Routing Protocol for Low Power and Lossy Network

Subjects: Computer Science, Artificial Intelligence

Contributor: Mohammed Anbar, Taief Al-Amiedy, Arkan Kabla, Iznan Hasbullah

The IETF Routing Over Low power and Lossy network (ROLL) working group defined IPv6 Routing Protocol for Low Power and Lossy Network (RPL) to facilitate efficient routing in IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN). Limited resources of 6LoWPAN nodes make it challenging to secure the environment, leaving it vulnerable to threats and security attacks. Machine Learning (ML) and Deep Learning (DL) approaches have shown promise as effective and efficient mechanisms for detecting anomalous behaviors in RPL-based 6LoWPAN.

Keywords: 6LoWPAN ; Internet of Thing (IoT) ; IPv6 ; Low Power and Lossy Network (LLN)

1. Introduction

Internet of Things (IoT) has become one of the most important elements of the Information and Communication Technology (ICT) revolution. IoT plays a significant role in connecting smart objects anytime, anywhere, and any service through any network. The entire world looks forward to creating a new smart world that changes people's lifestyles and how things work in our world [1][2]. Consequently, the IoT affects everything from our lifestyle to how we live in this era of technological convergence and inter-connectivity. The IoT incorporates the linkage of human culture—our "things"—considering the interconnection of our computerized data framework—"the Internet". The paradigm of IoT has spread all over the world. It foresees the networking of billions to trillions of smart things around us, specifically ordinary things that are extraordinarily traceable, addressable, and have the ability to collect, store, analyze, and communicate data about themselves and their physical surroundings [3][4].

In addition, IoT objects or devices may connect bidirectionally for data exchange over the Internet. Furthermore, it is highly advantageous to people since it optimizes their time and boosts productivity. Consequently, we can reinvent ourselves while simultaneously making the world and our lives smarter with the help of IoT. Moreover, the benefits of IoT are nearly limitless, and its applications are transforming how we work and live by exchanging time and assets and opening up new prospects for growth and development [5]. Moreover, a recent forecast from International Data Corporation (IDC), a well-known provider of industry intelligence, predicts that by 2025, there will be around 41.6 billion connected IoT devices/things (a combination of sensors, machines, cameras, etc.), generating around 79.4 zettabytes of data. The forecast was based on an analysis spanning the years from 2018 to 2025, and during that period, they expected IoT devices to grow at a Compound Annual Growth Rate (CAGR) of 28.7%.

The various IoT sensors deployed in different environments are responsible for collecting data in the network and sending them to the backbone servers and control centers for further analysis to assist in decision making. The number of IoT-based applications has increased exponentially in recent years, and while many are still in the early research stage, many economically attractive application scenarios already exist that span several domains [6]. Some of these applications include smart firefighting for forest fire detection and personal protective equipment monitoring; smart manufacturing for monitoring air quality, temperature, and cyber-physical systems; and intelligent healthcare for detecting Ultraviolet (UV) radiation, monitoring patient conditions, and controlling emergency response vehicles. Since the IoT exchanges massive quantities of essential and sensitive data, the lack of security of those networks, especially involving security breaches or penetration, could lead to severe repercussions economically and endanger human lives [7][8].

In IoT, the information is exchanged and routed among the linked devices through a specially designed network that supports IoT specifications. An example of such networks is Low power and Lossy Networks (LLNs), comprising a wide range of embedded devices, such as sensors and actuators. Those devices are the driving force behind the IoT, since they enable global connections to items that are not connected to the Internet. However, these embedded devices have a low power supply, small memory space, limited computing capabilities, and a short radio range. Hence, to enable communication among those appliances, the Internet Engineering Task Force (IETF) specified IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) to serve as an adaptation layer and effectively encapsulate long IPv6 headers in packets of 128 bytes [9][10].

2. Routing Protocol for Low Power and Lossy Network (RPL)

Due to the constrained environment of LLN, it is obligatory to conserve the energy of such devices while transmitting and transferring information among networks' nodes. Therefore, several protocols have been devised and standardized to allow and manage the communication amongst LLN's resource-constrained devices. One of the most popular proposed protocols for routing purposes in LLNs is RPL [11].

The RPL is a standard routing protocol for LLNs established by the IETF Routing Over Low power and Lossy network (ROLL) task force in 2012 and detailed in Request for Comment (RFC) 6550 [12]. IEEE licensed the development of RPL to overcome the current gap in the routing of IoT networks and attain the limited capabilities of LLN's devices. The fundamental concept underlying RPL is the topological concept of Destination-Oriented Directed Acyclic Graphs (DODAGs).

