DETECTION OF HATCHETMAN ATTACK IN LOW POWER AND LOSSY NETWORKS

Amardeep Goyal[1], Dinesh Kumar[2]

[1]*Research Scholar, Associate Professor, CSE Department*

Guru Gobind Singh College of Engineering and Technology, Guru Kashi University, Talwandi Sabo, Bathinda, India

Abstract: The devices in the Low power and Lossy networks have limited resources. Routing Protocol for these networks suffer from various attacks out of which Hatchetman is one of them. In this attack, the malicious node modifies the DAO-ACO packet with address of fictitious destination node. This attack leads to consumption of energy resources and degrades the network's performance. This paper proposes detection scheme for these attacks which require the coordination of the neighboring nodes to validate the piggybacked source address. The performance of the proposed scheme was analyzed based on remaining energy, throughput and packet delivery ratio. The scheme showed improvement against the network under the attack.

Keywords: LLNs, RPL, Hatchetman attack, DAO-ACK, fictitious destination, piggybacking

I. INTRODUCTION

The Low Power and Lossy Networks (LLNs) is a special class of the IoT where elements of the network are resource-constrained (i.e., limited processing, storage, communication and power sources) and the environment is lossy [1]. The IETF and the IEEE proposed several standards to connect such networks to the Internet and allow various applications to be supported efficiently. The set of protocols are called as the standardized protocol stack [2].

Routing Protocol for Low power and Lossy Networks (RPL), is the de facto IoT routing protocol for communication. On initiation, a RPL protocol creates a tree like topology called Directed Acyclic Graph (DAG) and every sensor node operating in a RPL network selects a parent node which acts like a packet gateway for that node. Information regarding the topology of RPL is maintained as a graph-like structure called the Destination Oriented Directed Acyclic Graph (DODAG). The DODAG consists of paths from the sender nodes to the sink node. During routing, every node maintains its rank relative to its position in the DODAG tree, and every DODAG is populated with parent information. A security design weakness in the IETF RPL standard is the lack of specification of how the authentication and secure network connection among sensor devices running security critical missions is defined. This exposes such devices to attacks. In fact, studies [3, 4] have shown the RPL protocol to be vulnerable to several routing attacks including: Route Falsification, Byzantine, Rank, Routing Information Replay, Sybil, Selective Forwarding, Sinkhole, Blackhole, Greyhole and Version Number attacks.

Section II of this paper presents review of existing techniques that focus on security of RPL networks. Section III presents detection scheme for Hatchetman attack. Results have been shown in

Section IV and finally the paper has been concluded in last section.

II. LITERATURE REVIEW

In this paper [5], the authors investigate a new type of DoS attack, called *hatchetman attack*, in promptly emerging RPL-based LLNs. In hatchetman attack, the malicious node manipulates the source route header of the received packets, and then generates and sends a large number of invalid packets with error route to legitimate nodes, which cause the legitimate nodes to drop the received packets and reply an excessive number of Error messages back to the DODAG root. As a result, a great number of packets are dropped by legitimate nodes and excessive Error messages exhaust the communication bandwidth and node energy, which lead to a denial of service in RPL-based LLNs. They conduct extensive simulation experiments for performance evaluation of hatchetman attack and comparison with jamming attack and original RPL without adversary. The simulation results indicate that the hatchetman attack is an extremely severe attack in RPL-based LLNs.

This paper [6] considered the Rank Inconsistency Attack (RInA), which is illegitimately change the rank value and makes the network vulnerable. The proposed architecture E2V has three phases such as rank calculation, substantiation and malicious node elimination. The ultimate aim of E2V method is to detect and mitigate the RInA attack which includes sinkhole, selective forwarding and blackhole attacks. This system also identifies rank inconsistency based on the energy of each node. Hence, this approach enhances the secure routing in RPL based Internet of Things.

This paper [7] presents two lightweight mitigation techniques for RPL Version Number Attacks (VNA) which affect the performance of IPv6-connected Low Power and Lossy Networks (LLNs) detrimentally. By means of the proposed techniques, the delay caused by the attacker can be shortened up to 87%, the average power consumption can be reduced up to 63%, the control message overhead can be lowered up to 71% and the data packets delivery ratio can be increased up to 86%. The proposed techniques, while allowing the ordinary RPL operation, trade off the mitigation performance against the resource overheads and thus allow network administrators to choose the right scheme for their RPL network.

