International Journal on Recent and Innovation Trends in Computing and Communication
ISSN: 2321-8169 Volume: 11 Issue: 9
***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

Trust based Mechanism for Isolation of Malicious Nodes in Internet of Things

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

Abstract— The Internet of Things systems are prone to the attacks as they have ad-hoc and limited resource structure. IoT-based systems are utilized for managing a large volume of information and assist in services related to industrial and medical applications. Due to this, the IoT attains becomes a target for a multitude of attackers and adversaries namely occasional hackers, cybercriminals, hacktivists, government, etc. The major goal of potential attackers is to steal the sensitive information such as credit card numbers, location data, credential of financial account and information related to health, by hacking the Internet of Things devices. The version number attack is one of malicious activity of IoT which affect network performance to great extend. The version number attack is triggered by the malicious nodes which can flood unlimited hello packets in the network. The hello flood attack raised situation of denial of service in the network. The trust based mechanism is proposed in this research work in which trust value is assigned to each node based on their activities. The node which is least trusted will be marked as malicious and get isolated from the network. The proposed scheme is implemented in NS2 and results are analyzed in terms of throughput, packetloss, energy consumption and delay.

Keywords- IoT, Trust Calculation, Version number, ICMP.

I. INTRODUCTION

The growing interest in the Internet of Things (IoT) has led to the widespread deployment of Low Power and Lossy Networks. These networks enable various applications, from smart grids to home automation. However, the devices in these networks have limitations, making traditional security measures challenging to implement [1]. Many of these devices are easily accessible, making them vulnerable to physical and eavesdropping attacks. Additionally, end users often neglect device security, such as changing passwords, and many vendors don't prioritize security in their products. To address these challenges, the Internet Engineering Task Force's Routing Protocol for Low-power and Lossy Networks (RPL) was developed. RPL organizes nodes into Destination Oriented Directed Acyclic Graphs (DODAGs) and optimizes network topology for specific goals, such as energy conservation [2], by means of metrics and constraints accessible to each device.

An RPL instance consists of a collection of DODAGs, each having a specific objective function. Networks can run multiple RPL instances simultaneously. A node is allowed to join a single DODAG within one instance but can be part of multiple DODAGs if they belong to distinct instances. Nodes are assigned a rank value that signifies their position relative to the DODAG root, always increasing towards the root [3]. To prevent the need for rebuilding the entire DODAG when a parent node vanishes, RPL incorporates two local repair mechanisms. The first one permits nodes to temporarily route through peers of the same rank, while the second involves selecting an alternative parent node. Additionally, RPL offers a global repair option to completely reconstruct the DODAG. While these mechanisms provide network flexibility, they also introduce potential vulnerabilities that malicious nodes can exploit to disrupt the network. One specific vulnerability is the "version number attack," which takes advantage of a RPL feature typically used to ensure a loop-free and error-free network topology [4]. In this attack, a malicious node manipulates the version number associated with the network topology, compelling a complete rebuilding of the routing tree. As the version number is included in control messages by parent nodes, the standardized protocol lacks mechanisms to ensure the integrity of the advertised version number. The consequences of a forced rebuild due to this attack can include increased network overhead, depletion of energy reserves, availability issues with the communication channels, and even the formation of undesirable routing loops in the network topology [5]. Several research works have demonstrated that such attacks can significantly disrupt RPL networks, underscoring the imperative need to address these security concerns.

***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

1.1 Version Number Attacks in RPL Networks.

The RPL protocol faces a wide range of attacks, which can be categorized into three primary groups. The first category encompasses attacks focused on depleting network resources, including energy, memory, and power. These attacks are particularly detrimental to constrained networks because they significantly reduce device lifetimes and [6], consequently, the lifespan of the RPL network. The second category involves attacks targeting the RPL network's topology. These attacks disrupt the network's normal operation, leading to suboptimal topologies compared to a typical network convergence process or isolating specific sets of RPL nodes from the network. The third category includes attacks on network traffic, such as eavesdropping or misappropriation attacks. Version number attacks fall within the first category and pose a significant threat to the longevity of an IoT network [7]. These attacks can be executed at a minimal cost by the attacker and exploit the global repair mechanism, which can be viewed as a critical component of the protocol's immune system.

