International Journal of Computer Science and Engineering Communications,
Volume.5, Issue.5 (2017): Page.1715-1721
www.ijcsec.com

Addressing Attacks and Security Mechanism in the RPL based IOT

V.K.Karthik[1] and M.Pushpalatha[2]
[1]PG Scholar, [2]Professor,
[1,2]Department of Computer Science and Engineering, Faculty of Engineering and Technology,
[1,2]SRM University, Kattankulathur- 603203, Kancheepuram District, Tamil Nadu, India
karthik_kumar93@srmuniv.edu.in[1], pushpalatha.m@ktr.srmuniv.ac.in[2]

Abstract: *Addressing and Mitigating the Routing Attacks in the RPL (Routing Protocol for Low Power and Lossy Networks) based IOT (Internet of Things) is challenging endeavor. RPL is peculiar for the IPv6, which is concerned to substitute IPv4 to overcome the long-lasting foretell problem of IPv4 address lethargy. The RPL protocol, contradict more functions while running on the support less devices. Through this prolonged severe behavior leads to the attack in the network topology constraints. The objective of the paper is to address the Rank Attack which has significant performance degradation in the network. This Attack creates a fleeting change in a network to diverse the regular paths and stop sending packets to the sink (destination). A Mechanism is proposed to mitigate the attack which leads to secure communication from source to destination. Due to secure communication, the packet delivery ratio is increased to 90% and above with a trade-off in latency.*

Keywords: *RPL, IOT, IPv4, IPv6, Rank Attack, Cooja Simulator, Contiki Operating System.*

1. Introduction

The Routing Protocol for Low Power and Lossy Networks (RPL) is an optimistic routing protocol for the WSN (Wireless Sensor Networks), because the devices are connected to the various internet enabled systems. Preferably, the RPL [1] is capable of identifying the devices which the communication links are not proper according to their nodes. In the family of Low Power and Lossy Networks [2], routers are constrained with operations such as power trace, energy efficiency, in order to process their interconnect networks. Even the interconnects have the characterized by the constraints such as lack of data rates, stability less, loss rates. The Low Power and Lossy Network [4] have the capability to constitute with more routers. RPL supports the variant traffic flow mechanisms comprising with point-to-point (internal connected devices), point-to-multipoint (the central point of control enabled device to the subset of internal devices) and multipoint-to-point (the subset of internal devices to the central point of control enabled device) traffics [9]. The Internet of Things (IOT) is the combination of multiple objects, such as Smart Devices, Embedded Devices, Electronic Bugs, Sensors and Transducer actuated systems connected to a network that enables the devices to receive and transmit the data with interpretability. The IOT [10] enhances the capability of the devices to controllable over the network for the greater flexibility, performance, cost-effective utility and optimistic results. Physical World amalgamation of sensing devices to the computer network creates the IOT as the most empowering technology across the entire network enabled technologies [5]. The IOT becomes the instance, when comparing with the electronic communication devices and the virtual reality which could also overcome the technologies such as the smart grids, cities, homes.

2. RPL Protocol

The RPL is designed and implemented to meet the specific objectives of constrained devices of IOT. The constraint includes the minimal memory, limited power for processing, energy when the device needs more operations while deployment or inter processing. These phenomenal characteristics invokes the protocol to a greater challenges in routing properties, processing mechanism, protocol design, secure reliable considerations and their internal functionalities.

2.1 RPL Functionality

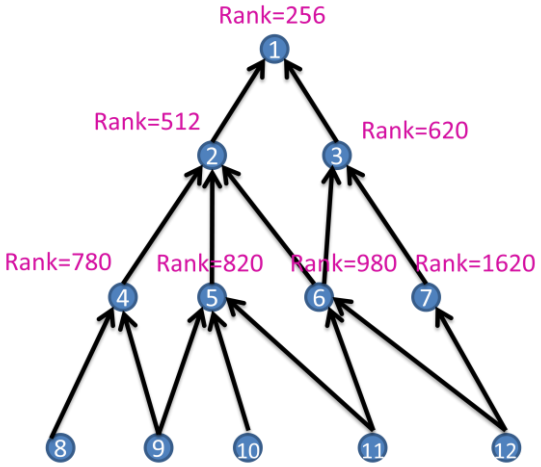

Fig. 1: The strategy of the best parent selection topology in the RPL.

