the node's current rank to its previous rank and any node with a difference greater than a specific threshold is considered as malicious. NS2 was used to evaluate the proposed and is claimed to show better detection capacity with less overhead. However, it is unclear why the messages were encrypted. In addition, the nodes are communicating a bunch of information to the sink raising the concern of significant overhead introduced especially if the network has a high churn (i.e., continues change of the preferred parent). A hybrid anomaly-based and specification-based IDS was developed in [22] for detecting the selective forwarding and sinkhole attacks in 6LoWPAN networks. The proposed framework deploys specification-based agents in the router nodes to analyze the behavior of such nodes and send the results to the sink node. The received results at the sink node are then analyzed further using an anomaly-based agent based on the distributed MapReduce architecture to detect any malicious nodes. It was shown that the developed model achieved promising classification accuracy in comparison to other approaches in the litterateur. However, such a hybrid system may introduce a significant overhead to the resource constrained devices. Like other proposed detection approaches, this approach did not elaborate on how the detection accuracy might be affected under different locations of the attacker node.

IV. ML-Based Detection of the Decreased Rank Attack

Several publicly available datasets that can be used for intrusion detection are exist, however, these are not specifically created for IoT 6LoWPAN networks and they only include traces of general attacks. There are also some recent datasets devoted for routing attacks in 6LoWPAN networks including the Decreased Rank attack, however, these are not publicly available such as the IRAD dataset [23]. In addition, such private datasets do not include the specific scenarios that we aim to investigate in this study. Hence, we opted to create a new dataset devoted for the Decreased Rank Attack. The distinguishing aspect of this new dataset is that we have varied the location of the attacker as we theorize that the location of the attacker with respect to the DODAG root would have a profound effect on the efficiency of the ML-based solution.

A. Raw Data Generation

To generate the dataset, we used Contiki operating system and Cooja emulator following the methodology in [23]. Contiki is a lightweight and open-source operating system designed specifically for low-power resource-constrained IoT networks [17]. It features a highly optimized networking stack including several IoT standards such as CoAP, UDP, 6LoWPAN and IPv6 on the top of implementing the RPL standard fundamental mechanisms.

To emulate the exact binary code that runs on real sensor devices, Cooja [18], a cross-level simulator for Contiki, was used to carry out the simulation experiments. Cooja incorporates an internal hardware emulator called MSPsim [19], which is used in our simulations to impose hardware constraints of the Tmote Sky platform, an MSP430-based board with an ultra-low power IEEE 802.15.4 compliant CC2420 radio chip. We used the Unit Disk Graph Radio Medium (UDGM) radio protocol, the CSMA/CA protocol at the MAC layer and the ContikiMAC as a radio duty cycling (RDC) protocol. The ContikiRPL library was altered to implement the Decreased Rank attack. We aim to investigate the feasibility of ML-based solutions in detecting the Decreased Rank Attack under various locations of the attacker node. Thus, we simulated three different scenarios for the attacker in relation to the DODOAG root as follows:

- **Level 1:** we placed the attacker in the range of the DODAG root (one hop away from the root).
- **Level 2:** we placed the attacker two hops away from the DODAG root, so it is in the range of at least one immediate neighbor of the root, but not in the range of the root.
- **Level 3:** we placed the attacker three hops away from the DODAG root, so it is neither in the range of the root nor in the range of one of its immediate neighbours.

Contiki OS and Cooja simulator are used to emulate an IoT network and collect the results of both abnormal and benign traffic for the three scenarios (i.e., Level1, Level 2 and Level 3). Cooja has 6LoWPAN packet analyzer within the radio messages plugin that gathers raw data pertaining to the traffic exchanged in the network. The raw data includes the sequence number, the time, the source and destination addresses (reduced to node IDs), the packet length, the packet type (i.e., DIO, DAO, DIS, ACK, UDP) and the protocol type (i.e., IPv6, ICMPv6, RPL, IEEE802.15.4). Table 1 shows a sample of the raw data obtained by the Cooja 6LoWPAN packet analyzer. In addition, Cooja allows transforming the raw data into a format suitable for pre-processing and classification directly from the plugin which is used to transform the raw data into a text format.

