International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8, Issue-1, May 2019

Attacks in RPL and Detection Technique used for Internet of Things

M.V.R Jyothisree, S. Sreekanth

Abstract: ***The Internet of Things (IoT) is a fast-growing technology. In IoT, the devices are connected through the Internet and controlled from any remote areas. Before the advent of IoT, the interaction between the users was only through the internet. By 2020 there will be 75.4 billion devices interconnected through the internet. Machine-to-machine (M2M) interaction is achieved by sending and receiving the information, such as room temperature, humidity etc. IoT can be viewed as heterogeneous networks that bring some security challenges like network privacy problems, confidentiality, integrity and availability. In IoT, we have Routing Protocol for Low-Power and Lossy networks (RPL). RPL is a light-weight protocol which has a good routing functionality, context aware and it supports dynamic topology but has only the basic security functionality. This paper elaborates on attacks in Routing Protocol for Low Power and Lossy networks (RPL) and its implementation using Cooja simulation methodologyand in Contiki operating system. Blackhole and version number attack are the most vulnerable security attacks based on routing of data in IoT networks. We proposed a common prevention technique to overcome those attacks based on the measurements of throughput, packet delay and packet delivery ratio values. The results show that our proposed detection technique is very secure from both the attacks. This technique can be used in real time applications like smart living, smart mobility and smart environment etc.***

Index Terms: ***Internet of Things, RPL, M2M, RPL security, Low Power and Lossy networks, Confidentiality, integrity,availability, Attacks, Contiki OS / Cooja Simulator.***

I. INTRODUCTION

The Internet of Things (IoT) is a technology that is advancing with rapid pace. The main aim of IoT is to create an environment where the devices communicate among themselves without human interference. IoT is a world-wide heterogeneous network consisting of interconnected objects and has a unique address based on the standard communication protocols. In IoT, 'Internet' is a world-wide network of interconnected computer networks based on the (TCP/IP) communication protocols and 'Thing' is an object or any IoT device. IoT allows human to be connected at any time to the remote devices. A device can be connected to other device using any path/ network or by any service. Various types of communication can be utilized in IoT if the communication process transmits the information between the heterogeneous devices via heterogeneous networks.Different routing protocols are needed in IoT for device-to-devicecommunication, but we require scalable routing protocols in different scenarios to find optional routes. The Routing Protocol for Low Power and Lossy Networks (RPL)[1] is one of the standardized routing protocol in IoT networks. In this paper, we explore RPL protocol by studying it's security with respect to different attacks in IoT. The rest of this paper is organized as follows. Section 2 presents a brief survey on RPL protocol and attacks in RPL, Section 3 deals with the implementation of attacks in RPL, Section 4 discusses the simulation results, Section 5 describes the proposed algorithm used to detect those attacks and Section 6 gives conclusion and highlights the research challenges in IoT.

Revised Manuscript Received on 22 May 2019.
***** Correspondence Author
M.V.R Jyothisree*, Computer Science Department, Research Scholar, Rayalaseema University, Kurnool, Andhra Pradesh, India.
Dr.S.Sreekanth, Dept. CSE, JNTU A / SITAMS, Ananthapur, Andhra Pradesh, India.

II. LITERATURE SURVEY

In IoT, security is a highly challenging issue[4]. Survey has been done on security modes available in IoT and different RPL attacks in network layer.

A. RPL Security

Security is associated with low power and lossy networks [3]. RPL motes operate mainly on three security modes. They are:
1) Unsecured mode
2) Pre-installed mode
3) Authentication mode
A brief description of these modes is now given as:
1) Unsecured Mode: In this mode, RPL control messages are forwarded without any extra security measures. It infers RPL network by using other security primitives to meet the specific requirements and application needs.
2) Pre-installed mode: In this mode, RPL instances have pre-installed keys to join them to process, safeguard and generate a secure RPL messages.
3) Authenticated mode: In this, nodes can be entered from the left node. It is like pre-installed mode, which forward the nodes by getting the key from an authentication authority.
The RPL security is based on three factors: Confidentiality, Integrity and Availability (CIA) [2]. Delay and replay protection are an added option in RPL security [5].