In this mechanism, the root node initiates a global repair when it detects too many inconsistencies within the network. This repair involves rebuilding the entire Destination Oriented Directed Acyclic Graph (DODAG) by incrementing the DODAG's version number, which is conveyed in control messages called DODAG Information Objects (DIO). Each receiving node compares its current version number with the one received from its parent [8]. If the received version number is higher, the node must disregard its current rank information, reset trickle timers, and initiate a new procedure to join the DODAG. While this global repair mechanism ensures a loop-free topology, it comes at a significant cost. An older version advertised in DIO messages indicates that a node has not transitioned to the new DODAG version [9].

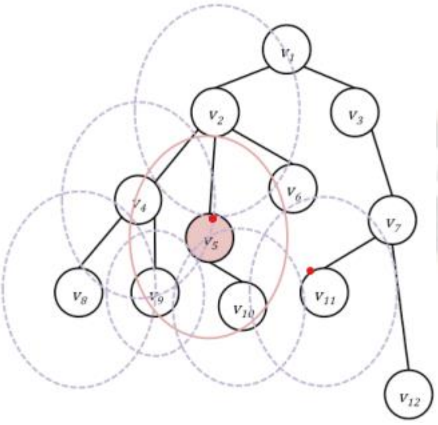


Fig. 1. Example of a version number attack. The incremented version number launched by the malicious node v5 (initial malicious broadcast plotted in red) is automatically propagated by legitimate network nodes (broadcast by relay nodes plotted in purple).

Consequently, other nodes should not choose such a node as their preferred parent. During a global repair, two versions of a DODAG can coexist. To prevent loops, data packets from the old version are allowed to traverse the new version but not vice versa. In the absence of network convergence during a global repair, the previous version of the DODAG stops functioning as a valid DODAG, and the assurance of loop-free network topologies cannot be maintained [10].

To prevent potential inconsistencies in the network, it's essential to maintain the integrity of the version number as it propagates through the Destination Oriented Directed Acyclic Graph (DODAG) in RPL. However, RPL lacks a mechanism to guarantee the authenticity of the version number provided in received DODAG Information Object (DIO) messages [11]. This vulnerability allows malicious nodes to alter the version number in their own DIO messages, which can have detrimental effects on the network. Upon receiving a malicious DIO message with a new version number, nodes respond by resetting their trickle timers, updating their version, and subsequently broadcasting this manipulated version number through their DIO messages to nearby nodes [12]. This malicious behaviour leads to the dissemination of the unauthorized version number throughout the network, as depicted in Figure 1. Such manipulation of the version number within DIO packets results in both unnecessary reconstruction of the entire DODAG and the creation of loops in the network topology [13]. Since the new version of the DODAG is not constructed from the root, the network's topology is no longer acyclic, permitting loops to form. These loops can adversely affect node energy resources, data packet routing, and channel availability. Detecting this attack at the local level is challenging for individual nodes [14]. A malicious DIO packet originating from a parent node may appear legitimate to a node, creating uncertainty. When such a packet comes from a child node, the receiving node might interpret it as an inconsistency in the network [15]. Additionally, pinpointing the source of the malicious DIO packets locally is difficult, as nodes only have knowledge of their immediate neighbours. To identify the source of the attack, nodes must communicate with each other, requiring a collaborative effort to trace the origin of the malicious activity [16]

II. LITERATURE REVIEW

D. Ray, et al. (2023) developed an innovative technique for detecting rank and version number attack (VNA) and recognizing the attacker location on the basis of active probing and Discrete Event System (DES) based Intrusion Detection System (IDS) [17]. The inputs were employed in this system after their centralization at the leaf levels. An intelligent probing method was adopted for distinguishing the normal behavior from the attacked ones. Moreover, DES approach was employed for modelling the normal and attack specifications, and creating a DES diagnoser in order to create an alert after detecting a malevolent mote. The developed technique was proved accurate and more effective and its system was exploited at root node. Thus, this technique was not modified and trained. An enormous amount of IoT devices was applied to simulate the developed technique. The experimental outcomes indicated that the developed technique was worked energy-efficiently and offered lower false positives (FPs) and accuracy of 99% to detect intrusions and recognize the malicious nodes.

