Communications on Applied Nonlinear Analysis
ISSN: 1074-133X
Vol 32 No. 9s (2025)

Isolating malicious nodes in the Internet of Things through a Trust-Based Mechanism

Zakiya Manzoor Khan[1], Harjit Singh[2]

[1]Department of Computer Science and Engineering, Lovely Professional University,Phagwara, Jalandhar, Punjab. zakiyamanzoorkhan@gmail.com

[2]Associate Professor and Assistant Dean– Department of Computer Science and Engineering, Lovely Professional University, Phagwara, Jalandhar, Punjab. harjit.14952@lpu.co.in

Article History:

Received: *11-11-2024*

Revised:*24-12-2024*

Accepted:*09-01-2025*

Abstract:

Introduction: IoT (Internet of Things) systems are open to attacks because of their resource-limited and ad hoc architecture. These systems support industrial and medical services and are used to manage massive amounts of data. IoT systems thus become vulnerable to a range of attackers, such as sporadic hackers, cybercriminals, hacktivists, and even governmental organizations. These hackers' main objective is to compromise IoT devices in order to obtain sensitive data, including credit card numbers, location information, bank account credentials, and health information. The version number attack is one serious danger; it is a malicious activity that negatively affects network performance. Malicious nodes launch this attack by overloading the network with hello packets, which causes a denial-of-service (DoS) condition. This study suggests a trust-based mechanism, in which each node is given a trust value determined by its activity, to solve this problem. The network isolates and labels as malicious the nodes with the lowest trust values. After the suggested scheme is put into practice in NS2, its effectiveness is assessed in terms of throughput, packet loss, delay, and energy usage.

Keywords*:* IoT, Trust Calculation, Version number, ICMP

1. Introduction

The growing interest in the Internet of Things has led to a widespread adoption of Low Power and Lossy Networks (IoT). Smart grids and home automation are just two examples of the many applications that are made possible by these networks. However, implementing conventional security measures can be challenging because of the constraints of the devices in these networks [1]. Many of these devices are vulnerable to both physical and listening intrusions because of their accessibility. Moreover, end users routinely ignore device security precautions like changing passwords, and a lot of vendors don't prioritize security in their products [2]. To address these problems, the Routing Protocol for Low-power and Lossy Networks (RPL) was developed by the Internet Engineering Task Force. RPL groups nodes into Destination Oriented Directed Acyclic Graphs (DODAGs) and optimizes network topology for specific goals, such as energy conservation, using metrics and constraints that are available to every device [3].

Each of the DODAGs that make up an RPL instance has a distinct objective function. RPL instances can run concurrently on networks. A node can participate in more than one DODAG if it is a part of different instances, but it can only join one DODAG within a single instance. Nodes are given a rank value, which always increases in the direction of the DODAG root, to

indicate where they are in relation to the root [4]. RPL includes two local repair mechanisms to avoid having to rebuild the entire DODAG in the event that a parent node disappears. The first one selects a different parent node, while the second one permits nodes to route temporarily through peers of the same rank. Moreover, RPL offers a global repair option that starts the DODAG reconstruction process from scratch. While these mechanisms provide flexibility to the network, there is a chance that malicious nodes could exploit these vulnerabilities to disrupt the network. One specific vulnerability that takes advantage of an RPL feature that is typically used to ensure an error-free and loop-free network topology is the "version number attack" [5]. A malicious node changes the version number associated with the network topology, necessitating a complete rebuild of the routing tree in order to counteract this attack. Because parent nodes include the version number in control messages, the standardized protocol lacks mechanisms to ensure the integrity of the advertised version number [6]. Increased network overhead, energy reserve depletion, communication channel availability problems, and even the creation of undesired routing loops in the network topology can result from a forced rebuild brought on by this attack [7]. Numerous studies have shown that these kinds of attacks are capable of seriously disrupting RPL networks, which emphasizes the urgent need to address these security issues.