B. Attacks in RPL

In RPL, classification of attacks is based on CIA [7]. There are different types of attacks in RPL that affect the network performance [8]. The types of attacks are as follows:

1)Rank attack: This attack mainly focuses on confidentiality and integrity which affects the network performance by generating loops, non-optional path, low packet delivery ratio, packet drops and packet delays.

2)Selective forwarding: This attack is also based on confidentially and integrity that affect the network performance by disrupting the traffic flow.

3)Sinkhole attack: This attack degrades the network performance by transmitting huge traffic passing via attacker node. This comes under confidentiality and integrity attack.

4)Hello flooding attack: This attack affects the network performance by using excess battery power and sensor energy. This attack falls in the category of availability attack in RPL.

5) Sybil and Clone ID Attack: It mainly focuses on confidentiality and integrity attack that affects the network performance by way of compromised route or broken network and traffic cannot reach the victim's node.

6) Denial of service (DOS) attack: This attack occurs due the unavailability of network resources, so it belongs to the classification of attacks.

7) Worm hole attack: This attack mainly focuses on the confidentiality and integrity attack because of which it affects the network performance by the destabilization of route topology and traffic flow.

8) Neighbor attack and DIS attacks: It mainly cause poor performance by giving false routes or no routs, resource consumption and route disruption. Network resource depletion by neighbor attack and network resource consumption takes place by DIS attacks. These attacks come under confidentiality, Integrity and Availability attacks.

9) Local repair control overhead attack: This attack leads to the disruption of routing traffic and control and it is classified under confidentiality and integrity attack.

III. IMPLEMENTATION OF RPL ATTACKS

A.Blackhole Attack

To implement the Blackhole attack in ContikiOS, we have used a Decreased rank attack. The goal is to demonstrate the impact of the DODAG[6] by channeling multiple links through the malicious mote. With the modified RPL configuration constant, the malicious mote will advertise a better rank than neighbors, causing the DAG to be modified. This attack does not damage a network, however, combining with other building blocks could be very effective because it allows the attacker to tunnel some traffic through the malicious mote (e.g. for eavesdropping).

B. Version Number Modification Attack

The goal is to demonstrate the effect of DODAG by triggering unnecessary global repairs. In the modified RPL file, the malicious mote increases the version number before forwarding the received DIO messages, thus triggering the unnecessary global repairs. The attack is composed of the following building blocks isincreasedversion. The Implementation of this attack is done in ContikiOS.

IV. SIMULATION RESULTS OF RPL

In the IoT, we use Instant Contiki 3.0 version platform to perform the simulation. Contiki is an open source operating system. It is designed mainly for the tiny devices and thus the memory footprint is less than that of other systems. It supports TCP with IPV6 addressing format that is mostly used in IoT applications. One of the most important features of ContikiOS is the use of Cooja simulator to emulate if any of the hardware devices is not available. Ubuntu is used to compile the programs for motes. ContikiOS is very robust and can be used as the universal operating system for smart objects (devices). Wireshark is a built-in tool used for analyzing the traffic between the motes (devices). In Cooja simulator, system considers the interference range of the surroundings of the other devices that are in use during the simulation.

Simulation results of Blackhole attack are shown below:

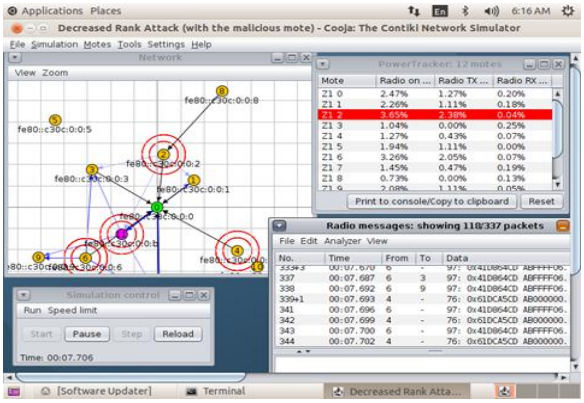

Fig 1.1 Simulation of Blackhole attack

Graphical representation with malicious mote:

The resulting Destination Oriented Directed Acyclic Graph (DODAG) is depicted in fig 1.2.

