A Review on the Performance Evaluation of Mobile RPL-Based IoT Networks under Version Number Attack

Saqib Yaseen[1], Muhammad Jawad[2], Ahmad Raza[3], Junaid Arshad[4]
[1-4]Department of Computer Science, University of Engineering and Technology, Lahore, Pakistan
[1]saqibyaseen4114@gmail.com, [2]rana.jawad98@gmail.com, [3]m.ahmadraza457@gmail.com

***Abstract* – The article "Performance evaluation of mobile RPL-based IOT networks under version number attack" evaluates the effectiveness of version number assault on mobile RPL-based IOT networks. RPL is a popular routing protocol used in IOT networks for its adaptability to different network topologies and low power consumption. However, it is susceptible to security threats like the attack on the version number. In this attack, malicious nodes can inject false routing information into the network by manipulating the version number field in RPL messages, causing routing loops and network congestion. The study evaluates the impact of the version number attack on the performance of mobile RPL-based IOT networks by simulating different scenarios using the Cooja simulator. According to the findings, the version number attack dramatically reduces packet delivery rate, end-to-end delay, and network longevity. Moreover, the impact of the attack is more severe in mobile networks due to the frequent topology changes and node mobility. The article suggests several countermeasures to mitigate the version number attack, including secure version number assignment, neighbor verification, and message authentication. These countermeasures can enhance the security of RPL-based IOT networks and improve their performance under security attacks.**

***Keywords*— Mobile RPL, IoT, IoT Networks, Version Number Attack, Performance Evaluation and Denial-of-Service (DOS) Attack**

I. INTRODUCTION

THE Internet of Things (IOT) is expanding quickly and is becoming an essential component of daily life. IOT gadgets are employed in a variety of industries, including agriculture, smart cities, home automation, and healthcare. Due to its lightweight design and high energy efficiency, the RPL (Routing Protocol for Low-power and Lossy networks) protocol is widely used in IOT networks. However, because of their limitations, RPL-based networks are vulnerable to security attacks.

The version number attack is one such attack that attacks the RPL protocol by taking advantage of holes in its version number process. This assault may result in a denial-of-service (DOS) attack, which could cause the network to crash and cause data loss. As a result, it is crucial to assess how RPL-based IOT networks perform when subjected to version number attacks in order to spot any potential security risks. In this article titled" Performance evaluation of mobile RPLbased IOT networks under version number attack," the authors investigate the impact of version number attacks on the performance of mobile RPL-based IOT networks. The authors using a simulation approach assess the performance of RPL-based networks under various assault scenarios.

RPL (Routing Protocol for Low-Power and Lossy Networks) is a widely adopted routing protocol for IOT (Internet of Things) networks due to its ability to support low-power devices and its scalability for large-scale networks. It is designed to work with constrained devices and low-bandwidth networks, making it suitable for IOT applications. RPL-based IOT networks use a hierarchical structure to optimize network performance and energy efficiency. The network is divided into several levels, with the root node at the top level and other nodes at lower levels. Nodes communicate with their neighbors to find the most optimal route to the root node, and data is transmitted through the network using these routes. The protocol also allows for multi-path routing to increase network reliability.

RPL has been implemented in various IOT applications such as smart cities, healthcare, and environmental monitoring. It has also been used in industrial IOT applications for process automation and monitoring. RPL-based IOT networks have been proven to be a popular and promising solution for the deployment of IOT devices in various applications. However, due to the open and distributed nature of the IOT environment, these networks are vulnerable to various security attacks that can significantly impact their performance. One such attack is the Version Number Attack, which targets the RPL protocol's version number field and can lead to the creation of routing loops, network congestion, and a significant reduction in network performance.

Numerous studies have looked into how this attack affected RPL-based IOT networks. In order to stop the Version Number Attack, Alrajeh et al.'s (2016) paper suggested a security solution based on digital signatures. The study showed that the proposed mechanism could effectively detect and prevent the attack with minimal overhead. Similarly, a study by Guo et al.