RPL follows the DODAG (Destination Oriented Directed Acyclic Graph), which constitutes of DIO (DODAG Information Object). Each node intimates the information periodically through this DIO to the subsequent node or neighbor node. Mostly, the information is DODAG ID, RPL Instance ID and necessary relevant information corresponding to the DIS (DODAG Information Solicitation) request. In RPL, the best parent node selection [7] is always based on the rank of the nearby nodes by the child node. The Rank is governed by the following equation 1 calculation, which consists of ETX of the node (Expected Number of Transmissions, done by the node) and the base rank (rank of the root node) of the node.

$$Calculation\ of\ Rank = ETX\ of\ the\ node + Base\ Rank\ of\ the\ node \qquad (1)$$

After the best parent selection, child node continues the procedure of sending the data packets through this parent node as the next hop. In the Figure 1, the parent node receives the data packets and recognizes its child node with the generated DAO (Destination Advertisement Object) message of the particular child node. This parent node further sends the data packets to the concern subsequent or neighbor another parent node until it reaches to the destination.

2.2 Addressing Attacks against RPL

Generally, in the most of the IOT interoperation deployments rely on the RPL, specifically in the Network Layer protocol stack. While running RPL on the network layer it should follows some strategic operations as well as the security capabilities over the communication links from the various

counter attacks. Severer Consequences will takes place after the every counter injected attack in the network layer over WSN. Each of the attack can injected through significant malicious routing topologies to disorganize the entire network routing paths.

2.2.1 Rank Attack

The RPL encounters an attack often while in routing the packets from source to destination. These circumstances eventually occur through a rank of a node, known after a severe threat problem in the RPL. Rank Attack should easily diverse the routing paths as much as possible with greater tendency, due to the requirement of the neighbor nodes of the network. Loss of packet is directly proportional to the attack based on the rank while in the regular paths of a network. In RPL, the child node always prefer to parent node based on the rank of the neighbor node. It means, if a particular child node need to choose a parent node to manage the quality of services. It prefers to the node which is having the low rank (numerically low) to send a data packet. The Rank is the criteria for a node to check, whether to select as a parent node. The Rank is calculated by the Base rank plus the ETX (Expected Number of Transmissions). The base rank is the rank of the first parent node. Always the Rank of the initial parent node in RPL is 256 by default.

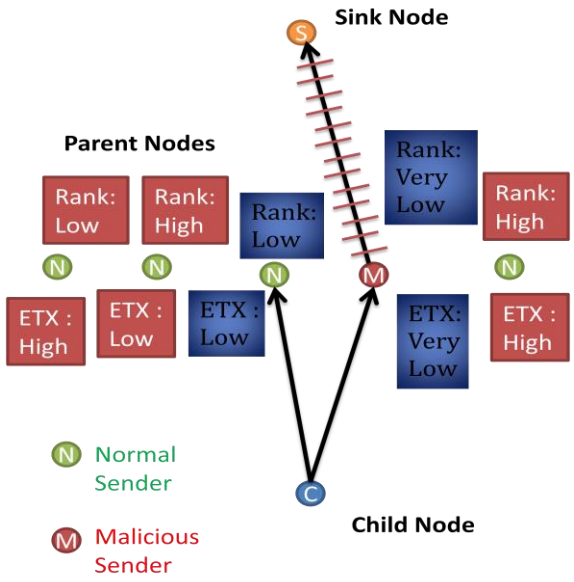

Fig. 2: The Occurrence of Rank Attack by choosing the malicious sender parent node.

