International Journal of Pure and Applied Mathematics
Volume 119 No. 16 2018, 1203-1210
ISSN: 1314-3395 (on-line version)
url: http://www.acadpubl.eu/hub/
Special Issue
http://www.acadpubl.eu/hub/

RIAIDRPL: Rank Increased Attack (RIA) Identification Algorithm for Avoiding Loop in the RPL DODAG

R. Stephen
Research Scholar,
Department of Computer Science,
St. Joseph's College (Autonomous),
Tiruchirappalli-620002.
stephenr1989@gmail.com

Dr. L. Arockiam
Associate Professor,
Department of Computer Science,
St. Joseph's College (Autonomous),
Tiruchirappalli-620002.
larockiam@yahoo.co.in

***Abstract* – The term Internet of Things (IoT) is a new paradigm in the context of the internet to objects. The objects are interacting with each other in the real world. The low power and lossy networks (LLNs) are used to connect the resource constraint objects such as memory, energy and processing capabilities. The routing protocol for low power and lossy network (RPL) is a proactive protocol which is designed for the IoT network. In RPL, the rank value takes an important role to construct and maintain the RPL DODAG (Destination Oriented Directed Acyclic Graph). The node's increased rank value creates a loop in the DODAG. Hence, the data packets fail to reach the destination. This paper proposes an algorithm called RIAIDRPL to identify the rank increased attacks (RIA) which create a loop in the RPL network. Also, it is stimulated with various parameters such as packet delivery ratio, packet delay, attacker identification ratio, false positive rate and identification rate of malicious node.**

***Index Terms:* RPL, Rank Increased Attack, RPL Loop**

I. INTRODUCTION

The term Internet of Things (IoT) is an emerging technology and connects more devices with the internet. IoT refers to the communication between physical devices like smart phones and other smart objects that exchange data and provide useful services via internet. Many research organizations predicted that in 2020 there will be 50 billion smart objects and devices connected to the internet. But, there is an issue regarding security and privacy in different IoT layers [1].

IoT is a new revolution in the world. It offers the possibilities to use in many fields of applications. It has been widely used in smart home, smart industry, smart city, retail, agriculture, environment monitoring etc [2]. The objective of IoT is to make interconnection between devices. The enhancements of Wireless Sensor Networks (WSNs) are widely popular. IoT objects are connected in the WSNs to collect data regarding environment [3]. Internet of Things is resource constrained due to the limited energy, memory and processing capabilities.

The Internet Engineering Task Force (IETF) introduced the protocol called routing protocol for low power and lossy networks (RPL). It is a standardized routing protocol for the IoT. It is primarily used in IPv6 over low power wireless personal area network (6LoWPAN). RPL creates a destination oriented directed acyclic graph (DODAG) between the nodes in a 6LoWPAN [4].

RPL DODAG construction is based on the rank value. This value is calculated with respect to the parents rank value. The rank value depends on the distance from the root node. Here, the attacker nodes misuse the rank value and attract the neighbor nodes to capture the data packets. These are Sinkhole attack, Selective forwarding attack, Sybil attack, Blackhole attack, Denial of Service attack, Rank attack, Rank increased attack etc. [5].

This paper is organized as follows. Section 2 explains the review of literature and section 3 describes the RPL loop with Rank Increased Attacker (RIA) node. Section 4 explains the proposed algorithm RIAIDRPL. Section 5 discusses the results to describe the strength of proposed algorithm and section 6 presents the conclusions and future work.

II. REVIEW OF LITERATURE

This section illustrates the related papers that discuss the RPL performance, various attacks, and importance of RPL loop detection. Accettura et al. [6] presented a performance evaluation of RPL routing protocol using the Contiki Cooja simulator. These performances are based on packet error rate, end-to-end packet delay, throughput and network overhead. Rual et al. [7] proposed an architecture with self-protection based MAPE-KL (monitor, analyze, plan, execute and knowledge) autonomic control loop that will run at the application layer. This paper addressed the impact of attacks such as sinkhole, selective forward, blackhole and flooding attacks.

Grgic et al. [8] analyzed the existing security threats and possible countermeasures in IPv6 based WSNs. Also, the paper analyzed the security framework for IPv6 based WSNs and a possible intrusion detection system for IPv6 based WSNs. Divya Sharma et al. [9] classified the routing attacks against RPL in Internet of Things. This classification of attacks are based on network resources, topology and network traffic. This paper compared the properties of these attacks and discussed methods and techniques to avoid or prevent them.

