IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Volume-6, Special Issue-2, March 2018 E-ISSN: 2347-2693

An Algorithm to Detect Rank Attack in RPL based 6LoWPAN Networks

R. Stephen[1*], A. Dalvin Vinoth Kumar[2], L. Arockiam [3]

[1*]Computer Science, St. Joseph's College (Autonomous), Bharathidasan University,Tiruchirappalli, India
[2] Computer Science, St. Joseph's College (Autonomous), Bharathidasan University,Tiruchirappalli, India
[3] Computer Science, St. Joseph's College (Autonomous), Bharathidasan University,Tiruchirappalli, India

[*]*Corresponding Author: stephenr1989@gmail.com*

Available online at: www.ijcseonline.org

***Abstract*—** Internet of Things (IoT) is connected with numerous number of heterogeneous devices and these devices are communicating with one another. They are deployed in low power lossy networks. These networks encounter various attacks. Such as sinkhole attack, selective forwarding, wormhole attack, rank attack. Internet Engineering Task Force (IETF) standardizes protocol for IoT. One such is IPv6 Routing Protocol for Low power and Lossy network (RPL). RPL is typically designed for IoT in the context of constrained resources. In RPL, source nodes select the preferred parent node based on the rank metric to select the optimum routes. However, the malicious node misuses the rank metric to attract its neighbor nodes. This issue is defined as the rank attack. This paper proposes an algorithm to detect the rank attack in RPL based Internet of Things.

***Keywords*—** Internet of Things, RPL, Rank attack, 6LoWPAN

I. INTRODUCTION

Internet of Things (IoT) integrates physical objects with the internet. In IoT, the heterogeneous devices are connected in low power and lossy network called 6LoWPAN (IPv6 Low Power over Wireless Personal Area Network). This network is connected with the internet using 6LoWPAN Border Routers (6BR) [1] as shown in figure 1. Here, 6BR acts as a gateway between the 6LoWPAN network and the internet. In 6LoWPAN network, huge number of heterogeneous devices are connected. These devices are communicating using routing protocol called RPL. It is mainly designed for the Internet of Things to connect the constrained devices.

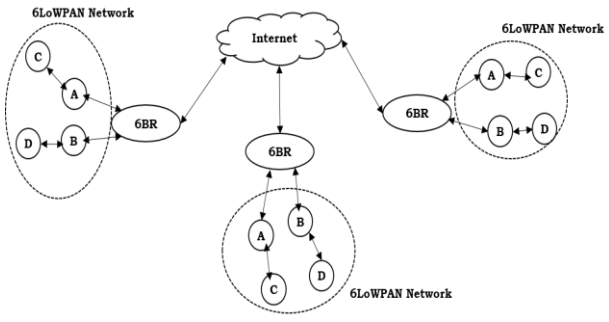

Figure 1: IoT devices connected with the Internet across 6BR

The RPL is affected by various internal and external attacks due to constrained resources. Particularly, internal attacks create more vulnerabilities to disrupt the network performances. So, it needs the standard security mechanism to detect and mitigate the attacks. RPL construction is based on the Rank metric. But, the malicious node used the rank metric as a fake to compromise to its neighbor nodes. The nodes which are compromised with the malicious node will loss the data packets. Consequently, the network parameters such as packet delivery ratio and throughput are affected. Hence, this paper proposes an algorithm to detect the rank attack in RPL based Internet of Things.

This paper is presented as follows: section II describes the related works. Section III specifies overview of research. Section IV defines the problem. Section V proposes a mechanism. Finally, section VI concludes the paper.

II. RELATED WORK

Dharmini et al. [6] proposed the intrusion detection module to detect intrusions against the 6LoWPAN networks. In this paper, the authors used ETX metric and geographical hints with the IDS module to identify malicious nodes that conduct attacks against 6LoWPAN networks. Karthik et al. [7] proposed a security mechanism to address and mitigate the rank attack in RPL. The authors invoked a security mechanism in the motes to increase the packet delivery ratio towards the sink node. Mahmood et al. [8] reviewed the existing mechanisms for detecting sinkhole attacks on RPLs.

The authors discussed and compared their advantages and drawbacks with regard to resource consumption and false positive rate. Faiza et al. [9] proposed a trust-based intrusion detection system for mobile RPL based networks. The authors introduced a new timer and minor extensions to RPL messages format to deal with mobility, identity and multicast issues. Yulong fu et al. [10] proposed an automata based intrusion detection method to detect and report the possible IoT attacks and also designed an experiment to verify the proposed IDS method and examine the attack of RADIUS application. The summary of existing mechanisms and attacks are tabulated in table 1.

