JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Analyze Black Hole Attack in RPL Using Cooja Environment

K.Kowsalyadevi[1], Dr.N.V.Balaji[2]

[1]Research Scholar, [2]Dean, Faculty of Arts, Science and Humanities,

[1]Department of Computer Science, Karpagam Academy of Higher Education,

Coimbatore

ABSTRACT

Communication of devices through restricted networks, unpredictable Internet access, lossy nature of communication links, and heterogeneous nature of IoT devices are all characteristics of RPL-based Internet of Things (IoT). As a result, they are vulnerable to assaults such as black holes, floods, and rank attacks, among others, making security for RPL-based IoT a significant concern. In this paper the black hole attack from the address based attack from the DAG inherited attack are simulated using cooja simulator and the power consumption of each device is examined.

Keywords: IoT, Attacker, RPL, Black hole

1. INTRODUCTION

The Internet of Things (IoT) is a modern-day technology especially connects everything on the planet via the internet [7]. To communicate with one another, connected items in an IoT system have unique IDs. These items can be accessible through the internet by PCs, smarphones, and IoT enabled devices [5]. IoT enables automated services in variety of industries, including home automation, agriculture business, smart cities and smart health care among others. The sensitive information collected by the IoT system from these fields must be protected from attackers. The most pressing issue is network security based on RPL.

2. RPL (ROUTING PROTOCOL FOR LOW POWER AND LOSSY NETWORKS)

RPL is a protocol designed as networks with low resources. The Low Power Lossy Network is comprised of a small number of nodes and links. There are various LLN standards [10]. RPL is one of the standards RFC 6550. It's a protocol that allows data to be routed from a source. It enables the packets transmitted to specify the entire or partial transmission route of the packet [8]. As a result, the reach ability of a destination should be evaluated before broadcasting. It is verified through the transmission of RPL control packets [1].

Routing protocol (RPL) as networks with limited resources [2]. It's a routing protocol known as Distance Vector. Any link in the network's distance and direction are determined by it. The distance is a measure of how much it costs to go to a specific node in the network. The next hop's address is specified by the direction. LLN's like Radio Network do not have predefined topologies, such as wires connecting nodes [3]. As a result, the RPL protocol must efficiently discover linkages and pick nodes. It's also a source routing protocol. It allows the packet's transmitter to specify the packet's whole or partial transmission route. The RPL's pathways have been improved for traffic in both directions [6]. For topology, the root nodes will be sink nodes.

Finally, RPL creates the DAG (Directed Acyclic Graph) structure [8]. One or more DODAGs make up the DAG. Each sink node will have its own DO (Destination Oriented) DAG. For maintaining and recognizing a topology [5], RPL employs 4 values, RPL instance ID, DODAG version number, DODAG ID and Rank value.

RPL Power Message is identified by the value 155 in the type of field of an ICMPV6 [9] message. Five RPL [12] control messages are available. The code field can be used to identify the RPL control message. The actual field in the control message is dependent on the code.

DIS (DODAG Information Solicitation) is used to request DIO message from the RPL node. It's analogous to the router desire in IPv6, which is used for nearest location [4]. A node uses the DIS message to investigate its neighbors in order to find adjacent DODAGs.

DIO (DODAG Information Object) contains data i.e. allows the node to identify an instance of RPL, learn the configuration parameters, identify a DODAG parent, and maintain the DODAG [11]. Its multicast and RPL instance ID, Version number, Rank, DTSN (Destination Advertisement Trigger Sequence Number, grounded flag, mode of operation and DODAG preference are the message's base object fields.

Destination Advertisement Object (DAO) is to transmit information about the destination in a upward direction. DAO message is unicasted to the root in non storing mode. The receiver acknowledges the DAO message with a DAO-ACK message.

Destination Advertisement Object Acknowledgement is message receiver might be either the DAO's parent or the DODAG's root. In accept to a separate DAO message [9], this message is intended. The recipient of the

message could be the DAO's parent or the DODAG's root.

Consistent Check (CC) is sent in a secure format. It's used to synchronies the security counters between every pair of nodes and check the secure message counts.

The building of a DODAG consists of two steps [12]; for creating routes from the root to the client, DIO control messages are broadcast in a downward direction, and the DAO message in order to build upward routes.

For the DODAG's construction: i) A DIO messages are sent out. It provides ID field ii) A node that is wants or unwilling and go to the DODAG can receive a DIO message.