Xie et al. [10] studied the simulations and the time required by the network to give converge to a stable and loop-free state following a rank increased operation. This rank increased operation creates a routing loop within a Directed Acyclic Graph (DAG). This paper measured three mechanisms such as loop prevention, loop detection and loop avoidance. Mayzaud et al. [11] presented taxonomy of the attacks against RPL protocol. These attacks targeting network resources, network topology and network traffic. Also, this paper described the routing loop based on rank increased attack.

Anhtuan Le et al. [12] presented a simulation based study of the impacts of different types of internal attacks on RPL. These are rank attack, local repair attack, neighbor attack and DIS attack. Zhang Ta et al. [13] analyzed and evaluated the performance of the RPL protocol using Cooja simulator. This performance evaluation identified a set of important metrics such as latency of message delivery, signaling overhead and convergence time. Dvir et al. [14] identified the attacker nodes which increased version number and decreased rank value. These two attacks create more traffic in the LLN network and exhaust the node's batteries against RPL.

Anhtuan Le et al. [15] analyzed different types of internal threats that affect rank property and also studied their impact on the performance of the WSNs. Gaddour Olfa et al. [16] evaluated the performance of the RPL protocol based on energy, storage overhead, communication overhead, network convergence time and the maximum hop count using Contiki simulations. Hence, RPL has several benefits for LLN networks as compared to the current routing protocols. Guo Jianlin et al. [17] provided an innovative rank computation method and a loop-free local route repair mechanism to eliminate routing loops in RPL. The simulation results disclosed that the proposed loop free routing protocol RPL performed much better than conventional routing protocols in terms of packet delivery rate, end-to-end packet delay and routing overhead. Sharma Rahul et al. [18] described the various types of attacks at the network layer of 6LoWPAN and RPL. The authors introduced a new node count security mechanism to prevent from the rank increased attack. This attack leads to loop formation between nodes.

Glissa Ghada et al. [19] proposed a new secure routing protocol based on RPL referred to as Secure-RPL (SRPL). The authors introduced the concept of rank threshold along with hash chain authentication technique to deal with internal attacks. Conti Mauro et al. [20] presented a reliable and secure multicast routing protocol for IoT networks called REMI. The main objective of REMI is to enable efficient communication in low power and lossy networks such as IoT. Stephen et al. [20] proposed an algorithm to detect rank attack in RPL based Internet of Things. This paper used the verification and validation techniques to identify the rank attacker node.

III. RPL LOOP WITH RANK INCREASED ATTACK (RIA)

The rank value represents the relative position of each node within a DAG according to the root node. The nodes increase their rank values to find a new parent node. The node's rank value is always increasing in downward direction in order to form the DODAG (Destination Oriented Directed Acyclic Graph). The node's rank value must be greater than the rank values of its parents. If a node wants to change its rank value, it has to update its parent list by removing the nodes having a higher rank than its new rank value [11]. It selects the preferred parent node from this list in order to optimize the route for transmitting a packet to the root node. An attacker node increases its rank value and selects its child as a preferred parent.

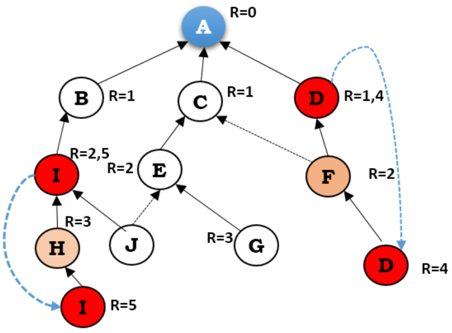


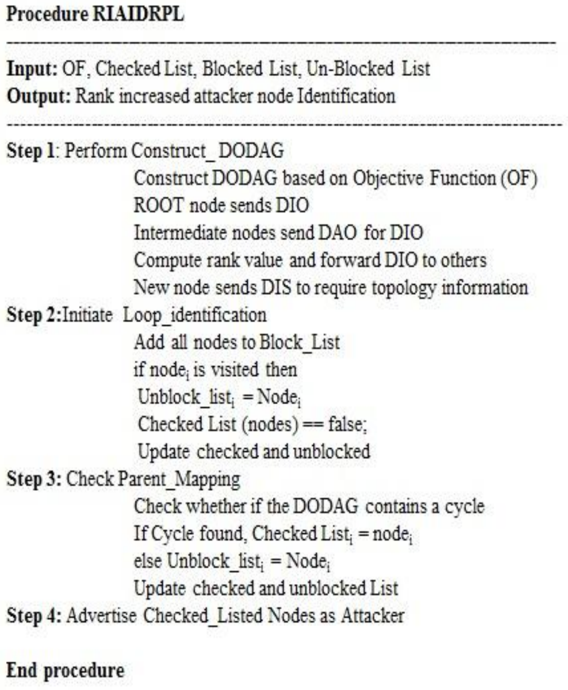
Figure 1: Rank Increased Attack

The RPL loop is created by the attacker nodes (D and I) with higher rank value as illustrated in Figure 1. In this scenario, the attacker node (D) calculates its rank value to 4 and chooses node (F) as the new preferred parent. This operation creates a routing loop, because the node (D) is the preferred parent of node (F). This attack becomes more problematic when the node (H) does not have an alternate parent.