The DODAG is a directed graph with no loops oriented towards a root node. The nodes that provide Internet access (gateways) are called root nodes, and the other nodes in the network are linked with it either directly or indirectly through a sequence of parent nodes. Furthermore, each node is responsible for selecting the desired parent, who is then used for forwarding the application packets. The parent node selection depends on the rank value that a device (node) can achieve. Moreover, the rank value refers to the position of a node in the DODAG. Hence, the rank value is affected by the node's distance from the root and the Objective Function (OF). The OF determines numerous metrics, such as rank of nodes, selection of the parent node, and route optimization. The versatility of RPL to interact with many limited devices is the primary reason for its adoption in LLNs [11].

The RPL adds five new control messages for constructing and maintaining the DODAG and communication routes. The RPL control messages are a specific type of Internet Control Messages Protocol version 6 (ICMPv6) control message, as follows:

- **DODAG Information Solicitation (DIS).** Nodes intending to join a network but have yet to receive DODAG Information Object (DIO message advertise a DIS message to inquire for available DODAG to create a connection).
- **DODAG Information Object (DIO)**. Nodes use the DIO message for locating RPL instances, learning about DODAG configurations, choosing a preferred parent, keeping DODAG structure in place, and knowing the current rank of the node and the IPv6 address of the root [13].
- A **Destination Advertisement Object (DAO)** message is used for advertising backward route information by building upward and downward routes between nodes and then creating routing tables on receiving nodes [14].
- A **Destination Advertisement Object Acknowledgement (DAO-ACK)** message is a response message to a DAO message.
- **Consistency Check (CC).** The RPL protocol employs CC to ensure the synchronization of the "security counter or timestamp between each pair of nodes" [15].

The RPL supports various communication paradigms, Point-to-MultiPoint (P2MP), Point-to-Point (P2P), and MultiPoint-to-Point (MP2P) [15]. In addition, the RPL supports two modes of operation. First, the storing mode, where each node maintains a downward routing table for its sub-DODAG and uses it to transmit P2P traffic. Consequently, the traffic will go upward until it arrives at a common predecessor (of the sender and destination), then it will be forwarded downward to the destination node. Second, the non-storing mode, where the root node is the sole device that retains. Application packets are first sent to the root node, then re-routed to their destination in this mode. Those looking for further explanations of the architecture and implementation of the RPL protocol can find them in [16].

3. Security Issues and Threats in the RPL Protocol

According to a recent report by Nokia [17], attacks on IoT devices are increasing at an alarming rate. The increase is due to the proliferation of automated tools to exploit IoTs' vulnerabilities. The report states that IoT devices now make up roughly 33% of exploited devices, compared to only 16% in 2019. The statistics are the outcome of monitoring aggregated network traffic data of more than 150 million devices globally. Furthermore, researchers claim that more than half of all deployed IoT devices are vulnerable to medium to high severity attacks [7].

The exponential increase in the demand for IoT devices has accelerated research and development efforts in IoT-related areas, including security. It has attracted many researchers to investigate attacks targeting IoT networks. Many IoT applications use the RPL protocol, since it is purposely developed for constrained devices commonly used in modern IoT applications. Nonetheless, the RPL protocol is still vulnerable to many threats that could harm the entire network

infrastructure. Consequently, researchers invest their time and efforts investigating various threats in LLNs that use the RPL protocol [18].

Routing security is a major concern, as routing-related attacks impede sensor data transmission and adversely affect network layer performance. It can also significantly affect the upper layers of the IoT network, which frequently causes Denial of Service (DoS) attacks [19]. In addition, providing a suitable security mechanism for the routing protocol in the IoT is challenging due to the characteristics inherited from other networks. Furthermore, the packet forwarding process in IoT-constrained devices is influenced by potential security threats, affecting the delivered services to end-users as the performance of the malignant nodes is rapidly increased during the data packet routing process. Eventually, the network's topology will be disrupted, and the resulting overhead will deplete the nodes' power resources and eventually break down the whole network [20].

In addition, the RPL security specification allows the protocol to operate in an open or optionally secured mode. In open mode, any node can join the LLN without an authentication key. In a secure mode, a node requires a preinstalled key to join the LLN and an additional authentication key to join as a sensor with routing capability. RPL also provides an optional consistency check feature for protection against replay attacks. Although RPL provides these optional features to address the security of the routing process, most of the security features are implemented only for external attacks owing to the constrained nature of IoT-LLNs. When a malicious node joins the IoT-LLN, RPL has several exploitable vulnerabilities, allowing adversaries to instigate insider attacks that deplete network resources and degrade performance. Thus, the security of RPL is crucial due to its significance in IoT networks [21][22].