I. S. Alsukayti, et al. (2022) projected a lightweight and effectual algorithm to detect and mitigate Version Number (VN) attacks [18]. The RPL functionality was enhanced for integrating a collaborative and distributed security method into the protocol design (CDRPL). The simulation outcomes confirmed the security and scalability of the projected algorithm to maximize the resiliency of the protocol against simple and composite VN assaults in diverse experimental setups. The generated method detected the attacks quickly and accurately, and offered higher convergence rate in any attack attempt. Moreover, this method resulted in keeping the network stable, controlling traffic overhead, enhancing Quality of Service (QoS), and mitigating energy usage during the occurrence of diverse VN attack scenarios. The results indicated that the generated method had performed well. Moreover, it had not required any extra entity, and offered lower communication overhead.

M. Osman, et al. (2021) devised a lightweight technique known as Machine Learning Model Based on Light Gradient Boosting Machine (ML-LGBM) to detect Version Number Attacks (VNAs) [19]. The major emphasis was on generating an enormous sized dataset, a feature extraction technique and a Light Gradient Boosting Machine (LGBM) algorithm, and optimizing the maximum metrics. Diverse metrics were utilized for evaluating the devised technique. According to experiments, the devised technique yielded an accuracy of 99.6%, precision of 99%, F-score of 99.6%, true negative rate (TNR) of 99.3% and false-positive rate (FPR) of 0.0093, respectively. Furthermore, the execution time of this technique had consumed 140.217 seconds and memory resource up to 347,530 bytes that offered suitability for resource-restricted devices.

S. M. Muzammal, et al. (2020) formulated a conceptual mechanism known as SMTrust in order to secure the routing protocol in Internet of Things (IoT) relied on the mobility-based trust parameters [20]. This mechanism was focused on defending against popular RPL assaults, such as Rank, Version Number attacks (VNA), etc. This mechanism had performed well to detect VNA attacks at higher accuracy and it was found scalable and dynamic in comparison with the traditional methods. Unlike the traditional methods, this mechanism was capable of tackling mobility parameters of sensor nodes (SNs) and Base stations (BSs). Hence, this mechanism attained applicability for mobile IoT environment. The results exhibited the security of the formulated mechanism after its embedding in RPL and ensured that this mechanism was confidential, reliable, and available among SNs during routing process in IoT networks.

A. A. Anitha, et al. (2021) designed a Version Number Attack Detection System (VeNADet) to detect version number attack (VNA). This system had three stages in which the attack was verified, validated and detected [21]. According to simulation, there was an association amid the evaluation parameters and amount of assaulter. This system was effective for detecting the attacker due to its localization in dissimilar locations such as leaf node, intermediate node or neighbor node were placed at the root. The node receiving a DIO message led to update its VN in case of satisfying certain circumstances and declared it as a malicious node. It resulted in alleviating the redundant Version updates. The links were disconnected from the DODAG to isolate the attacker from the IoT network. The findings confirmed that the designed system offered an accuracy of 94.4% for detecting version attacks in an efficient way.

Z. A. Almusaylim, et al. (2020) investigated a Secure RPL Routing Protocol (SRPL-RP) to detect rank and version number (VN) attacks [22]. This protocol was implemented for detecting, mitigating, and isolating the assaults in RPL networks. A comparative analysis was conducted on the rank approach to detect the attack. The threshold and attack status tables were employed for mitigating the attacks and further inserted in a blacklist table and alerts nodes for isolating the attacks after skipping those nodes. Various network topologies were employed in this protocol and an analysis was conducted on diverse studies considering Standard RPL with Attacks, Sink-Based Intrusion Detection Systems (SBIDS), and RPL+Shield. The outcomes revealed that the investigated protocol was effective for enhancing the Packet Delivery Ratio (PDR) up to 98.48%, a control message value up to 991 packets/s, an average energy utilization upto 1231.75 joules and accuracy up to 98.30% for detecting VN attacks.