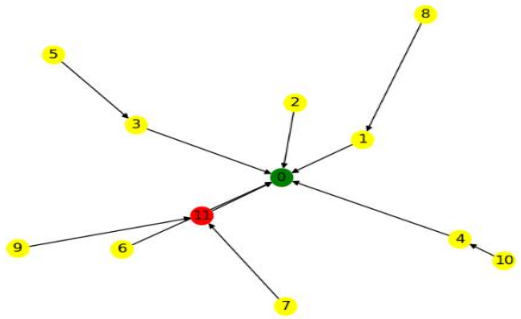

Fig 1.2 Final DODAG for the simulation with malicious mote.

Simulation results of Version number attack is shown

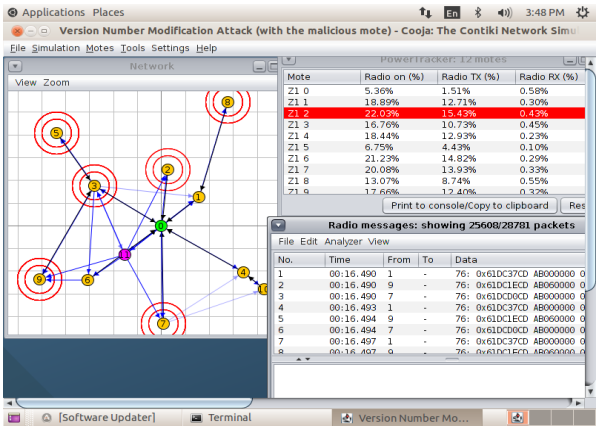

Fig 1.3 version number attack with malicious mote Graphical representation with malicious mote

The resulting Destination Oriented Directed Acyclic Graph (DODAG) is depicted in fig 1.5.

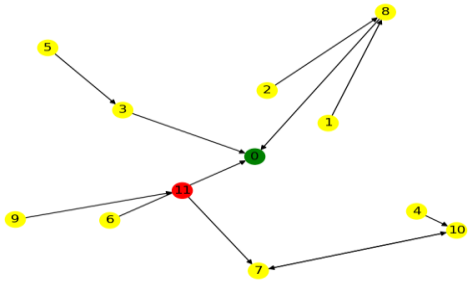

Fig: 1.5 Final DODAG for the simulation with the malicious mote.

The DODAG is affected by the malicious node (in red) due to the repeated global repairs.

V. PROPOSED ALGORITHM

We proposed a common detection algorithm for both the attacks in RPL. The algorithm called Trust Based Blackhole and version number detection(TBBVD) is used to detect the attacks. The algorithm is given below:

Detection Algorithm(Trust based black hole and version number detection algorithm in RPL-> TBBVD-RPL)
Neighbor1, Neighbor2 – Neighbor motes
ETX - expected transmission count of the mote
Rank – Node degree or Rank
Trust – Node trust
FN – Forwarder mote
##
For All the Motes
Calculate Trust [Mote] = Packets delivered / Packet sent
If (ETX [Neighbor1] <= ETX [Limit]) & (ETX [Neighbor2] <= ETX [Limit])
If (Rank [Neighbor1] <= Rank [Self]) & (Rank [Neighbor2] <= Rank [Self])
If Trust [Neighbor 1] > Trust [Neighbor 2]
FN = Neighbor 1
Else
FN = Neighbor 2
EndIf
EndIf
EndIf
Else
If (ETX [Neighbor1] <= ETX [Limit]) || (ETX [Neighbor2] <= ETX [Limit])
If (ETX [Neighbor1] > ETX [Neighbor2])
FN = Neighbor 1
Else
FN = Neighbor 2
EndIf

In the above algorithm, each mote verifies with the neighboring motes about the communication behavior and transmitting of data packets. If the expected transmission count is greater than the limit (threshold value) then it detected as malicious mote which is affected by blackhole and version number attack. After using the above algorithm, we have examined the packet is dropped by the malicious mote because of which they fail to reach the destination mote. The proposed trust-based detection technique can detect the type of attack and isolate the blackhole and version number attacks during the routing operations.

