A Cross-Layer Intrusion Detection System for RPL-Based Internet of Things

Erdem Canbalaban and Sevil Sen[0000−0001−5814−9973]

WISE Lab., Department of Computer Engineering, Hacettepe University,
Ankara, Turkey,
ecanbalaban@hacettepe.edu.tr
ssen@cs.hacettepe.edu.tr

Abstract. The Internet of Things (IoT) is a heterogeneous network of constrained devices connected both to each other and to the Internet. Since the significance of IoT has risen remarkably in recent years, a considerable amount of research has been conducted in this area, and especially on, new mechanisms and protocols suited to such complex systems. Routing Procotol for Lower-Power and Lossy Networks (RPL) is one of the well-accepted routing protocols for IoT. Even though RPL has defined some specifications for its security, it is still vulnerable to insider attacks. Moreover, lossy communication links and resource-constraints of devices introduce a challenge for developing suitable security solutions for such networks. Therefore, in this study, a new intrusion detection system based on neural networks is proposed for detecting specific attacks against RPL. Besides features collected from the routing layer, the effects of link layer-based features are investigated on intrusion detection. To the best of our knowledge, this study presents the first cross-layer intrusion detection system in the literature.

Keywords: Internet of Things · Security · Cross-Layer Intrusion Detection · Routing Attacks · RPL · Neural Networks

1 Introduction

With the development of technology, the usage of the Internet and smart devices together has become a part of our daily lives. Advances in smart sensors, embedded devices, and wireless communication technologies have led to the emergence of a new concept called the Internet of Things (IoT). The use of IoT has been growing exponentially in different areas such as smart grid, medical care, and smart home systems [25, 15]. According to the research conducted by the Statistica Research Department [1], the number of devices connected to IoT will be over 50 billion in 2023 and 75 billion in 2025. The rapid increase in the number of IoT devices has also accelerated research in IoT. Due to attracting attackers' interest, security has become one of the important research areas in IoT.

Many IoT applications collect a large amount of data from various devices. Besides the heterogeneity of these devices, most of them have constraints related to power, communication, and computation capabilities. This also brings a challenge for developing complex security solutions. Hence, the existing security solutions might not be suitable for such heterogeneous and complex networks. Therefore, new solutions should be developed, or the existing ones should be adapted to this new environment, which is the main aim of this current study.

New protocols that are less complex and consume less power are introduced for IoT. Routing Protocol for Low-Power and Lossy Networks (RPL) is one of them [4] and designed to provide efficient routing paths especially for resource-constrained devices. Although some security mechanisms are proposed for external attackers in RPL, it is still open to insider attacks such as rank and version attacks, which could affect the entire network. Hence, suitable IDSs for RPL-based IoT should be improved to detect such attacks. As it is stated above, existing IDSs for wired/wireless networks may not be suitable for these networks. Hence, new solutions that consider the specific characteristics of RPL should be proposed.

In this study, a novel cross-layer intrusion detection system based on neural networks is introduced for RPL. Features from both link layer and network layer are employed. The following specific attacks against RPL are targeted: version number, worst parent, and hello flood. The effects of different percentages of attackers are also explored. The results show that the proposed IDS could detect attacks effectively for both binary and multi-class classification. The use of link layer-based features decreased the false positive rate further. The positive effect of link layer features on the detection of version number attacks are also observed in the results. The contributions of the study are summarized as follows:

- A novel neural network-based IDS both for binary and multiclass classification of the version number, worst parent, and hello flood attacks are introduced.
- An attack dataset for RPL-based IoT networks, which covers three attack types specific to RPL with different attacker densities, is introduced and shared with the community[1].
- To the best of the authors' knowledge, this study is the first cross-layer intrusion detection system for RPL-based networks that explores the effect of features obtained from both link and routing layers on intrusion detection.

The study is organized as follows. Section 2 discusses the related studies. Section 3 gives the details of the proposed solution. The targeted attacks and the neural network-based approach for detecting those are explained. Section 4 gives the details of the simulation environment and discusses the experimental results thoroughly. The last section is devoted to concluding remarks.