1.1 Attacks with Version Numbers in RPL Networks.

There are many different types of attacks against the RPL protocol, but they fall into three main categories. The initial group consists of assaults aimed at exhausting network resources, such as power, memory, and energy. Because these attacks drastically shorten device lifetimes and, as a result, the lifespan of the RPL network, they are especially harmful to constrained networks [8]. Attacks directed against the topology of the RPL network fall into the second category. By isolating particular groups of RPL nodes from the network or causing suboptimal topologies in comparison to a typical network convergence process, these attacks impair the regular operation of the network [9]. Attacks on network traffic, such as eavesdropping and misappropriation attacks, fall under the third category. The first category includes version number attacks, which are a serious risk to an IoT network's endurance [10]. The global repair mechanism, which can be thought of as an essential part of the protocol's defense mechanism, is exploited by these attacks, which the attacker can carry out for very little money.

Under this mechanism, if the root node finds too many discrepancies in the network, it starts a global repair. In order to perform this repair, the Destination Oriented Directed Acyclic Graph (DODAG) must be rebuilt in its entirety by increasing the version number of DODAG, which is communicated through control messages known as DODAG Information Objects (DIO) [11]. Every receiving node verifies that the version number it currently has matches the one it obtained from its parent [12]. The node must reset trickle timers, ignore its current rank information, and start a new process to join the DODAG if the version number it received is higher. This global repair mechanism guarantees a topology free of loops, but it costs a lot. A node that has not updated to the new DODAG version is indicated by an older version that is advertised in DIO messages [13].

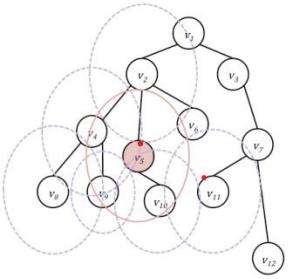

Fig. 1. A version number attack example. Plotting the initial malicious broadcast in red, the malicious node v5 launched an incremented version number that is automatically propagated by legitimate network nodes (broadcast by relay nodes plotted in purple).

As a result, other nodes ought not to select this kind of node as their preferred parent. Two versions of a DODAG are allowed to coexist during a global repair. Data packets from the old version can traverse the new version, but not the other way around, to avoid loops. When network convergence is not achieved during a global repair, the prior iteration of the DODAG ceases to be a legitimate DODAG, and loop-free network topologies can no longer be guaranteed [14].

Maintaining the integrity of the version number during its propagation through the Destination Oriented Directed Acyclic Graph (DODAG) in RPL is crucial to averting potential inconsistencies in the network. RPL does not, however, have a way to ensure that the version number supplied in received DODAG Information Object (DIO) messages is authentic [15]. The network may suffer if malicious nodes are able to change the version number in their own DIO messages due to this vulnerability. Nodes react to malicious DIO messages by updating their version, resetting their trickle timers, and broadcasting the new, manipulated version number to other nodes in the vicinity via DIO messages [16]. As shown in Figure 1, this malevolent behavior causes the unauthorized version number to spread throughout the network.

Such version number manipulation in DIO packets leads to loops in the network topology and needless reconstruction of the complete DODAG [17]. Loops are allowed to form because the network's topology is no longer acyclic due to the new version of the DODAG not being built from the root [18]. The availability of channels, data packet routing, and node energy resources can all be negatively impacted by these loops. For individual nodes, detecting this attack at the local level is difficult [19]. Uncertainty can arise from a malicious DIO packet that seems to be legitimate to a node coming from a parent node. A receiving node may perceive a packet originating from a child node as a network inconsistency [20]. Additionally, because nodes only know about their immediate neighbors, it is challenging to identify the source of the malicious DIO packets locally. Nodes must communicate with one another in order to determine the attack's origin, necessitating teamwork to track down the malicious activity's beginning [21].

