IJCSE International Journal of Computer Sciences and Engineering Open Access

Survey Paper Vol-6, Special Issue-4, May 2018 E-ISSN: 2347-2693

A Survey: Attacks against RPL network in IoT

S. Yuvarani

Department of Computer Science and Applications, The Gandhigram Rural Institute-Deemed to be University,
Dindigul, India.

*Corresponding Author: yuvarani2231995@gmail.com

Available online at: www.ijcseonline.org

Abstract— The security is the most important issue in Internet of Things (IoT) nowadays. In this paper we discuss the attacks against Routing Protocol for Low power and Lossy Networks (RPL).The IoT contains the constrained devices which are limited in resources like limited power, memory and processing capabilities. Healthcare, Home appliances, Transport, Social Networking, Defences, Banking are some examples of IoT applications. For this purpose the new protocol is designed called RPL. The RPL is a network layer protocol .The RPL is a leight weight distance vector protocol. In IoT to provide the security and privacy is challenging when the devices are connected to the lossy networks. In this paper the research is focus on the attacks against the RPL.

Keywords— RPL, Attacks, IoT, Malicious, Security, Nodes.

I. Introduction

The RPL is a standardized protocol for IoT and it is designed for Low Power and Lossy Networks (LLNS).It is also known as Ipv6 over Low Power Wireless Personal Area Network(6LowPAN). In IoT the constrained devices are connected to the internet and the devices can be a sensor node or home appliances.RPL is based on the Destination Oriented Direct Acyclic Graph(DODAG).It contains only one root node called sink node/destination node. The RPL supports both the point-point and point to multipoint communication. The root node sends the DIO messages and the nodes receives the message and select the parents rank. The rank is based on the distance from the root node.

In the 6LowPAN network the security provides the confidentiality of the packet during the transmission and authentication between the devices. The routing attacks are basically common in low power lossy networks. The attackers launch the attack against IoT devices or nodes in the network. In this paper the section II discusses about the routing attacks against RPL. And the section III describes the research opportunities of RPL attacks and the section IV describes the conclusion of this study.

II. ATTACKS AGAINST RPL

A) Sinkhole attack

It is one of the most dangerous and powerful attack compared to other attacks. The malicious node advertise the beneficial path to attract the neighbour node for traffic through it and it doesn't disturb the network operations. In [1] the defence against sinkhole attack that the root node generates the hash value when it is start by picking the random value and broadcast it in DIO messages. In this attack the malicious node doesn't calculate the hash value but it only broadcast received DIO messages. All other nodes calculate the hash value using previously received and each node store the hash value of its parent node. The IDS [2] define the solution of sinkhole attack. In[3] defines the mechanism to detect the attack and advantages /drawback with resource consumption and false positive ratio are compared.

B) Selective forwarding attack

The selective forwarding attack specially designed to disturb the routing path on the network. And the DoS attack also launched where the malicious node forward the packets. The malicious node could forward all the control messages and drop the rest of the traffic. It results finally creating the disjoint path between the parent and the children. The IDS [2] give the solution of end-to-end delay packet loss adaptation algorithm for detection of this attack.

C) Wormhole attack

The wormhole attacks mainly disturb the network topology and the traffic flow. It can take place by creating the tunnel between the two attackers. The tree is constructed from root node to leaf nodes and this attack prevented by the Markle tree authentication [4]. It constructs the tree from leaf to root node and the hash value is calculated by using the public key and the node ID. If the node failed to authenticate, then the child avoids the node select as its parent. In [5] designed to detect the attack and it results 94% detection rate.

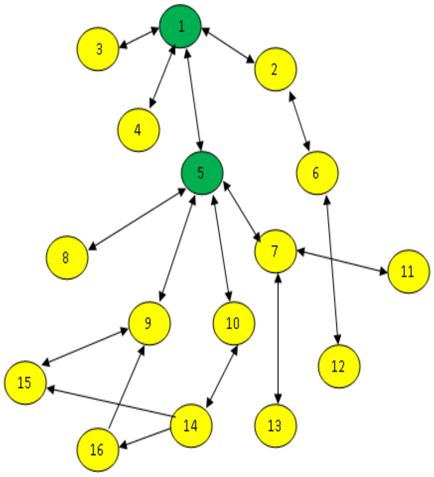

Figure1: Sinkhole attack.

D) Blackhole attack

In this attack the crime node drops all packets that mean it drops all the packets routing through that node. It reflects the high damaging rather than the other attacks. In [6] it provides the new protocol which is to be reliable that provides a feedback aware trust based security system for IOT.