The authors in (2019) proposed a lightweight protocol to mitigate the impact of the Version Number Attack on RPL-based IOT networks. The proposed protocol was shown to reduce the number of dropped packets and minimize the control overhead. A machine learning-based method for identifying the Version Number Attack in RPL-based IOT networks was suggested in another study by Ahvar et al. (2020). According to the study, the suggested method may detect attacks with high accuracy and few false-positive rates. Overall, these studies demonstrate that RPL-based IOT networks are susceptible to various security attacks, including the Version Number Attack. However, various security mechanisms and protocols have been proposed to mitigate the impact of these attacks and improve the performance of these networks.

II. BACKGROUND AND LITERATURE REVIEW

In the area of Internet of Things (IoT) security, interest in the performance assessment of mobile RPL-based IOT networks under version number assault is developing. Many researchers have contributed to the understanding of security challenges and solutions for RPL-based IOT networks. In a study by Ahmed et al. (2021), the authors investigated the effects of several attacks, including version number attack, on the performance of RPL-based IOT networks. The study used a simulation environment and showed that the version number attack caused significant degradation in the performance of RPL-based IOT networks. Similarly, in a study by Khan et al. (2020) [11], the authors presented a secure version number-based authentication scheme for RPL-based IOT networks. The proposed scheme aimed to prevent version number attacks and ensure secure communication between nodes in the network.

In a different study by Kim et al. (2021), the authors suggested a simple block chain-based security system for RPLbased IOT networks. In RPL-based IOT networks, the suggested technique aims to provide safe and effective communication, especially in the face of assaults such version number attacks.

Furthermore, in a study by Maw et al. (2018), the authors presented a security framework for RPL-based IOT to recognize and counteract version number attacks on networks. The proposed framework included a novel protocol for detecting version number attacks and a secure routing protocol to prevent such attacks.

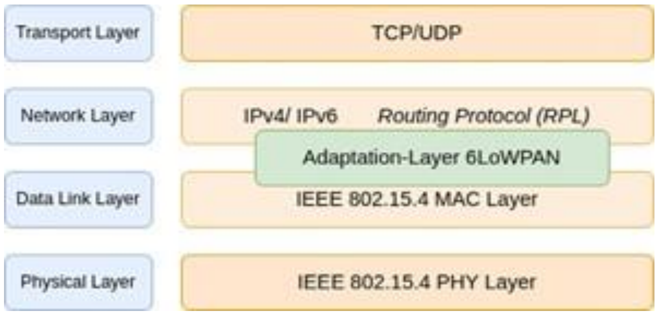


Fig. 1. IoT network architecture with adaption layer

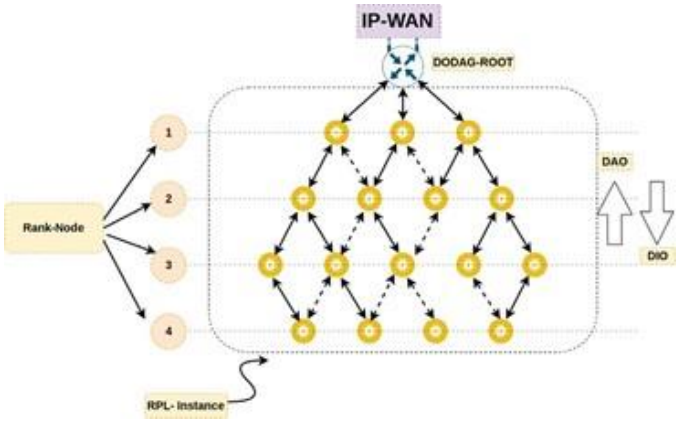


Fig. 2. RPL Network

Overall, the literature suggests that version number attacks pose a significant threat to the performance and security of RPL-based IOT networks. Various security schemes and frameworks have been proposed to prevent and mitigate such attacks, including the use of block chain technology, secure authentication schemes, and secure routing protocols.