2 Related Work

Researchers have been exploring the development of suitable IDS for RPL. SVELTE [26] is the first IDS proposed in the literature. It aims to detect sinkhole and selective forwarding attacks by using a hybrid approach of signature

[1] https://wise.cs.hacettepe.edu.tr/projects/rplsec/

and anomaly-based techniques. There are also recent approaches that take the advantage of both techniques. An approach that utilizes 6LoWPAN compression header to detect hello flood, sinkhole, and wormhole attacks are proposed in [20]. The most discriminate features in the header are selected by using a correlation-based feature selection algorithm. Then, machine learning algorithms are applied and shown that the selected features (5 out of 77) outperform previous studies [24, 26].

An anomaly-based IDS for detecting version number and hello flood attacks is given in [29]. They used a small feature set for training a neural network-based model. Recently, another anomaly-based IDS is proposed for detecting version number and hello flood attacks [19]. A feature set consisting the number of topology control messages (DIS/DIO/DAO), the number of different DODAG versions and the UDP forward ratio are used by Kernel Density Algorithm. Another IDS [7] is generated by using genetic algorithm on a rich feature set and located at the root node. The experimental results show that the proposed IDS has high accuracy and low false positive rate on detection of hello flood and version number attacks.

A few specification-based IDSs are proposed in the literature. In [11], the states of RPL and the transitions between these states with corresponding statistics are defined, IDS rules according to them are extracted for detecting rank, neighbor, and sinkhole attacks. The network is divided into clusters to decrease the usage of resources. Each cluster member reports information about itself and its neighbors to the cluster head. Each cluster head runs an IDS agent that analyzes the reports coming from its members and generates an alarm if a node visits a state more than a threshold in a unit period of time. Another specification-based IDS is proposed for sybil attacks. Each node in the network is a monitoring node that cooperates with its neighbors to detect attacks and report them to the border router. Since the nodes in the network need to send a message to the sink node when they detect an inconsistency, it brings extra overhead to the network. Nodes in the network are equipped with a cryptographic co-processor chips to build hardware support identification, store security parameters, and handle cryptography calculations. It also requires a trusted entity for authentication.

There are also prevention and mitigation techniques against RPL attacks. A mitigation method is proposed for version number attacks in [6]. If a version update is coming from leaf nodes is ignored. Otherwise, if most of the neighbors with better ranks agree upon the validity of the version number update, it is accepted. Recently, a mitigation method against DIS flooding attacks is proposed [28]. Here, thresholds for limiting the number of unnecessary trickle timer resets are defined, and hence the number of control message transmissions caused by the attack is controlled. Secure-RPL [9] is a threshold-based detection system based on rank updates and uses hash chain authentication to eliminate illegitimate modification of rank value. SecTrust-RPL [3] is a detection and isolation mechanism against rank and Sybil attacks. The nodes compute the trustworthiness of its neighbors based on direct and recommended trust metrics and each node chooses a parent having higher trust values for routing whereas the nodes with lower trust values are marked as malicious. A distributed monitoring strategy for detecting version number attacks and attackers is proposed in [16]. Monitoring nodes construct a separate network and use it to periodically forward collected information about the version number of DIO messages coming from neighbor nodes to the root, which runs IDS.

A recent survey study [27] reviews the existing security mechanisms proposed for RPL. More than 100 studies are reviewed and shown that there is no cross-layer security solution. It is also emphasized that there is no effective solution against flood attacks. Furthermore, most of the studies use a small number of nodes in their simulation, which can be unscalable and unrealistic for a multi-hop network. The main contribution of this study is to fill this gap in the literature by proposing a cross-layer IDS. Link layer features besides routing layer features are included to distinguish the natural packet losses due to using wireless links from the packet losses caused by attacks. Moreover, the proposed system is simulated on large networks with different settings, which are shared with the community[1]. Finally, besides developing different algorithms for detecting each attack separately, one algorithm that distinguishes all attack types is developed.

3 RPL and Target Attacks

RPL connects nodes to each other and to border router(s) by creating a destination-oriented directed acyclic graph (DODAG). Three types of nodes can exist in a DODAG. The first one is low power and lossy border router (LBR), which is the root of a DODAG and a collection point for the multipoint-to-point (MP2P) traffic. LBR can create a directed acyclic graph and provides a connection between the Internet and remaining nodes. The second type is routers, which can generate data traffic and forward packets. They can join an existing DAG. The last type is hosts which can only generate data traffic as end-devices. Each node in a DODAG has an ID, a list of its neighbors, a parent node, and a rank value that shows the position of the node itself with respect to the border router. Each node calculates its rank according to the rank of its preferred parent by using the objective function (OF). OF determines the route selection by using different objectives such as ETX, latency.