E) *Clone ID Attack*

In this attack the crime node clones the ID of all other nodes in the network to get access to traffic destined to victim node. But we can easily identify both the malicious and original nodes by using its geographical location of the node with its identity. To minimize this attack, we can track the number of instances of each identity and easily find out the cloned identities also. In [7] it provides the detection mechanism and removes the attack using Witness Approach Algorithm.

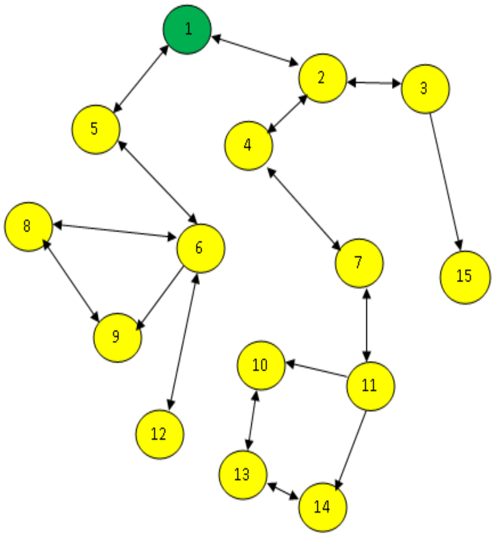

Figure2: Warmhole attack.

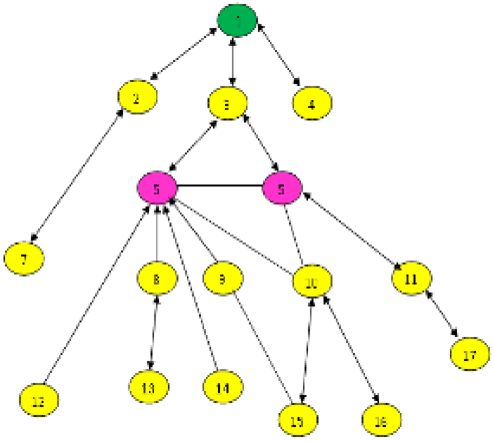

Figure3:CloneID attack.

F) Sybil attack

It is similar to the clone ID attack because the malicious node in the Sybil attack uses the node identities. But this attack is not evaluated in RPL. In [8] the author describes the defense against this attack. It could not deploy any nodes to implement this attack but it takes a network under control.

G) Hello flood attack

The malicious node sends the “hello” message as an initial message when it joins in a network. It broadcasts the hello messages and introduced himself as neighbour to all the nodes in the network. The hello messages are the DIS message which is used to advertise information about DODAG. [1] Definite solution to this attack. To calculate the default path it uses the link layer metric but the no acknowledgement is received from the link layer then it defines the path as bad.

H) DOS(Denail Of Service) Attack

It is difficult to identify the malicious node and it uses the ipv6 UDP packet flooding in the RPL. This attack is an attempt to make the resources unavailable for other nodes. In [9] IDS provides the framework for detecting this attack. In [14] define the countermeasures to secure the network from this attack by using this parameter packet forwarding ratio, packet delivery ratio, packet drop ratio, a packet received ratio, packet sending ratio and so on.

I) SPOOFING ATTACKS:

(a) NEIGHBOR ATTACK:

In this attack the attacker node /malicious node broadcast the DIO messages to the entire node in a network but they can’t add any information about himself. The node which receives this DIO messages is a new neighbor node and send the messages. The crime node select the node which is not a parent node and change the route which is to be out of range neighbour. This attack increases the end-to-end delay and damage the QoS[10] and network topology but it doesn't change the Packet Delivery Ratio(PDR).

(b) Version Attack

In this attack the node receives the latest version of the DIO messages, then it forms the new DODAG tree and it causes the inconsistencies in network topology. And it also causes the loop and rank inconsistencies around the neighbor of the crime node. In [11] it reduces the PDR and increases the control overhead. It also impacts the power consumption and availability of channels. In [12] provide the Distributed Detection Algorithm to detect the attack and acceptable false positive ratio.

(c) Rank Attack

The attacker changes the rank value himself to attract the leaf/child node for selecting this as a parent node because the rank increases from root to leaf nodes in the RPL. In [13] this attack is simply detected based on the attack existing duration and updated on DIO information.

The consequences of this attack are as follows:

1. Reduce PDR
2. Optimize the path in RPL topology
3. Formation of loop and un-optimized path
4. Changing of network topology around the malicious node

(d) DIS Attack (DODAG Information Solicitation):

In this attack the new node sends the DIS messages for joining the RPL network. The crime node sends the DIS message periodically to its neighbor node during the attack. In [10] the end-to-end delay is increased and no impact on a PDR.

(e) Local Repair Attack

In this attack the victim node sends the local repair messages for all the nodes. It causes the local repair around the nodes which receives this message. And it impacts high in the PDR and generate more control overheads.