Figure 1 shows the taxonomy of RPL attacks, classified into three categories, and each category has two subclasses based on the intent of threats [23]. These attacks may cause severe network issues, such as exhausting network resources, destructing network topology, and stealing sensitive information. Further, **Figure 1** lists the recent attacks addressed by the existing studies. Section 7.6 provides further details about those attacks.

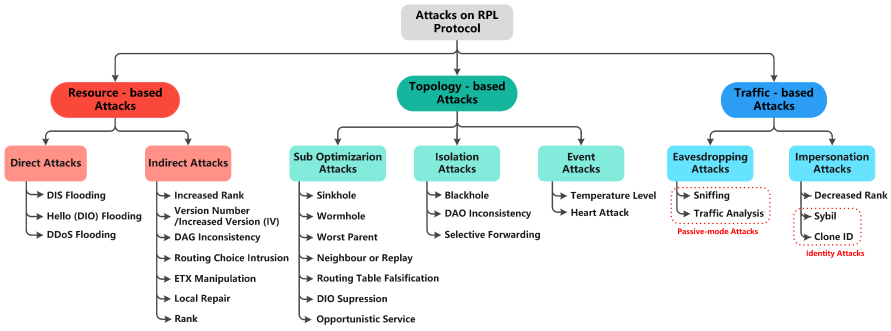

Figure 1. Taxonomy of RPL attacks.

To this end, many researchers have suggested that addressing routing attacks in RPL- based LLNs is still an open research issue [23]. However, due to the constrained and open nature of RPL-supported IoT-LLNs, implementing complex security solutions is difficult, and that leaves the network vulnerable to attacks. Therefore, there is a need for designing an efficient approach/solution to address routing attacks in the early stage of any malicious activity within the network [24].

4. Machine Learning (ML) and Deep Learning (DL) Technique for RPL Security

The existing traditional security mechanisms, such as those based on cryptography, trust, threshold, and Intrusion Detection systems (IDS), cannot detect or prevent RPL-LLN attacks effectively due to differences in the topology, complexity, and dissimilarity in the traffic patterns [18][20].

In addition, these mechanisms fail to detect sophisticated and devastating huge attack surfaces and require heavy resources, which drastically deplete the resources of constrained devices and impact the normal operation of network nodes [25]. Furthermore, detecting a complex and a combination of multiple attacks in the network requires an intelligent detection mechanism. Hence, there is a need to design a detection mechanism capable of handling the issues described above. The security mechanisms should be eligible to identify known and unknown (zero-day) attacks with a thorough examination of their actions. Additionally, the vast amounts of data traffic exchanged between the sensors (devices) of the LNN-based IoT network constitutes another challenge that should be considered throughout the design of the detection mechanism.

The term “big data” refers to a high volume of data. Such data necessitate advanced techniques to extract valuable information to analyze legal and harmful behavioral packet patterns. "Big Data" is a buzzword that includes methods to extract extremely vital information from the massive amounts of data traffic exchanged in the IoT networks. In other words, not all the data traffic is necessary for further analysis and learning. The advancements in big data technology make it more practical to extract different legitimate and malicious behavioral packet patterns from the immense data traffic [26].

Unfortunately, conventional intrusion detection methods cannot effectively process large amounts of data, resulting in a lack of useful information. Thus, more intelligent and adaptable mechanisms are needed to expand the detection capabilities of the existing security defenses systems for the next generation of IoT networks. ML learning and DL-based intrusion detection techniques have attracted much interest in enhancing security in IoT networks [27]. With its ability to learn from datasets, ML is particularly suited to complexities that are too complex to be fully explained or performed precisely. Furthermore, ML requires a small amount of data for training and testing but has lower accuracy. On the contrary, DL, a subset of ML, requires a vast quantity of data to train the system and takes a long time, but it usually gives higher accuracy [28][29]. In that sense, ML and DL are the most successful computational techniques for providing embedded intelligence in the IoT context due to their ability to deal with a tremendous amount of data, maximize feature engineering, learn from latent abnormal patterns, and reduce the time for detecting known and unknown attacks [30][31][32][33]. Thus, the ML and DL approaches improve the IoT security and RPL network in particular and overcome the weaknesses of other conventional solutions.