RPL uses three types of routing control messages namely DAO, DIS, and DIO. In point-to-point (P2P) and point-to-multipoint (P2MP) traffic scenarios, the root node needs to know the path to the remaining devices. Therefore, each node announces its routing path to the root node by sending a Destination Advertisement Object (DAO) messages. DAO propagates upward direction in the DODAG via the parent of each node and the border router becomes aware of the path to each node. DIS (DODAG Information Solicitation) helps new nodes to ask for topology information before joining the network. DIO (DODAG Information Object) helps to set and update the topology. DIO message is sent by each node to inform other nodes about its rank value. RPL uses a trickle algorithm [14] for scheduling DIO message frequency. In this algorithm, to reduce the number of routing control messages, each node holds two parameters: trickle time and DIO counter. Trickle time stands for the time interval that the node waits before sending the next DIO message. If the parameters which cause a topology change in the network are not modified in the incoming DIO message, then the DIO counter will be increased and the trickle timer increases the duration of the idle state. If there is a change in the DIO message, the node will reset the DIO counter and minimize its trigger time.

The main focus of this study is to detect specific attacks against RPL. Three attacks based on their potential effects on RPL are simulated: version number, worst parent, and hello flood attack, which are given in detail below.

Version Number Attack (VNA) The change of version number is triggered only by the root node if the global repair of DODAG is required. When the root node changes the version number, this information is carried with DIO messages to all nodes in the network and a new DODAG is reconstructed. VNA results in unnecessary reconstruction of the DODAG graph and creates overhead. This attack has been analyzed in several studies in the literature [5, 17]. In [17], the attacker has been placed in all possible locations via a grid topology. The experimental results show that the effect of attack increases while the attacker is moving away from the root node since the attacker can spread the damage further [17]. In order to help to localize the attacker, loops and rank inconsistencies can be used because they are mainly located in the neighborhood of the attacker. In [5], it is also shown that mobile nodes harm the network with the same impact of far nodes from the root. In the attack scenario, a malicious node illegally changes the version number field before it forwards received DIO message to its neighbors. Here, in the simulations, malicious node increases version number by one in every minute in order to disrupt the network.

Worst Parent Attack (WPA) Rank Attack aims to change the topology of a DODAG. It is one of the most dangerous attacks against RPL. A rank value is calculated by each node in the network and it indicates the quality of a path between the node itself and the root node. The rank value has important roles in RPL such as creating an optimal topology, prevention of routing loops, and managing the overhead of routing control messages. In a rank attack scenario, the attacker falsifies its rank information and sends a DIO message to its neighbors which has a different rank value than its genuine. In WPA, the worst parent (with the highest rank value) is chosen instead of the best one as specified in RPL. As a result of this attack, a child node could find itself in a non-optimal routing path and choose an attacker node as its parent. WPA is implemented for the first time in [12] and the network performance under attack is analyzed by putting the attacker in every possible location in a grid topology. It is shown that the attack cannot be detected easily, since child nodes assume that routing information supplied by their parents via DIO packets are genuine and, they do not have any mechanism to verify the reliability of the parent nodes according to the protocol specification. Here, in the simulations, the malicious node selects the node which has the worst rank value in its neighborhood as its parent. The nodes who select the malicious node as a parent node might find themselves in non-optimal paths.

Hello Flood Attack (HFA) In RPL, a node who wants to join to the network multicasts DIS messages to its neighbors. The new node transmits DIS messages with a fixed interval of time and waits for a reply from nodes in its transmission range. However, RFC 6550 [4] does not specify the time interval for the transmission of DIS messages, and it may vary in different RPL implementations. When the new node receives DIO message(s) as a reply to its DIS messages, it stops sending DIS messages and joins to the network. In P2P and P2MP traffic scenarios, the new node also sends a DAO message to its parent in order to inform the root node. It is shown that HFA is the most influential attack that degrades the performance of IoT network [13]. In this attack scenario, a malicious node pretends to be a new node and multicasts DIS messages periodically to its neighbors. Hence, nodes in the neighborhood of the attacker are forced to reset the trickle timer or to unicast DIS message to a node that has to respond with a DIO message. This can overload RPL nodes by increasing the number of routing control messages and hence might cause network congestion. Here, in the simulations, malicious node multicasts DIS message to its neighbor nodes in every 500 milliseconds. In the simulations, it is observed that if DIS messages are sent more frequently, the network becomes overwhelmed by these messages and unresponsive to legitimate requests.