2. LITERATURE REVIEW

Ray D., and others. (2023) created a novel method based on active probing and an Intrusion Detection System (IDS) based on the Discrete Event System (DES) for identifying rank and

version number attacks (VNA) and pinpointing the attacker's location [22]. After the inputs were centralized at the leaf levels, they were used in this system. The technique of intelligent probing was used to differentiate between the attacked and normal behavior. Additionally, the DES technique was used to model the attack and normal specifications and to develop a DES diagnoser that would trigger an alert upon the discovery of a malevolent mole. The system of the developed technique was exploited at the root node and it was shown to be more accurate and effective. As a result, this method was not trained and altered. A vast number of Internet of Things devices were used to mimic the developed method. The results of the experiment showed that the developed method had a 99 percent accuracy rate in identifying malicious nodes and produced fewer false positives (FPs) while operating with minimal energy consumption.

I. Alsukayti, S., et al. envisioned a simple and efficient algorithm for Version Number (VN) attack detection and mitigation in 2022 [23]. In order to incorporate a cooperative and distributed security technique into the protocol design, the RPL functionality was improved (CDRPL). The results of the simulation validated the security and scalability of the proposed algorithm to optimize the protocol's resilience against basic and complex VN attacks in various experimental configurations. The developed method provided a higher convergence rate in every attack attempt and swiftly and accurately detected the attacks. Additionally, this approach-maintained network stability, reduced energy consumption, improved Quality of Service (QoS), and managed traffic overhead during the occurrence of various VN attack scenarios. The outcomes showed that the generated method had worked effectively. Furthermore, it offered less communication overhead and didn't require any additional entities.

Osman M., et al. developed a lightweight method to identify Version Number Attacks (VNAs) called Machine Learning Model Based on Light Gradient Boosting Machine (ML-LGBM) in 2021 [24]. The creation of a massive dataset, a feature extraction method, the Light Gradient Boosting Machine (LGBM) algorithm, and maximizing metrics were the main priorities. The developed method was assessed using a variety of metrics. Experiments showed that the developed method produced results with accuracy of 99.6%, precision of 99.0%, F-score of 99.6%, true negative rate (TNR) of 99.3%, and false-positive rate (FPR) of 0.0093, in that order. Additionally, this method's execution time was 140.217 seconds, and its memory usage was up to 347,530 bytes, making it suitable for devices with limited resources.

M Sdot. Muzammal and associates. (2020) developed the SMTrust conceptual mechanism, which uses mobility-based trust parameters to secure the Internet of Things (IoT) routing protocol [25]. The primary goal of this mechanism was to protect against common RPL attacks, like Rank and Version Number Attacks (VNA). This mechanism was found to be scalable and dynamic when compared to traditional methods, and it had demonstrated good performance in detecting VNA attacks with a higher degree of accuracy. This mechanism was able to address the mobility parameters of base stations (BSs) and sensor nodes (SNs), in contrast to the conventional methods. As a result, this mechanism became applicable in a mobile Internet of things setting. The outcomes demonstrated the security of the developed mechanism following its integration into RPL and confirmed that it remained private, dependable, and accessible

across SNs throughout the routing process in Internet of Things networks.

A. A. Anitha along with others. In order to identify version number attacks (VNAs), (2021) created the Version Number Attack Detection System (VeNADet). This system verified, validated, and detected the attack in three stages [26]. The simulation indicated a relationship between the attack volume and the evaluation parameters. Because the system was localized in different locations, such as leaf node, intermediate node, or neighbor node placed at the root, it was successful in identifying the attacker. After receiving a DIO message, the node updated its VN and reported itself as malicious if certain conditions were met. As a result, the needless Version updates were reduced. To cut off the attacker from the Internet of Things network, the links were severed from the DODAG. The results demonstrated that the system's design provided an effective method of detecting version attacks with an accuracy of 94.4%.

