IDS TO DETECT AND PREVENT LOW POWER LOSSY NETWORKS FROM HATCHETMAN ATTACK

Hanan Hassan Khan[1], Manmeen Kaur[2]

[1]*Research Scholar,* [2]*Assitant Professor, CSE Department*

Swami Vivekanand Institute of Engineering and Technology, Patiala, India.

Abstract: The work was aimed at securing the low power lossy networks against new kind of attack, i.e. Hatchetman attack. In this attack, RPL is exploited and the malicious node changes the address of the piggybacked source route with fictitious destination address. The attack was simulated in network simulator 2.35. Also, the detection and prevention scheme was simulated under the same simulation scenario. The performance of the network was compared based on bandwidth consumed, packet delivery ratio and number of packet drops in the network. The performance parameters showed an improvement in network's performance after successful detection and prevention of the malicious node.

Keywords: RPL, Hatchetman attack, DODAG, packet delivery ratio

I. INTRODUCTION

Highly increasing physical objects being connection with the Internet are knowing the concept of Internet-of Things and its applications also, in which a myriad of multiscale sensors and objects are flawlessly blended and communication is between them. Internet of Things (IOT) is a theory shift in networks that actually make connection nearly among all things Given the constrained nature of smart devices, energy efficient routing performs a major role in well deployment of such networks. [1] The Internet Engineering Task Force Working Group [2] has presented a routing protocol for low power and lossy networks, referred to as RPL [3]. RPL a routing protocol for low power and lossy networks is planned to be an easy and inter-operable networking protocol for resource-constrained objects in industrial, home, and urban environments, intended to support the vision of the Internet of Things with number of devices connected through multi hop mesh networks. Around five years have passed since the standardization of RPL, and it is assumed that it is time to study and understand its existing state. It is also envision that wirelessly connected IP smart nodes under internet of things will develop information accessibility and availability as well as our lives advancement further. But because of the shared medium and the lack of resource requirement , physical protection and security requirements of inherent network protocols, LLNs are undoubtedly exposed to Denial-of-Service attacks [4].The Internet of Things is known as a globally network infrastructure that promotes wireless communication among devices . One instant challenge is the management of these objects, knowing that they may have limited computational resources. This management can be performed by using gateways, i.e., devices that transition wireless communications, minimizing resource consumption of the restrained objects.

A new type of denial-of-service DOS attack, called hatchetman attack, in RPL-based LLNs is presented. a nasty node manipulates the source

route header of the arrived packet, and then generates and transfers the invalid data with error route to valid nodes In hatchetman attack. When the legitimate node obtain the invalid packets with error route, the dropping of packets will be done since the arriving node cannot transfer the packets with the error route. The arrived node will reply an Error message back to the DODAG root for reporting the error in source route header. If the malicious node arrives and transfers huge amount of invalid packets with error route to legitimate nodes, this will cause the valid nodes to drop the received packets and replying huge Error messages, which leads to a denial of service in RPL-based LLNs and evaluation of its performance impact through broad simulation experiments in terms of packet delivery ratio, throughput, packet delivery latency, energy consumption, the number of attack packets, and attack energy inefficiency is done . The simulation results states that the hatchetman attack is really a severe attack in RPL-based LLNs [5].

The rest of the paper is organized as follows:

An overview of related work is provided in Section II. Section III describes the detection and prevention technique for the Hatchetman attack. Section IV shows the results and finally, paper has been concluded in last section of the paper.

II. RELATED WORK

While the paper [4] studies the history of research efforts in RPL and future research directions on which RPL should evolve, the authors in [5] have come up with new kind of attack in RPL known as Hatchetman attack.

In [6], the RPL attacks are studied and analyses is also done here. The unique performance can be seen in the analysis of network topology that constitute both static and mobile. This also presented that how version attacks effected the power consumption of the nodes.

In [7] a rank attack that goals in the property of rank in RPL and its effect on the performance are investigation of the wireless sensor networks, where the adversary can settle with the rank rule for the downgrade of the performance of RPL. Four adversarial areas consulted by violating rank rule permanently and non-permanently and their potential performance impact are studied.