4 The Proposed Intrusion Detection System

In this section, the proposed neural network-based IDS for RPL-based IoT networks will be given in detail. Firstly, the features used as inputs to the neural network will be presented. For developing an effective IDS, it is important to determine suitable features for training a machine learning system. The selected features should have sufficient information to distinguish malicious activities from benign ones. Furthermore, they are preferred to have non-redundant information, because too many features could negatively affect training. A recent study [7] uses a set that covers most of the features related to the RPL control messages and data packets in the network. In addition to this feature set, the features related to link-layer are employed here, as listed in Table 1.

Data related features include information about data packets received by the root node in a time interval. These features could show whether each node effectively participates in the periodic reporting process to the root node and hence, give indirect information about the stability of a network. Topology related features include information about routing control messages received by the root node. These topology messages could give useful insights for detecting different types of attacks. For example, an abrupt increase in the number of DIS messages could be an indicator of hello flood attacks. However, this situation should be effectively discriminated from the natural increase of DIS messages as

Table 1. List of the Features

Feature Group	Explanation	Number of Features
Data	-Number of data messages -Max/Min/Average length of data messages -Max/Min/Average time difference between data messages	7
Topology	-Number of DIO/DIS/DAO messages -Max/Min of version numbers, the difference between version numbers -Max/Min of rank values, the difference between rank values -Max/Min/Average time difference between DIO/DIS/DAO messages	16
Link-Layer	-Number of dropped packets due to collision /neighbor allocation/queueing/packeting	4

a result of a new node(s)'s participation in the network. Similarly, the features collected about version number and rank value give useful information for detecting version number attack and worst parent attack respectively. Link-layer features give information about the reasons for dropped packets in this layer such as collisions, neighbor allocation, queuing, and buffer management. These features are collected from the root node and its one-hop neighbors. It is assumed that each node periodically forwards these features to the root node. It is shown that while most of the packets are dropped at the routing layer as a result of version number attack, the packet drops in normal networks (under no attack) have mainly resulted from link-layer issues [6]. Therefore, it is believed that link-layer features could help distinguishing normal cases from malicious activities. Hence they are employed for the first time in intrusion detection in RPL. These features are collected periodically at the root node. The time interval for data collection is chosen experimentally by comparing the detection accuracy of the proposed system at different time intervals. The results of this evaluation are presented in Figure 1. According to these results, the time interval for data collection is set as 5 seconds to achieve the highest detection rate for the proposed design.

RPL-based IoT networks are generally used for MP2P communication, therefore the data (such as data collected from sensor nodes) flows from leaf nodes to the sink node. The sink node is usually responsible either for forwarding collected data to other applications or analyzing the data locally. Therefore, the root node is generally a more powerful device than other nodes in the network. In addition, it has a better view of the network. Based on these assumptions, a centralized IDS placed in the root node is proposed for applications based on MP2P communication in this study. Moreover, a centralized IDS can fit better than a distributed one to the resource-constrained structure of IoT. Here, three attacks are implemented separately on different networks with different percentage of attackers (2%, 6%, 10%, 20%). Each attack is simulated on 5 network topologies for each attacker density. Hence, in total 20 different networks are constructed for each attack. The same simulations are also run in a larger net-

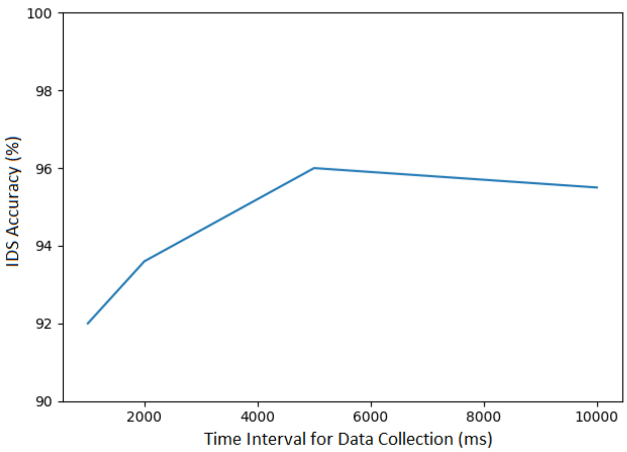

Fig. 1. Accuracy of IDS at varying time intervals for data collection

work area in order to observe the effect of node density on intrusion detection. Similarly, 20 networks under no-attack are run for generating benign traffic. The details of simulations are given in Table 2.