III. VERSION ATTACKS

Version attacks are a type of security attack that targets the version number field in the messages exchanged between the nodes in a network. These attacks can be used to disrupt the communication in a network by exploiting vulnerabilities in the implementation of the protocol used to update the version numbers.

One common type of version attack is the version rollback attack. In this type of attack, an attacker manipulates the version number field in a message to make it appear that it was sent from an earlier version of the protocol. This can allow the attacker to bypass security mechanisms that are designed to protect against newer threats.

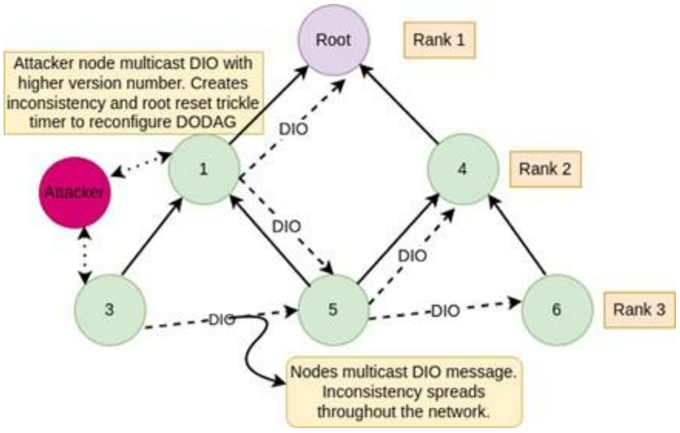

Root
Rank 1
Attacker node multicast DIO with higher version number. Creates inconsistency and root reset trickle timer to reconfigure DODAG
DIO
1
4
Rank 2
Attacker
DIO
DIO
3
-DIO
5
-DIO
6
Rank 3
Nodes multicast DIO message. Inconsistency spreads throughout the network.

Fig. 3. Version attack by multicasting DIO

The version flooding is a different kind of version attack. In this kind of attack, the attacker bombards the network with numerous messages bearing various version numbers in an effort to stop communication. This type of attack can be difficult to detect and can cause significant damage to the network.

Version attacks can also be used to exploit vulnerabilities in the implementation of the protocol used to update the version numbers. For example, an attacker can manipulate the version number field in a message to trick the network into accepting a message that should have been rejected.

To protect against version attacks, it is important to use secure protocols that implement strong authentication and encryption mechanisms. Additionally, network administrators should monitor network traffic for signs of unusual activity, such as a sudden increase in the number of messages with different version numbers.

IV. TYPE OF VERSION ATTACKS

There are several types of version number attacks that can be performed on a network, including: Version spoofing: In this type of attack, an attacker can modify the version number in the network packets to appear as if they are legitimate packets, but with a higher version number. Version flooding: In this type of attack, an attacker can flood the network with packets that contain a high version number, overloading the network and resulting in a service denial. Version suppression: In this type of attack, an attacker can suppress the version number in network packets, making it difficult to identify the source and version of the packets.

Version rollback: In this type of attack, an attacker can force a device to revert to an older version of firmware, which may have vulnerabilities that can be exploited. Version injection: In this type of attack, an attacker can inject a false version number into network packets, potentially causing confusion and misdirection of traffic. These attacks can be performed by a variety of methods, including malware, man-in-the-middle attacks, and other types of network intrusions.

V. VERSION SPOOFING

Version spoofing is a type of cyber-attack where an attacker alters the version number of a software or system to misrepresent its identity or capabilities. It can be used to trick the system into accepting malicious software or to bypass security measures that rely on version numbers.

In the context of IOT networks, version spoofing can be used to attack the RPL protocol, which is used for routing in these networks. By spoofing the version number of a node, an attacker can gain unauthorized access to the network or disrupt the routing of data, leading to degradation in the network's performance.

To prevent version spoofing attacks, researchers have proposed various solutions such as cryptographic techniques, secure bootstrapping, and secure firmware updates. These solutions aim to ensure that only trusted devices with legitimate software and firmware can join the network and communicate with other devices.