In this paper [8], the authors present a novel detection method for malicious packet dropping attacks against RPL-based networks. The proposed method is based on the anomaly intrusion detection system and detects malicious packet dropping in the presence of normal packet losses. They evaluate the performance of the method on Contiki's network simulator, Cooja. The evaluation results show that the method has good performance in detecting malicious packet dropping attacks. In every case, the successful detection rate is greater than 94% and the false alarm rate is less than 3%.

This paper [9] proposed a detection technique for rank attack based on the machine learning approach called MLTKNN, based on K-nearest neighbor algorithm. The proposed technique was simulated in the Cooja simulation with 30 motes and calculated

the true positive rate and false positive rate of the proposed detection mechanism. Finally proved that, the performance of the proposed technique was efficient in terms of the delay, packet delivery rate and in detection of the rank attack.

In this paper [10], the authors propose a misbehavior-aware detection scheme, called MAD, against energy depletion attack in RPLbased LLNs, where a malicious node intentionally generates and sends a large number of packets to legitimate node to excessively consume the energy resource of intermediate nodes located along the forwarding path, and finally makes the resource-constrained network suffer from denial of service. In the MAD, each node maintains a count of the number of received packets from its child node within a specific time window, and then compares the count with a dynamically calculated threshold to detect potential energy depletion attack. They conduct extensive simulation experiments for performance evaluation and comparison with the original RPL with and without adversary, respectively. The simulation results show that the proposed scheme is a viable approach against energy depletion attack in RPL-based LLNs.

In this paper [11], the authors investigate the effects and challenges of using RPL's security mechanisms under common routing attacks. First, a comparison of RPL's performance, with and without its security mechanisms, under three routing attacks (Blackhole, Selective Forward, and Neighbor attacks) is conducted using several metrics (e.g., average data packet delivery rate, average data packet delay, average power consumption... etc.) Based on the observations from this comparison, they came with few suggestions that could reduce the effects of such attacks, without having added security mechanisms for RPL.

This paper [12] attempts to identify intrusions aimed to disrupt the Routing Protocol for Low-Power and Lossy Networks (RPL). In order to improve the security within 6LoWPAN networks, the authors extend SVELTE, an intrusion detection system for the Internet of Things, with an intrusion detection module that uses the ETX (Expected Transmissions) metric. In RPL, ETX is a link reliability metric and monitoring the ETX value can prevent an intruder from actively engaging 6LoWPAN nodes in malicious activities. They also propose geographic hints to identify malicious nodes that conduct attacks against ETX-based networks. They implement these extensions in the Contiki OS and evaluate them using the Cooja simulator.

III PROPOSED SCHEME

In the proposed work, the first focus is given on the selection mechanism of the route to the sink node. Our detection scheme requires the cooperation of the nearest neighbors of the nodes (that are in the path to the sink node) to detect the manipulated piggybacked source route.

To have the nearest neighbors, the DODAG root will create two disjoint paths to the sink node. First path will be the one having maximum value of RSSI. The second path will be the one having second maximum value of RSSI. When two paths to the sink node are created, the DODAG will send DAO message over both the paths to the sink node. These messages will contain piggybacked source

route of two paths i.e. the information of second path will be piggybacked over the first path and vice-versa.

Under the attack, when the invalid packet reaches the legitimate node that is one-hop prior to the fictitious destination, the receiving node will cross-verify the information about the path from the nearest neighbor in the second path.

The receiving node will send verification packet to the nearest neighbor in the second path. This verification packet will contain the piggybacked address of the received source route (manipulated by the malicious node). Since the nodes in the second path have original information (not manipulated by the attacker node), the nearest node can verify the piggybacked source route of the verification packet.

If any abnormality is found, the node in the second path will confirm that predecessor node has manipulated the route address. It will inform the same to the DODGA root node and to the node (which sent the verification packet). DODAG root will also inform about the malicious node to the nodes in the first path. Then, it can send data to the sink node over the second path.

IV. RESULTS

The proposed detection scheme was aimed at making the network secure againt Hatchetman attack. The authors in the existing scheme [5] had only described this attack without giving any solution to detect it. The scenario for the attack and the detection scheme was implemented and analyzed in network simulator 2.35. The network's performance was analyzed based on packet delivery ratio, throughput and remaining energy of the network.