The Rank Attack constitutes the rank of the deeper child nodes of a network topology to create an attack. Based on the rank calculation, the child nodes should have the high ranks (numerically high). In the Figure 2, if reduce the rank of the particular deeper child node, certainly the neighbor node should choose this particular deeper child node as the parent node to send the data packet to sink. Once the packet is forwarded to the particular deeper child node from the neighbor node, it drops the packet. Hence, that particular deeper child node is treated as the malicious node of the network topology. In this way, the rank attack can be formed through the network topology to disrupt the data delivery path. Through this diversion from the malicious node the data delivery should be low to the sink. Certainly, it affects the Packet Delivery Ratio (PDR) of the network by dropping packets at the intermediate level of the nodes which is malicious. It affects the following factors of the network constrained properties like Through-put, Latency, Energy Consumption and Data Rate.

The ETX of the particular malicious nodes is inversely proportional to the neighbor nodes ETX of the network topology. The constraint behind this ETX is, while forwarding the packet from the neighbor node to the malicious node, the malicious node receives the packet and drops the packet. So the expected number of transmissions is inversely proportional to the neighbor nodes, because of not sending the packet to the sink.

3. An Approach to Address Rank Attack in RPL

3.1 Implementation of Security Mechanism to Mitigate the Rank Attack

The Security Mechanism [6] is the analyses of the ETX of parent nodes without malicious and the ETX of parent nodes with malicious. First, we will analyze the parent nodes ETX difference which is without malicious. Second, we will analyze for with including malicious parent nodes difference. Certainly, the difference of the malicious parent node is very high compare to the without malicious parent nodes. In the Figure3, the reason behind the more ETX difference is, generally in RPL the node which is having the low rank (numerically low) is direct proportional to the ETX. The parent node which is having the higher rank should hold higher ETX.

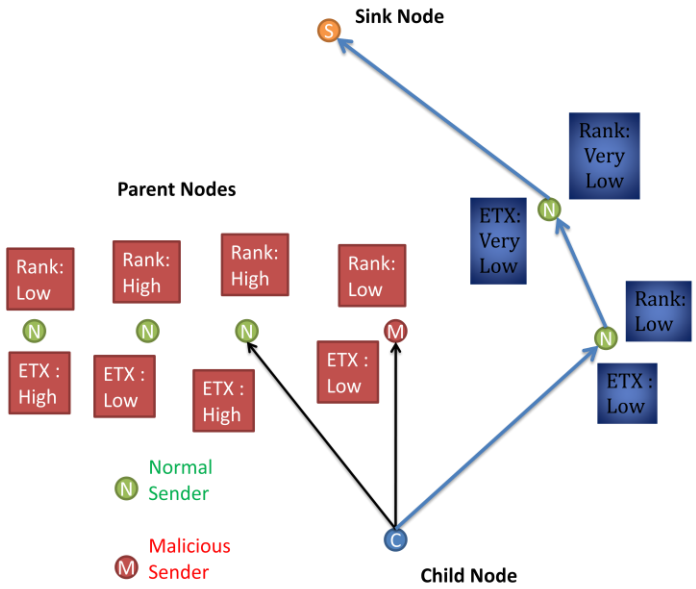

Fig. 3: The optimistic routing path after the mitigation of rank attack by the security driven mechanism.

Hence, with the differences of two ETX‘s will raise to a threshold value to fix. If the difference of the nodes ETX would cross the threshold [3], the lower ETX parent node should be the malicious node. Once, the neighbor node or child node notice the malicious node, it never chooses that for parent to send data packet to sink. In this way attack can be mitigated from the network.

