Performance Evaluation of RPL under Black Hole Attack and Flooding Attack in Internet of Things using ContikiOS

M.V.R JYOTHISREE [1] Dr.S.SREEKANTH [2]

[1]*Research Scholar Computer Science Rayalaseema University Kurnool A.P. India*

[2] *Professor Dept. CSE SITAMS JNTU A A.P. India*

Abstract— The Internet of Things (IoT) is a novel paradigm that is rapidly gaining ground in the scenario of modern wireless telecommunications. The basic idea of this concept is the pervasive presence around us of a variety of things or objects – such as Radio-Frequency Identification (RFID) tags, sensors, actuators, mobile phones, etc. – which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to reach common goals. RPL supports message confidentiality and integrity. Supports Data-Path Validation and Loop Detection. Security is a highly challenging issue in Internet of Things. Understanding possible forms of attacks is the first step towards developing good security solutions. The presence of malicious nodes will affect the performance and reliability of the network. **Flooding** consists of generating a large amount of traffic through DIS messages, causing nodes within range to send DIO messages (used to advertise information about DODAG's to new nodes) and reset their trickle timers(supposed to increase as the network stabilizes). Note that, if secure DIS are used, this attack can still be performed using a compromised node. **Black hole attack,** aims to drop all the packets that the malicious node is supposed to forward, combined with a sinkhole attack, it can be very damaging as it causes the loss of the whole deflected traffic. This attack can be seen as a denial of service attack

.

Keywords *- Internet of Things (IoT), RFID, RPL, Flooding and Black hole Attacks.*

I. INTRODUCTION

In our paper, we evaluated the performance of the network when there is a Black hole attack and Flooding attack while routing the Packets between the Source and the Destination node using RPL Routing protocol and simulated the results using Cooja Simulator in ContikiRPL.

6LowPAN Introduction:

1. Low-power Wireless Personal Area Networks over IPv6.
2. Allows for the smallest devices with limited processing ability to transmit information wirelessly using an Internet protocol.
3. Allows low-power devices to connect to the Internet.
4. Created by the Internet Engineering Task Force (IETF) - RFC5933 and RFC 4919.

6LowPAN Routing Considerations

1. Mesh routing within the PAN space.
2. Routing between IPv6 and the PAN domain
3. Routing protocols in use:
   1. **LOADng**
   2. **RPL**

1. LOADng Routing

1. Derived from AODV and extended for use in IoT.
2. Basic operations of LOADng include:
3. Generation of **Route Requests (RREQs)** by a LOADng Router (originator) for discovering a route to a destination.
4. **Forwarding of such RREQs** until they reach the destination LOADng.
5. Router, Generation of **Route Replies (RREPs)** upon receipt of an RREQ by the indicated destination, and unicast hop-by-hop forwarding of these RREPs towards the originator.
6. If a route is detected to be broken, a **Route Error (RERR)** message is returned to the originator of that data packet to inform the originator about the route breakage.
7. **Optimized flooding** is supported, reducing the overhead incurred by RREQ generation and flooding.
8. Only the destination is permitted to respond to an RREQ.
9. Intermediate LOADng Routers are explicitly prohibited from responding to RREQs, even if they may have active routes to the sought destination.
10. RREQ/RREP messages generated by a given LOADng Router share a single unique, monotonically increasing sequence number.

2. Routing Protocol for Low Power and Lossy Networks (RPL)

RPL Routing

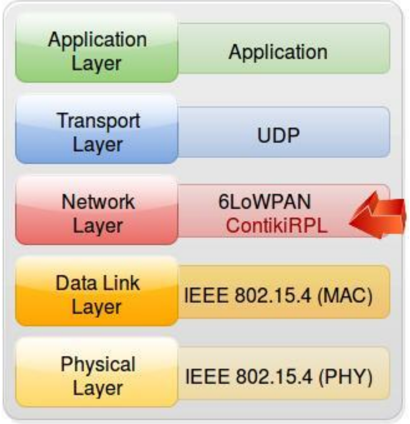

Fig 1.1: Contiki network stack (with the attacked layer highlighted)

