Analysis of Version and Dis Attack in IPV6 Vera Routing Protocol for IOT for Low Lossy Networks

K.R.R.Mohan Rao, N. Jaga Jeevan P.Subba Rao, A.naga raju

Abstract: ***The concomitant offers a survey of the writing which will be divided into four elementary areas. The initial phase displays a general portrayal of what's understood by the net of things and its applications. It likewise offers a summation of the Central Intelligence Agency cluster of 3 model to any orall the additional probably comprehend the essential security factors that IoT devices should face, even as their problems and difficulties. The second half introduces a compendious portrayal of the structure within which RPL is connected to urge a superior comprehension of the task, even as the difficulties that the convention should face. developing next is Associate in Nursing itemized summation of RPL, with distinctive accentuation on its choice of words, topology development, management messages, and security parts which will facilitate see however the guiding convention functions. This space can likewise be a key angle to in all probability break down and assess the distinctive types of attacks against WSN utilizing RPL. At long last, we have a tendency to gift a general portrayal of the foremost essential security attacks against WSN utilizing RPL, what methods are utilised and conceivable countermeasures and aversion methods to remain faraway from or alleviate these attacks.***

Keywords : iot,rpl attacks,VeRA,dis,version,contiki os,cooja,

I. INTRODUCTION

1. RPL: IPv6 Routing Protocol for LLNs

The incidental to provides a survey of the writing that may be divided into four basic areas. The initial phase displays a general portrayal of what's silent by the net of things and its applications. It likewise provides a summing up of the Central Intelligence Agency cluster of 3 model to all or any the a lot of possible comprehend the essential security factors that IoT devices should face, even as their problems and difficulties. The second half introduces a compact portrayal of the structure during which RPL is connected to induce a superior comprehension of the task, even as the difficulties that the convention should face. arising next is Associate in Nursing itemized summing up of RPL, with distinctive accentuation on its formulation, topology development, management messages, and security elements which will facilitate see however the guiding convention functions. This space can likewise be a key angle to in all probability break down and assess the distinctive varieties of attacks against WSN utilizing RPL. At long last, we have a tendency to gift a general portrayal of the foremost important security attacks against WSN utilizing RPL, what ways are used and conceivable countermeasures and aversion methods to remain aloof from or alleviate these attacks.

II. TPROBLEMTSTATEMENT

As demonstrated above, remote sensors are devices that have restrictions in equipment and CPU handling, accompany low memory and oversee low speed information. Moreover, given their temperament, they have a vitality constraint, since they can regularly just be furnished with little batteries or restricted vitality sources. In this manner, the span of the sensor hub depends to a huge degree on the term of the battery. Therefore, remote sensor systems could be truly influenced by hubs that show battery consumption regarding topology changes, parcel redirection, and course changes.

III. TSIMULATIONTENVIRONMENT

As it was shown in the literature review in section 2.2.3, there are a wide range of IoT operating systems due to the sensors heterogeneity and the rapid change that IoT devices are suffering. Therefore, it must be chosen a platform that may comply with the aims and objectives of the project.

Instant Contiki is a complete Contiki development environment running within an Ubuntu Linux virtual machine (Ubuntu 14.04 LTS that has all the compilers, development tools and simulators needed to the study.

IV. NETWORKTDESIGNTSETUPTANDTPARAMETERS

Motes

It should be created the different motes that will conform the testbeds. It will use the motes firmware within the rpl-

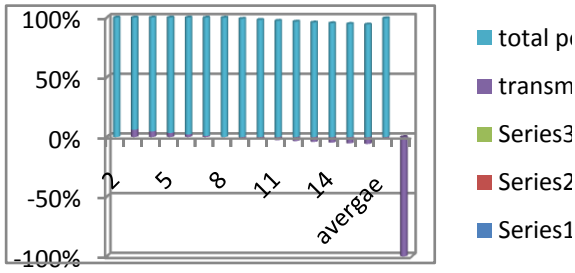
collect directory due to Contiki collect view (Java module integration that collects power consumption motes, ETX values among others (reference) is already implemented. It provides power indicators among others (reference). The implementation study will be based on Tmote Sky

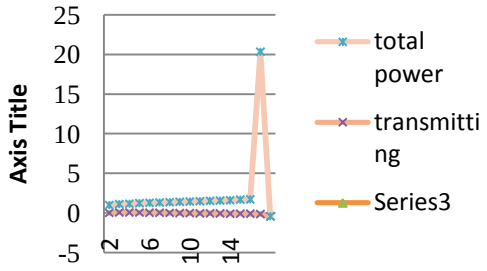
nodes firmware acting in different roles:
Sink mote -
The sink mote will operate as a destination point where leaf nodes will send their collected data. It will also act as the DODAG router of the network and there will be just one. The code path is located at *~/Contiki/examples/ipv6/rpl-collect/udpsink.c*
Leaf mote -
The leaf motes will operate as data collectors. A mote will send its data to its preferred parent until data eventually reaches the sink node. The code path is located at *~/Contiki/examples/ipv6/rpl-collect/ udp-sender.c* Malicious mode –
The malicious node will perform the attack will be meant to do. It will keep the same code as a leaf node, but there will be changes in how rpl works
modifying the rpl core files located at *~/Contiki/core/net/rpl/*. To keep the routing protocol unaltered for the rest of the nodes, it will create a Contiki instance for each malicious node5.