Table 1: Summary of existing mechanisms and detected attacks

Author (s)	Detected Attacks	Methods/Techniques	Parameters
Shahid et al. [11]	Sinkhole, selective forwarding	Intrusion detection algorithms	True positive rate, energy
Anhutuan et al. [12]	Rank, sinkhole, local repair, neighbor and DIS	Specification based intrusion detection system	True positive rate, False positive rate, energy
Heiner et al. [13]	Rank attack	TRAIL - Topology authentication	Overhead, message size
Kevin et al. [14]	Rank, sinkhole	Parent fail-over, rank authentication	End-to-end packet delivery ratio
Christian et al. [15]	Sinkhole attack	INTI intrusion detection system, watchdog, reputation, trust	False positive rate, false negative rate, delivery rate of packets
Abdul et al. [16]	Rank attack	Objective function	Packet delivery ratio, end-to-end delay

III. TOPOLOGY CONSTRUCTION IN RPL

RPL is one of the routing protocols for IoT. RPL is a routing protocol for low power and lossy network. It is primarily designed for 6LoWPAN networks. RPL is a proactive and distance vector routing protocol for LLNs which creates a DODAG of the network devices. An important characteristic of RPL is its design for network of resource constrained devices [2]. RPL topology is connected using three control messages, these are DODAG Information Object (DIO), DODAG Advertisement Object (DAO), and DODAG Information Solicitation (DIS). RPL supports the Multipoint-to-Point (MP2P), Point-to-Multipoint (P2MP) and Point-to-Point (P2P) traffics [17]. In RPL, there are two types of modes are operated. These are storing and non-storing modes. In storing mode, the Point-to-Point (P2P) traffic between source to destination traverse through the common parent node. In non-storing mode, the P2P traffic between source to destination traverse through the DODAG root node. To produce a route topology, every node selects a set of parents that comprises nodes with equal or better paths towards the sink. The node with the best route link is chosen as the parent [3]. The figure 2 shows the construction of RPL topology.

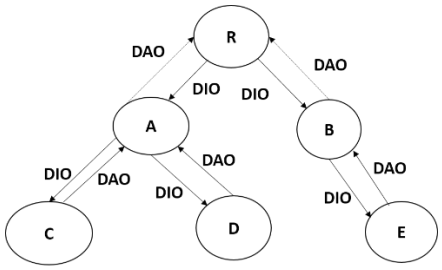

Figure 2: RPL Construction

IV. PROBLEM DEFINITION

As the energy is an important parameter to calculate the rank, manipulation of energy would lead to fake rank value. The consumption of energy depends on idle time, transfer time and listen time. The accurate energy level is after calculating these parameters. If there is a variation in energy level, then there is a possibility of rank attacks in the network. This attack is handled by calculating the energy of each individual nodes in the network. The initial energy of each devices are same. The border router which maintains the routing table and the energy of each node. The rank of each node depends on the energy.

RPL is a rank based DODAG tree topology protocol. Here, the source nodes select the set of parent nodes in which each node selects the preferred parent node based on better rank value. Here, non-optimized path is created when the node selects the attacker node in the context of fake rank value [4]. In RPL, different types of routing attacks occur such as sinkhole attack, selective forwarding attack, wormhole attack, rank attack etc. Among these, rank attack is most crucial issue in RPL protocol [5].

This paper proposes a mechanism to handle attacker nodes in IoT environment.

V. THE PROPOSED FAKE RANK NODE DETECTION ALGORITHM (FRND)

The proposed FRND algorithm, presented below, is used to detect the attacker node based on rank of the node. The rank of a node is calculated based on its distance from the root node. The node which has lowest rank is selected as the preferable parent. This algorithm collects n nodes as an input and eliminates the attacker node based on its fake rank value. The procedure of the FRND algorithm is presented in figure 3.

Procedure FRND()
Step 1: Start
Step 2: Read N nodes
Step 3: Perform DODAG Construction using Rank for given N nodes
Step 4: Select a parent and calculate the rank of the parent
Step 5: Calculate rank of every child
Step 6: Calculate energy required for each packets
Step 7: Identify the attacker node using the table Tab_Rnk_Id
Step 8: If attacked node (A) is mitigated by the root then
Perform global repair
Else
Perform local repair
End if
Step 9: Stop

Figure 3: Procedure of FRND algorithm

The pseudo code for procedure FRND is presented below.

Algorithm Rank_Detect()

Input : *Input nodes N*
Process: *Detection and Elimination of Attacker node*
Output: *Eliminated Attacker node*

