Rank Attack using Objective Function in RPL for Low Power and Lossy Networks

Abdul Rehman
Dept. of Computer Science
Bahria University
Islamabad, Pakistan
Abdul.mul103@gmail.com

Meer Muhammad khan
Dept. of Computer Science
Bahria University
Islamabad, Pakistan
Meer.khan78@gmail.com

M. Ali Lodhi
Dept. of Computer Science
Bahria University
Islamabad, Pakistan
Alilodhi30@gmail.com

Faisal Bashir Hussain
Dept. of Computer Science
Bahria University
Islamabad, Pakistan
faisalbashir@bahria.edu.pk

***Abstract*—**The Routing Protocol for Low power and lossy network (RPL) is recommended by Internet Engineering Task force (IETF) for IPv6 based Low Power Personal Area Network (6LoWPAN). RPL is a proactive routing protocol for Internet of Things (IoT) that has applications in smart homes, smart cities and smart world. RPL creates a Directed Acyclic Graph (DAG) of the network topology. Rank in a primitive construct in RPL and it defines the relative position of node within the DAG. It is used for topology formation, maintenance and prevention of loops in routing paths. Few internal attacks are identified in existing literatures which maliciously use the rank property within RPL networks. In this paper, we introduce a new rank attack in RPL networks that modifies Objective Function (OF) along with rank value. The OF is used by RPL nodes to select forwarding nodes based on application defined routing metric e. g., expected transmission count, residual energy etc. The proposed rank attack is more distractive in nature because the attacking node can easily force its neighboring nodes to route their data through the attacking node. Comprehensive simulation analysis has shown that the proposed rank attack can be used to introduce false routing path for decreasing network throughput and increasing latency of communication.

Keywords—IoT, LLNs, RPL, Rank attack, Internal threat.

I. INTRODUCTION

Low power and Lossy Networks (LLNs) are used for data acquisition in industrial monitoring, health care, home automation, security and military surveillance etc. LLNs are categorized as a type of Wireless Personal Area Networks (WPAN). RPL is the underlying routing protocol for 6LoWPAN. RPL is recommended by IETF to be used in Internet of Things (IoT). IETF has emphasized the use of RPL because it outperforms other wireless and ad hoc routing protocols in term of quality of service (device management and efficient energy saving performance) for LLNs [1]. RPL creates a directed acyclic graph (DAG) of the network topology for routing. Research efforts are made to evaluate the performance of RPL in different network scenarios and topologies for LLNs [1]. RPL provides some solutions for securing communication between devices however various internal attacks are recently highlighted [2].Rank attack is one of the most critical attacks that can be launched over RPL. It is a variation of sinkhole attack [3] in ad hoc networks. Rank in RPL is the relative distance of a node from the DAG root (sink). Rank of node increases downstream and decreases upstream. Rank of a node in RPL serves multiple purposes apart from distance to the sink, it ensures route optimization, prevent loops, and manages control overhead. In a rank attack, a malicious node advertises false rank information (lower rank than neighboring nodes) to its possible child nodes. As result, neighboring nodes select the malicious as their next hop node for routing information to the sink node. This attack can have very adverse impact on the operation of network if it is launched near the sink [3].

The Objective Function (OF) in RPL determines how RPL nodes select the optimal path towards the DODAG root in a network. For example, RPL nodes can select the Expected Transmission Count (ETX) as a routing metric. In this case, all the nodes in the network can select OF that selects next hop node based on minimum ETX. A RPL node joins DAG finds a set of parents (neighbors) and then selects the preferred parent with the help of both rank and the defined OF. Rank attacks [3, 4, 5] introduced in existing literatures do not exploit the vulnerabilities available in objective function and have a very limited impact on the network performance. In this paper, we introduce a new rank based attack, in which the adversary announces both false rank and routing metric value to increase the severity of the attack. The proposed attack is termed as Rank Attack using Objective Function (RAOF) and it is capable of maliciously forcing the neighboring nodes of the attacker to create routing paths through the attacking node. RAOF is a more powerful and successful attack as compared to the existing rank attacks.