Ze Z. An A. Almusaylim and associates. In order to identify rank and version number (VN) attacks, (2020) looked into the Secure RPL Routing Protocol (SRPL-RP) [27]. This protocol was put in place to identify, lessen, and isolate attacks on RPL networks. To find the attack, a comparative analysis of the rank approach was done. In order to mitigate the attacks, the threshold and attack status tables were used. They were also added to a blacklist table and alerts nodes, which helped isolate the attacks after excluding those nodes. This protocol used a variety of network topologies, and an analysis was carried out on various studies that took Standard RPL with Attacks, Sink-Based Intrusion Detection Systems (SBIDS), and RPL+Shield into consideration. The results showed that the protocol under investigation could improve the Packet Delivery Ratio (PDR) by up to 98.48 percent, the control message value by up to 991 packets/s, the average energy consumption by up to 1231.75 joules, and the accuracy of VN attack detection by up to 98.30 percent [28].

Rouissat M., et al. Among the dishonest Denial of Service attacks in Internet of Things networks, version number attack (VNA) is one that can be detected and mitigated by a decentralized, lightweight algorithm presented in 2023 [29]. The network's edge was the focus of this algorithm. The malicious node parent used this algorithm to send a DAO message alerting the sink node in the event of an unauthentic increased VN. The information was then distributed throughout the network to promote the malicious originator. The suggested algorithm was efficient and did not use any encryption techniques. It didn't require the deployment of an additional node to monitor the network, and its computation rate was low. The simulation results showed that the algorithm that was presented was robust in terms of latency, memory footprint, energy efficiency, and control overhead.

Rouissat, M. et coll., a distributed denial of service (DDoS) attack directed against RPL-based (Routing Protocol for Low Power and Lossy Networks) Internet of Things networks, in 2023 proposed a novel way for countering the version number attack (VNA) [30]. This attack was launched in order to increase control overhead through malevolent behavior and to directly impact network availability by imposing an impact on node resources related to processing and memory. This algorithm was implemented by every mote in order to recover the victim nodes and stop the forged VN from being transmitted over the network. Under Contiki OS, the Cooja tool was used to assess the suggested approach. The outcomes of the simulation demonstrated

the superiority of the proposed approach in terms of various parameters for optimizing the node resources in terms of memory and processing capacity [31]. Additionally, this method demonstrated a strong ability to reduce control overhead by up to 83 percent, energy consumption by up to 74 percent, and improve packet delivery ratio (PDR) by approximately 99-point six percent [32].

DotS. Ambarkar and associates. (2021) proposed a mutual authentication system that incorporated modifications to the traditional RPL protocol standard to offer strong defense against a variety of RPL attacks, including version number attack (VNA) [33]. This system might shield the network from harm and stop the dishonest node from joining it. The proposed system was compared to the conventional approaches. The recommended solution proved secure in an IoT network with few constraints and provided less overhead on the RPL network. When simulating the proposed system, the energy consumption and ETX parameters were taken into account. The results showed how effective the recommended system was at both preventing bogus nodes and improving network performance.

3. Research Methodology

This research work proposes a technique that can identify and remove malicious nodes from a network. Based on the monitor mode system and node rating, the suggested approach is designed. This work discusses the source and destination nodes that are placed in the network and creates the network deployment. The network's RREP (route request packet) flood is the source node's fault. The destination's neighboring nodes must use the route reply packets to respond to the source node. The optimal path between the source and the destination is chosen by the source node based on the number of hops and the sequence number. The recommended approach carries out several steps to separate the network node, which are as follows:

1. Based on the number of hops and sequence number, the optimal path is chosen between the source and the destination.

2. The established path will be tested to determine whether it can isolate the malicious nodes from the network. Through the network's source node, ICMP messages are sent to confirm the established path. After receiving ICMP messages, the nodes switch to monitor mode so they can observe the nodes next to them.

3. The nodes watch the neighboring nodes, and the nodes that are deemed malicious receive the lowest rating.

4. Malicious nodes are identified in the network as those with lower ratings. Nodes are given different colors based on their rating values, such as red, green, and yellow.

5. Every node has its location provided by the Delphi method, which also deploys the location of the node with the lowest rating to isolate it from the network.