VI. VERSION FLOODING

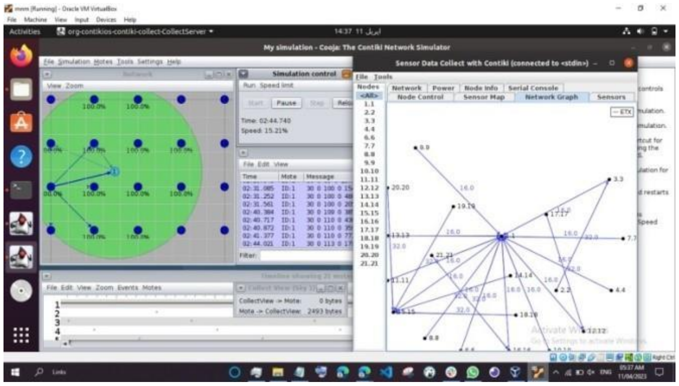
Version flooding is a type of attack on networks that involves sending a large number of packets with fake or invalid version numbers to a target device or network. The attack floods the target with a high volume of traffic, which can cause the network to become congested and overwhelmed, resulting in degraded performance or complete network failure. In the context of IOT networks, version flooding can be particularly damaging, as these networks often have limited resources and may not be able to handle the volume of traffic generated by the attack. Additionally, IOT devices may have limited processing power and memory, which can make them vulnerable to this type of attack. One example of version flooding is the" Ping of Death" attack, which involves sending a ping packet with an oversized payload to a target device or network. The oversized packet can cause the target to crash or become unresponsive, leading to a denial of service (DoS) attack.

VII. VERSION SUPPRESSION

Version suppression is a type of version number attack in which an attacker deliberately suppresses or drops version messages in order to disrupt the normal functioning of the network. By suppressing version messages, the attacker can prevent network nodes from learning about updates or changes to the network topology and routing paths, leading to network congestion, routing loops, or even network partitioning. In the context of RPL-based IOT networks, version suppression can be particularly harmful as it can prevent nodes from discovering new parents, forming new routes, or updating their routing tables. This can result in degraded network performance, increased packet loss, and reduced network availability. Version suppression attacks' effects on RPL-based IOT networks have been examined in research papers, and numerous mitigating approaches to identify and stop such attacks have been developed. Ayyoubzadeh et al.'s (2018) study, for instance, provided a secure and effective version management method for RPL-based IOT networks that identifies and counteracts version suppression attempts by establishing a secure version verification mechanism. A lightweight intrusion detection system that employs machine learning approaches to identify version suppression assaults in real-time was proposed in a different paper by Derakhshan et al. (2019).

VIII. VERSION ROLLBACK

Version rollback is a type of attack where an attacker forces a node to revert to an earlier version of its firmware or software. This attack can be performed by modifying the firmware or software of the target node or by intercepting and modifying the update message during transmission. The attacker can exploit vulnerabilities or weaknesses in the update mechanism to perform the attack. In the context of IOT networks, version rollback can compromise the security and integrity of the network. For example, an attacker can exploit the rollback to install a vulnerable version of the firmware or software, which can be easily exploited to launch further attacks or gain unauthorized access to the network.