As the number of nodes increases, RPL produces lots of routing control messages which are gathered in the root node. In order to process such a large amount of data, a neural network-based IDS is proposed. The aim is to differentiate malicious attempts from normal network behavior with the data collected in the root node. The aim is not only to predict whether there is an attack in the network or not, but also predict the type of RPL attack with high accuracy. Therefore, the problem has been explored as both binary and multiclass classification.

The proposed neural network architecture is demonstrated in Figure 2. In order to calculate the weights of the input set, 4 fully-connected neural network layer with different output sizes is proposed. As an activation function, the Rectified Linear Unit (ReLU) function is employed. The number of neurons for hidden layers are set as 128, 64, 32, and 16 respectively. There are dropout layers between each fully-connected layer with a 0.5 drop rate to prevent over-fitting. Then, there is a fully-connected layer with a softmax function. The output size of this layer depends on the problem type, namely binary and multi-class classification. So, it has two neurons for binary classification to represent benign and attacked behaviour of the network, and four neurons for multi-class classification. Before training the model, data is pre-processed by applying feature scaling using the standard scaler function of the scikit library [23]. Other libraries used for neural network implementation in this study are Pandas [18], Numpy [21], and Keras [8].

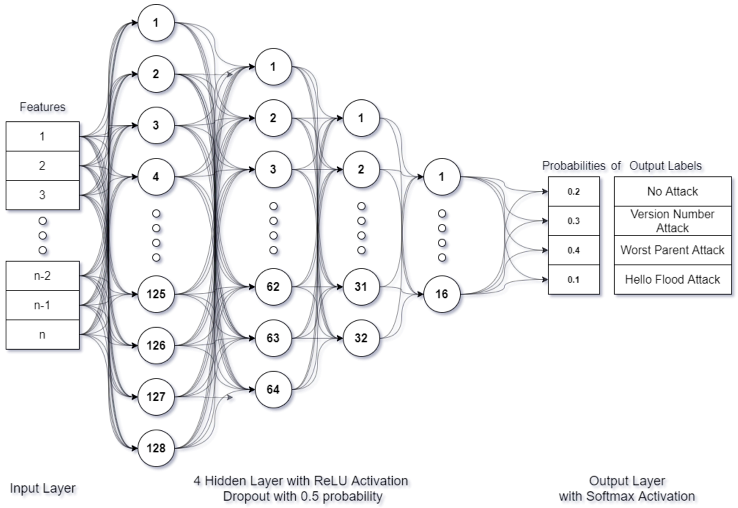

Fig. 2. The proposed neural network architecture

5 Experiments and Results

In this chapter, the simulation environment with its parameters and the performance metrics used in the analysis of the routing attacks in the experiments are detailed. Also, the performance of the proposed IDS solution is analyzed and discussed in this section.

5.1 Experimental Environment

Cooja Contiki Simulator 2.7 [22] is used to simulate IoT networks. Tmote Sky [2] nodes which are low power wireless modules and typically used in sensor networks are used as IoT devices. The sink node is a border router that connects the remaining nodes to the internet. It collects data from other nodes and helps them to create DODAG. The sender node represents an IoT device that sends periodic data messages to the sink node via its preferred parent. When the preferred node has data packets to forward, it sends the packet to its own parent, the packet is forwarded until it reaches the sink node. A malicious node is also a sender node, who manipulates the network and decreases the network performance.