Table 1. A sample of the raw data extracted by Cooja analyzer

No.	Time	From	To	Length	Data
330	00:02.1	9	-	64	IPv6:RPL:DIS
331	00:02.3	7	3	64	IPv6:RPL:DIS
332	00:02.5	11	-	76	IPv6:RPL:DIO
334	00:02.8	3	-	76	IPv6:RPL:DIO
335	00:02.9	8	9	76	IPv6:RPL:DIO
336	00:03.1	5	6	97	IPv6:RPL:DAO
337	00:03.2	3	7	5	IPv6:RPL:Ack
338	00:03.4	7	3	61	IPv6:RPL:UDP
339	00:03.5	2	12	70	IPv6:RPL:UDP

B. Data Preprocessing and Feature Generation.

It is important to pre-process the dataset and extract the features and then transform it into a format that is understood by the underlying learning model. For instance, raw data in the form of text may contain errors and inconsistencies, and is often incomplete, making it hard for the model to extract representative information and capture the dependencies among dataset features. In addition, the pre-processing of raw dataset reduces its complexity and allows for more efficient learning. For these reasons, data pre-processing stage was carried out through several steps. For example, the nonnumeric data was converted to numerical data for optimal performance. The time was converted from the analyzer format into seconds.

In the Decreased Rank attack, a malicious node can announce a lower rank in a DIO message forcing other neighboring nodes to choose the attacker as their next hop to the DODAG root. In theory, it is expected that the attack will affect the network through creating loops, thus triggering RPL repair mechanisms to resolve such loops which is achieved through more frequent transmission of control messages. Hence, it is projected that the number of control messages would increase significantly under the attack. Accordingly, we aim to use the counts of control messages per time unit as a feature. Additionally, it is obvious that if the attack is successful, the nodes will forward their data-plane traffic via the attacker leading to an increase in the number of data packets of the malicious node. Thus, we use the count of data-plane traffic per time unit as a metric. We aim to use this anomaly as a feature. Finally, we ended up with a total of 7 features collected over a time frame of 10 seconds including time, dioCount, daoCount, disCount, ackCount and udpCount in addition to the class label (Note we also done experiments on 1-second window as in [23], however, the results were less accurate). We followed the same methodology [23] for the labelling process so the traffic which includes the malicious activity is labelled as 1 and benign traffic is labelled as 0. A sample of the dataset created is shown in Table 2. Then three separate datasets were created as follows.

- **Dataset 1:** This combines the benign traffic and malicious traffic of level 1 and level 2 attacks.
- **Dataset 2:** This combines benign traffic and malicious traffic of all levels.
- **Dataset 3:** This combines the benign traffic and malicious traffic of level 3.

Table 2. A sample of the generated dataset

Time	DIOs	DAOs	DISs	UDPs	ACKs	Class
100	78	0	0	62	5	1
110	36	39	0	150	1	1
120	118	144	0	262	25	1
200	21	0	0	66	77	0
210	23	0	0	69	13	0

C. ML Models Training

Several ML-based classification models are used for intrusion detection including Decision tree (DT), Random forests (RF), K-Nearest Neighbours (KNN), Naïve Bayes (NB) and Logistic Regression (LR) utilising the following performance metrics:

- **Accuracy**: refers to the percentage of correctly predicted instances, True Positive (TP) and True Negative (TN), made by the classification model out of all the predictions made, True Positive (TP), False Positive (FP), False Negative (FN) and True Negative (TN). It is calculated as in Eq. 1.

$$Accuracy = (TP + TN) / (TP+FP+ TN + FN) \qquad (1)$$

- **Precision**: refers to the ratio between the True Positive and all the positive instances. In our model, it refers to the number of true instances classified as abnormal out of all abnormal instances as given in Eq. 2.

$$Precision = TP / (TP+FP) \qquad (2)$$

- **Recall**: refers to the ratio between the True Positive and all the instances classified as positive. In our model, it refers to the number of true instances classified as abnormal out of all instances classified abnormal by the model as given in Eq. 3.

$$Recall = TP / (TP+FN) \qquad (3)$$

D. Results and Discussion

As mentioned above, five ML models have been trained on the created datasets. The performance metrics of Dataset 1, Dataset 2 and Dataset 3 are given in Table 3, Table 4 and Table 5 respectively. While all models seem to show promising detection results for Dataset 3 (Table 3) when the attacker is located more than two hops away from the DODAG root, reaching a classification accuracy rate of around 98%, that efficiency in detecting the attack did not hold up for Dataset 1 and Dataset 2. The accuracy of ML models for Dataset 1 and Dataset 2 dropped to around 78% and 67% respectively showing limited effectiveness in this context. In general, the effectiveness of ML models in detecting the attack under Dataset 3 can be attributed to the fact the attack, where the attacker is located in the third level, has affected the performance metrics used for training the models. However, the attack, where the attacker is located in the first or the second levels, has not shown any noticeable impact on the performance metrics.