The rest of the paper is organized as follows. Section II describes the basic operation of RPL. Section III discusses the literature review and Section IV presents the network model used for RAOF attack. Section V presents the proposed RAOF attack and Section VI provides the detailed simulation analysis. Last section VII concludes this paper.

978-1-4673-8743-9/16/$31.00 ©2016 IEEE

II. RPL Operation

RPL is proactive and distance vector routing protocol for LLNs which creates a DAG of the network devices [6]. DAG topology can be divided into multiple DODAGs (Destination Oriented Acyclic graph) where each DODAG consist of a sink and many tiny sensor nodes. DODAG topology formation is triggered by the DODAG root node. RPL uses different control message that are periodically transmitted by network devices using trickle timer [7].DIO (DODAG Information Object) message transmitted from DODAG sink node to DODAG sensor nodes. DIO messages are responsible for topology formation and maintenance, DAO (DODAG Advertisement Objet) message is forwarded in upwards from DODAG sensor nodes to DODAG sink node and using these messages the sink updates its view of the network. The DIS (DODAG Information Solicitation) is used by new node to join a DODAG topology.

The flow of DIO and DAO messages are shown in Figure 1.

Rank of a node in RPL is represented as a scalar number which depicts the location of that node within the DODAG. The rank property helps to avoid and detect loops formation. Also, forwarding node selection can be performed only on the basis of rank of the nodes. In particularly the rank of the nodes must monotonically increase from sink to leaf nodes in downwards direction and it must decrease in the same way in upwards direction to the sink node.

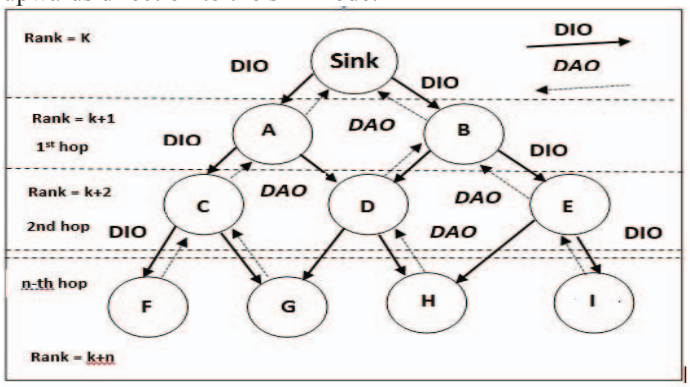

Figure 1: Control messages in RPL network

III. Related Works

Existing rank attack [4] has the objectives of making attacking node lucrative to neighbouring nodes for the next hop selection. Apart from converging and routing the traffic through attacking nodes similar attacks [3, 5] are introduced in RPL in which the adversary selects suboptimal forwarding nodes.

To the best of our knowledge the only pure rank attack on RPL is introduced in [4]. The attack is similar to sinkhole attack [8] in ad hoc networks. The work assumes a network topology that is created only on the basis of rank metric and no other routing metric is considered. The attacking node joins the network and suddenly announces a lower rank value than its neighbouring nodes. As a result, the neighbouring nodes select the attacking node as their preferred parent and they further announce this network change to their child nodes. However, in RPL based networks, it is recommended to use OF [9] using some routing metrics because otherwise the topology will be created only on the basis of hop count. If the attack presented in [3] is launched in RPL network that also uses OF along with rank then the attack will not be successful in attracting neighbouring nodes.

In [3] attacking nodes do not change the rank rules and behaves as a totally legitimate node but it only selects the worst forwarding node as its next hop node (preferred parent). This attack is hard to detect. The worst parent selected can have longer path to the sink. As a result latency increases and throughput of the network is partially affected. However, the attack proposed in [3] does not significantly change the network performance and only nodes routing through the attacking node are affected. For a malicious node to join and launch an attack presented in [3] may not be possible after network is established because the attacking nodes does not change the rank rules, therefore it cannot attract neighbours to select the attacking node as preferred parent node.