IV. RIAIDRPL: A PROPOSED ALGORITHM

The RIAIDRPL handles four types of lists to identify the loop in the DODAG. These are Blocked List, Unblocked List, Checked List and Parent Mapping list. Blocked List represents that all the nodes that have not been visited at all. Unblocked List represents that the nodes that are visited. Checked List represents the attacker node which creates the loop. Parent mapping refers to the node's parent mapping to identify the link process.

The RIAIDRPL method searches until it finds a loop in the DODAG which is created by the Rank Increased Attacker (RIA) node. Working procedure of the proposed algorithm is explained below:



```
Procedure RIAIDRPL
----------------------------------------------------------------
Input: OF, Checked List, Blocked List, Un-Blocked List
Output: Rank increased attacker node Identification
----------------------------------------------------------------
Step 1: Perform Construct_ DODAG
            Construct DODAG based on Objective Function (OF)
            ROOT node sends DIO
            Intermediate nodes send DAO for DIO
            Compute rank value and forward DIO to others
            New node sends DIS to require topology information
Step 2:Initiate Loop_identification
            Add all nodes to Block_List
            if $node_i$ is visited then
             $Unblock\_list_i = Node_i$
             Checked List (nodes) == false;
             Update checked and unblocked
Step 3: Check Parent_Mapping
            Check whether if the DODAG contains a cycle
            If Cycle found, $Checked\ List_i = node_i$
            else $Unblock\_list_i = Node_i$
            Update checked and unblocked List
Step 4: Advertise Checked_Listed Nodes as Attacker

End procedure
```

The detection method of proposed algorithm RIAIDRPL is explained with figure 1. Here, the node D is the rank increased attacker node which has node F as a child. The affected node F selects node D as a preferred parent node. Now, the attacker node D increased its rank value and selects its child node F as a preferred node. The loop is created between nodes D and F. The RIAIDRPL method identified the loop from the repeated node in the checked list. For example, in figure 1 the loop formed as **D←F←D**. The RIAIDRPL identified the node D as the rank increased attacker node which is in the Checked List.

V. RESULTS AND DISCUSSIONS

The performance of RIAIDRPL has been evaluated considerably. The Cooja simulator is used to simulate the performance of proposed algorithm RIAIDRPL. This simulation results are obtained with small and large number of nodes. The algorithm is proposed by considering the following parameters which is shown in table 1.

Table 1: Simulation Parameters

Parameters	Description
No. of nodes	10, 50, 100
Simulation Area	1000 x 1000 m
Node Arrangement	Random, Grid
Radio Medium	UDGM-Distance Loss
Operating System	Contiki
Simulator	Cooja
Types of sensor node	Tmote Sky(Sink), Tmote Sky(Sender), Tmote Sky(Border router),
Packet Analyzer	Wireshark

Packet delivery rate: The RIAIDRPL achieved almost 90% of the packet delivery rate than normal RPL packet transmission which is shown in figure 2.

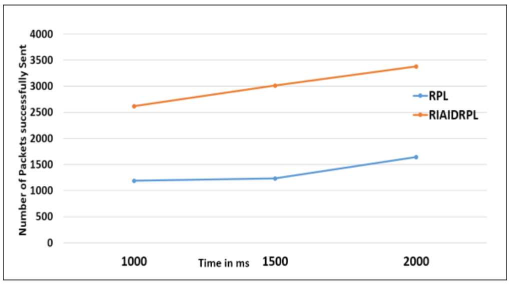


Figure 2. Packet delivery rate

Packet delay: The RIAIDRPL reduced the packet transmission delay with different attacker ratio. Figure 3 shows the comparison between RIAIDRPL with LRPL when varying the ratio of attacker node.

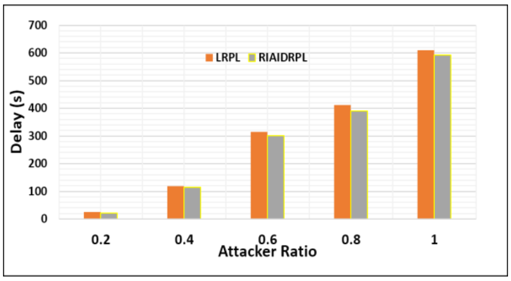


Figure 3. Packet delay

Attacker identification ratio: The RIAIDRPL achieved almost 90% of detection accuracy when increasing the number of nodes. Figure 4 shows the attacker identification ratio.