1. Distance Vector IPv6 **routing protocol for Lossy and low power networks.**
2. Maintains routing topology using low rate beaconing.
3. Beaconing rate increases on detecting inconsistencies (e.g. Node/link in a route is down).
4. Routing information included in the datagram itself.
5. **Proactive**: Maintaining routing topology.
6. **Reactive**: Resolving routing inconsistencies.
7. RPL separates packet processing and forwarding from the routing optimization objective, which helps in Low power Lossy Networks (LLN).
8. RPL supports message confidentiality and integrity.
9. Supports Data-Path Validation and Loop Detection.
10. Routing optimization objectives include minimizing energy, minimizing latency and satisfying constraints (w.r.t node power, bandwidth, etc.)
11. RPL operations require bidirectional links.
12. In some LLN scenarios, those links may exhibit asymmetric properties.
13. It is required that the reachability of a router be verified before the router can be used as a parent.

Objectives:
The objectives are twofold:
1. Build a convenient framework for testing a malicious node into Cooja simulations.
2. Test and show the effects of some chosen attacks.

II. ATTACKS IN RPL

Security in IoT network is a highly challenging issue. For good security solutions, understanding possible form of attacks is very much required. Absence of any mechanism for detection of attacks make wireless network more vulnerable than wired network. Attacks are categorized into two type's namely external and internal attack.

a. RPL ATTACKS

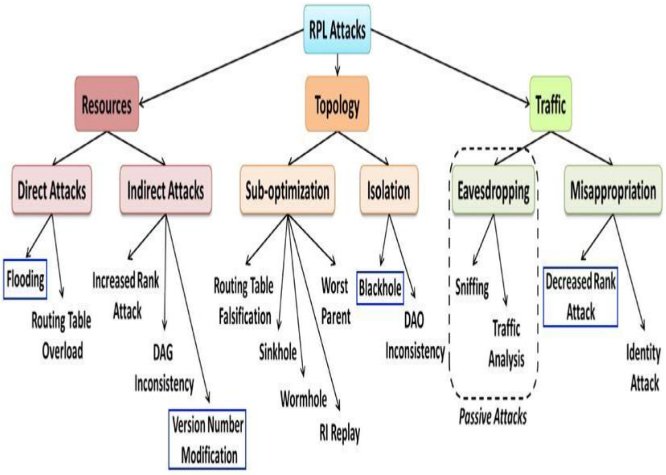

Fig: 1.2 Taxonomy of RPL attacks

The taxonomy of RPL attacks, mentions the attack we want to test.The first category concerns the **exhaustion of network resources**, meaning that malicious node's purpose is to overload the consumption of energy, memory or/and power. This can be done by forcing the legitimate nodes to perform unnecessary actions to increase the use of their resources. This may impact on the availability of the network by congesting available links or by incapacitating nodes and may therefore impact on the lifetime of the network.
This category can be further subdivided in two subcategories:
1. Direct attacks, in which the malicious node directly generates the overload disturbing the network.
2. **Indirect attacks**, in which the malicious node provokes the other nodes to make them generate the overload.
The second category holds the **attacks targeting the RPL network topology**. The goal of these attacks is to disturb the normal operation of the network. These could then cause the isolation of one or more nodes. This category can also be subdivided in two subcategories:

1. Sub optimization, meaning that the network will converge to a non-optimal form, inducing poor performance.
2. Isolation of a node or a subset of nodes, cutting them from the rest of the network and hence the root node.
The third category covers **attacks against the network traffic**. These attacks are aimed to make a malicious node introduce itself inside the network, not disturbing it's working. This leads to information leakage by eavesdropping the traffic or impersonating legitimate nodes.
This category is again subdivided in two subcategories:
1. **Eaves dropping** (passively) the information that is forwarded through the network.
2. **Misappropriation** of a node or a set of nodes, namely for tampering the legitimate exchanged information.

b. FLOODING ATTACK

- **Flooding** [Resources | Direct attack] : consists of generating a large amount of traffic through DIS(DODAG Information Solicitation) messages, causing nodes within range to send DIO(DODAG Information Object) messages (used to advertise information about DODAG's to new nodes) and reset their trickle timers(supposed to increase as the network stabilizes). Note that, if secure DIS are used, this attack can still be performed using a compromised node.