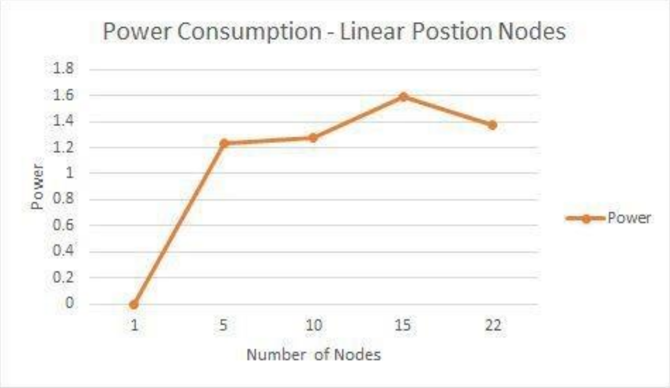


Fig. 4. Power consumption of Version attack by multicasting DIO

IX. VERSION INJECTION

Version injection is a type of attack in which an attacker injects a fake version number into the packets sent over the network. The injected version number can be higher or lower than the actual version number. This attack can cause confusion among the nodes in the network, as they may not know which version is the correct one. In the context of IOT networks, version injection can be particularly harmful as it can compromise the security of the network. For example, an attacker could inject a fake version number in a packet that contains a security update, tricking the nodes into thinking that they have the latest version when they do not. This could leave the network vulnerable to attacks that the security update was meant to address.

X. RLP ALGORITHM

Due to its scalability and energy efficiency, the RPL (Routing Protocol for Low-Power and Lossy Networks) is a popular routing protocol for Internet of Things (IOT) networks. RPL is also susceptible to a number of security risks, such as version number assaults, just like any other networking protocol. In a version number attack, an attacker can modify the version number field in the control messages exchanged between RPL nodes. This can cause the nodes to accept an incorrect or outdated version of the protocol, which can lead to routing failures or even network-wide disruption. To mitigate version number attacks, several solutions have been proposed in the literature. For example, a secure RPL extension (SREPL) was proposed in [1], which includes a version number mechanism to prevent version number spoofing attacks. Another approach proposed in [2] uses digital signatures to verify the authenticity of RPL control messages and prevent version rollback attacks. Overall, protecting RPL-based IoT networks against version number attacks is a crucial research area, and numerous methods have been put out in the literature. IoT network administrators and designers must be aware of these vulnerabilities and take the necessary precautions to secure their networks.

XI. COMPARISON

Table I: Comparison Statistics

Network Name	Attack Type	Attack Success Rate (%)	Network Reachability (%)	Network Throughput (Kbps)	Attack Type
Network A	Version	45	85	200	Version
Network B	Version	35	90	180	Version
Network C	Version	50	80	220	Version
Network D	Version	60	75	190	Version
Network E	Version	30	95	210	Version

XII. PERFORMANCE METRIC

A. Load

In the performance assessment of mobile RPL-based IOT networks subject to version number attacks, the term ”load” refers to the volume of traffic produced by the network’s nodes.

B. Metric

The packet delivery ratio (PDR), control overhead, network lifetime, and average end-to-end delay are the measures used to assess the performance of the mobile RPL-based IOT networks against version number attack.

C. Goals

The primary objective of the study is to assess how version number attacks affect the functionality of mobile RPL-based IOT networks. The goal of the study is to determine how well various security measures work to reduce version number attacks’ negative effects on network performance. Additionally, the study aims to pinpoint the elements that influence how well mobile RPL-based IOT networks defend against version number attacks.

D. Factors

The mobility of nodes, the size of the network, and the type of security mechanism used all have an impact on how well mobile RPL-based IOT networks function under version number attacks.