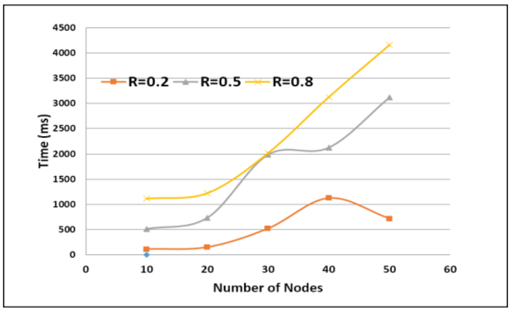


Figure 4. Attacker identification ratio

False positive rate: It determines the amount of times that the system has detected an attacker node as negative. Some nodes legitimately increase its rank value. The LRPL determined the node as negative. Figure 5 shows RIAIDRPL and the LRPL false positive rate as 4% and 8% respectively.

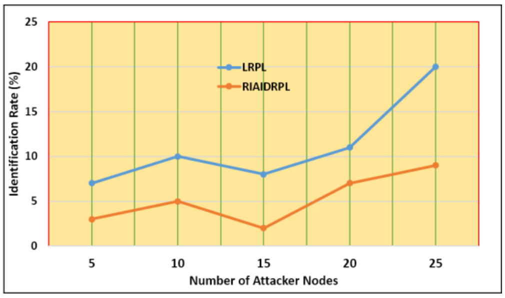


Figure 5. False positive rate

Identification rate of malicious node: It determines the identification rate of malicious node among 100 nodes. Figure 6 shows the result of RIAIDRPL. It achieved almost 90% of the malicious node identification.

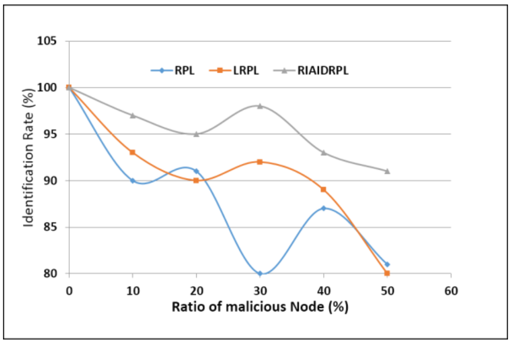


Figure 6. Identification rate of malicious node

As a result, the RIAIDRPL gives the better performance based on different network parameters. Also, the RIAIDRPL has compared with the existing protocols LRPL and RPL. The simulation setup is same as for all the parameters. The existing protocol LRPL considered only the loop avoidance, but RIAIDRPL gives solution for the loop avoidance and rank increased attack.

VI. CONCLUSION

The objective of RIAIDRPL is to identify the rank increased attacker node in LLNs. Also, it increases packet delivery ratio, reduces packet delay and controls the DIO messages. The proposed algorithm RIAIDRPL uses four types of lists to detect the rank increased attacker node. It encounters the attacker node which increases the rank value multiple times illegitimately. The proposed work RIAIDRPL has been compared with existing protocols RPL and LRPL based on various network parameters. The simulation results show that the RIAIDRPL achieved almost 90% of detection accuracy and reduces packet delay. In future, the efficiency of the proposed algorithm will be tested with other types of routing attacks based on different network parameters.

REFERENCES

[1] Ahmed Abdul Wahab, Mian Muhammad Ahmed, Omair Ahmad Khan and Munam Ali Sha, "A comprehensive analysis on the security threats and their countermeasures of IoT", International Journal of Advanced Computer Science and Applications, Vol. 8, Issue 7, 2017, pp. 489-501.

[2] Torgul Belkiz, Lutfu Sagbansua, and Figen Balo, "Internet of Things: a survey", International Journal of Applied Mathematics, Electronics and Computers 4, Special Issue-1, 2016, pp.104-110.

[3] Choudhary Gaurav and A. K. Jain, "Internet of Things: A survey on architecture, technologies, protocols and challenges", Recent Advances and Innovations in Engineering (ICRAIE), International Conference on. IEEE, 2016, pp.1-8.

[4] Wallgren Linus, Shahid Raza and Thiemo Voigt, "Routing Attacks and Countermeasures in the RPL-based Internet of Things", International Journal of Distributed Sensor Networks, Vol.9, Issue 8, 2013.

