A REVIEW OF ROUTING ATTACKS IN LOW POWER LOSSY NETWORKS

Amardeep Goyal, Dr. Dinesh Kumar
Research Scholar
Guru Kashi University

Abstract: Low power and Lossy Networks (LLNs) are made up of many embedded devices with limited power, memory, and processing resources. They are interconnected by a variety of links, such as IEEE 802.15.4, Bluetooth, Low Power WiFi, wired or other low power PLC (Powerline Communication) links. The Routing protocols for these networks have security issues. This paper describes the review of various attacks in LLNs with special reference to Hatchetman attack. This attack in lossy networks happens when malicious node changes the contents of the DAO-ACK packet. It adds the address of the non-existent destination in the piggybacked source route. When the uplink node receives the packet, it finds non-existent address of the node. Now, the node starts dropping all the received packets in the network. This decreases the network throughput, causes more energy consumption and less packet delivery rate.

Keywords: LLNs, RPL, Hatchetman attack, DAO-ACK, packet delivery rate

I. INTRODUCTION

The Internet-of-Things (IoT) has become a new focus for both industry and academia involving information and communication technologies (ICTs), and it is predicted that there would be almost 50 billion devices connected with each other through IoT by 2020 [1]. The concept of IoT can be traced back to the pioneering work done by Kevin Ashton in 1999 and it is initially linked to the new idea of using radio frequency identification in supply chains. Soon after, this term became popular and is well known as a new ICT where the Internet is connected to the physical world via ubiquitous wireless sensor networks (WSNs) [2]. The embedded devices in these networks have met some kind of constraints with limited power, memory, and processing resources, WSNs which is also called Low power and Lossy Networks (LLNs) consisting of an enormous number of embedded devices [3]. A sensing node has some constraints and limited resources such as energy resources, processing capability, memory size, limited radio range and minimal human intervention moreover it operates in unstable environments[4].In order to cope with those challenges, a number of breakthrough solutions have been developed, for example, efficient channel hopping in IEEE 802.15.4e TSCH [5], emerging IPv6 protocol stack for connected devices [6] and improved bandwidth of mobile transmission. Routing, particular in large scale networks, is always challenging for resource constrained sensor devices. The IETF Routing Over Low-power and Lossy networks (ROLL) working group has been focusing on routing protocol design and is committed to standardize the IPv6 routing protocol for Low-power and Lossy Networks (LLN). RFC6550 [7], first proposed by ROLL group of IETF in the form of draft to define Routing Protocol over Low Power and Lossy Networks (RPL), serves as a milestone in solving routing problems in LLNs. RPL suffers security issues from various attacks.

This paper presents the RPL in the next section with the review of existing techniques presented in section III that have proposed as security solution to various attacks in RPLs. Finally the paper has been concluded in last section.

II.RPL: Routing Protocol over Low Power and Lossy Networks

Low power and Lossy Networks (LLNs) are WSNs in which routers and nodes are highly resource constrained in terms of processing capability, battery and memory size, and their interconnects links are unstable with high loss rates, low data rates, and low packet delivery rates. In addition, they have different traffic patterns: point to point (P2P), point to multipoint (P2MP) or multipoint to point (MP2P) [8]. These networks may potentially involve thousands of nodes. Since IoT emergence, Routing in LLNs is one of the key challenges.

The ROLL working group conducted a detailed analysis and evaluations on the existing routing protocols[9] that led ROLL to found these protocols failed in satisfying the requirements of LLNs, obviously, the traditional IP routing protocols are not able to satisfy the requirements of multipoint-to-point application in WSNs[10], therefore the ROLL WG argued that the IoT technologies to transition to IPv6, thus it aimed to provide IPv6 routing architectural framework for IoT's application scenarios.

The RPL is one of an infrastructure protocols[11], it is a distance-vector and a source routing protocol that is designed on top of several link layer mechanisms including IEEE 802.15.4 PHY and media access control (MAC) layers [7]. RPL supports the different three patterns of traffic flow [4]: point-to-point(P2P) between nodes, point-to-multipoint (P2MP) for configuration purpose and multipoint-to-point (MP2P) for the data collection process. As stated in [7], the principle of RPL is to organize the WSN as a Direct Acyclic Graph (DAG) rooted at the sink node and to minimize the cost (i.e. shortest paths) to reach the sink from any node in the WSN using an objective function.