Due to the limitations of IoT devices in terms of computing and power resources, designing ML and DL algorithms for the IoT network is a challenging endeavor [34]. In this context, ML and DL techniques are applicable at RPL nodes, fog/edge nodes, and (or) cloud nodes to extract and analyze large-scale data to detect malicious behaviors. As a result, Artificial Intelligence (AI)-assisted security analysis approaches can transform end-to-end IoT security into an intelligence-based monitoring system [35]. Recently, ML- and DL-based security solutions for identifying attacks and countering threats intelligently in the RPL network have become a promising research area and have attracted attention from many researchers to add more to this field.

References

1. Kamel, S.O.M.; Elhamayed, S.A. Mitigating the impact of iot routing attacks on power consumption in iot healthcare environment using convolutional neural network. Int. J. Comput. Netw. Inf. Secur. 2020, 12, 11–29.
2. Alamiedy, T.A.; Anbar, M.; Alqattan, Z.N.; Alzubi, Q.M. Anomaly-based intrusion detection system using multi-objective grey wolf optimisation algorithm. J. Ambient. Intell. Humaniz. Comput. 2020, 11, 3735–3756.
3. Canbalaban, E.; Sen, S. A Cross-Layer Intrusion Detection System for RPL-Based Internet of Things. In International Conference on Ad-Hoc Networks and Wireless; Springer: Bari, Italy, 2020; Volume 12338, pp. 214–227.
4. Al-mashhadi, S.; Anbar, M.; Hasbullah, I.; Alamiedy, T.A. Hybrid rule-based botnet detection approach using machine learning for analysing DNS traffic. PeerJ Comput. Sci. 2021, 7, e640.
5. Morales-Molina, C.D.; Hernandez-Suarez, A.; Sanchez-Perez, G.; Toscano-Medina, L.K.; Perez-Meana, H.; Olivares-Mercado, J.; Portillo-Portillo, J.; Sanchez, V.; Garcia-Villalba, L.J. A dense neural network approach for detecting clone id attacks on the rpl protocol of the iot. Sensors 2021, 21, 3173.
6. Samaila, M.G.; Sequeiros, J.B.; Freire, M.M.; Inácio, P.R. Security threats and possible countermeasures in IoT applications covering different industry domains. In Proceedings of the 13th International Conference on Availability, Reliability and Security, Hamburg, Germany, 27–30 August 2018.
7. Said, A.M.; Yahyaoui, A.; Abdellatif, T. Efficient anomaly detection for smart hospital iot systems. Sensors 2021, 21, 1026.
8. Shukla, P. ML-IDS: A machine learning approach to detect wormhole attacks in Internet of Things. In Proceedings of the 2017 Intelligent Systems Conference (IntelliSys), London, UK, 7–8 September 2017; pp. 234–240.
9. Vinet, L.; Zhedanov, A. A ‘missing’ family of classical orthogonal polynomials. J. Phys. A Math. Theor. 2011, 44, 085201.
10. Sahay, R.; Geethakumari, G.; Mitra, B.; Sahoo, I. Efficient Framework for Detection of Version Number Attack in Internet of Things. In Advances in Intelligent Systems and Computing; Springer International Publishing: Berlin/Heidelberg, Germany, 2020; Volume 941, pp. 480–492.
11. Alamiedy, T.A.; Anbar, M.F.; Belaton, B.; Kabla, A.H.; Khudayer, B.H. Ensemble Feature Selection Approach for Detecting Denial of Service Attacks in RPL Networks. In Communications in Computer and Information Science;

Springer Science and Business Media Deutschland GmbH: Berlin/Heidelberg, Germany, 2021; Volume 1487, pp. 340–360.