III. RESEARCH OPPORTUNITES ON RPL ATTACKS

All attacks are not evaluated in RPL network. The prevention mechanism of blackhole attack is not evaluated. It is one of the research areas in RPL. And the clone ID attack also not evaluated in this network. The sink hole prevention mechanism of sinkhole is another research area in this network. Detection and prevention mechanism are other research areas in RPL. The neighbor attack, Local repair attack, DIS attacks detection and prevention mechanism are the main research on the RPL network.

Table1: RPL attacks and its effects

RPL attacks	Effects
Sink hole	Large amount of traffic flow
Selective forwarding attack	Path distributed
Wormhole	Disturb topology
Blackhole	Packet delay and control overhead
Clone ID	Traffic unreachable to malicious node
Sybil	Similar to cloneID
Hello flooding	Victim node formation route
DOS	Resource unavailable to other nodes
Neighbor	Packet delay
Version attack	end-to-end delay and delay PDR
Rank	Packet delay and loop formation
DIS	Packet delay

IV. CONCLUSION

In this paper the research concludes by presenting the various types of attacks on RPL networks in IOT and the research opportunities on RPL attacks. All the attacks are not detected in RPL. The Clone ID attack, Black hole attack needs a detection mechanism and also the prevention mechanism. And the attacks on RPL affect the network topology, PDR value, and packet delay and energy consumptions.

REFERENCES

[1] Weekly, Kevin, and Kristofer Pister. "*Evaluating sinkhole defense techniques in RPL networks*." Network Protocols (ICNP), 20th IEEE International Conference 2012.

[2] Raza, Shahid, Linus Wallgren, and Thiemo Voigt."*SVELTE: Real-time intrusion detection in the Internet of Things*." Ad hoc networks vol.11 ,Issue.8,pp.2661-2674(2013).

[3] Mohammad Alzubaidi, Mohammed Anbar et al ,"*Review on the mechanism of detecting sinkhole attacks on RPL* " International Conference on Information Technology 2017.

[4] Khan, Faraz Idris, et al. *"A wormhole attack prevention mechanism for RPL based LLN network.*" Ubiquitous and Future Networks (ICUFN), 2013 Fifth IEEE International Conference, 2013.

[5] Gurunath chavan, pongle *"Real time intrusion and wormhole attack detection in IOT*" International journal of computer applications,vol.121,Issue.9,pp.0975-8887,(2015).

[6] David Airehour, Sayan Kumar Ray "*Securing RPL routing protocol from black hole attacks using a Trust-based mechanism"* 26th International Telecommunication Networks and Applications Conference (ITNAC) 2016.

[7] ChakShu Goyal "*Detection of clone attack in mobile wireless sensors*" International journal of computer application,vol.132,Issue.16,pp.51-55(2015).

[8] Shang Kuan et al,"Sybil attack and their differences in the Internet of Things"IEEE Internet of Things Journal,vol.1,Issue.5,pp.372-383(2014).

[9] Kasinathan,prabaharan *"Denial of Service detection in 6LowPAN based internet of things*" International conference on IEEE 2013.

[10] Lee Anhtrun et al " *The impact of internal threats towards routing protocol for low power and lossy network performance*" IEEE Symposium on IEEE 2013.

[11] Anthea mayzaud et al“A study on RPL DODAG version attacks”International conference on Atonomous Infrastructure, Management and Security, vol.850, pp.92-104(2014).

[12] Anthea, Remi “*Detecting version number attacks in RPL based network using a Distributed Monitoring Architecture*” 12th International conference on Network and Service Management 2016.

[13] Lee Anhtrun”*The impact of rank attack on network topology of routing protocol for low power and lossy networks”*, IEEE Sensor Journal,vol.13,Issue.10,pp.3685-3692(2013).

[14] Annas RGHIOUI, Annas KHANNOUS “*Denial of service attacks on 6LowPAN RPL networks:Threats and an intrusion detection system proposition*.” Journal of Advanced Computer Science and Technologies,vol.3,Issue.2,pp.143-153,(2014).

Authors Profile

Ms. S. Yuvarani obtain Bachelor of Computer Science from Mother Teresa Womens University in 2015. And she also pursed Master of Computer Science from Mother Teresa Womens University and completed the project “WOMENS SAFETY”. It is based on the safety of the womens and it is one of the Android based safety Application for mobile.Now she is an M. Phil Research Scholar in Gandhigram Rural Institute-Deemed to be University, Gandhigram, Dindigul, India. She does research on IoT.His area of research is computer networks.She does the research which is the current trend in computer networks is Internet of Things(IoT). The RPL is a routing protocol for IoT sensors or devices.While the current research is based on attacks against RPL networks in IoT.