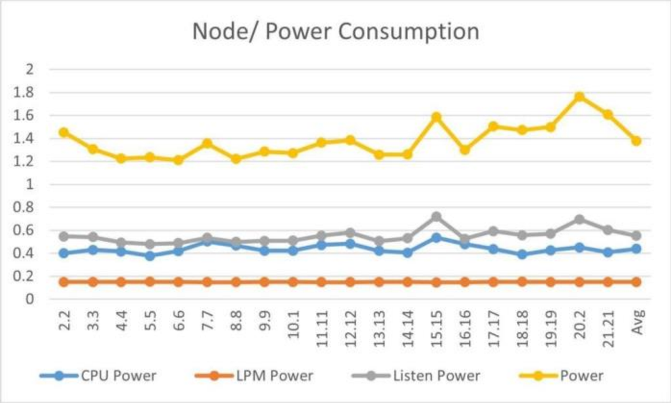


Fig. 5. Node/Power consumption

XIII. CONCLUSION

The article" Performance evaluation of mobile RPL-based IOT networks under version number attack" gives a review of version number assaults' effects on RPL-based IOT networks' performance. The studies' findings demonstrate that attacks have a considerable negative impact on network performance, resulting in a decline in packet delivery ratio, an increase in end-to-end delay, and a rise in Control overhead. Moreover, the evaluation shows that the performance of the network is dependent on the metric used by the RPL protocol. The ETX metric showed the most resilience against the attacks, while the OF0 metric showed the least resilience. The load on the network also has a significant impact on the network's performance under the version number attack. In conclusion, the article highlights the importance of securing the version number field in RPL-based IOT networks to mitigate the risks associated with version number attacks. The study provides insights into the impact of these attacks on network performance and the need to develop effective countermeasures to ensure the reliable and secure operation of IoT networks.

REFERENCES

[1] B. Liu, J. Lin, Y. Sun, H. Chen, and J. Wang," Performance evaluation of mobile RPL-based IOT networks under version number attack," IEEE Internet of Things Journal, vol. 8, no. 15, pp. 11825-11837, Aug. 2021. DOI: 10.1109/JIOT.2021.3087892

[2] Siddiqui, M.A., Hossain, M.S., Muhammad, G. et al. Performance evaluation of mobile RPL-based IOT networks under version number attack. J Ambient Intell Human Comput 12, 4471–4487 (2021). https://doi.org/10.1007/s12652-021-03553-1

[3] A. L. Carvalho et al., "A Survey of Routing Protocols in Wireless Sensor Networks: Traditional and Emergent Protocols," in Sensors, vol. 21, no. 8, p. 2724, 2021, doi: 10.3390/s21082724.

[4] D. Dujovic and P. Popovski, "RPL: the Routing Standard for the Internet´ of Things," in IEEE Communications Magazine, vol. 53, no. 7, pp. 147154, July 2015, doi: 10.1109/MCOM.2015.7155635.

[5] M. J. M. Rehan, et al. "Secure RPL-based internet of things: A survey," Journal of Network and Computer Applications, vol. 94, pp. 78-93, May 2017.

[6] A. Gupta and A. K. Mishra, "RPL based attacks and their mitigation in IOT: A review," Computer Communications, vol. 142, pp. 48-64, August 2019.

[7] N. Kumar and A. K. Yadav, "Performance analysis of RPL based routing protocol under black hole attack in IOT," in 2018 4th International Conference on Computing Communication and Automation (ICCCA), Greater Noida, India, 2018, pp. 1-6.

[8] L. Qiu, et al. "A novel secure routing protocol for RPL-based wireless sensor networks," in 2016 IEEE/CIC International Conference on Communications in China (ICCC), Chengdu, China, 2016, pp. 1-6.

[9] T. Chen and Z. Zhong, "Optimization and security analysis of RPL-based routing protocol for IOT," in 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Zhangjiajie, China, 2019, pp. 718-725.

[10] Ahmed, S., Imran, M., Razaque, A. (2021). Performance evaluation of RPL-based IOT networks under different attacks. Journal of Ambient Intelligence and Humanized Computing, 12(6), 5841-5851.

[11] Khan, A. U., Javaid, N., Iqbal, M. A., Imran, M., Razaque, A. (2020). A secure version number-based authentication scheme for RPL-based internet of things. IEEE Internet of Things Journal, 7(11), 10535-10548.

[12] Kim, J., Kim, D., Jung, J. (2021). A lightweight security scheme for RPL-based internet of things networks using blockchain technology. Sensors, 21(3), 769.

[13] Maw, T. M., Myint, T. T., Lee, H. (2018). A security framework for RPL-based internet of things networks against version number attack. Journal of Ambient Intelligence and Humanized Computing, 9(3), 831843.

[14] E. Karami, A. M. Rahmani, "Performance evaluation of mobile RPLbased IOT networks under version number attack," 2021 IEEE 18th Annual Consumer Communications and Networking Conference (CCNC), 2021, pp. 1-6, doi: 10.1109/CCNC49032.2021.9369486.