In [8] summarization of the emerging work for protection of Internet-of-Things IOT networks against Denial-of-Service DOS attacks. The attacks that the anomaly-based for error Detection System intruder can be insider or outsider attacks. The system presented can be of as an improved version of SVELTE IDS which in best case solves the problem of detection system components' placement within the low power and lossy network. Also, the monitoring part of the detection system to the resource constrained objects and the detection part to the border router. In addition to this, the extended 6LoWPAN networks and incorporate the cooperative autonomous detection model so that multiple IoT networks sharing the same DODAG ID cooperate get stronger against coordinated attacks where potential security issues and fundamental countermeasures are presented. It also analyses the security capability of the IEEE 802.15.4 MAC protocol as well as the limitations there of in the area of Internet-of Things.

In [9], the authors proposed a light-weight counter measure to a choosy forwarding attack, called SCAD, in which a random single checkpoint node

selected is deployed to find the forwarding misbehaviour of invalid node. The presented countermeasure is included with timeout and hop-by-hop retransmission models to for fast recovering of not expected packet losses because of the forwarding misbehaviour or awful channel quality. It is also presented that a simple analytical approach and its numerical result in terms of fake detection rate. The authors perform extensive simulation experiments for performance evaluation and compare it with the existing CHEMAS and CAD models. The results of simulation show that the proposed countermeasure can advance the detection rate and packet delivery ratio (PDR) as well as also be helpful in the energy consumption, false detection rate, and successful drop rate reduction.

A very lightweight countermeasure to choosy forwarding attack is presented by deploying a single checkpoint node included with timeout and hop-by-hop retransmission models. An optimal monitoring node selection model is presented to protect the network against denial-of-service DOS attacks in wireless sensor networks WSNs in [10].

The SVELTE [11] proposes that the IOT resources things are connected to the non-reliable and non-trusted internet through IPv6 and 6LoWPAN networking scenario. Also the provided with security with encryption and authentication, and these things are known to wireless attacks inside the 6LoWPAN networking and from the internet. These attacks may achieve some success but there is a need of intrusion detection system. A novel intrusion detection system for the security of Low-Power Wireless Personal Area Network (6LoWPAN) running with RPL from network layer and routing attacks. The CMD presents a monitor-based technique to moderate the forwarding misbehaviours in LLNs running with RPL, in which each node follows the forwarding behaviours of the selected parent node to study the packet loss rate PLR, the observation result is compared with the collected packet loss rate from one-hop neighbour nodes, and detection of the forwarding misbehaviours of the selected parent node.

III. PROPOSED WORK

In this work, we proposed IDS system for detection of Hatchetman attack in lossy networks. In the proposed IDS system, IDS nodes will be deployed in the network in such a way that each IDS node is in direct connection with other normal nodes in the network. These IDS nodes can share information with each other also such that they have complete knowledge of the network.

When the DODAG root has to forward any data to the sink node, it will broadcast DIO control message first to build routes to the sink node. When the routes are build, the sink node will send DAO message to the DODAG root node. To this DAO message, the DODAG root replies back with DAO-ACK packet. If there is any attacker node in the route, it will modify the DAO-ACK message contents such that the next node could not find route to original destination node.

When the next node receives such a packet, instead of sending the error message back to the DODAG root node, it will send the received packet to the immediate IDS node. We refer to this node as requesting node. The IDS nodes will coordinate with each other to find if the destination address (which is in the packet) actually exists in the network. For this, each IDS

node will mutually exchange the information regarding the ID of the nodes which are in their communication range.

If the required address is not found, the IDS node will mark the nodes as malicious (which sent packet to the requesting node). IDS node will also inform DODAG root node and the immediate neighbors of the malicious node about it so that they do not receive any packet from it. DODAG root will now send data to the sink node via another path.