4. Flow Chart

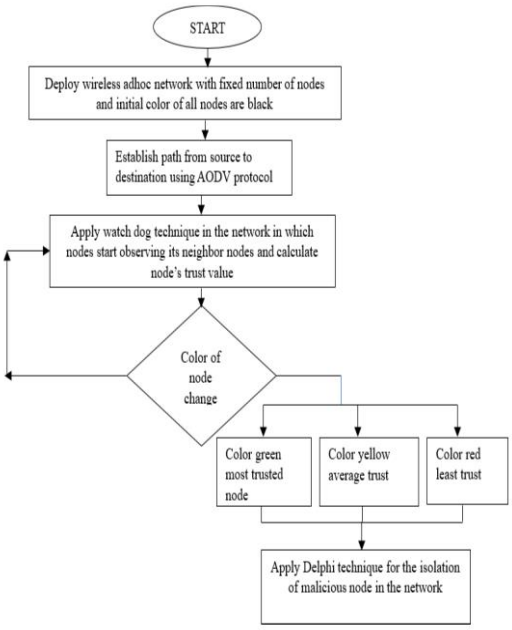

Figure 1. Proposed Flowchart

5. Result and Discussion

Since there is no central controller in a decentralized network like the internet of things, security is the main concern for the network. The attack's version number is what determines how the network performs in terms of different metrics. Table 1 describes the different simulation parameters that are taken into consideration.

Simulation Parameter	Value
Number of Nodes	38
Antenna Type	Omi-Directional
Area	800*800 meters
Queue Type	Priority Queue
Queue Size	50
Propagation Model	Two Ray

Table 1: Simulation Parameters

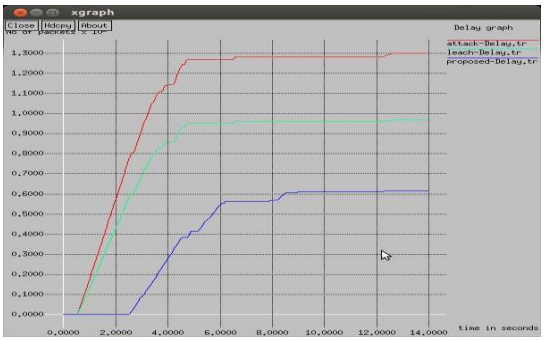

Figure 3: Delay Analysis

Figure 3 illustrates how the attack scenario's delay, the current scheme, and the suggested scheme are compared for performance analysis. Analysis shows that the network delay

increases steadily as an attack is initiated. Delay is minimized when the suggested methodology for malicious node detection is put into practice.

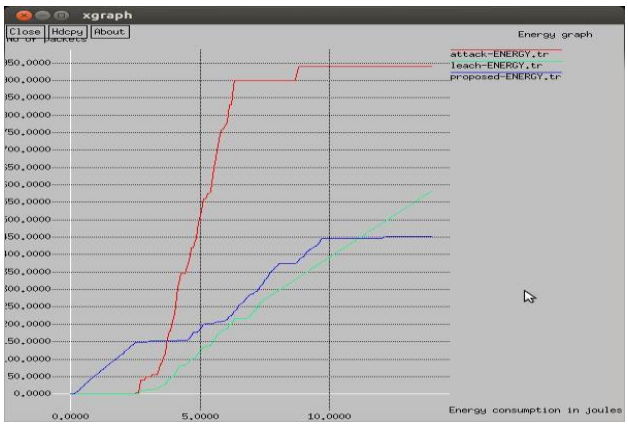

Fig 4: Energy Consumption Analysis

Figure 4 illustrates a comparison between the energy consumption of the proposed scheme, the attack scenario, and the current scheme. Energy consumption is analyzed to determine the lowest level at which the attack is isolated and a malicious node is found within the network.