2.1 RPL components (characteristics)

A. Destination Oriented Directed Acyclic Graph (DODAG). In the context of network routing, the collection of nodes (vertices) and links (edges) shape a Directed Acyclic Graph (DAG). The principle of DAG, it is not possible for cycle path from node X back to the same node, RPL organizes the WSN topology into a Destination-Oriented Directed Acyclic Graphs (DODAGs), actually, DODAG represent the core of RPL and rooted at a single destination (i.e. sink node) that has no outgoing edges as shown in Figure1. In RPL, a DODAG is determined by the link costs and node properties which are combined for path costs computation. This information may include energy resources, throughput, latency, hop count, and reliability. In other words, RPL aims to minimize the costs of any path (from the source node to the sink node) by using an objective function[12]. There are four identifiers used by RPL protocol to maintain and define its topology. A single DODAG is uniquely identified in the network by the combination of RPLInstanceID and DODAGID.

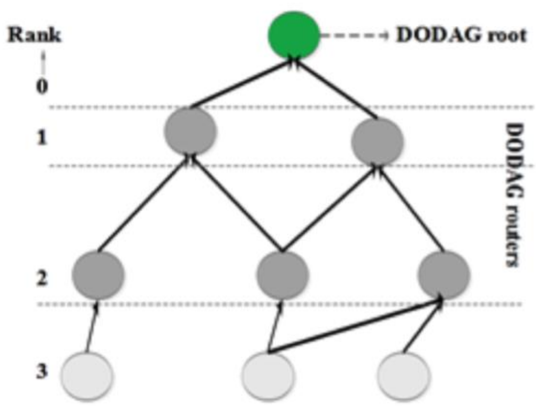

Figure 1: DODAG graph [13]

B. RPL's Control Massages. For the purpose of maintaining the routing topology and updating routing information [11], five types of control messages are used by RPL:

• DODAG Information Object (DIO): a DIO message carries important information such as an RPL Instance, configuration parameters and a DODAG parent set to maintain or rebuild the DODAG.

• DODAG Information Solicitation (DIS): a node which wants to join in DAG uses this message to solicit a DIO from RPL node.

• Destination Advertisement Object (DAO): a DAO message is used to transfer destination information upward along the DODAG to the sink node. In other words, it is used to announce the distance to the sink.

• Destination Advertisement Object Acknowledgement (DAO-ACK): a unicast packet is sent by a DAO recipient as a response to a unicast DAO message.

• Consistency Check (CC): it is a secured RPL message.

III. LITERATURE REVIEW

In this paper [14], the authorsinvestigate 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 thereceived packets, and then generates and sends a large number ofinvalid packets with error route to legitimate nodes, which causethe legitimate nodes to drop the received packets and reply anexcessive number of Error messages back to the DODAG root.As a result, a great number of packets are dropped by legitimatenodes and excessive Error messages exhaust the communicationbandwidth and node energy, which lead to a denial of service inRPL-based LLNs. We conduct extensive simulation experimentsfor performance evaluation of hatchetman attack and comparisonwith jamming attack and original RPL without adversary. Thesimulation results indicate that the hatchetman attack is anextremely severe attack in RPL-based LLNs.

The authorsin [15] have proposed a scheme to detect and mitigate this attack based on two techniques using Area Border Router and Sensing Aware Nodes. The proposed scheme monitors the signal strength of nodes, if distance found greater than default distance attack is detected. Both techniques act as backup of each other such that if one method fails other will detect the attack. This scheme doesn't require excessive power or specialized hardware equipment which is quite useful in resource constrained environment.

In this paper [16], the authors introduce a new rank attack in RPL networks that modifies Objective Function (OF) along with rank value. The OF is used by RPL nodes to select forwarding nodes based on application defined routing metric e. g., expected transmission count, residual energy etc. The proposed rank attack is more distractive in nature because the attacking node can easily force its neighboring nodes to route their data through the attacking node. Comprehensive simulation analysis has shown that the proposed rank attack can be used to introduce false routing path for decreasing network throughput and increasing latency of communication.