Results of parameters for one mote with attacks and after prevention are shown in the table below:

Table I Blackhole and version attack and prevention

Parameters	Attacks (for single mote)	Prevention (for single mote)
Throughput	89.23kbps	98.45kbps
Delay	1.71m/sec	0.034m/sec
Packet Delivery Ratio	88.59%	96.29%

In RPL routing, a mote rank change results in the re-alignment of DIO child-motes to another preferred DIS parent-mote. When the rank changes there is a possibility of high level blackhole and version number attacks but if we use trust-based technique the high-level comes down to low-level of susceptibility. Throughput, delay and packet delivery ratio are calculated using following formulae:

Throughput (kbps) = [(data received / (stop time – start time)) * (8/1000)]

End to End delay (ms) = (Communication end time – start time) / data received

Packet Delivery Ratio (PDR) = Generated packets – Received packets.After the proposed algorithm is implemented, the measurement of network throughput, packet delivery ratio and packet delay are determined to show that the proposed detection technique was able to deliver packets from source to destination mote at reasonable levels of network performance as compared to blackhole attack and version number attack. So, the result of the packets delivered from source to destination is analyzed that with the implementation of proposed prevention technique packet delivery ratio is increased by 8%, packet delay time is reduced from 1.71m/sec to 0.034m/sec and throughput is increased by 9%.

VI. CONCLUSION

We conclude that our proposed algorithm is very efficient in detecting the blackhole and version number modification attack. TBBVD algorithm is a common detection algorithm for both the attacks which is mainly used to detect the type of attack based on the behavior and trust between the motes. The proposed algorithm not only increases the packet delivery ratio but also decreases the delay time. We have focused on two main attacks in RPL and gave a common solution. There are other vulnerable attacks like flooding attack and overload attack in RPL which can be implemented as future work.

REFERENCES

1. P. Thubert et al., "RPL: IPv6 Routing Protocols for Low Power and Lossy Networks", RFC6550,2012.
2. Linus Wallgren , Shahid Raza , and Thiemo Voigt ,"Routing Attacks and Countermeasures in the RPL-based Internet of Things", Int. J. Distributed Sensors Networks,Vol.2013,794326,2013.
3. Mayuri A.Bhabad, Sudhir T. Bagade," Internet of Things: Architecture, Security Issues and countermeasures", Volume 125-No.14, September 2015.
4. JyotiranjanHota, Pritish Kumar Sinha, "Scope and Challenges of Internet of Things: An Emerging Technological Innovation", February 2015.
5. T. Tsao,R. Alexander,M. Dohler , V.Daza,A. Lozano, and M. Richardson," A Security Threat Analysis for Routing Protocol for Low-power and Lossy networks(RPL),"2014.
6. A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, J. Schönwälder, AStudy of RPLDODAG Version Attacks,8th IFIP WG 6.6 International Conference on Autonomous Infrastructure, Management, and Security, AIMS 2014, Jun 2014, Brno, Czech Republic. pp.92-104, 2014.
7. A. Mayzaud, R. Badonnel, I. Chrisment, A Taxonomy of Attacks in RPL-basedInternet of Things,International Journal of Network Security, Vol.18, No.3,pp.459-473, May 2016.
8. Pongle, Pavan , and Gurunath Chavan ." A Survey : Attacks on RPL and 6LoWPAN in IoT."Pervasive Computing (ICPC), 2015 International Conference on.IEEE 2015.

AUTHORS PROFILE

M.V.R Jyothisree, Research Scholar, Computer Science, Rayalaseema University,Kurnool. Papers published: 4 International journals 2 Scopus Indexed journals. Conferences: 2 International Conferences.

S.Sreekanth , Professor, Computer Science Department, SITAMS, CHITTOOR,A.P.
Emailid::pranavsree_2000@rediffmail.com
Papers published: 6 National journalsand 28 International journals. Conferences: 4 National Conferences. Consultancy: TCS ION