In [5] preferred parent based attack is introduced that is similar to [3] only the attacking node selects the next best preferred parent as its forwarding node. The impact of this attack on network performance is less than worst parent selection attack discussed in [3]. However, it is even harder to detect this attack as compared to the worst parent attack presented in [3].

IV. Network Model

In this section, basic network assumption, definition and network characteristic are discussed. All network nodes considered are homogeneous in terms of communication range. Sensor nodes are densely deployed where data is reported in a multi hop fashion. It is further assumed that the network is fully connected and all non-bordering nodes (nodes are at the edge of sensor field) have more than one link disjoint or node disjoint path to the sink node. The network devices are non-mobile and the proposed RAOF attack is launched after the initial network setup. Following are few terminologies that are used in the design of RAOF attack.

- Candidate Parent Node (CPN): Any neighbour of a node possessing lesser rank value is termed as CPN. In a network a node can have number of Candidate Parent Nodes (CPNs) and any CPN can be selected for forwarding data to the sink node in RPL.
- Preferred Parent Node (PPN): It is one of the CPN with lowest rank and best routing metric selected for forwarding data to the sink node by a node in RPL network.
- Malicious Node (MN): This node will launch RAOF attack in the RPL network. The words MN and Attacking Node (AN) are interchangeably used in this paper.

According to RPL, the rank computation is linked with OF and it must be implemented in a generic method to include rank of preferred parent, node metrics, link metrics and the node configuration policies. We consider a simplistic rank calculation as recommended by RPL in RFC [9] based on OF

that uses ETX for path selection. In this case, rank of a node R(N) is calculated based on the rank of the parent R(P) and is shown in the following equations:

$$R(N) = R(P) + rank_{increase}$$

$$rank_{increase} = (Rf \times Sp + Sr) \times MinHopRankIncrease$$

Rank_factor(Rf) defines rank factor which is a configurable factor that is used to multiply the effect of the link properties in the rank_increase computation. Step_of_rank (Sp) is computed for that link (e.g., based on ETX) is multiplied by the Rf. Stretch_of_rank(Sr)that is less than or equal to the configured stretch_of_rank per hop rank increase computing. MinHopRankIncrease is a variable that can be distributed in the network with a fixed constant [11].

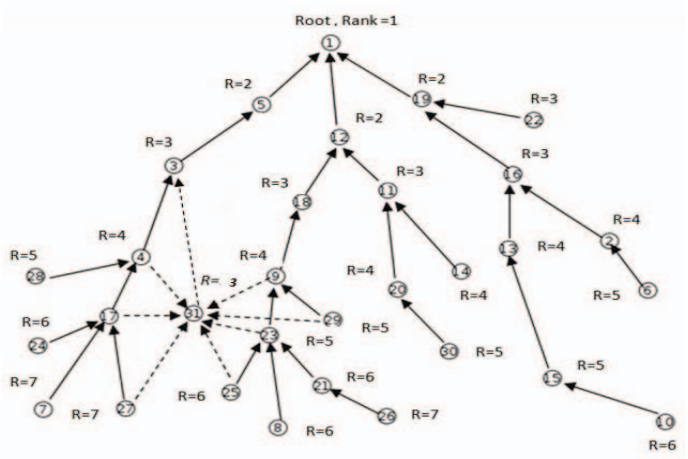

Figure 2: RAOF launched by node 31 in an RPL network

V. RAOF ATTACK

In this section, the RAOF attack is explained in length. An important factor in parent selection along with rank is objective function (OF). If a node receives a valid rank then before changing the PPN it must calculate the OF value based on routing metrics. For example, if the routing metric is based on ETX and the OF is defined to maintain routing path having lowest ETX value then a node will receive both rank and ETX for its PPN.

In this scenario to successfully launch a RAOF the attacking node must corrupt the routing metric announced by the parent node so that OF of the neighboring nodes favor the attacking node. In this work, we have used ETX as basic routing metric. Each node calculates ETX for successful transmission from source to destination using the following formula [10].

$$ETX = 1/Df * Dr$$

Where, Df is the measured probability that a packet is received by the neighbor and Dr is the measured probability that the acknowledgment packet is successfully received. To use ETX as OF it is included in DAG metric container. A DODAG uses single OF for topology formation and maintenance.