Most of the studies in the literature use a single malicious node in their simulations. Moreover, they are generally simulated with a limited number of devices [17, 28]. However, as pointed out in [10], at least 25 or 30 devices are needed to see the multi-hop characteristics of RPL. In these studies, the simulations are also usually run for up to 30 minutes at most. Considering the time passed for the network to stabilize, this time can be limited to see the real effects of attacks. Moreover, the experiments are always carried out on a grid topology to see the effects of attackers at different locations. However, more realistic scenarios such as the random distribution of nodes and attackers, the partitioning of networks are not discovered in these studies. Therefore, in this study, simulation parameters are selected by considering these critical issues and given in Table 2. As shown in the table, two different networks (small and large) are simulated to see the effects of node density on intrusion detection. Moreover, each attack is carried out with different number of attackers.

Table 2. The simulation parameters

Simulation Parameters	
Simulation run time	60 min
Number of nodes	50
Sink node	1
Radio Medium	Unit Disc Graph Medium: Distance Loss
Transmission range	50m
Interference range	100m
Seed Type	Random Seed
Positioning	Random Positioning
Simulation Area	125x125m (small), 250x250m (large)
MAC Protocol	IEEE 802.15.4
Objective Function	MRHOF
Traffic Type	UDP
Traffic Rate	each node sends 1 packet every 60 seconds

5.2 Experimental Results

The model for binary classification is trained using two different schemes: 10-fold cross-validation and 60% percentage split. While the percentage split scheme acquires 96.88% DR and 0.13% FPR, the other scheme has 97.11% DR and 0.34% FPR. Therefore, the percentage method is used in subsequent evaluations. The experimental results for each attack type are given in Table 3. It shows that the proposed IDS could detect each attack effectively. Hello flood becomes the easiest attack type to detect even when it is carried out by a few attackers. In general, when the number of attackers increases, their effects on the network become more observable. Since WPA does not become effective until a considerable amount of attackers (10%) participate into the network, these cases were not considered in training/testing. In the large network, the detection rate of WPA is dropped. It is observed that small network is obviously affected by this attack and change parents more frequently. On the other hand, due to low node density in the large network, the clear effects of this attack on the network are less observed. This would cause a decrease in the detection rate.

To see the capability of the proposed method on detection of attacks on networks with different number of attackers, the model is trained only by using networks under high percentage of attackers (10%-20% for VNA, HFA, and 20% for WPA), then tested on networks under low percentage of attackers (2%-6% for VNA, HFA, and 10% for WPA). The results show that the IDS can still detect attacks with high detection rates (VNA: 88.93% WPA: 86.90%, HFA: 99.87%).

Table 3. The performance of IDS-binary classification

Attack Type	**Node Density**	**Small Network**	**Large Network**
		Detection Rate	**Detection Rate**
Version Number Attack (VNA)	2% Attacker	86.66%	93.99%
	6% Attacker	92.99%	92.33%
	10% Attacker	98.58%	94.75%
	20% Attacker	94.83%	90.99%
	Entire Dataset	**93.20%**	**92.96%**
Worst Parent Attack (WPA)	10% Attacker	96.91%	76.56%
	20% Attacker	99.42%	95.75%
	Entire Dataset	**98.17%**	**86.16%**
Hello Flood Attack (HFA)	2% Attacker	99.83%	99.67%
	6% Attacker	100%	100%
	10% Attacker	100%	100%
	20% Attacker	100%	100%
	Entire Dataset	**99.96%**	**99.92%**

To see the effects of routing layer and link layer features, two models are trained with different groups of features and compared in Table 4. Link layer features have caused a decrease in false positive rate since they help to discriminate normal cases from attack case in case of collisions in the link layer. These features have also slightly increased the detection rate of version number attacks since this attack is the main cause of packet drops at the routing layer [6].

Table 4. The effects of link layer features

Attack Type	**Routing Layer Features**		**Routing and Link Layer Features**	
	DR	**FPR**	**DR**	**FPR**
Version Number Attack	91.52%	-	93.20%	-
Worst Parent Attack	99.08%	-	98.17%	-
Hello Flood Attack	100%	-	99.96%	-
Entire Dataset	97.06%	0.61%	96.88%	0.13%

Finally, a model is trained for detecting all types of attacks and labeling them. The model has also a high detection rate (97.52%). As shown in the confusion matrix below, in some cases, VNA is confused with attack-free traffic. It is observed that this attack needs some time to affect the network. Hence, at this initial state of the attack, it cannot be distinguished from benign traffic.