M. Rouissat, et al. (2023) presented a lightweight and decentralized algorithm for detecting and mitigating version number attack (VNA) among the deceitful Denial of Service attacks in IoT networks [23]. This algorithm emphasized on the edge portion of the network. In case of an unauthentic incremented VN, an alert was sent to the sink node with a DAO message through the malevolent node parent, and this algorithm led to disseminate this information over the overall network for advertising the malicious originator. The presented algorithm worked effectively and no encryption algorithm was employed in it. Its computation rate was lightweight and no extra node was deployed to monitor the network. The simulations results depicted that the presented algorithm was robust concerning control overhead, energy efficiency, latency, and memory footrpint.

M. Rouissat, et al. (2023) projected a novel method for mitigating the version number attack (VNA), that was a distributed denial of service (DDoS) attack and launched at RPL-based (Routing Protocol for Low Power and Lossy Networks) IoTs networks [24]. This attack was activated for maximizing the control overhead via the malicious behavior and imposing impact on the resources of nodes in accordance with processing and memory to affect the availability of network in a direct way. Every mote deployed this algorithm for halting the transmission of a forged VN over the network and recovering the victim nodes. The Cooja tool was executed under Contiki OS for evaluating the projected method. The simulation results indicated the supremacy of the projected method with respect to different parameters to optimize the node resources concerning processing and memory usage. Furthermore, this technique was robust for mitigating the control overhead up to 83% and the energy utilization up to 74% and enhancing the packet delivery ratio (PDR) around 99.6%.

S.S.Ambarkar et al. (2021) suggested a mutual authentication system in which the traditional standard of RPL protocol was modified for providing a robust resistance against diverse RPL attacks such as version number attack (VNA) [25]. This system had potential for preventing the dishonest node from joining the network, and protecting the network. The comparison of the suggested system was done with the traditional methods. The suggested system had offered lower overhead on the RPL network and proved secured in low constraint IoT network. The energy consumption and ETX parameters were considered for simulating the suggested system. The outcomes demonstrated that the suggested system was resilient for blocking the unauthentic nodes as well as enhancing the network performance.

III. RESEARCH METHODOLOGY

This research work suggests a method that is capable of detect and isolated malicious nodes from the network. The suggested method is planned on the basis of the monitor mode system and node rating. This work makes the deployment of the network and discusses the source node and destination nodes which placed in the network. The source node is responsible of flooding RREP (route request packets) in the network. The adjacent nodes of the destination have to reply to the source node using the route reply packets. The source node is utilized to select the best path amid source and destination depending upon the hop count and sequence number. The suggested method executes diverse stages in order to isolate the node in the network, which are defined as:

1. The selection of best path is done amid source to destination based on the hop count and sequence number.
2. The established path will be tested for isolating the malicious nodes from the network. The established path is tested by transmitting the ICMP messages in the network through the source node. The nodes receive ICMP messages and move to the monitor mode for watching its adjacent nodes.
3. The adjacent nodes are watched by the nodes, the nodes that are found malicious give least rating.
4. The nodes having lower rating in the network are detected as the malicious nodes. Different colors such as red, green and yellow are assigned to nodes in accordance with their rating values.
5. The Delphi method is utilized to provide location to every node and it makes the deployment of location of node having least rating to isolate it from the network