IV. RESULTS

The simulation of the low power lossy network under the Hatchetman attack and the proposed detection as well as prevention scheme were implemented in network simulator 2.35. This is open source simulator and works in UNIX environment. The network simulator makes use of tool command language in the front end and in the back end the simulator uses C++ language. The various simulation parameters that were used to simulate the network are listed in the table below:

Parameter	Value
Channel	Wireless
Propagation	Two Ray Ground
Antenna	Omni Directional
Number of nodes	100
Number of IDS nodes	9
Network area	1100*1100 sq meters
Initial Energy	100 Joules
Number of attackers	1

Table 4.1 Simulation Parameters

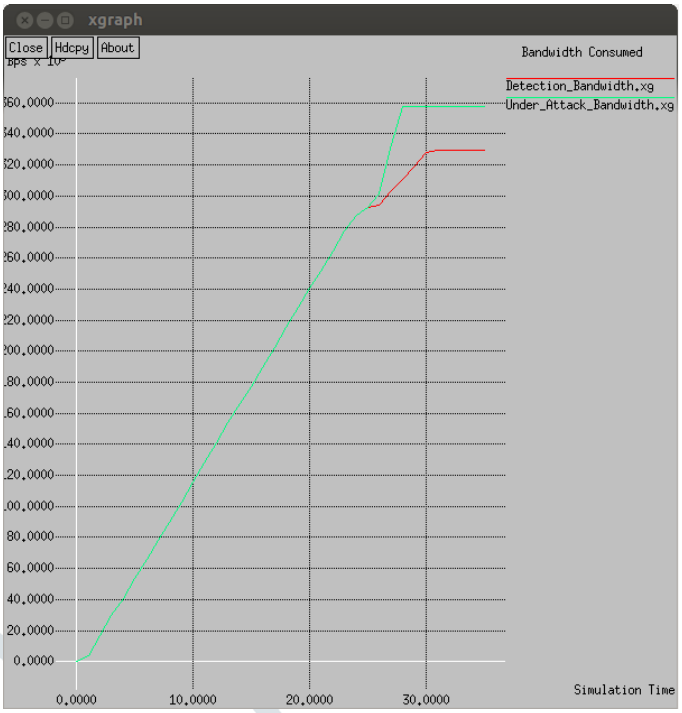

Fig 4.1: Bandwidth consumed comparison

This graph shows the comparison of bandwidth consumed in the network under the effect of the attack and the after the detection of the attack. The value of bandwidth consumed is 357 Kbps under the effect of the attack whereas when the attack gets detected using the proposed scheme, the bandwidth consumed is 329 Kbps.

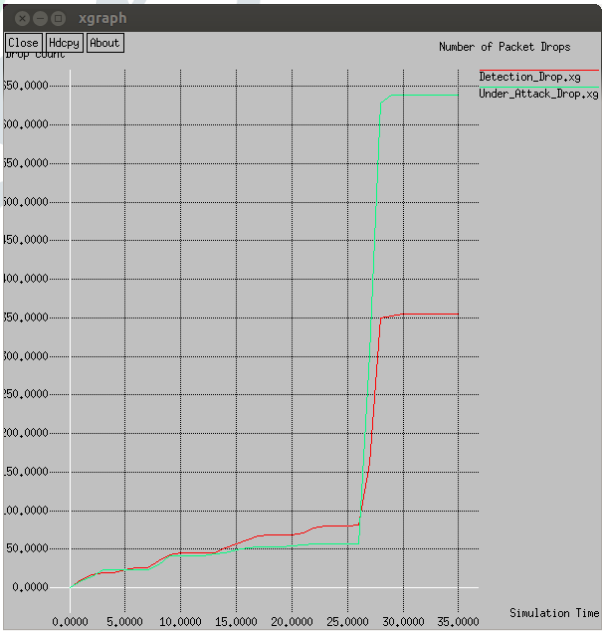

Fig 4.2: Number of packet drops comparison

This graph shows the comparison between the numbers of packet drops in the network. The value rises gradually in the network till 25 seconds. The

packets are dropped during this time due to the congestion experienced due to the broadcasting of DIO packets in the network. After 25 seconds, the value rises suddenly indicating the attack. The network experiences 639 packet drops under the attack and 355 packet drops under the detection technique.