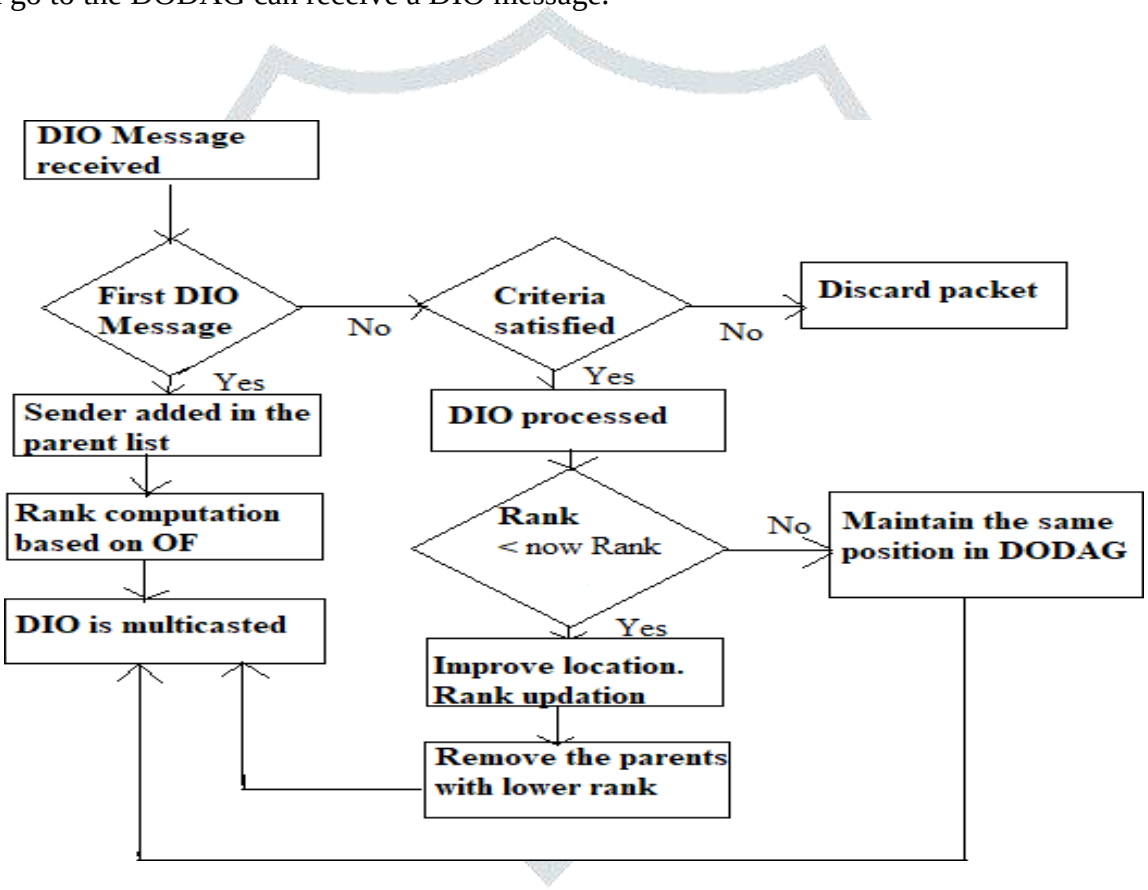

Fig. 1.1. DODAG Construction & Maintenance

If a client node wants to join the Destination Oriented Directed Acyclic Graph, it must do the following:

i) Add the client's address to the sink node

ii) Compute rank according to the objective function

iii) Forwards the updated rank to DIO

iv) If a node's rank is modified, it dropped the node in the sink node to avoid loops .

Figure 1.1 depicts the procedures involved in DODAG construction and maintenance.

3. CLASSIFICATION OFATTACKS

RPL is vulnerable to a variety of routing attacks [11]. An attacks into two categories based on their origin: Address based Attacks (The manipulation of addresses is the basis of address based attacks) and DAG inherited attacks (Based on manipulating version numbers, control packets, rank and other variables) as shown in Fig.1.2 .