IV. FLOW CHART

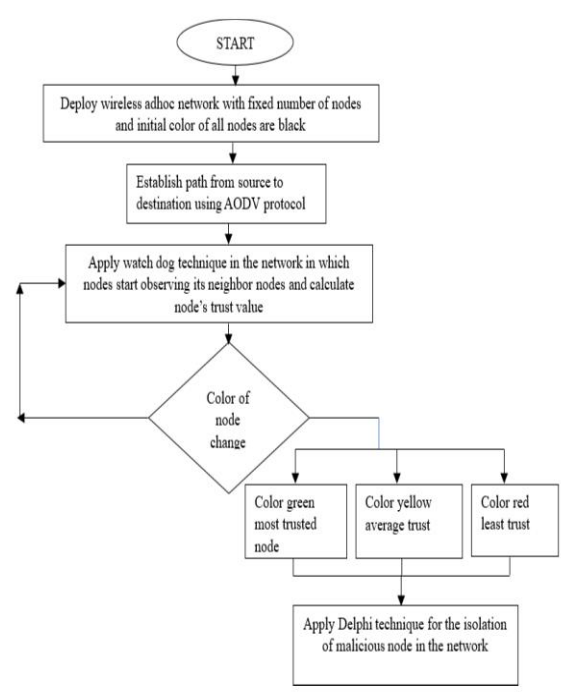
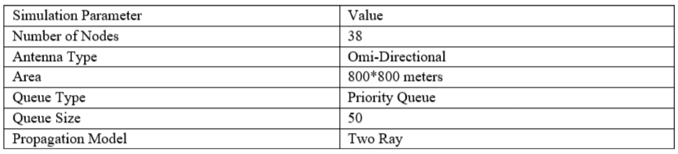

START
Deploy wireless adhoc network with fixed number of nodes and initial color of all nodes are black
Establish path from source to destination using AODV protocol
Apply watch dog technique in the network in which nodes start observing its neighbor nodes and calculate node's trust value
Color of node change
Color green most trusted node
Color yellow average trust
Color red least trust
Apply Delphi technique for the isolation of malicious node in the network

Figure 1. Proposed Flowchart

V. RESULT AND DISCUSSION

The internet of things is the decentralized type of network in which no central controller is present due to which security is the major issue of the network. The version number is the attack which can affect the network performance in terms of various parameters. The various simulation parameters are considered which are described in table 1.



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

Article Received: *25 July 2023* ***Revised:*** *12 September 2023* ***Accepted:*** *30 September 2023*

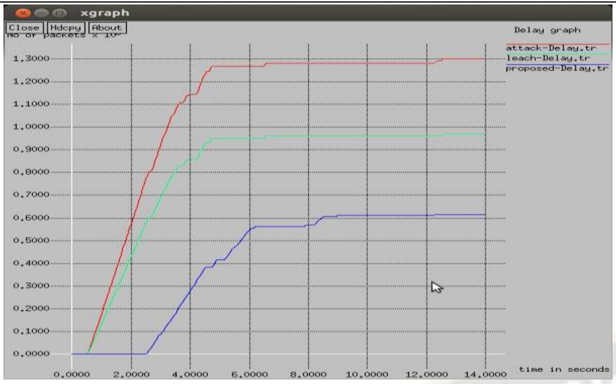


Figure 3: Delay Analysis

As shown in figure 3,the delay in the attack scenario, existing scheme and proposed scheme is compared for the performance analysis. It is analyzed that when attack is triggered in the network delay is increased at the steady rate. When the proposed methodology is implemented for the detection of malicious node delay is reduced at its least level.

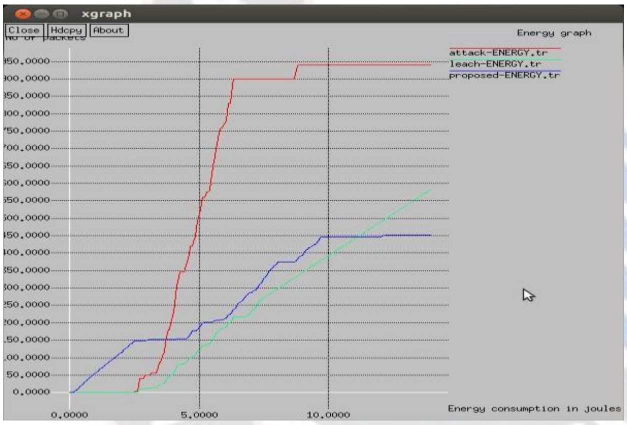


Fig 4: Energy Consumption Analysis

As shown in figure 4, the energy consumption of proposed scheme is compared with the attack scenario and existing scheme. It is analyzed that when the attack is isolated and malicious node is detected from the network energy consumption is reduced to least level.