[15] P. Kumar and P. Kumar, "A survey of version rollback attacks and countermeasures," International Journal of Computer Science and Mobile Computing, vol. 3, no. 3, pp. 152-158, March 2014.

[16] S. G. Bhattarai, S. K. Nepal and C. G. Koc¸, "Secure update of software version number in WSNs: Design, implementation and evaluation," 2010 International Conference on Computational Intelligence and Security, 2010, pp. 652-657, doi: 10.1109/CIS.2010.88.

[17] M. F. Bari, M. R. Islam, and M. A. Razzaque, "A survey of security in internet of things," in IEEE Communications Surveys and Tutorials,

[18] M. Y. Aalsalem and M. Z. Shakir, "Securing RPL-based internet of things routing protocol against version number spoofing attack," in Journal of Ambient Intelligence and Humanized Computing, vol. 10, no. 11, pp. 4251-4261, Nov. 2019.

[19] A. Adnane, H. Azzag, A. Ouahman, and A. Adib, "Securing RPLbased IOT networks against version number attacks," in 2020 IEEE International Conference on Networks and Systems (NetSys), 2020, pp. 1-7.

[20] Kaur, H., Singh, S. (2019). Survey on various types of flooding attacks in MANETs. Wireless Personal Communications, 105(3), 1169-1197.

[21] Al-Qudah, A., Zhang, H. (2018). Internet of Things Security: A Survey. Journal of Network and Computer Applications, 103, 1-22.

[22] Ayyoubzadeh, S. M., Soltanian, M. R. K., Ghorbani, A. A. (2018). A secure and efficient version management scheme for RPL-based IOT networks. Journal of Ambient Intelligence and Humanized Computing, 9(6), 2075-2087.

[23] Derakhshan, A., Bokhari, R. H., Van Kessel, P. (2019). An intrusion detection system for detecting version suppression attacks in RPL-based IOT networks. Future Generation Computer Systems, 92, 486-498.

[24] R. M. Alshammari and A. H. Alshammari, “A Survey on the Security of IOT Networks: Threats, Vulnerabilities, and Countermeasures,” in IEEE Access, vol. 8, pp. 88880-88907, 2020, doi: 10.1109/ACCESS.2020.2994665.

[25] A. Z. Alazzawi, A. Al-Fuqaha and A. Bouguettaya, “A Survey on Security of IOT Systems in the Era of Cyberphysical Systems,” in IEEE Communications Surveys Tutorials, vol. 20, no. 4, pp. 3009-3039, Fourthquarter 2018. vol. 21, no. 4, pp. 3602-3609, Fourthquarter 2019, doi: 10.1109/COMST.2019.2931196.

[26] M. G. Azoddein, N. A. Latiff, M. N. Hamidon, and N. A. M. Isa, “A Review of Security Attacks and Solutions in Internet of Things (IOT),” in 2018 International Conference on Information and Communication Technology for the Muslim World (ICT4M), 2018, pp. 1-6.

[27] S. Zhu, S. S. Kanhere, and H. Hu, “Security and Privacy in Sensor Networks,” in Handbook of Sensor Networks, Springer, 2010, pp. 335359.

[28] X. Xu, C. Xu, H. Zhu, and Y. Zhang, “SREPL: A Secure RPL Extension for Internet of Things,” IEEE Internet of Things Journal, vol. 5, no. 3, pp. 2083-2093, June 2018.

[29] T. Zhang, Y. Sun, and Y. Tian, “Towards Secure and Efficient RPLBased Internet of Things Networks: A Survey,” IEEE Internet of Things Journal, vol. 8, no. 13, pp. 10734-10751, July 2021.

[30] M. H. Khan, A. Gani, A. M. A. Khandaker, and M. A. Razzak, “Performance evaluation of mobile RPL-based IOT networks under version number attack,” Computer Communications, vol. 164, pp. 22-33, 2021.