Consider, a network topology where an attacking node has a legitimate rank R_{LA} and the minimum rank among its neighbors is R_{NA}. In this case the attacker will announce a rank value that is less than $R_{NA}$to launch the attack. Hence in order to launch the attack the attacker will decrease it rank below $R_{NA}$and the advertised rank for the attacker $R_A$can be expressed as $R_A < R_{NA}$. In this case, if the announced rank R_A is very low then the neighbors of the attacker will discard this rank value. This is because RPL recommends that rank change should be within some limits otherwise sudden change of rank can result in the creation of very unstable network topologies. Hence, in RAOF the attacker announces a rank with the relation $R_{PPN\_A} < R_A < R_{NA}$, where R_{PPN_A} is the rank of PPN of the attacker. In this way, the rank change announced by the attacker is not very drastic but is less than most of the neighboring nodes.

In order to further elevate the intensity of the attack the routing metric (ETX) announced in the DIO message is drastically lowered as compared to the minimum observed among the neighbors. Since routing metric values can change very dynamically in real networks as compared to rank value therefore RPL suggests no measures to monitor the change in routing metric values.

As illustrated in Figure2, the neighboring nodes of the attacking node 31 will converge towards the node 31 by selecting it as their new PPN. The solid lines shows original connectivity before the launching of RAOF attack and the dotted lines depicts the new connectivity after the launch of RAOF. Once the attacking node becomes the PPN in the attacking region it can affect the network performance in the following ways.

VI. SIMULATIONS ANALYSIS

To measure the impacts of intruders on network Cooja simulator [12] is used which runs over Contiki OS, malicious nodes placed on different locations and circle around the malicious nodes indicate transmission range and data reporting nodes as shown in Figure 3. Node 1 is the sink/root node in the network. Network parameters used for simulations analysis as listed in table 1 and nodes characteristics are mirrored according to mote sky sensor nodes [12].

Table 1.Network Parameter used in simulation analysis

Parameter	Value
Network Layer	RPL
MAC Layer	IEEE 802.15.4
Simulation runtime	600s
Event reporting	500s
Objective Function (OF)	mrhf, ETX
Number of Sensor nodes	100
DIO minimum interval	4 sec
DIO maximum interval	17.5 min
Sending rate	1 packet every 10 sec
Number of source nodes	2-40
Number of attacking nodes	1-30
TX range	20 m

Interference range	30m
Packet size (excluding header)	50 Bytes

Figure 3:Simulation setup for RAOF attack at various places.

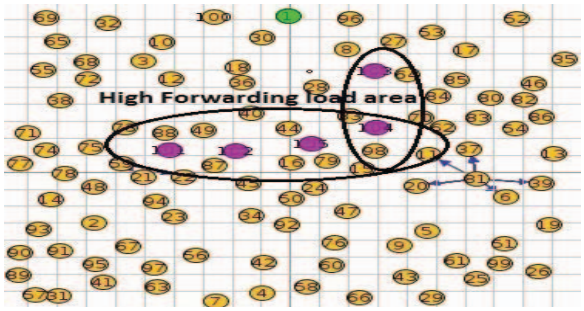

Figure 4 : RAOF attack near sink

Figure 5 shows the percentage of network nodes converged at the attacking due to RAOF attack. Five malicious nodes launch the attack in the network shown in Figure 3. After the RAOF attack, when a node selects the attacking node as its preferred parent then it is termed as affected node or converged. Also, nodes that are child of affected nodes selects a route through malicious node are also converged nodes. It is noticeable that when the attack is launched near to the sink more network nodes affected by the attack as demonstrate in Figure 4. Also, by the addition of only five attacking nodes in random locations almost 30% of the network nodes have converged towards the attacking nodes. Figure 6 shows the percentage of one hop nodes or neighbors converged in different regions by RAOF attack is launched in each region. Up to 60% of neighboring nodes have changed their PPN and converged towards attacking node.