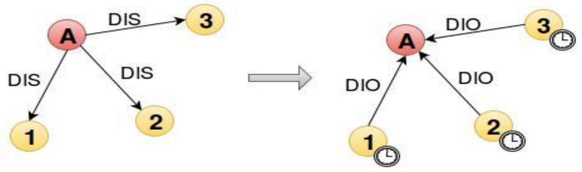

Fig: 1.3 Flooding Attack

C. BLACK HOLE ATTACK

- **Black hole [*Topology* | *Isolation]*** [6] : aims to drop all the packets that the malicious node is supposed to forward ; Combined with a sinkhole attack, it can be very damaging as it causes the loss of the whole deflected traffic. This attack can be seen as a denial-of-service attack. If the position of the node is well chosen, it can isolate several nodes from the network. The selective forwarding attack (gray hole) is a variant of this type of attack. With this variant, it is possible to do DoS attacks but the malicious node selects the packets to forward. This attack has as consequence to disturb routing paths, it can be used to filter any protocol.

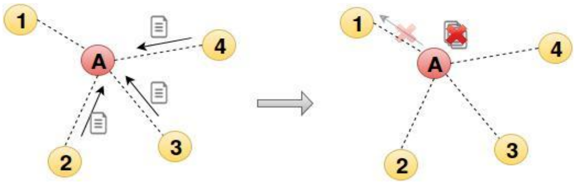

Fig: 1.4 Black hole Attack

III. ANALYSIS OF RPL ATTACKS

a. FLOODING ATTACK

While entering the WSN thanks to the ContikiRPL configuration constants set with the building block, the malicious node immediately starts sending DIS messages to its neighbors, then triggering DIO messages and trickle timers reset.

Expected Impact: No change in DAG, important energy exhaustion. After running the simulation a few (virtual) minutes, the graph looks like this:

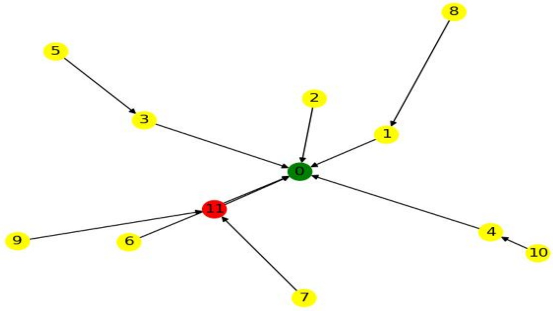

Fig 2.1 Simulation graph with Malicious node

Simulation with the malicious node, as it tells, holding the same topology but with the malicious node that can be built with a different platform (e.g. a Sky mote).As we can see, the malicious node (in red) impacts nodes 9, 7 and 6

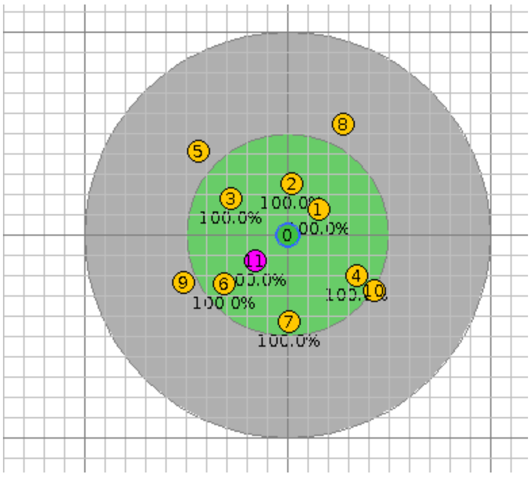

Fig: 2.2 Simulation with Malicious node

Simulation without the malicious node, holding a topology with a root and a User defined number of sensors built on a same platform.