Indeed, in RPL's networks, an extension header option "RPL Option" is used to indicate the direction of the packet using a flag named the Down 'O' flag. Hence, a packet sent by a child node to its parent should not set the Down flag indicating that the packet is heading upward and vice versa. DODAG inconsistency is detected when a RPL node receives a packet with the Down 'O' bit set from a node with a higher rank (child node) and vice-versa. This case is controlled by another flag named the Rank-Error 'R' bit. When an inconsistency is detected by a node, two scenarios are possible: i) if the Rank-Error flag is not set, the forwarder node sets that flag and the packet is forwarded or, ii) if the 'R' bit is already set, the node discards the packet and the timer is reset and, control messages are sent more frequently.

Evidently, when the attacker is located three hops away from the DODAG root, the Decreased Rank attack will create loops as a result of the attacker's parents selecting the attacker as their parent. Clearly, this would trigger the scenario described in the previous paragraph "DODAG Inconsistency" which is resolved in RPL by more frequent transmission of control messages, a phenomenon that is picked up by the learning models. When the attacker is in the immediate range of the DODAG root (Level 1), there is no chance that loops will be formed and the case of DODAG Inconsistency would not occur as the only possible parent for the attacker is the DODAG root itself. Hence, the attack will go silent without disrupting the network and hence no metrics could be affected that could be fed into the learning model.

The case is slightly different when the attacker is located two hops away from the DODAG root (Level 2). Under this scenario, the attacker should announce a rank that is not less than that of the DODAG root to mount a successful attack, otherwise its announcement will be rejected. Therefore, the chance of forming loops is small or unexpected as the attacker potential parent should be from nodes in level 1 (nodes in the rang of the DODAG root). Evidently, such a potential parent would not change its own parent to the attacker node (no switch between parents of similar ranks). Like Level 1 attack, Level 2 will go silent without disrupting the network through creating loops and so no noticeable effect on the network that could be fed into the learning algorithm. This indicates that the location of the attacker should be considered carefully when designing introduction detection systems for the Decreased rank attack.

Table 3. Dataset 1 Performance of ML models (representing the attack at level 1)

Classification algorithm	Accuracy	Precision	Recall
DT	0.583	0.584	0.583
RF	0.616	0.617	0.617
KNN	0.519	0.519	0.519
NB	0.55	0.578	0.556
LR	0.673	0.674	0.674

Table 4. Dataset 2 Performance of ML models (representing the attack at all levels)

Classification algorithm	Accuracy	Precision	Recall
DT	0.741	0.733	0.742
RF	0.737	0.737	0.737
KNN	0.683	0.685	0.683
NB	0.672	0.80	0.67
LR	0.779	0.778	0.78

Table 5. Dataset 3 Performance of ML models (representing the attack at level 3)

Classification algorithm	Accuracy	Precision	Recall
DT	0.976	0.977	0.967
RF	0.976	0.976	0.976
KNN	0.975	0.975	0.975
NB	0.98	0.981	0.981
LR	0.979	0.979	0.979

V. CONCLUSION

In this study, we investigate the capacity of ML-based techniques in detecting the Decreased Rank Attack in IoT networks. This study reveals an interesting fact pertaining to the attack and how effective ML-based are in detecting such an attack. While ML-based solutions can effectively detect the attack under some scenarios, the study shows that such solutions will fail when the attacker is wisely positioned by placing it at most two hops away from the DODAG root. To the best of our knowledge, this has not been reported by any other study in the literature indicating the need for more proactive solutions that aim at preventing the occurrence of the attack rather than detecting it.

ACKNOWLEDGMENT

This work was supported by Edinburgh Napier University Research Starter Grants

REFERENCES

[1] J. W. Hui and D. E. Culler, "Extending IP to Low-Power, Wireless Personal Area Networks," in IEEE Internet Computing, vol. 12, no. 4, pp. 37-45, July-Aug. 2008.

[2] J. Hui, P. Thubert, "RFC 6282 Internet Engineering Task Force RFC 6282", Compression Format for IPv6 Datagrams over IEEE 802.15.4-Based Networks, September 2011.

[3] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, K. Pister, R. Struik, J. P. Vasseur, R. Alexander, "RPL: IPv6 routing protocol for low-power and lossy networks", RFC6550, Mar. 2012.