4. Simulation Analysis

In the simulation (cooja with contiki OS [8]), it is having the receiver and sender motes.
1. One mote is Sink (1st mote)
2. Nine motes are normal Sender (2 to 10 motes)

3. Three motes are malicious Sender (11th, 12th, 13th motes)

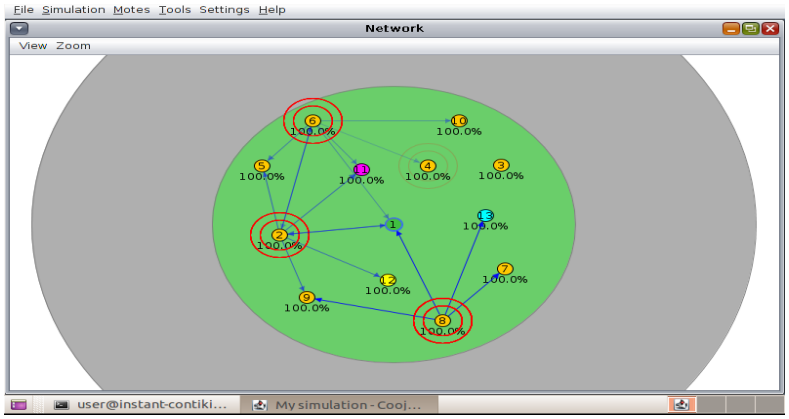

Fig. 4: The network topology of 11, 12 & 13 as malicious in simulation.

In the Figure4, the malicious node receives the packet from the neighbor node to drop the packet but it acknowledge as data is being send to the sink. Through this packet loss, PDR reduces and the quality of data should be the worst to leads as duplication of data.

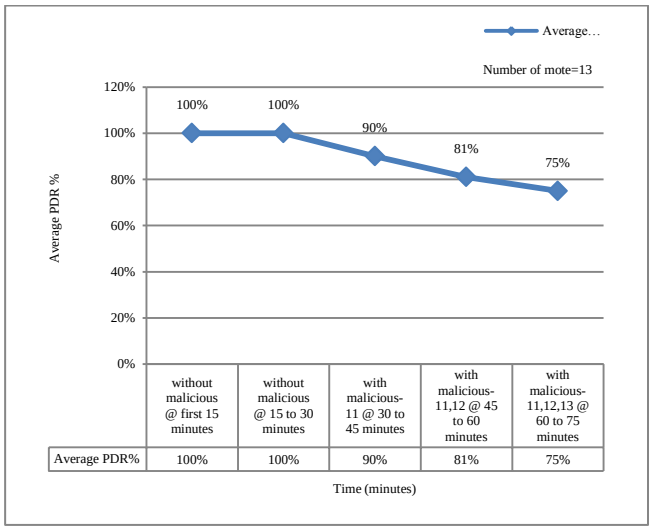

Fig. 5: Time Vs Average PDR of 11, 12 & 13 as malicious in simulation.

In the Fig.5, the packet delivery ratio is maximum when the simulation of no malicious motes. After the invocation of the malicious motes the packet delivery ratio decreases and while increasing the malicious motes the packet delivery ratio goes on decreasing.

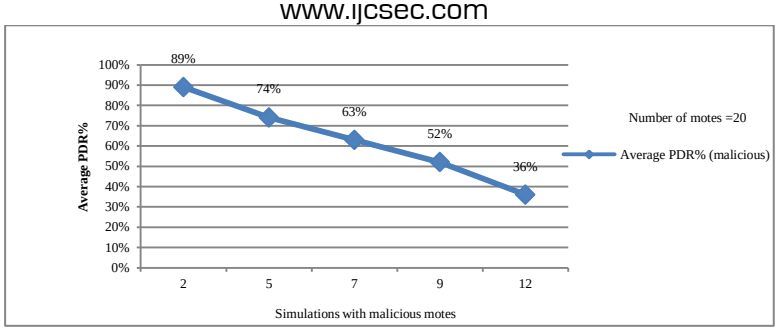

Fig. 6: Simulations with malicious motes Vs Average PDR.

In the Fig.6, the packet delivery ratio gradually decreases due to the invocation of the malicious motes enhancement with increase in simulation. In the simulation process, the time maintained for the each and individual network topology is consistent over a period of time.