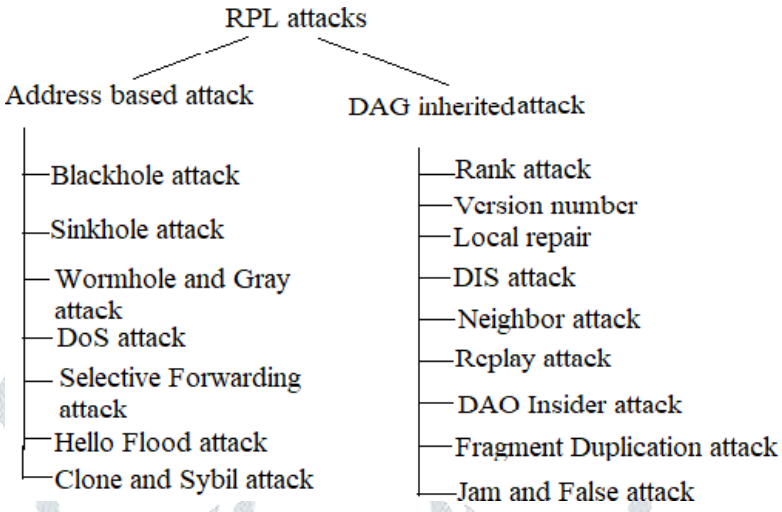

Fig.1.2. It shown the Classification of Attacks

4. BLACKHOLE ATTACK

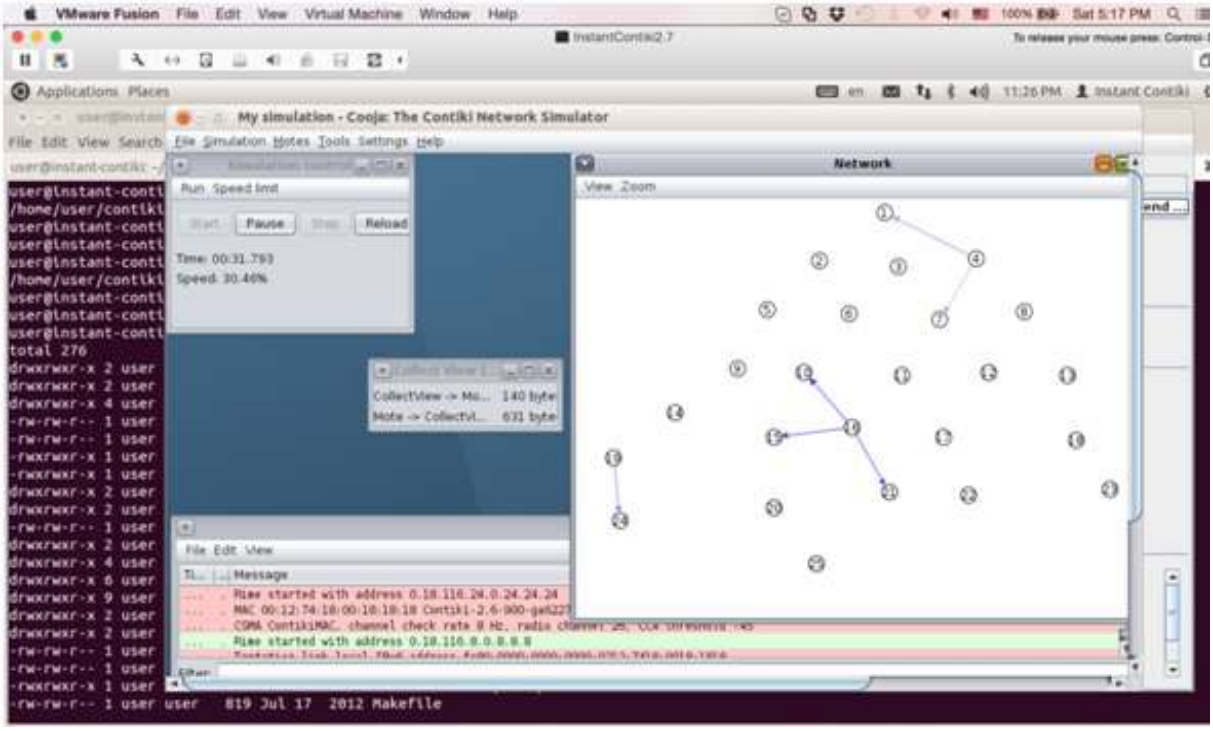

Fig. 1.3. Shown Cooja Environment

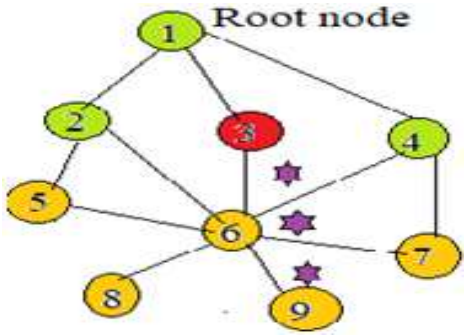

Fig.1.4. Blackhole Attack

The attacker node dumps the packet silently in a blackhole attack. The attackers drop all packets that pass through them depicted in Fig.1.3. The attacker in the aforementioned topology in node 3. It discards the packet it has received. Contiki OS has been changed in order to implement the blackhole attack using cooja tool shown in Fig.1.3. All data packets from its neighbor nodes were dropped by the blackhole attacker.