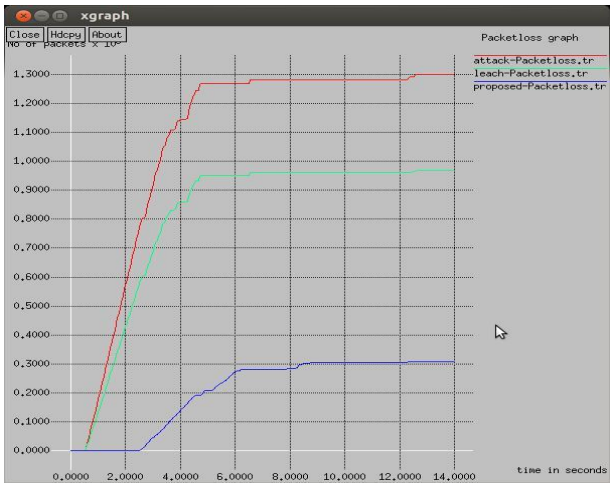

Fig 5: Packet loss Analysis

Figure 5 illustrates how the packet loss of the suggested scheme is contrasted with an attack scenario and with an existing scheme that is employed to identify malicious nodes. The suggested scheme has the least packet loss when compared to other schemes because the network has detected a hello flood attack. Malicious nodes flood the network with an infinite number of hello packets during the hello flood attack.

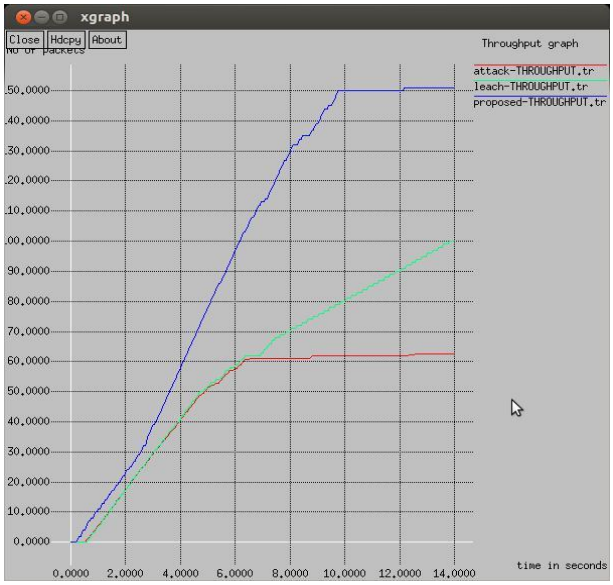

Fig 6: Throughput Analysis

Figure 6 illustrates how the throughput of the suggested scheme is compared to both the attack scenario and the current scheme. It is analyzed that throughput increases steadily once a malicious node is removed from the network.

6. Conclusion

A decentralized network such as the internet of things can be breached by malicious nodes, which can then initiate a range of active and passive attacks. The basis of this research project is the identification of hello flood attacks from IOT. In a version number attack, malicious nodes bombard the network with an endless stream of hello packets. An unending barrage of packets caused a denial-of-service condition on the network. This paper proposes a trust-based malicious node detection mechanism. Under the trust-based mechanism, each node in the network is assigned a trust value based on their activity. The nodes that are most trustworthy are shown as green, the nodes that are moderately trustworthy as yellow, and the nodes that are least trustworthy as red. The nodes that are highlighted in red will be recognized as malicious ones. The simulation is conducted using Version 2 of the network simulator, and the outcomes are

analyzed in terms of throughput, energy consumption, packet loss, and delay. The suggested method outperforms the existing one in every way when it comes to identifying malicious nodes.

References

[1] D. Airehrour, J. A. Gutierrez, S. K. Ray, “SecTrust-RPL: A secure trust-aware RPL routing protocol for Internet of Things”, Future Generation Computer Systems, 2018.

[2] Fatima-tuz-Zahra, NZ Jhanjhi, S. Nawaz Brohi, Nazir A. Malik, “Proposing a Rank and Wormhole Attack Detection Framework using Machine Learning”, 13th International Conference on Mathematics, Actuarial Science, Computer Science and Statistics (MACS), 2019.