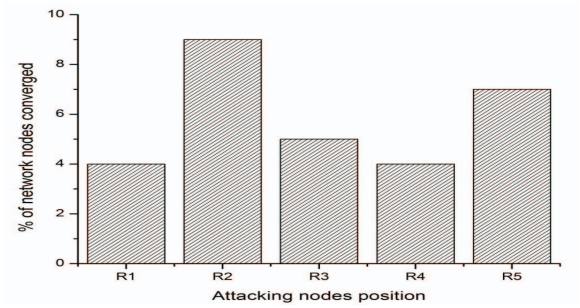

Figure 5: Network nodes converged by RAOF at various regions

Figure 7 shows the impact of RAOF in packet delivery ratio as the malicious node drops 10%, 20% and 30% forwarding packets. The simulation setup is same as shown in Figure 3. All nodes within the event reporting region from R1 to R5 and sending data at 6 packets/min [3]. During the normal operation of RPL without any attacking node high throughput is observed and delivery ratio is above 97%. When the attacking nodes drop only 10% of the traffic the routing metric ETX does not change significantly and the source nodes continue to route data through the attacking node. However, if the attacking nodes drop more than 20% of the forwarding traffic the ETX of the source nodes through the attacking nodes increases and they change their routing path, eliminating routes through the attacking node.This is visible in Figure 9 that the delivery ratio drops when packet drop ratio is 20 or 30% but then increases source nodes from the event region change their routing paths.

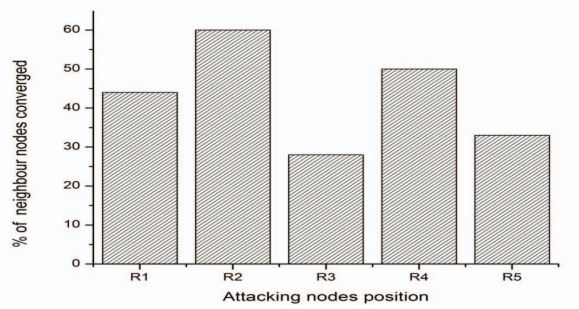

Figure 6: Neighbour nodes converged by RAOF at various regions

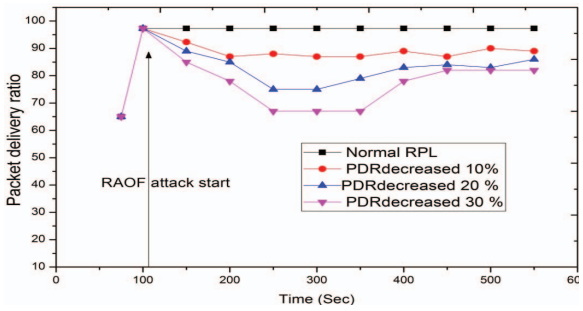

Figure 7: Impact of RAOF attack on PDR

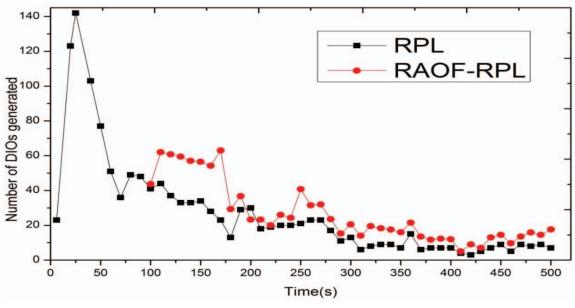

Figure 8:DIOs generated against RAOF attacking regions

In RPL, DIO and DAO messages are periodically communicated to create/maintain topology and update the sink

regarding the topology, respectively. Both the aforementioned messages contribute to the control message overhead. Figure 8 shows how the control overhead increases with respect to time. The attack is launched simultaneously using five nodes after 100 seconds in the simulation time from different regions. Only DIO results are included as number of DAOs generated is almost similar to DIOs because DAO is generated after receiving DIO message from the PPN node.