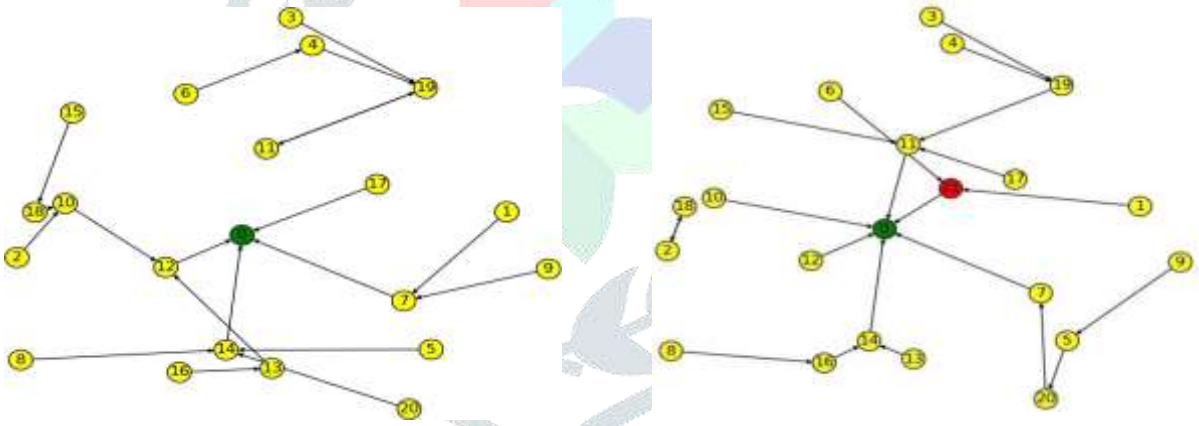

Fig. 1.5. Final DODAG (a)Without Blackhole attacker (b) With Blackhole attacker

Fig.1.4 (a), shows a Nodes are all having without attacker Fig.1.4.(b), Nodes are all having with attacker(Red node- Black hole attacker, Green Node- Sink)