[3] Zakiya Manzoor Khan, et al. (2023). Trust Based Mechanism for Isolation of Malicious Nodes in Internet of Things. International Journal on Recent and Innovation Trends in Computing and Communication, 11(10), 1689–1695. https://doi.org/10.17762/ijritcc.v11i10.8740

[4] Chandni, R. Kumar, “Trust Based Technique for the Mitigation of Version Number Attack in Internet of Things”, International Journal of Recent Technology and Engineering (IJRTE), Volume8 Issue3, 2019.
[5] P. Kaushik, “Dynamic Data Scaling Techniques for Streaming Machine Learning”, IJGASR, vol. 3, no. 1, pp. 1–12, Apr. 2024.
[6] M.V.R Jyothisree, S. Sreekanth, “Attacks in RPL and Detection Technique used for Internet of Things”, International Journal of Recent Technology and Engineering (IJRTE), Volume8, Issue1, 2019.
[7] A. Verma and V. Ranga, “Analysis of Routing Attacks on RPL based 6LoWPAN Networks”, International Journal of Grid and Soft Computing, Volume 11, Issue 8, pp. 43-56, 2018.
[8] P. Kaushik, R. Rathore, A. Kumar, Kanishka, G. Goshi, and P. Sharma, “Identifying Melanoma Skin Disease Using Convolutional Neural Net- work DenseNet-121,” 2024 IEEE International Conference on Inter-disciplinary Approaches in Technology and Management for Social Innovation (IATMSI). IEEE, Mar. 14, 2024.
[9] G. Vennila, Dr. D.Arivazhagan, Dr. R. Jayavadive, “Experimental Analysis Of RPL Routing Protocol In IOT”, International Journal of Scientific & Technology Research, Vol. 8, No. 10, 2019.
[10] R. Vaghela, Prof. Deepak Upadhyay, “A Survey on Routing Attacks in Internet of Things (IOT)”, International Research Journal of Engineering and Technology (IRJET), Vol. 07, no. 11, 2020.
[11] P. Kaushik, “Deep Learning Unveils Hidden Insights: Advancing Brain Tumor Diagnosis,” IJGASR, vol. 2, no. 2, pp. 01–22, Jun. 30, 2023.
[12] Syeda Mariam Muzammal, Raja Kumar Murugesan, et al., “SMTrust: Proposing Trust-Based Secure Routing Protocol for RPL Attacks for IoT Applications”, International Conference on Computational Intelligence (ICCI), 2020.
[13] Areej Althubaity, Tao Gong, Kim-Kwang Raymond, et al., “Specification-based Distributed Detection of Rank-related Attacks in RPL-based Resource-Constrained Real-Time Wireless Networks”, IEEE Conference on Industrial Cyberphysical Systems (ICPS), 2020.
[14] Aditya Tandon, Prakash Srivastava, “Trust-based Enhanced Secure Routing against Rank and Sybil Attacks in IoT”, Twelfth International Conference on Contemporary Computing (IC3), 2019.
[15] S. Kalyani, D. Vydeki, “Survey of Rank Attack Detection Algorithms in Internet of Things”, International Conference on Advances in Computing, Communications and Informatics (ICACCI), 2018.
[16] R. Rathore. (2022). A Study on Application of Stochastic Queuing Models for Control of Congestion and Crowding. International Journal for Global Academic & Scientific Research, 1(1), 1–6. https://doi.org/10.55938/ijgasr.v1i1.6
[17] W. Choukri, Hanane Lamaazi, N. Benamar, “RPL rank attack detection using Deep Learning”, International Conference on Innovation and Intelligence for Informatics, Computing and Technologies (3ICT), 2020.
[18] Kashif Naseer Qureshi, Shahid Saeed Rana, Gwanggil Jeon, “A novel and secure attacks detection framework for smart cities industrial internet of things”, Sustainable Cities and Society, 2020.
[19] Anthéa Mayzaud, Rémi Badonnel, Isabelle Chrisment, “A Distributed Monitoring Strategy for Detecting Version Number Attacks in RPL-Based Networks”, IEEE Transactions on Network and Service Management, 2017.
[20] P.S. Nandhini, B.M. Mehtre, “Intrusion Detection System Based RPL Attack Detection Techniques and Countermeasures in IoT: A Comparison”, International Conference on Communication and Electronics Systems (ICCES), 2019.
[21] R. Rathore, P. Kaushik, S. S. Sikarwar, H. Joshi, A. K. Mishra, and Y. Hudda, “Intelligent Transportation Systems Make Use of Fog and Edge Computing for Navigation,” 2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI). IEEE, Mar. 14, 2024.
[22] Mohammed Amine Boudouaia, Adda Ali-Pacha, et al., “Security Against Rank Attack in RPL Protocol”, IEEE Network, 2020.
[23] D. Ray, P. Bhale, S. Biswas, P. Mitra and S. Nandi, "A Novel Energy-Efficient Scheme for RPL Attacker Identification in IoT Networks Using Discrete Event Modeling," in IEEE Access, vol. 11, pp. 77267-77291,doi: 10.1109/ACCESS.2023.3296558, 2023.