1. *Begin*
2. ***For*** *all nodes N*
   {
3. *DODAG construct ( ) {*
   For *CN(i) ← 1 to N // CN – Child Node*
   {
   Parent selection ( ) //Choosing the best parent based on rank
   {
   Rank ( ) // Calculating the rank value
   {
   $Credit = \frac{Available\ energy}{Initial\ energy}$
   $Rank_{increase}$ = *credit + MinHopRankIncrease*
   SR= Parent Rank + $Rank_{increase}$
   // Self Rank Calculation
   Expenditure = (packets sent x required energy) + (ideal time x ideal require energy)
   $Rank_{decrease}$ = *Expenditure + MinHopRankIncrease*
   Child rank = Parent Rank + $Rank_{decrease}$
   }
   }
   End for
   }
   }
4. *Total Transaction count ( ) // number of packet sent by the child node*
   {
   For P_{Pi} ← *1 to n // Number of packet received*
   P_{Pi} *++*
   }
5. *Calculate Child Rank ( )*
   {
   For CN_i ← *1 to n // Number of child Nodes*
   {
   Receive DIO
   For DIO_j ← *1 to m*
   // Number of DIO received
   {
   End for j
   }
   End for i
   }
   }
6. $E(P_{Pi}) = P_{Pi} *$ *energy required per packet*
7. ***If*** $CUR_i == RCR_i$ *// fake rank identification -*
8. *Attacker Node Identification ( )*
9. ***For*** *NR=1 to n*
10. ***if*** $PR_i > NR_i + A_i$
11. A_{++}
12. ***for*** NR_i, *i= 1 to n*
    if NA > NA_{th}
    If A is near to Root // Attacker alarm given to the network, Global Repair ( )
    Else Local Repair ( )
    End if
    End if
13. *End*

VI. CONCLUSION

This paper proposes an algorithm to detect rank attack in RPL based Internet of Things. In RPL, various types of parameters used to select the best optimum routes to the destination. The intruder misuses the rank value to disrupt the network operations. This algorithm detects the rank attack based on energy metric. In future work, packet delivery ratio, network overhead and throughput will be evaluated using this algorithm.

REFERENCES

[1] 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.

[2] Airehrour David, Jairo Gutierrez, and Sayan Kumar Ray, "A testbed implementation of a trust-aware RPL routing protocol", *27th International Telecommunication Networks and Applications Conference (ITNAC) on* IEEE, pp. 1-6, 2017.

[3] Airehrour David, Jairo Gutierrez, and Sayan Kumar Ray, "Secure routing for internet of things: A survey", *Journal of Network and Computer Applications* 66, 2016, pp.198-213.

[4] Anhtuan Le, Jonathan Loo, Yuan Luo, Aboubaker Lasebae, "Specification-based IDS for securing RPL from topology attacks", ISSN: 2156-9711, 2011, pp. 1-3, DOI: 10.1109/WD.2011.6098218.

[5] 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.

[6] Shreenivas Dharmini, Shahid Raza, and Thiemo Voigt, "Intrusion Detection in the RPL-connected 6LoWPAN Networks", *Proceedings of the 3rd ACM International Workshop on IoT Privacy, Trust, and Security*, ACM, 2017, pp. 31-38.

[7] Karthik V.K. and Pushpalatha M, "Addressing attacks and security mechanism in the RPL based IoT", *International journal of computer science and engineering communications*, vol.5, Issue.5, 2017, pp. 1715-1721.

[8] Alzubaidi Mahmood, Mohammed Anbar, Samer Al-Saleem, Shadi Al-Sarawi, and Kamal Alieyan, "Review on mechanisms for detecting sinkhole attacks on RPLs", *Information Technology (ICIT), 8th International Conference on*. IEEE, 2017, pp.369-374.

[9] Medjek, F., Tandjaoui, D., Romdhani, I., and Djedjig, N, "A Trust-based Intrusion Detection System for Mobile RPL Based Networks", *In IEEE 10th International Conference on Internet of Things*, 2017.

[10] Fu, Y., Yan, Z., Cao, J., Koné, O., and Cao, X, "An Automata Based Intrusion Detection Method for Internet of Things", *Mobile Information Systems, 2017*.

[11] Shahid Raza, Linus Wallgren, and Thiemo Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things", *Journal on Ad hoc networks*, Vol.11, Issue.08, 2013, pp. 2661-2674.

[12] Anhtuan Le, Jonathan loo, Kok Keong Chai and Mahdi Aiash, "A specification-based IDS for detecting attacks on RPL-based network topology", *Information* 7. Issue.2, Vol.25, 2016.

[13] Heiner Perrey, Martin Landsmann, Osman Ugus, Matthias W¨ahlisch and Thomas C. Schmidt, "TRAIL: Topology authentication in RPL", 2013.

[14] Kevin Weekly and Kristofer Pister, "Evaluating sinkhole defense techniques in RPL networks", *Network Protocols (ICNP), 20th IEEE International Conference on*. IEEE, 2012, pp. 1-6.

[15] Christian Cervantes, Diego Poplade, Michele Nogueira and Aldri Santos, "Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet of things", *Integrated Network Management (IM), IFIP/IEEE International Symposium on. IEEE*, 2015.

[16] A. Rehman, M. M. Khan, M. A. Lodhi and F. B. Hussain, "Rank attack using objective function in RPL for low power and lossy networks", *International Conference on Industrial Informatics and Computer Systems (CIICS)*, 2016, pp. 1-5, DOI: 10.1109/ICCSII.2016.7462418.

[17] Airehrour David, Jairo Gutierrez, and Sayan Kumar Ray, "Secure routing for internet of things: A survey", *Journal of Network and Computer Applications* 66, 2016, pp.198-213, http://dx.doi.org/10.1016/j.jnca.2016.03.006.