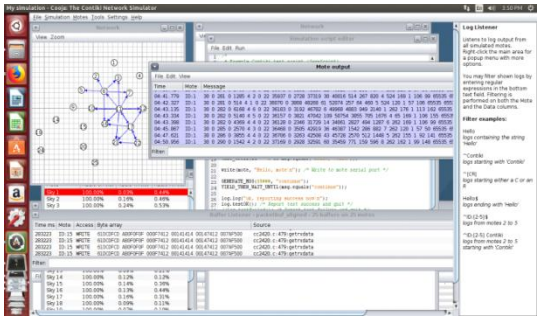
Radio environment and layout

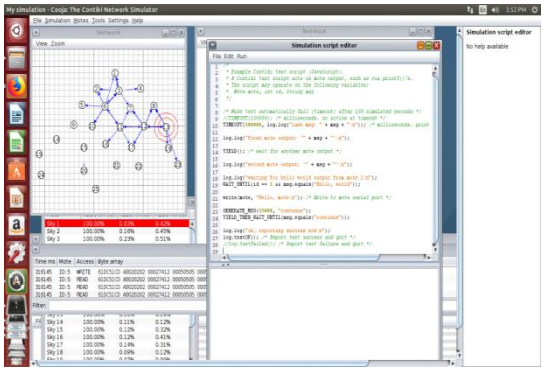
Cooja simulator allows to simulate different radio environments as well as the area where nodes will be spread around. In order to gain a better understanding of these parameters, they are briefly explained as follows:
Radio medium: Radio medium refers to radio surrounding behaviour. Due to Cooja is a software-
based simulator, it does not consider external interference as a real device does. Using *Unit Disk Graph Medium (UDGM): Distance Loss* channel model, Cooja simulator degrades the signal quality according to the distance between nodes and , therefore, provides realism to the simulates motes

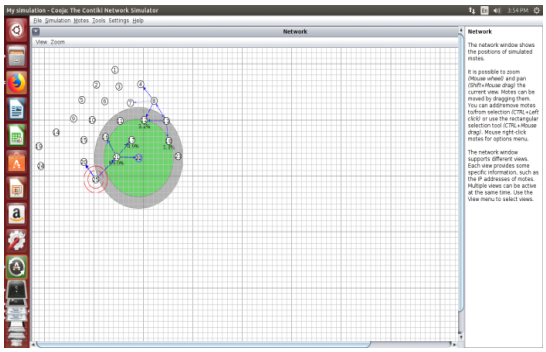
Transmission range: It refers to the transmission range of the node. Cooja simulator presents it through a green circle. All the nodes within that range will be able to communicate among each other. Tmote sensors devices work within that range
(Moteiv, 2006). Simulations will keep the default value of it (50 meters).