[4] A. Dvir, T. Holczer and L. Buttyan, "VeRA - Version Number and Rank Authentication in RPL," 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, Valencia, 2011, pp. 709-714.

[5] L. Wallgren, S. Raza, and T. Voigt, “Routing attacks and countermeasures in the rpl-based internet of things,” International Journal of Distributed Sensor Networks, vol. 9, 2013.

[6] B. Ghaleb, A. Al-Dubai, E. Ekonomou, M. Qasem, I. Romdhani and L. Mackenzie, "Addressing the DAO Insider Attack in RPL’s Internet of Things Networks," in IEEE Communications Letters, vol. 23, no. 1, pp. 68-71, Jan. 2019.

[7] P. Perazzo, C. Vallati, G. Anastasi and G. Dini, "DIO Suppression Attack Against Routing in the Internet of Things," in IEEE Communications Letters, vol. 21, no. 11, pp. 2524-2527, Nov. 2017.

[8] A. O. Bang and U. P. Rao, “EMBOF-RPL: Improved RPL for early detection and isolation of rank attack in RPL-based internet of things,” Peer-to-Peer Networking and Applications, vol. 15, no. 1. Springer Science and Business Media LLC, pp. 642–665, Jan. 2022.

[9] A. Le, J. Loo, A. Lasebae, A. Vinel, Y. Chen and M. Chai, "The Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and Lossy Networks," in IEEE Sensors Journal, vol. 13, no. 10, pp. 3685-3692, Oct. 2013.

[10] P. Thubert, “Objective Function Zero for the Routing Protocol for LowPower and Lossy Networks (RPL),” IETF RFC 6552, Mar. 2012.

[11] O. Gnawali and P. Levis, “The Minimum Rank with Hysteresis Objective Function”, IETF RFC 6719, Sep. 2012.

[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. MDPI AG, p. 3400, Apr. 29, 2022.

[13] A. Raoof, A. Matrawy and C. -H. Lung, "Routing Attacks and Mitigation Methods for RPL-Based Internet of Things," in IEEE Communications Surveys & Tutorials, vol. 21, no. 2, pp. 1582-1606, Secondquarter 2019.

[14] G. Glissa, A. Rachedi and A. Meddeb, "A Secure Routing Protocol Based on RPL for Internet of Things," 2016 IEEE Global Communications Conference (GLOBECOM), 2016, pp. 1-7.

[15] A. M. Said, A. Yahyaoui, F. Yaakoubi, and T. Abdellatif, “Machine Learning Based Rank Attack Detection for Smart Hospital Infrastructure,” Lecture Notes in Computer Science. Springer International Publishing, pp. 28–40, 2020.

[16] A. Verma and V. Ranga, "Security of RPL Based 6LoWPAN Networks in the Internet of Things: A Review," in IEEE Sensors Journal, vol. 20, no. 11, pp. 5666-5690, 1 June1, 2020.

[17] W. Choukri, H. Lamaazi and N. Benamar, "RPL rank attack detection using Deep Learning," 2020 International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT), 2020.

[18] M. A. Boudouaia, A. Abouaissa, A. Ali-Pacha, A. Benayache, and P. Lorenz, “RPL rank based-attack mitigation scheme in IoT environment,” International Journal of Communication Systems, vol. 34, no. 13. Wiley, Jul. 06, 2021.

[19] Z. A. Almusaylim, N. Jhanjhi, and A. Alhumam, “Detection and Mitigation of RPL Rank and Version Number Attacks in the Internet of Things: SRPL-RP,” Sensors, vol. 20, no. 21. MDPI AG, p. 5997, Oct. 22, 2020.

[20] S. Raza, L. Wallgren, and T. Voigt, “SVELTE: Real-time intrusion detection in the Internet of Things,” Ad Hoc Networks, vol. 11, no. 8. Elsevier BV, pp. 2661–2674, Nov. 2013.

[21] U. Shafique, A. Khan, A. Rehman, F. Bashir, and M. Alam, “Detection of rank attack in routing protocol for Low Power and Lossy Networks,” Annals of Telecommunications, vol. 73, no. 7–8. Springer Science and Business Media LLC, pp. 429–438, May 16, 2018.

[22] H. Bostani and M. Sheikhan, “Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on MapReduce approach,” Computer Communications, vol. 98. Elsevier BV, pp. 52–71, Jan. 2017.

[23] F.Y. Yavuz, D. Ünal, E. Gül, Deep learning for detection of routing attacks in the Internet of Things, Int. J. Comput. Intell. Syst. 12 (1) (2018) 39–58.