[24] I. S. Alsukayti and A. Singh, "A Lightweight Scheme for Mitigating RPL Version Number Attacks in IoT Networks," in IEEE Access, vol. 10, pp. 111115-111133, doi: 10.1109/ACCESS.2022.3215460, 2022.

[25] P. Kaushik, S. P. S. Rathore, L. Sachdeva, M. Poonia, D. Singh, and L. Bir, "Intelligent transportation systems trusted user's security and privacy," 2024 IEEE International Conference on Interdisciplinary Approaches in Technology and Management for Social Innovation (IATMSI). IEEE, Mar. 14, 2024.

[26] M. Osman, F. M. Mokbal, "ML-LGBM: A Machine Learning Model Based on Light Gradient Boosting Machine for the Detection of Version Number Attacks in RPL-Based Networks," in IEEE Access, vol. 9, pp. 83654-83665, doi: 10.1109/ACCESS.2021.3087175, 2021.

[27] S. M. Muzammal, R. K. Murugesan, et al, "SMTrust: Proposing Trust-Based Secure Routing Protocol for RPL Attacks for IoT Applications," 2020 International Conference on Computational Intelligence (ICCI), Bandar Seri Iskandar, Malaysia, pp. 305-310, doi: 10.1109/ICCI51257.2020.9247818, 2020.

[28] A. A. Anitha and L. Arockiam, "VeNADet: Version Number Attack Detection for RPL based Internet of Things", Solid State Technology, vol. 64, no. 2, pp. :2225-2237, February 2021.

[29] Z. A. Almusaylim, N. Z. 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, pp. 12-20, doi: 10.3390/s20215997 , 2020.

[30] Kaushik, P. (2024). Dynamic Data Scaling Techniques for Streaming Machine Learning. International Journal for Global Academic & Scientific Research, 3(1), 1–12. https://doi.org/10.55938/ijgasr.v3i1.68

[31] M. Rouissat, M. Belkheir and A. Mokaddem, "Parent supervision lightweight solution against version number attacks for IoT networks", Research Square, vol. 2, no. 1, pp. 102-111, doi: 10.21203/rs.3.rs-2605250/v1 , 2023.

[32] M. Rouissat, M. Belkheir, H. S. A. Belkhira, S. B. Hacene, P. Lorenz and M. Bouziani, "A new lightweight decentralized mitigation solution against Version Number Attacks for IoT Networks", Journal of Universal Computer Science, vol. 29, no. 2, 118-151, doi: 10.3897/jucs.85506 , 2023.

[33] S. S. Ambarkar and N. Shekokar, "An Efficient Authentication Technique to Protect IoT Networks from Impact of RPL Attacks", International Journal of Engineering Trends and Technology, vol. 69, no. 10, pp. 137-145, doi:10.14445/22315381/IJETT-V69I10P217 , October, 2021.