Table 5. The performance of IDS-multiclass classification

True Label\Predicted as	**NA**	**VNA**	**WPA**	**HFA**
No Attack (NA)	99.7%	0%	0.3%	0%
Version Number Attack (VNA)	6.94%	92.42%	0.48%	0.17%
Worst Parent Attack (WPA)	1.42%	0.42%	97.71%	0.46%
Hello Flood Attack (HFA)	0.04%	0.02%	0.04%	99.9%

6 Conclusion

In this study, a novel neural network-based cross-layer intrusion detection system for RPL-based IoT networks is introduced. Both binary and multiclass classification for the following RPL-specific attacks are covered: version number, worst parent, and hello flood attacks. To the best of the authors' knowledge, the proposed IDS is the first cross-layer intrusion detection system in RPL that explores the effect of features obtained from link-layer on intrusion detection. The experimental results show that the proposed IDS detects each attack type with a high detection rate and an even lower false positive rate using the link-layer features.

Acknowledgement

Thanks to Emre Aydogan and Selim Yilmaz for sharing their experiences during the feature selection and feature extraction process of our neural-network based intrusion detection system.

References

1. Iot:number of connected devices wworldwide 2012-2025—statistica. https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/, accessed: 2020-01-08
2. Tmote sky from moteiv. https://insense.cs.st-andrews.ac.uk/files/2013/04/tmote-sky-datasheet.pdf, accessed: 2020-01-13
3. Airehrour, D., Gutierrez, J.A., Ray, S.K.: Sectrust-rpl: A secure trust-aware rpl routing protocol for internet of things. Future Generation Computer Systems **93**, 860 – 876 (2019). https://doi.org/https://doi.org/10.1016/j.future.2018.03.021, http://www.sciencedirect.com/science/article/pii/S0167739X17306581
4. Alexander, R., Brandt, A., Vasseur, J., Hui, J., Pister, K., Thubert, P., Levis, P., Struik, R., Kelsey, R., Winter, T.: RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks. RFC 6550 (Mar 2012). https://doi.org/10.17487/RFC6550, https://rfc-editor.org/rfc/rfc6550.txt
5. Aris, A., Oktug, S.F., Berna Ors Yalcin, S.: Rpl version number attacks: In-depth study. In: NOMS 2016 - 2016 IEEE/IFIP Network Operations and Management Symposium. pp. 776–779 (2016)
6. Arış, A., Örs Yalçın, S.B., Oktuğ, S.F.: New lightweight mitigation techniques for rpl version number attacks. Ad Hoc Networks **85**, 81 – 91 (2019). https://doi.org/https://doi.org/10.1016/j.adhoc.2018.10.022, http://www.sciencedirect.com/science/article/pii/S1570870518307625
7. Aydogan, E., Yilmaz, S., Sen, S., Butun, I., Forsström, S., Gidlund, M.: A central intrusion detection system for rpl-based industrial internet of things. In: 2019 15th IEEE International Workshop on Factory Communication Systems (WFCS). pp. 1–5 (2019)
8. Chollet, F., et al.: Keras. https://keras.io (2015)
9. Glissa, G., Rachedi, A., Meddeb, A.: A secure routing protocol based on rpl for internet of things. In: 2016 IEEE Global Communications Conference (GLOBECOM). pp. 1–7 (2016)