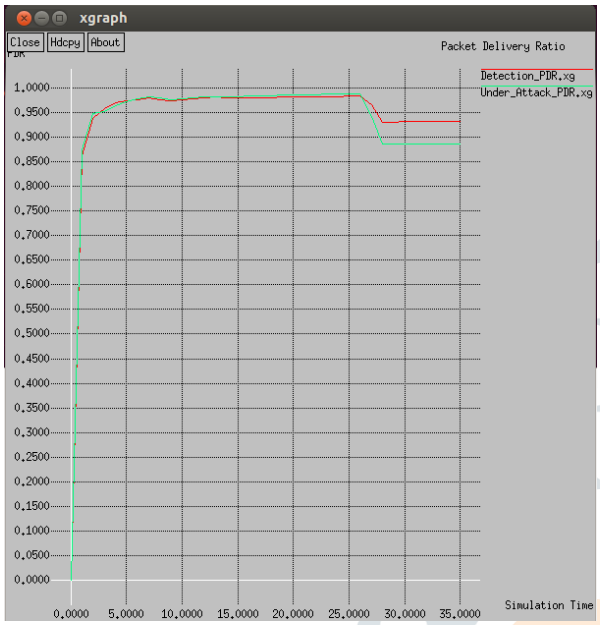

Fig 4.3: PDR comparison

This graph shows the value of packet delivery ratio of the network. The value of PDR obtained under the attack is 88.61 % and the after the detection of the malicious node using the proposed scheme, the value obtained is 93.25 %.

V. CONCLUSION

The work was aimed at securing the low power lossy networks against new kind of attack, i.e. Hatchetman attack. In this attack, RPL is exploited and the malicious node changes the address of the piggybacked source route with fictitious destination address. The attack was simulated in network simulator 2.35. Also, the detection and prevention scheme was simulated under the same simulation scenario. The performance of the network was compared based on bandwidth consumed, packet delivery ratio and number of packet drops in the network. The proposed scheme successfully detects the malicious nodes which reduces the consumption of bandwidth of the network. The more value of packet delivery ratio indicates the less packets get dropped in the network and the malicious node is successfully detected in the network. This also leads to better values for the third parameter, i.e. number of packet drops. Therefore, the improved network performance helps us to conclude that the proposed scheme successfully secures the network from the Hatchetman attack.

This study analyzes three parameters only. In future, other parameters such as the energy consumption and throughput of the network can also be analyzed. Also, the use of cryptographic techniques can be made to make the network more secure from the attacks.

REFERENCES

[1] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, “Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications,” IEEE Commun. Surveys Tuts., vol. 17, no. 4, pp. 2347–2376, 2015.

[2] The Internet Engineering Task Force (IETF), https://www.ietf.org.

[3] T. Winter and P. Thubert, “RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks,” RFC Standard 6550, March 2012.

[4] H. Kim, J. Ko, D. Culler, and J. Paek, “Challenging the IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL): A Survey,” IEEE Commun. Surveys Tuts., Sep 2017.

[5] Cong Pu ,Tianyi Song , "Hatchetman Attack: A Denial of Service Attack Against Routing in Low Power and Lossy Networks", 5th IEEE International Conference,2018

[6] A. Le, J. Loo, A. Lasebae, A. Vinel, Y. Chen, and M. Chai, "The Impact of Rank Attack on Network Topology of Routing Protocol for LowPower and Lossy Networks," IEEE Sensors J., vol. 11, no. 10, pp. 3685– 3692, 2013.

[7] A. Dvir, T. Holczer, and L. Buttyan, "VeRA-Version Number and Rank Authentication in RPL," in Proc. IEEE MASS, 2011, pp. 709–714.

[8] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denialof-Service detection in 6LoWPAN based Internet of Things," in Proc. IEEE WiMob, 2013, pp. 600–607.

[9] S. Challa, M. Wazid, A. Das, N. Kumar, A. Reddy, E. Yoon, and K. Yoo, "Secure Signature-Based Authenticated Key Establishment Scheme for Future IoT Applications," IEEE Access, vol. 5, pp. 3028–3043, 2017.

[10] C. Pu and S. Lim, "A Light-Weight Countermeasure to Forwarding Misbehavior in Wireless Sensor Networks: Design, Analysis, and Evaluation," IEEE Systems Journal, pp. 1–9, 2016.

[11] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," Ad Hoc Networks, vol. 11, no. 8, pp. 2661–2674, 2013.