12. Agiollo, A.; Conti, M.; Kaliyar, P.; Lin, T.N.; Pajola, L. DETONAR: Detection of Routing Attacks in RPL-Based IoT. IEEE Trans. Netw. Serv. Manag. 2021, 18, 1178–1190.
13. AlSawafi, Y.; Touzene, A.; Day, K.; Alzeidi, N. Hybrid RPL-based sensing and routing protocol for smart city. Int. J. Pervasive Comput. Commun. 2020, 16, 279–306.
14. Raoof, A.; Matrawy, A.; Lung, C.H. Routing Attacks and Mitigation Methods for RPL-Based Internet of Things. IEEE Commun. Surv. Tutor. 2019, 21, 1582–1606.
15. Faraj, O.; Megías, D.; Ahmad, A.M.; Garcia-Alfaro, J. Taxonomy and challenges in machine learning-based approaches to detect attacks in the internet of things. In Proceedings of the 15th International Conference on Availability, Reliability and Security, Virtual Event, Ireland, 25–28 August 2020; pp. 1–10.
16. 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 Commun. Surv. Tutor. 2017, 19, 2502–2525.
17. Nokia. Nokia: Threat Intelligence Report 2020. 2020. Available online: https://doi.org/10.1016/s1361-3723(20)30115-9 (accessed on 1 April 2022).
18. Pu, C.; Carpenter, L. Digital Signature Based Countermeasure Against Puppet Attack in the Internet of Things. In Proceedings of the 2019 IEEE 18th International Symposium on Network Computing and Applications (NCA), Cambridge, MA, USA, 26–28 September 2019; pp. 1–4.
19. Sahay, R.; Geethakumari, G.; Mitra, B. A novel blockchain based framework to secure IoT-LLNs against routing attacks. Computing 2020, 102, 2445–2470.
20. Almusaylim, Z.A.; Jhanjhi, N.Z.; Alhumam, A. Detection and mitigation of RPL rank and version number attacks in the internet of things: SRPL-RP. Sensors 2020, 20, 5997.
21. Neerugatti, V.; Rama Mohan Reddy, A. Artificial Intelligence-Based Technique for Detection of Selective Forwarding Attack in RPL-Based Internet of Things Networks. In Advances in Intelligent Systems and Computing; Springer: Singapore, 2020; Volume 1054, pp. 67–77.
22. Alzubaidi, M.; Anbar, M.; Chong, Y.W.; Al-Sarawi, S. Hybrid monitoring technique for detecting abnormal behaviour in rpl-based network. J. Commun. 2018, 13, 198–208.
23. Mayzaud, A.; Badonnel, R.; Chrisment, I. A taxonomy of attacks in RPL-based internet of things. Int. J. Netw. Secur. 2016, 18, 459–473.
24. Sahay, R.; Geethakumari, G.; Mitra, B. A Feedforward Neural Network based Model to Predict Sub-optimal Path Attack in IoT-LLNs. In Proceedings of the 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing, Melbourne, VIC, Australia, 11–14 May 2020; pp. 400–409.
25. Tahsien, S.M.; Karimipour, H.; Spachos, P. Machine learning based solutions for security of Internet of Things (IoT): A survey. J. Netw. Comput. Appl. 2020, 161, 102630.
26. Jamalipour, A.; Murali, S. A Taxonomy of Machine Learning based Intrusion Detection Systems for the Internet of Things: A Survey. IEEE Internet Things J. 2021, 111, 2287–2310.
27. da Costa, K.A.; Papa, J.P.; Lisboa, C.O.; Munoz, R.; de Albuquerque, V.H.C. Internet of Things: A survey on machine learning-based intrusion detection approaches. Comput. Netw. 2019, 151, 147–157.
28. Zarpelão, B.B.; Miani, R.S.; Kawakani, C.T.; de Alvarenga, S.C. A Survey of Intrusion Detection in Internet of Things; Elsevier: Amsterdam, The Netherlands, 2017.
29. Mohammadi, M.; Al-Fuqaha, A.; Sorour, S.; Guizani, M. Deep learning for IoT big data and streaming analytics: A survey. IEEE Commun. Surv. Tutor. 2018, 20, 2923–2960.
30. Cakir, S.; Toklu, S.; Yalcin, N. Rpl attack detection and prevention in the internet of things networks using a gru based deep learning. IEEE Access 2020, 8, 183678–183689.
31. Osman, M.; He, J.; Mokbal, F.M.M.; Zhu, N.; Qureshi, S. ML-LGBM: A Machine Learning Model Based on Light Gradient Boosting Machine for the Detection of Version Number Attacks in RPL-Based Networks. IEEE Access 2021, 9, 83654–83665.
32. Bokka, R.; Sadasivam, D.T. Machine Learning Techniques To Detect Routing Attacks in Rpl Based Internet of Things. Int. J. Electr. Eng. Technol. (IJEET) 2021, 12, 346–356.
33. Alamiedy, T.A.; Anbar, M.; Al-Ani, A.K.; Al-Tamimi, B.N.; Faleh, N. Review on feature selection algorithms for anomaly-based intrusion detection system. Adv. Intell. Syst. Comput. 2019, 843, 605–619.

34. Aversano, L.; Bernardi, M.L.; Cimitile, M.; Pecori, R. A systematic review on Deep Learning approaches for IoT security. Comput. Sci. Rev. 2021, 40, 100389.
35. Medjek, F.; Tandjaoui, D.; Djedjig, N.; Romdhani, I. Fault-tolerant AI-driven Intrusion Detection System for the Internet of Things. Int. J. Crit. Infrastruct. Prot. 2021, 34, 100436.