[5] Pongle Pavan, and Gurunath Chavan, "A survey: Attacks on RPL and 6LoWPAN in IoT", Pervasive Computing (ICPC), International Conference on. IEEE, 2015, pp.1-6.

[6] Accettura Nicola, Luigi Alfredo Grieco, Gennaro Boggia, and Pietro Camarda, "Performance analysis of the RPL routing protocol", Mechatronics (ICM), 2011 IEEE International Conference on. IEEE, 2011, pp. 767-772.

[7] Ruan de A. C. Mello, Admilson de R. L. Ribeiro, Fernando M. de Almeida, Edward D. Moreno, “Mitigating Attacks in the Internet of Things with a Self-protecting Architecture”, Thirteenth Advanced International Conference on Telecommunication, 2017, ISBN: 978-1-61208-562-3, pp. 14-19.

[8] Grgic Kresimir, Visnja Krizanovic Cik, and Vanja Mandric Radivojevic, "Security Aspects of IPv6-based Wireless Sensor Networks", International journal of electrical and computer engineering systems, Vol. 7, Issue 1, 2016, pp.29-37.

[9] Divya Sharma, Ishani Mishra, and Sanjay Jain, "A Detailed Classification of Routing Attacks against RPL in Internet of Things", International Journal of Advance Research, Ideas and Innovations in Technology, Vol. 03, Issue 1, 2017, pp. 692-703.

[10] Xie Weigao, Goyal M., Hosseini H., Martocci J., Bashir Y., Baccelli E., and Durresi A., "Routing loops in DAG-based low power and lossy networks", Advanced Information Networking and Applications (AINA), 2010 24th IEEE International Conference on. IEEE, 2010. pp. 888-895.

[11] Mayzaud Anthéa, Rémi Badonnel, and Isabelle Chrisment, "A Taxonomy of Attacks in RPL-based Internet of Things", International Journal of Network Security, Vol. 18, Issue 3, 2016, pp. 459-473.

[12] Le Anhtuan, Jonathan Loo, Yuan Luo, and Aboubaker Lasebae, "The impacts of internal threats towards routing protocol for low power and lossy network performance", In Computers and Communications (ISCC), IEEE Symposium on, 2013, pp.789-794.

[13] Zhang Tao and Xianfeng Li, "Evaluating and Analyzing the Performance of RPL in Contiki", In Proceedings of the first international workshop on Mobile sensing, computing and communication, ACM, 2014, pp. 19-24.

[14] Dvir Amit and Levente Buttyan, "VeRA-version number and rank authentication in RPL", Mobile Adhoc and Sensor Systems (MASS), 8th International Conference on. IEEE, 2011, pp. 709-714.

[15] Le Anhtuan, Jonathan Loo, Aboubaker Lasebae, Alexey Vinel, Yue Chen, and Michael Chai, "The impact of rank attack on network topology of routing protocol for low-power and lossy networks", IEEE Sensors Journal, Vol.13, Issue 10, 2013, pp. 3685-3692.

[16]Gaddour Olfa, Anis Koubaa, Shafique Chaudhry, Miled Tezeghdanti, Rihab Chaari, and Mohamed Abid, "Simulation and performance evaluation of DAG construction with RPL", In Communications and Networking (ComNet), Third International Conference on IEEE, 2012, pp. 1-8.

[17] Guo Jianlin, Chuan Han, Philip Orlik, Jinyun Zhang, and K. Ishibashi, "Loop-free routing in low-power and lossy networks", In SENSORCOMM 2012, The Sixth International Conference on Sensor Technologies and Applications, 2012, pp. 59-66.

[18] Sharma Rahul, Nitin Pandey, and Sunil Kumar Khatri, "Analysis of IoT security at network layer", In Reliability, Infocom Technologies and Optimization (Trends and Future Directions) (ICRITO), 6th International Conference on IEEE, 2017, pp. 585-590.

[19] Glissa Ghada, Abderrezak Rachedi, and Aref Meddeb, "A secure routing protocol based on RPL for Internet of

Things", Global Communications Conference (GLOBECOM), 2016 IEEE, 2016, pp. 1-7.

[20] Conti Mauro, Pallavi Kaliyar, and Chhagan Lal, "REMI: A Reliable and Secure Multicast Routing Protocol for IoT Networks," In Proceedings of the 12th International Conference on Availability, Reliability and Security, ACM, 2017, p. 84.

[21] R. Stephen, A. Dalvin Vinoth Kumar, Dr. L. Arockiam, “An Algorithm to Detect Rank Attack in RPL based 6LoWPAN Networks”, International Journal of Computer Sciences and Engineering (IJCSE), Vol. 05, Issue 08, 2017, E-ISSN: 2347-2693.