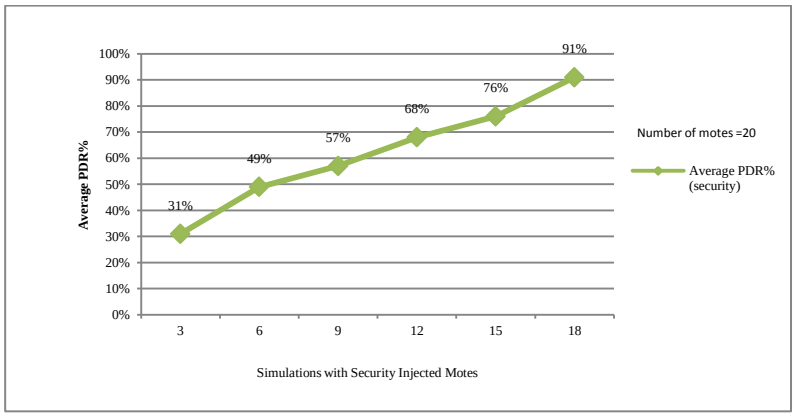

Fig.7: Simulations with Security Injected Motes Vs Average PDR.

In the Fig.7, the packet delivery ratio is low at the initial due to only the two motes are injected with the security mechanism. The malicious motes degradation is carried out by injecting the security motes as many as possible, in order to get the packet delivery ratio. After the enhancement of security driven motes; the through put increases with the increase of the security injected motes in the network. The through put should attain the optimum level of improvement with the invocation of specific objective function in the mechanism. The objective function considered in the security mechanism is completely relying on the routing metric in performance criterion. The through put is directly proportional to the balancing of the number of packets sent for transmission and the number of packets has received. The packet delivery ratio increases after the combat of attacks with security driven motes injection in the simulation.

5. Conclusion

RPL protocol is vulnerable to different routing attacks; hence it needs an efficient security mechanism. In our paper, we mitigate Rank Attack which has significant performance degradation in the network. To mitigate the rank attack, a security mechanism is implemented, so that a reliable routing path is taken from source to destination. In other words, nodes participation in routing are all secured to handle rank attack. By implementing this mechanism, packet delivery ratio is substantially increased and therefore performance of the network is not degraded.

REFERENCES

[1] T. Winter, P. Thubert, A. Brandt et al., "RPL: IPV6 routing protocol for low-power and lossy networks," RFC 6550, March 2012.

[2] N. Kushalnagar, G. Montenegro, and C. Schumacher, "IPv6 over low-power wireless personal Area networks (6LoWPANs): overview, assumptions, problem statement, and goals," RFC 4919, 2007.

[3] S. Raza, S. Duquennoy, T. Chung, D. Yazar, T. Voigt, and U. Roedig, "Securing communication in 6LoWPAN with compressed IPsec," in Proceeding of the 7th IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS '11), Barcelona, Spain, June 2011.

[4] T. Kothmayr, C. Schmitt,W.Hu, M. Brunig, and G. Carle, DTLS Based Security and Two way authentication for the Internet of Things, Ad Hoc Networks, 2013.

[5] S. Raza, D. Trabalza, and T. Voigt, "6low-pan compressed dtls for coap," in Proceeding IEEE 8th International Conference of Distributed Computing in Sensor Systems (DCOSS '12), pp. 287-289, IEEE, 2012.

[6] S. Raza, S. Duquennoy, J. H¨oglund, U. Roedig, and T. Voigt, Secure Communication for the Internet of Things— A Comparison of Link- Layer Security and IP sec for 6LoWPAN, Security and Communication Networks, John Wiley & Sons, 2012.

[7] O. Garcia-Morchon, R. Hummen, S. S. Kumar, R. Struik, and S. L. Keoh, "Security Considerations in the IP- based Internet of Things," March 2012.

[8] A. Dunkels et al., "The contiki operatingsystem," 2012, http:// www.sics.se/contiki/.

[9] N. Tsiftes, J. Eriksson, and A. Dunkels, "Low-power wireless IPv6 routing with Contiki RPL," in Proceeding of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN '10), pp. 406-407,ACM, April 2010.

[10] Z. Shelby, K. Kartke, C. Bormann, and B. Frank, "Constrained application protocol (CoAP)," draft-ietf-core-coap- 12, October 2012.