The authors in [17] propose a secure parent node selection scheme in the IPv6 Routing Protocol for Low-power and Lossy networks (RPL) so that each child node can select a legitimate node as its parent. In the proposed scheme, each node chooses a parent after excluding too good candidate if multiple parent candidates exist. The scheme utilizes the fact that an attacking node claims falsely a lower rank than that of legitimate nodes. Simulation results show that the proposed scheme reduces the total number of child nodes attached to attacking nodes.

The authorsin [18] propose a low false alarm attackers detection in the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) by considering timing inconstancy between rank measurements. In the proposed scheme, each node sends the latest rank broadcasted to neighbor nodes instead of its current rank to a sink so as to avoid the rank mismatch due to timing inconstancy. They also introduce the timestamp for reporting rank measurements to decrease the false alarm due to packet loss. Simulation results show that the proposed scheme reduces the false alarm rate.

In this paper [19], the authors propose a dynamic threshold mechanism, called DTM, to mitigate DAO inconsistency attack in RPL-based LLNs, where a malicious node intentionally drops the received data packet and replies the forwardingerrorpackettocausetheparentnodetodiscardvalid downward routes in the routing table. In the DTM, each parent node dynamically adjusts the threshold of accepting forwarding error packets within a time period based on the number of receivedforwardingerrorpacketsaswellastheestimatednormal forwarding error rate to counter DAO inconsistency attack. Simulationresults indicatethat the proposed scheme can provide higher packet delivery ratio but lower energy consumption compared to the fixed threshold scheme.

In this paper [20], the authors propose a heuristic-based detection scheme, called HED, against the suppression attack in MPL-based LLNs, where a malicious node multicasts a series of spoof data messages with continuous sequence numbers to prevent normal nodes from accepting valid data messages and cause them to delete cached data messages. In the HED, each node maintains an increment rate of the minimum sequence number in the Seed Set to detect the potential malicious node by comparing the recent increment of sequence numbers with the heuristically calculated increment threshold of sequence numbers. They evaluate the proposed scheme through extensive simulation experiments using OMNeT++ and compare its performance with original MPL with and without adversary, respectively. The simulation results show high detection rate and packet reception rate but low false detection rate, and indicate that the proposed scheme is a potentially viable approach against the suppression attack in MPL-based LLNs.

The proposed technique in [21] consists of a local decision and a global verification process. First, each node observes the communication behavior of its neighboring nodes by overhearing packets transmitted by its neighbors and attempts to identify suspicious nodes based on their behavior. In the second process, if a node identifies a suspicious node, then it verifies whether the suspicious node is a black hole. The authors demonstrate that the proposed approach increases packet delivery rate significantly and detects black hole attack effectively.

In this paper [22] the authors stud the performance of IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) under packet drop attacks. They consider an external jamming attacker who can selectively interfere with traffic around a targeted router. They show that the RPL implementation in Contiki OS allows such an attacker to continuously drop packets forwarded via the targeted router without triggering any rerouting, even when link-layer security mechanisms are in place. To counter such attacks, they design and analyze additional measures that can be built on RPL. In particular, it is shown that adding measures at the targeted router is more effective than doing so at affected children nodes. They also evaluate the performance of our enhanced RPL using Cooja, the Contiki network simulator. The results show that the proposed measures have the potential to significantly reduce the fraction of packets being dropped without affecting RPL's performance when there is no attack.

IV. CONCLUSION

The Low Poer Lossy networks have very dense deployment scenarios. RPL is used to construct the routes from the nodes to the root node. This paper has presented secure routing techniques against various attacks. Hatchetman attack is one new kind of attack that uses the comprised node to alter the address of the DAO-ACK packet. This attack causes packet drops in the network and energy drainage by sending large amount of compromised packets. Its defense mechanism has not been worked upon in literature. In future, we can work on securing the RPL networks against such kind of attacks.

References

1. D. Evans, "The internet of things: How the next evolution of the internet is changingeverything," CISCO white paper, Volume 1, pp. 1–11.

2. C. Alcaraz, P. Najera, J. Lopez, and R. Roman, "Wireless sensor networks and the internet of things: Do we need a complete integration?" Proceedings International Workshop on the Security of the Internet of Things (SecIoT'10), Tokyo, Nov 2010.