POWER CONSUMPTION ANALYSIS OF EACH MOTE

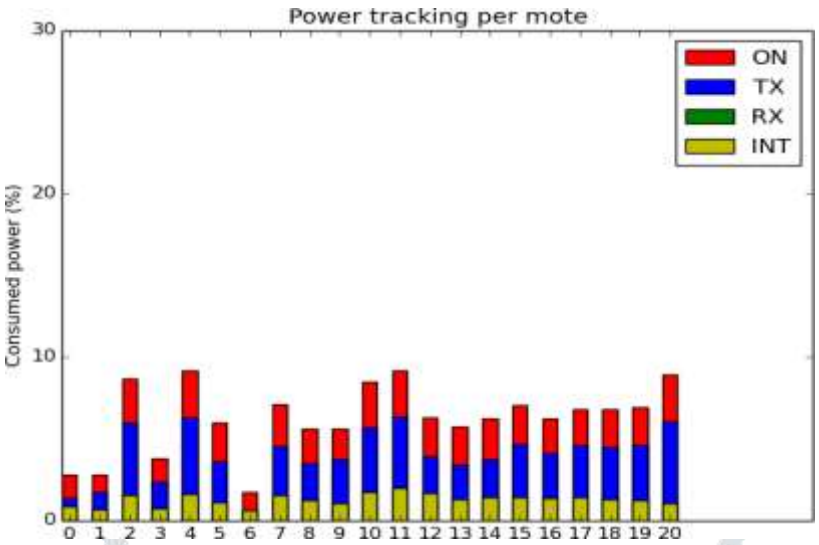

Fig.1.6. (a) Without Blackhole attacker

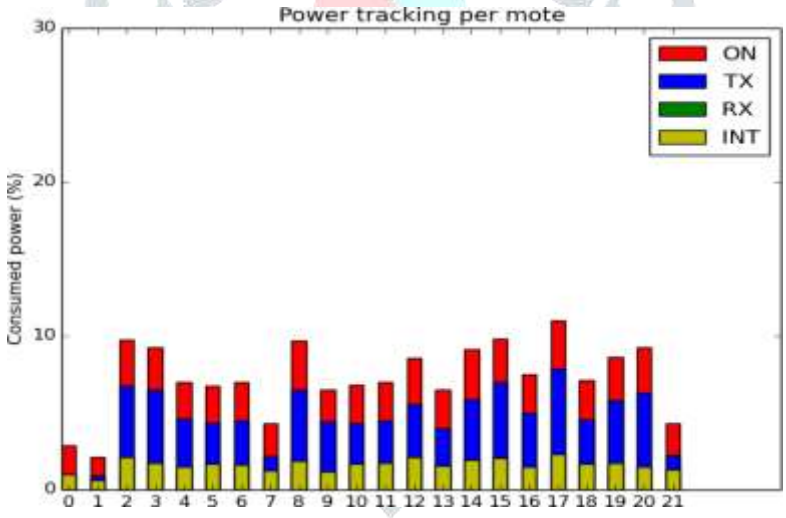

Fig.1.6 (b)With Blackhole attacker

CONCLUSION

For detection of intruders, the security mechanisms provided in RPL can be examined and implemented. Furthermore, this evaluation will aid future into RPL related attacks and mitigation measures. There are other vulnerable attacks like Rank attack, and Flood attack in RPL which can be implemented as future work.

REFERENCES

1. Airehrour, David, Jairo Gutierrez, and Sayan Kumar Ray. "A trust-based defence schemefor mitigating blackhole and selective forwarding attacks in the RPL routing protocol". Australian Journal of Telecommunications and the Digital Economy 6.1 (2018):41.
2. Jiang, Jun, Yuhong Liu, and Behnam Dezfouli. "A Root-based Defense Mechanism Against RPLBlackholeAttacksinInternetofThingsNetworks."2018Asia-PacificSignalandInformation Processing Association Annual Summit and Conference (APSIPA ASC). IEEE,2018.
3. Sahay, Rashmi, et al. "Exponential Smoothing based Approach for Detection of Blackhole Attacks in IoT." 2018 IEEE International Conference on Advanced Networks and Telecommunications Systems (ANTS). IEEE,2018.
4. Chen, Binbin, Yuan Li, and Daisuke Mashima. "Analysis and enhancement of RPL under packetdropattacks."201810thInternationalConferenceonCommunicationSystems&Networks (COMSNETS). IEEE, 2018.
5. Conti, Mauro, Pallavi Kaliyar, and Chhagan Lal. "Reliable Group Communication Protocol for Internet of Things." arXiv preprint arXiv:1904.04542(2019).
6. Jiang, Jun, Yuhong Liu, and Behnam Dezfouli. "A Root-based Defense Mechanism Against RPLBlackholeAttacksinInternetofThingsNetworks."2018Asia-PacificSignalandInformation Processing Association Annual Summit and Conference (APSIPA ASC). IEEE,2018.
7. Kfoury, Elie, et al. "A Self Organizing Map Intrusion Detection System for RPL Protocol Attacks." International Journal of Interdisciplinary Telecommunications and Networking (IJITN) 11.1 (2019):30-43.
8. Mohammad Nikravan, Ali Movaghar and Mehdi Hosseinzadeh, "A Lightweight Defense Approach to Mitigate Version Number and Rank Attacks in Low-Power and Lossy Networks", Wireless Personal Communications, Volume 99, Issue 2, 2018, pp. 1035-1059.
9. Loganathan, J., Latchoumi, T. P., Janakiraman, S., & parthiban, L. (2016, August). A novel multi-criteria channel decision in co-operative cognitive radio network using E-TOPSIS. In Proceedings of the International Conference on Informatics and Analytics (pp. 1-6).
10. Aditya Tandon and Prakash Srivastava, "Trust-based Enhanced Secure Routing against Rank and Sybil Attacks in IoT," Twelfth International Conference on Contemporary Computing (IC3), Noida, India, 2019, pp. 1-7, doi: 10.1109/IC3.2019.8844935.
11. Abd Mlak Said, Aymen Yahyaoui, Faicel Yaakoubi, and Takoua Abdellatif, "Machine Learning Based Rank Attack Detection for Smart Hospital Infrastructure." In International Conference on Smart Homes and Health Telematics, Springer, Cham, pp. 28-40, 2020, doi: 10.1007/978-3-030-51517-1_3.
12. Manjula C Belavagi and Balachandra Muniyal, "Multiple intrusion detection in RPL based networks", International Journal of Electrical and Computer Engineering, Volume 10, Issue 1, 2020, pp. 467-476.