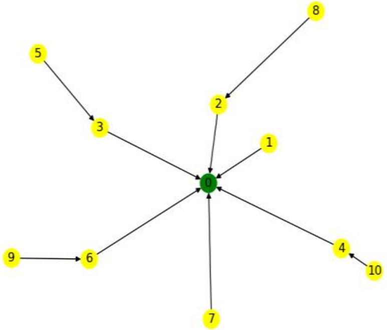

Fig: 2.3 Simulation graph without Malicious node

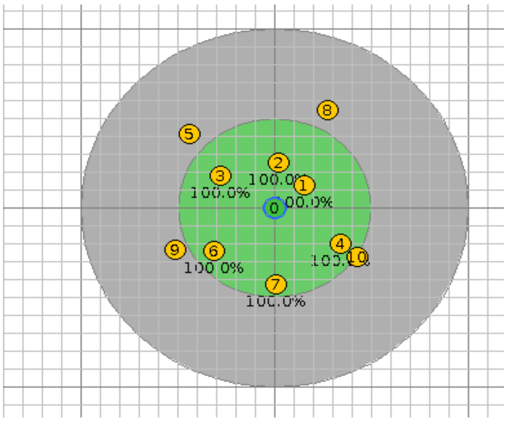

Fig:2.4 Simulation without Malicious node

b. BLACK HOLE ATTACK

The malicious node simply drops the collected application data plane messages instead of forwarding them. DAG changed, legitimate nodes in the neighborhood of the malicious node have now set it as their parent. The malicious node drops the received data plane messages.

The transformation of DODAG causes the same effect as the previous attack but also operates at the data plane by preventing hijacked messages to come to the malicious' parent node.

Efficiency: Potentially dramatic (i.e. for integrity), depending on the malicious.

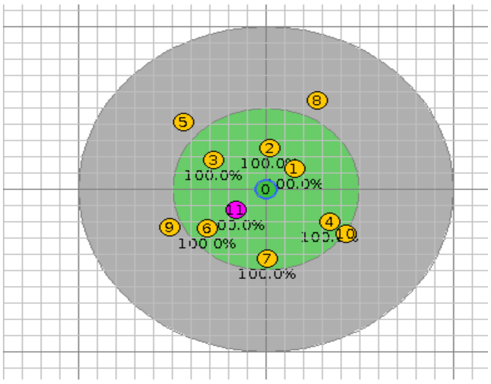

Fig: 2.5 Simulation with malicious node

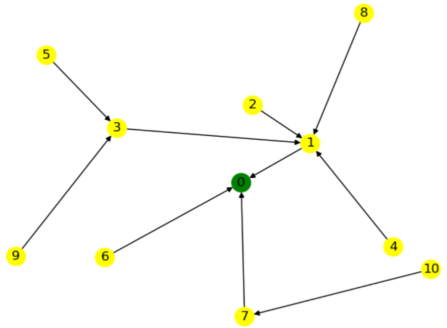

Fig: 2.6 Graph for DODAG without malicious node

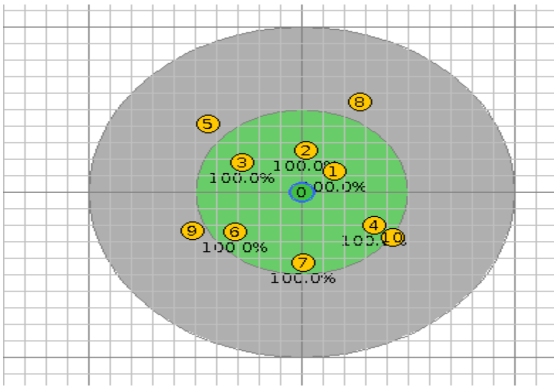

Fig: 2.7 Simulation without Malicious node

IV. PERFORMANCE EVALUATION

FLOODING ATTACK:

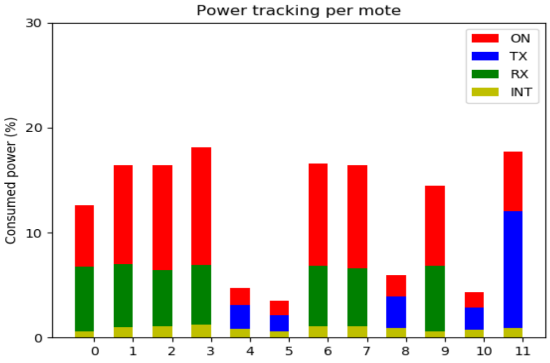

Fig:3.1 Power tracking with malicious attack

The attack efficiency using this information to compare the power consumption in the simulation with the malicious node. As it can easily be observed, nodes 0,1,2,3,6, 7 and 9 are particularly impacted by the attack in terms of ON and RX times.

Important note: However, these nodes are not impacted in term of TX time. The reason is that upon the reception of a DIS, the nodes reset their trickle timers but do not immediately send a DIO, due to the multicast nature of the sent DIS.