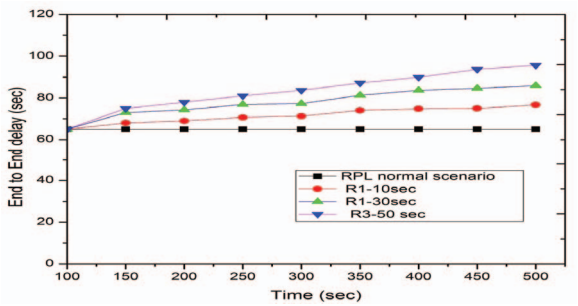

Figure 8: Average end-to-end delay

End to end data delivery time is another important parameter for the performance evaluation of network protocols. Figure 11 shows the impact on latency of communication as the malicious nodes adds 10%, 20% and 30% delay in data forwarding. During the normal operation of RPL without any attacking node the average delay observed is 65sec. When the malicious nodes add extra delay then latency is increased but the amount of delay is not significant for RPL to change the topology. Therefore, forwarding nodes do not change their PPN node and topology remains the same.

VII CONCLUSION

RPL is the IETF's recommended routing protocol for LLNs. In this paper, we have proposed a modified rank attack in which a malicious node advertises not only a false rank but also a false routing metric value. The proposed attack is more severe in nature as compared to simple rank attack. Simulation analysis has revealed that the proposed attack can easily forces neighbors of the attacking node to select the attacker as their forwarding node and it results in the convergence of data flows at the attacker. In addition, the results indicated that the proposed attack can decrease 30% to 57% of the data delivery ratio depending on the position of the attacking node within the network.

REFERENCES

[1] T. Winter, P. Thubert, "RFC 6550: RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," *Internet Engineering Task Force (IETF) Request For Comments*, March 2010.

[2]N. Accettura, L. Grieco, G. Boggia, P. Camarda, "Performance Analysis of the RPL Routing Protocol", *IEEE International Conference on Mechatronics (ICM),* pp.767-772, Turkey, April 2011.

[3] L.Anhtuan, L. Jonathan, and L. Aboubaker,"The Impacts of Internal Threats towards Routing Protocol for Low power and lossy Network Performance".IEEE Symposium on Comupters and Communication, Split,July 2013.

[4] L. Wallagren, S. Raza, and T. Voigt, "Routing Attacks and Countermeasures in the RPL –Based Internet of Things." International Journal of Distributed Sensor Networks, Vol. 2013, pp. 840-851, 2013.

[5] L. Anhtuan, L. Jonathan, and L. Aboubaker, "The Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and LossyNetworks".IEEE Sensor Journal, Vol. 13, PP. 3685-3692, 2013.

[6] T. Winter, P. Thubert, "RFC 6550: RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," *Internet Engineering Task Force (IETF) Request For Comments*, March 2010.

[7] P. Levis, T. Clausen, J. Hui, O. Gnawali, J. Ko, "RFC 6206: The Trickle Algorithm draft-ietf-roll-trickle-08," *Internet Engineering Task Force (IETF) Request For Comments*, Jan 2011.

[8] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: attacks and countermeasures", International Journal of Ad Hoc Networks, Vol.1, pp. 293–315, 2003.

[9] P. Thubert, "RFC 6552: Objective Function Zero for theRouting Protocol for Low-Power and Lossy Networks (RPL)," Internet Engineering Task Force (IETF) Request For Comments, March 2012.

[10] J.P. Vasseur, M. Kim, K. Pister, N. Dejean, D. Barthel, "RFC 6551: Routing Metrics Used for Path Calculation in Low-Power and Lossy Networks," Internet Engineering Task Force (IETF) Request For Comments, March 2012.

[11] O. Gnawali,P. Levis, "RFC 6719: The Minimum Rank with Hysteresis Objective Function," *Internet Engineering Task Force (IETF) Request For Comments*, Sept 2012.

[12] "Contiki: The Open Source OS for the Internet of Things," Contiki OS. [Online]. Available: http://www.contiki-os.org/index.html .