3.https://datatracker.ietf.org/wg/roll/charter/

4.Sheng, Z., Yang, S., Yu, Y., Vasilakos, A.V., McCann, J.A., and Leung, K.K.: 'A survey on the ietf protocol suite for the internet of things: Standards, challenges, and opportunities', IEEE Wireless Communications, 2013, 20, (6), pp. 91-98

5. A. Paventhan, D. D. B, H. Krishna, N. Pahuja, M. F. Khan, and A. Jain, "Experimental evaluation of ietf 6tisch in the context of smart grid," Proceedings IEEE 2nd World Forum on Internet of Things (WF-IoT), Milan, Dec 2015, pp. 530–535.

6. G. Montenegro, C. Schumacher, and N. Kushalnagar, "IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs): Overview, Assumptions, Problem Statement, and Goals," RFC 4919, August 2007.

7. T. Winter, "RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," RFC 6550, March 2012.

8.Vučinić, M., Tourancheau, B., Duda, A., "Performance comparison of the RPL and LOADng routing protocols in a home automation scenario", IEEE, pp. 1974-1979, 2013.

9. Levis, P., Tavakoli, A., Dawson-Haggerty, S., "Overview of existing routing protocols for low power and lossy networks", Internet Engineering Task Force, Internet-Draft draftietf-roll-protocols-survey07, 2009.

10.Tripathi, J., de Oliveira, J.C., Vasseur, J.-P., "A performance evaluation study of RPL: Routing protocol for low power and lossy networks', IEEE, pp. 1-6, 2016.

11. Al-Fuqaha, A., Guizani, M., Mohammadi, M., Aledhari, M., Ayyash, M., "Internet of things: A survey on enabling technologies, protocols, and applications", IEEE Communications Surveys & Tutorials, 2015, 17, (4), pp. 2347-2376.

12. Wang, J., Li, H., "Researching and Hardware Implementation of RPL Routing Protocol Based on the Contiki Operating System", International Journal of Future Computer and Communication, 2014, 3, (6), pp. 411.

13. EmranAljarrah, MuneerBaniYassein, ShadiAljawarneh, "Routing Protocol of Low-Power and Lossy Network: Survey and Open Issues", International Conference on Engineering & MIS, IEEE, November 2016.

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

15. Muhammad Saad Ahsan, Muhammad Nasir, MumtazBhutta, MoazamMaqsood, "Wormhole attack detection in routing protocol for low power lossy networks", International Conference on Information and Communication Technologies, IEEE, March 2018.

16. Abdul Rehman, Meer Muhammad Khan,M. Ali Lodhi, Faisal Bashir Hussain, "Rank attack using objective function in RPL for low power and lossy networks", International Conference on Industrial Informatics and Computer Systems, IEEE, May 2016.

17. Kenji Iuchi, Matsunaga Takumi, Kentaroh Toyoda, I. Sasase, "Secure Parent Node Selection Scheme in Route Construction to Exclude Attacking Nodes from RPL Network", IEICE Communications Express, Vol.4, No.11, 340–345, November 2015.

18. Matsunaga Takumi, Kentaroh Toyoda, I. Sasase, “Low false alarm attackersdetection in RPL byconsidering timinginconstancy betweenthe rank measurements”, IEICE Communications Express, Vol.4, No.2, 44–49, February 2015.

19. Cong Pu, “Mitigating DAO inconsistency attack in RPL-based low power and lossy networks”, 8th Annual Computing and Communication Workshop and Conference, IEEE, February 2018.

20. Pu, C., Zhou, X., “Suppression Attack against Multicast Protocol in Low Power and LossyNetworks: Analysis and Defenses”,Sensors 2018, 18, 3236.

21. Ahmed, FirozKo, Young-Bae, “Mitigation of black hole attacks in Routing Protocol for Low Power and Lossy Networks”, Security and Communication Networks, Volume 9, no.18, December 2016.

22. Binbin Chen, Yuan Li, and Daisuke Mashima, “Analysis and Enhancement of RPL under Packet Drop Attacks”, 10th International Conference on Communication Systems & Networks, IEEE, April 2018.