10. Kim, H.S., Ko, J., Culler, D.E., Paek, J.: Challenging the ipv6 routing protocol for low-power and lossy networks (rpl): A survey. IEEE Communications Surveys & Tutorials **19**(4), 2502–2525 (2017)
11. Le, A., Loo, J., Chai, M., Aiash, M.: A specification-based ids for detecting attacks on rpl-based network topology. Information **7** (05 2016). https://doi.org/10.3390/info7020025
12. Le, A., Loo, J., Lasebae, A., Vinel, A., Chen, Y., Chai, M.: The impact of rank attack on network topology of routing protocol for low-power and lossy networks. Sensors Journal, IEEE **13**, 3685–3692 (10 2013). https://doi.org/10.1109/JSEN.2013.2266399
13. Le, A., Loo, J., Luo, Y., Lasebae, A.: The impacts of internal threats towards routing protocol for low power and lossy network performance. pp. 000789–000794 (07 2013). https://doi.org/10.1109/ISCC.2013.6755045
14. Levis, P., Clausen, T.H., Gnawali, O., Hui, J., Ko, J.: The Trickle Algorithm. RFC 6206 (Mar 2011). https://doi.org/10.17487/RFC6206, https://rfc-editor.org/rfc/rfc6206.txt
15. Maple, C.: Security and privacy in the internet of things. Journal of Cyber Policy **2**, 155–184 (05 2017). https://doi.org/10.1080/23738871.2017.1366536
16. Mayzaud, A., Badonnel, R., Chrisment, I.: A distributed monitoring strategy for detecting version number attacks in rpl-based networks. IEEE Transactions on Network and Service Management **PP**, 1–1 (05 2017). https://doi.org/10.1109/TNSM.2017.2705290
17. Mayzaud, A., Sehgal, A., Badonnel, R., Chrisment, I., Schönwälder, J.: A study of rpl dodag version attacks. In: Sperotto, A., Doyen, G., Latré, S., Charalambides, M., Stiller, B. (eds.) Monitoring and Securing Virtualized Networks and Services. pp. 92–104. Springer Berlin Heidelberg, Berlin, Heidelberg (2014)
18. McKinney, W., et al.: Data structures for statistical computing in python. In: Proceedings of the 9th Python in Science Conference. vol. 445, pp. 51–56. Austin, TX (2010)
19. Müller., N.M., Debus., P., Kowatsch., D., Böttinger., K.: Distributed anomaly detection of single mote attacks in rpl networks. In: Proceedings of the 16th International Joint Conference on e-Business and Telecommunications - Volume 2: SECRYPT,. pp. 378–385. INSTICC, SciTePress (2019). https://doi.org/10.5220/0007836003780385
20. Napiah, M.N., Bin Idris, M.Y.I., Ramli, R., Ahmedy, I.: Compression header analyzer intrusion detection system (cha - ids) for 6lowpan communication protocol. IEEE Access **6**, 16623–16638 (2018)
21. Oliphant, T.E.: A guide to NumPy, vol. 1. Trelgol Publishing USA (2006)
22. Osterlind, F., Dunkels, A., Eriksson, J., Finne, N., Voigt, T.: Cross-level sensor network simulation with cooja. Local Computer Networks, Annual IEEE Conference on **0**, 641–648 (11 2006). https://doi.org/10.1109/LCN.2006.322172
23. Pedregosa, F., Varoquaux, G., Gramfort, A., Michel, V., Thirion, B., Grisel, O., Blondel, M., Prettenhofer, P., Weiss, R., Dubourg, V., et al.: Scikit-learn: Machine learning in python. Journal of machine learning research **12**(Oct), 2825–2830 (2011)
24. Pongle, P.: Real time intrusion and wormhole attack detection in internet of things. International Journal of Computer Applications **121**, 1–9 (07 2015). https://doi.org/10.5120/21565-4589
25. Ray, P.: A survey on internet of things architectures. Journal of King Saud University - Computer and Information Sciences **30**(3), 291 –

319 (2018). https://doi.org/https://doi.org/10.1016/j.jksuci.2016.10.003, http://www.sciencedirect.com/science/article/pii/S1319157816300799

26. Raza, S., Wallgren, L., Voigt, T.: Svelte: Real-time intrusion detection in the internet of things. Ad Hoc Networks **11**(8), 2661 – 2674 (2013). https://doi.org/https://doi.org/10.1016/j.adhoc.2013.04.014, http://www.sciencedirect.com/science/article/pii/S1570870513001005
27. Verma, A., Ranga, V.: Security of rpl based 6lowpan networks in the internet of things: A review. IEEE Sensors Journal **20**(11), 5666–5690 (2020)
28. Verma, A., Ranga, V.: Mitigation of dis flooding attacks in rpl-based 6lowpan networks. Transactions on Emerging Telecommunications Technologies **31**(2), e3802 (2020). https://doi.org/10.1002/ett.3802, https://onlinelibrary.wiley.com/doi/abs/10.1002/ett.3802, e3802 ett.3802
29. Yavuz, F.Y., Unal, D., Gul, E.: Deep learning for detection of routing attacks in the internet of things. International Journal of Computational Intelligence Systems **12**, 39–58 (2018). https://doi.org/https://doi.org/10.2991/ijcis.2018.25905181, https://doi.org/10.2991/ijcis.2018.25905181