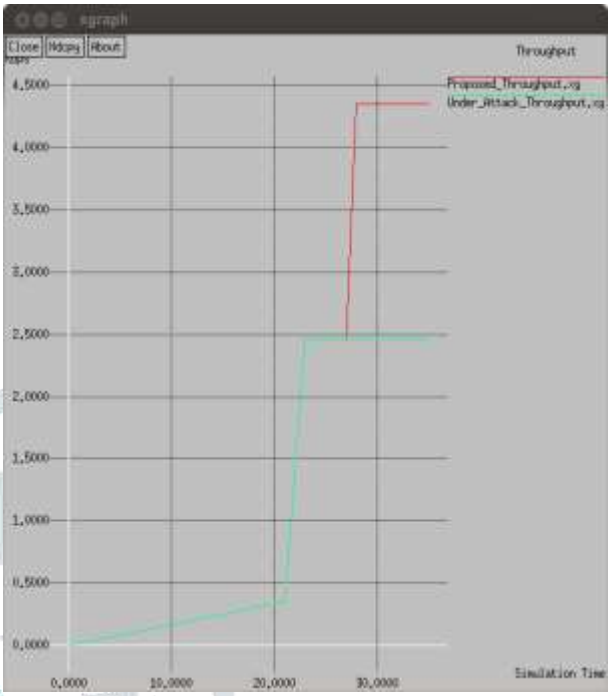

Figure 4.1: Throughput Comparison

The above graph shows the comparison of the throughput under attack and with detection scheme. The value of throughput for the proposed detection scheme was 4.3 Kbps and under the attack was 2.5 Kbps.

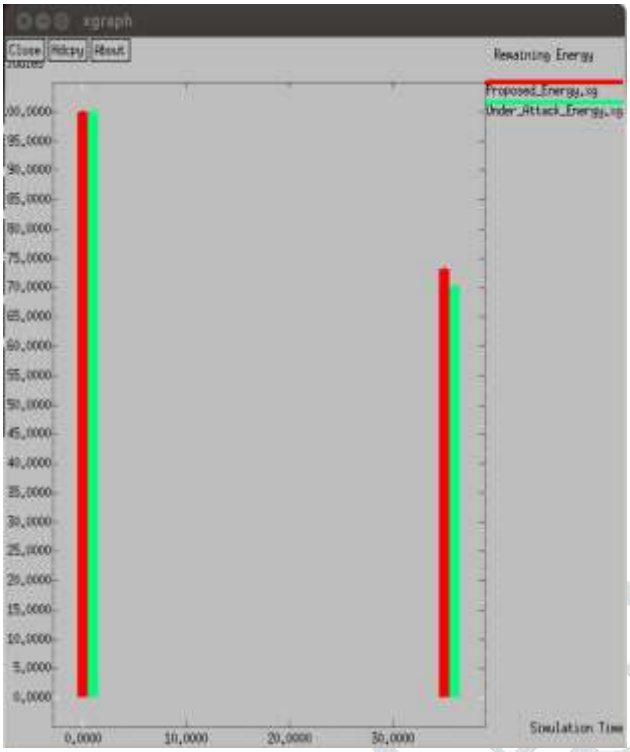

Figure 4.2: Remaining energy Comparison

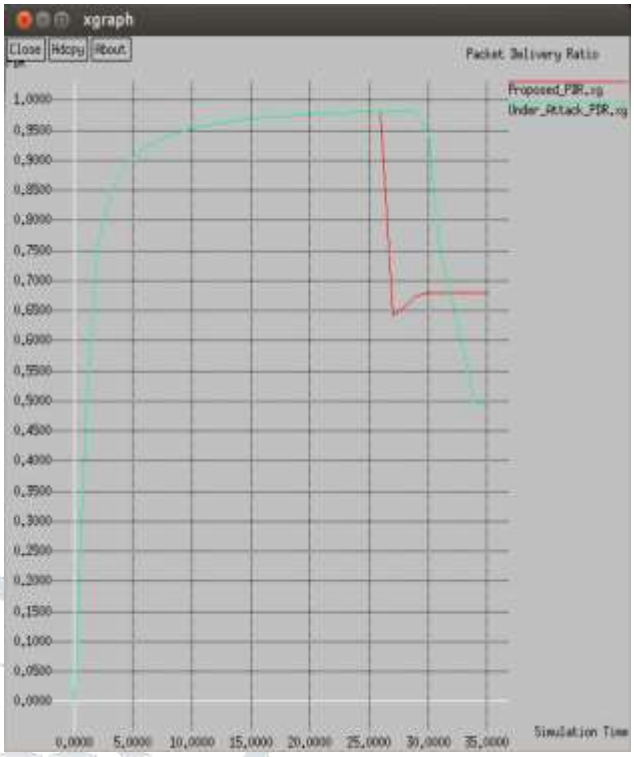

Figure 4.3: PDR Comparison

The above graphs shows the comparison of the remaining energy of the network under attack and with detection scheme. Initially the nodes have energy of the 100 Joules and at the end of simulation the value of remaining energy for the proposed detection scheme was 73.18 Joules and under the attack was 70 Joules.