Variant of the attack: Another way of performing a flooding attack can be to unicast DIS to the neighbors, immediately triggering a DIO in response but not the trickle timer reset.

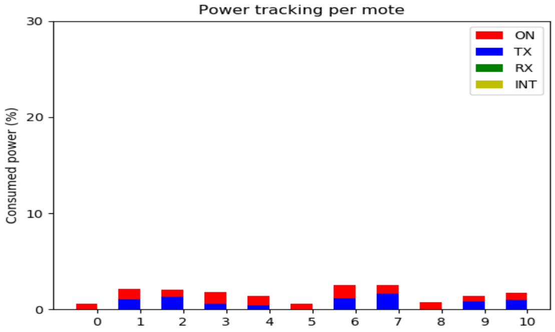

Fig:3.2 Power tracking without malicious attack

Important note: However, these nodes are not impacted in term of TX time. The reason is that upon the reception of a DIS, the nodes reset their trickle timers but do not immediately send a DIO, due to the multicast nature of the sent DIS.

BLACK HOLE ATTACK

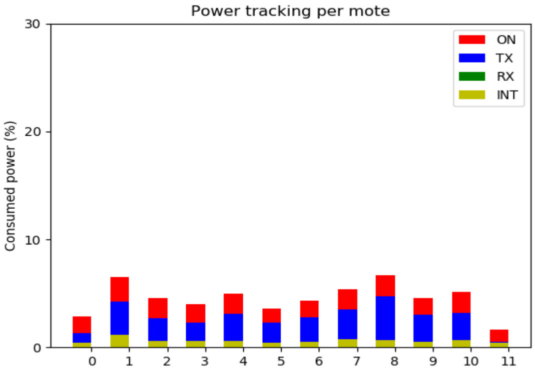

Fig: 3.3 Power tracking with malicious attack

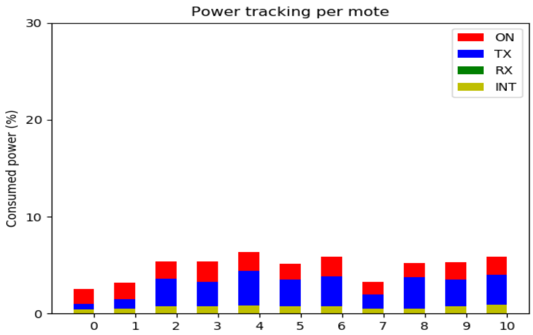

Fig:3.4 Power tracking without malicious node

V. CONCLUSION

Our first goal was to *build a convenient framework for testing a malicious node into Cooja simulations. R PL Attacks Framework is a* very promising as it already handles various interesting features for quickly designed and implementing malicious nodes.

Our second goal was to *test and show the effects of some chosen attacks*. Indeed, we have shown some relevant attacks, uniformly chosen amongst the presented taxonomy, and their expected results on some relevant WSN topologies.

VI. FUTURE WORK

Possible further improvements, regarding:

- Attack simulation test by Testing more attacks with new building blocks
- Add more WSN topology generation algorithms.
- Test a malicious node with some application level projects.
- Make the simulation support multiple malicious nodes.

REFERENCES

1.A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, J. Schönwälder, ***AStudy of RPL DODAG 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,

2.A. Mayzaud, R. Badonnel, I. Chrisment, ***A Taxonomy of Attacks in RPL-based Internet of Things***,International Journal of Network Security, Vol.18, No.3, pp.459-473, May 2016.

3. A. Sehgal, A. Mayzaud, R. Badonnel, I. Chrisment, J. Schönwälder, ***Addressing DODAG inconsistency attacks in RPL networks***,Global Information Infrastructure and Networking Symposium (GIIS), 2014, Sep 2014, Montreal, QC, Canada. pp.1-8, 2014.

4.K. Chugh, A. Lasebae, J. Loo, ***Case Study of a Black Hole Attack on 6LoWPAN-RPL***, SECURWARE 2012 : The Sixth International Conference on Emerging Security Information, Systems and Technologies, 2012.

5.L. Wallgren, S. Raza, T. Voigt, ***Routing Attacks and Countermeasures in the* RPL-Based Internet of Things** ,International Journal of Distributed Sensor Networks, Volume 2013, Article ID 794326, 11 pages, 5 June 2013.