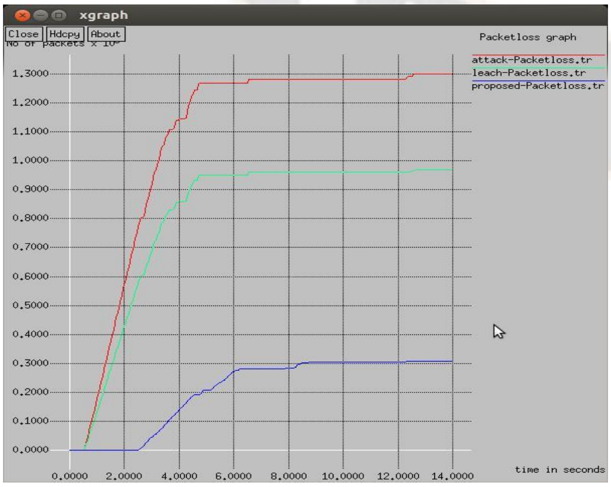


Fig 5: Packet loss Analysis

As shown in figure 5, the packet loss of proposed scheme is compared with attack scenario and also with existing scheme which is used for the detection of malicious node. The packet loss of proposed scheme is least as compared to other schemes because hello flood attack is detected from the network. In the hello flood attack malicious node flood the network with unlimited number of hello packets.

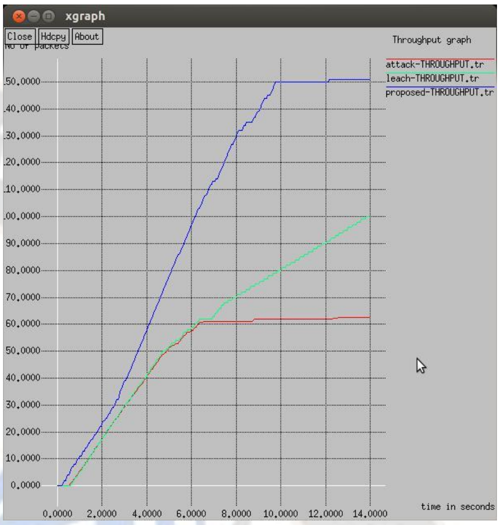


Fig 6: Throughput Analysis

As shown in figure 6, throughput of proposed scheme is compared with existing scheme and also with attack scenario. It is analyzed that when the malicious node is detected from the network then throughput is raised at steady rate.

CONCLUSION

The internet of things the decentralized type of network in which malicious nodes enter the network and trigger various type of active and passive attacks. This research work is based on the detection of hello flood attack from IOT. In the version number attack malicious node flood unlimited number of hello packets in the network. Due to flooding of unlimited number of packets it raised situation of denial of service in the network. The trust based mechanism is proposed in this paper for the detection of malicious nodes. In the trust based mechanism trust value is assigned to each node in the network based on their activities. The node which maximum trusted is marked with green color, medium level trusted node is marked with yellow color and least trusted node will be marked as red color. The nodes which are marked as red will be detected as the malicious nodes. The simulation is conducted in network simulator version 2 and results are analyzed in terms of delay, energy consumption, packet loss and throughput. The proposed scheme performs well in terms of all parameters as compared to existing scheme for the detection of malicious nodes.

***Article Received:** 25 July 2023 **Revised:** 12 September 2023 **Accepted:** 30 September 2023*

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] 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.

[4] 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.

[5] 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.

[6] 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.

[7] 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.

[8] 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.

[9] 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.

[10] Aditya Tandon, Prakash Srivastava, "Trust-based Enhanced Secure Routing against Rank and Sybil Attacks in IoT", Twelfth International Conference on Contemporary Computing (IC3), 2019.

[11] 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.

[12] 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.

[13] 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.

[14]] 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.

[15] 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.

[16] Mohammed Amine Boudouaia, Adda Ali-Pacha, et al., "Security Against Rank Attack in RPL Protocol", IEEE Network, 2020.

[17] 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.

[18] 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.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.