The above graphs shows the comparison of the packet delivery ratio under attack and with detection scheme. The value of PDR for the proposed detection scheme was 68.07 percent and under the attack was 49.46 percent.

Parameter\Scheme	Under Attack	Detection Scheme
PDR	49.46 %	68.07 %
Remaining Energy	70 Joules	73.18 Joules
Throughput	2.5 Kbps	4.3 Kbps

Table 4.1: Results Comparison

V. CONCLUSION

This work was aimed at making the lossy network more secure against Hatchetman attack. The proposed detection scheme worked on multi path scenario and ensures that malicious node is detected by the cooperation of the nodes mutually. The value

of PDR was less under the attack because legitimate nodes send so many route error messages to the DODAG root node upon receiving non-existent destination address. This creates packet drops in the network. The detection of the malicious node with the proposed scheme ensures higher value of packet delivery ratio which also augments the throughput of the network. Again, the increased sending of route error packets leads to more energy consumption of the nodes which reduces the network lifetime under the attack. Therefore, the better values of three parameters helps us to conclude that the proposed scheme has successfully detected the attack and improved the performance of the network.

This work considers that single malicious node is present in the network. In future, collaborative Hatchetman attack can be considered in the network.

References

1. T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, R. Alexander, RPL: IPv6 Routing Protocol for Low Power and Lossy Networks, RFC 6550 (Proposed Standard) (Mar. 2012).

2. M. Palattella, N. Accettura, X. Vilajosana, T. Watteyne, L. Grieco, G. Boggia, M. Dohler, Standardized Protocol Stack for the Internet of (Important) Things, IEEE Communications Surveys Tutorials 15 (3) (2013) 1389–1406.

3. L. Wallgren, S. Raza, and T. Voigt, "Routing Attacks and Countermeasures in the RPL-Based Internet of Things," International Journal of Distributed Sensor Networks, vol. 2013, p. 11, 2013.

4. T. Tsao, R. Alexander, M. Dohler, V. Daza, A. Lozano, and M. Richardson, "A Security Threat Analysis for the Routing Protocol for Low-power and lossy networks (RPLs)," Internet Engineering Task Force (IETF) 2015.

5. Cong Pu, Tianyi Song, “Hatchetman Attack: A Denial of Service Attack Against Routing in Low Power and Lossy Networks”, International Conference on Cyber Security and Cloud Computing (CSCloud), IEEE, 2018.

6. R Stephen, L Arockiam, “E2V: Techniques for Detecting and Mitigating Rank Inconsistency Attack (RInA) in RPL based Internet of Things”, Second National Conference on Computational Intelligence (NCCI 2018).

7. Ahmet Arış, Sıddıka Berna, Örs Sema, F. Oktuğ, “New lightweight mitigation techniques for RPL version number attacks”, Ad Hoc Networks, Volume 85, 15 March 2019, Pages 81-91.

8. Sooyeon Shin, Kyounghoon Kim, Taekyoung Kwon, “Detection of malicious packet dropping attacks in RPL-based internet of things”, International Journal of Ad Hoc and Ubiquitous Computing, List of Issues, Volume 31, Issue 2, June 2019.

9. Vikram Neerugatti, A. Rama Mohan Reddy, “Machine Learning Based Technique for Detection of Rank Attack in RPL based Internet of Things Networks”, International Journal of Innovative Technology and Exploring Engineering (IJITEE), Volume-8 Issue-9S3, July 2019.

10. Cong Pu, Bryan Groves, "Energy Depletion Attack in Low Power and Lossy Networks: Analysis and Defenses", 2019 2nd International Conference on Data Intelligence and Security (ICDIS).

11. Ahmed Raoof, Ashraf Matrawy, Chung-Horng Lung, "Secure Routing in IoT: Evaluation of RPL's Secure Mode under Attacks", arXiv:1905.10314v1 [cs.CR] 24 May 2019.

12. Dharmini Shreenivas, Shahid Raza, Thiemo Voigt, "Intrusion Detection in the RPL-connected 6LoWPAN Networks", IoTPTS '17 Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security, Pages 31-38, April 2017.