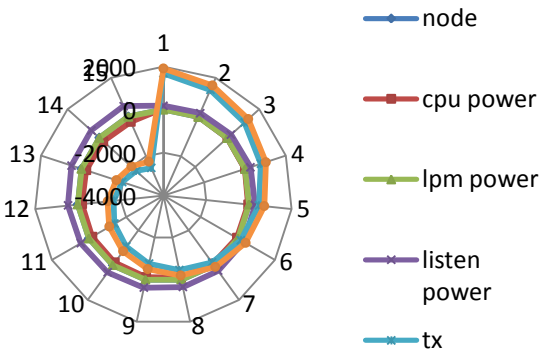




5.3 DIS Attack

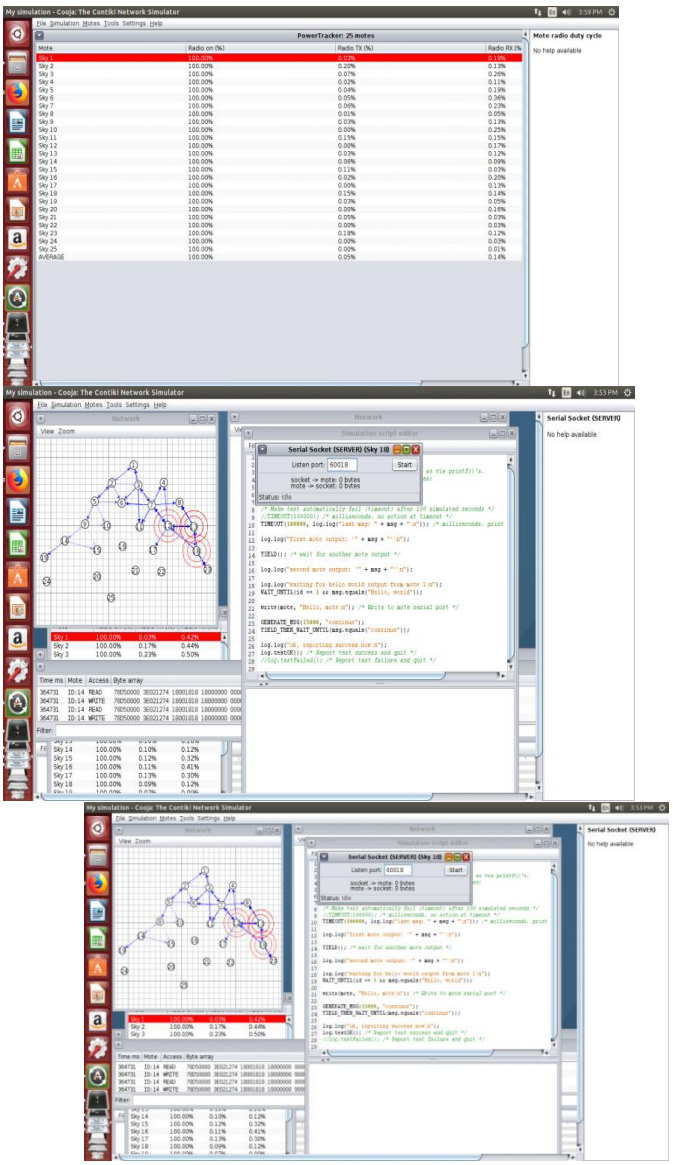
As detailed before in section 4.4, DIS attacks aim at sending DIS control messages in order to cause disruption on the network and, in the worst-
case scenario, to provoke
node resource exhaustion. Firstly, it will be shown the results obtained after running
the simulation with a malicious node to subsequently p

roceed with the analysis of the data compared to the baseline. Eventually, a solution or countermeasures will be considered to tackle the problem and, whenever p ossible, they will be implemented in Cooja.



Version Attack

2. A version attack aims at publishing a higher version number of the DODAG in order to provoke inconsiste ncies in the network. Due to differences in the versio n number, RPL
3. triggers a global repair to create a new DODAG. As a result, there will be traffic
4. overload and increase in the nodes power consumption (Sharma et al., n.d.).Firstly, it will be shown the resu lts obtained after running the simulation with a malici ous node o subsequently proceed with the analysis of the data compared to the baseline.
5. Eventually, a solution or countermeasures will be cons idered to tackle the problem and, whenever possible, t hey will be implemented in Cooja.



mechanisms.

V. CONCLUSION

Through an extensive literature review, it was prese nted RPL as an efficient routing protocol for WSN. It was outlined the types of con trol messages used to determine the topology formation, maintenance, paths routes as wel l as which repair mechanisms employed when loop messages or inconsistencies in the network happened. However, it was discovered t hat RPL presents weaknesses regarding security. Alt hough the standard contemplates a security version of these messages to secure communications, they are not deployed yet. In additi on, it was noted that most of the studies with regard of RPL insisted relying on diffe rent layers of the protocol stack to

secure communications as RPL does not provide rea l solutions. At this point, the study was focused on researching the RPL well-known attacks. Those attacks would be effective when either security on different layers we re bypassed or security measures were not implemented.

REFERENCES

1. A. Conta, Deering, S., M. Gupta, E. (2006). RFC 4443:Internet Control Message
2. Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Sp ecification. RFC
3. Airehrour, D., Gutierrez, J., & Ray, S. K. (2016). Secure routing for internet of things:
4. A survey. Journal of Network and Computer Applications, 66, 19 8–213.
5. https://doi.org/10.1016/j.jnca.2016.03.006
6. Chen, Y., Chanet, J.-P., Hou, K.-M., Shi, H., & De Sousa, G. (2015). A Scalable Context-Aware Objective Function (SCAOF) of Routing Protocol for Agri cultural Low-Power and Lossy Networks(RPAL).
7. D'Hondt, A., Bahmad, H., & Vanhee, J. (2016). RPL Attacks Fr amework. Retrieved
8. from https://github.com/dhondta/rpl-attacks/blob/master/doc/report.pdf
9. Dodig-crnkovic, G. (2002). Scientific Methods in Computer Science. Co mputer (Long.Beach. Calif)., Methods in Computer Science.pdf
10. Dodis, Y., Kiltz, E., Pietrzak, K., & Wichs, D. (2012). Message Authentication, Revisited
11. Dohler, M., Daza, C. V, & Lozano, A. (2012). draft-ietf-roll-security-framework-07 - ASecurity Framework for Routing over Low Power and Lossy Networks.
12. 9.Dohler CTTC Daza A Lozano Universitat Pompeu Fabra M Ri chardson, M. V. (2015).
13. RFC 7416 - A Security Threat Analysis for the Routing Protocol for Low-Power
14. and Lossy Networks …RPLs—.
15. 10.Dunkels, A., Schmidt, O., Finne, N., Eriksson, J., Österlind, F. , & Durvy, N. T. M.(2011). The Contiki OS: The Operating Sys tem for the Internet of Things.
16. 11.Dvir, A., Holczer, T., & Buttyan, L. (2011). VeRA - Version number and rank
17. authentication in RPL. Proceedings - 8th.