Level Based Rank Attack Detection Technique (LEACE)

A.Stephen [a] and Dr. L. Arockiam [b]

[a] *Research Scholar[1], Department of Computer Science, St. Joseph's College (Autonomous),(Affiliated to Bharathidasan University),Tiruchirappalli – 620 002, India*

[b] *Associate Professor, Department of Computer Science, St. Joseph's College (Autonomous),(Affiliated to Bharathidasan University),Tiruchirappalli – 620 002, India*

Article History: Received: 10 January 2021; Revised: 12 February 2021; Accepted: 27 March 2021; Published online: 20 April 2021

Abstract: *Internet of Things (IoT) prevails in the technological world among various technologies. The creation of IoT brings about a renaissance in the smart connected world. The security issues in IoT have risen alarmingly in recent years. These security issues are inalienable in IoT network. Particularly, attacks in IoT network layer exploit the entire IoT system. The most common attack which makes a big impacts on RPL based IoT network is rank attack. The impacts of rank attack could be reduced by providing efficient technique to identify and mitigate the rank attack. In this paper, a technique "LEACE" is proposed to identify and mitigate rank attack based on the level of the nodes in the network. Rank and level of the nodes are corresponded in the IoT system. For identifying rank attack, the level and rank of the nodes are checked whether the nodes' rank are corresponded with their level. The proposed technique outperforms the VeRa technique. It provides better results than the VeRa in terms of packet delivery ratio, detection accuracy and throughput.*

Key words: RPL, Rank attack, LEACE, IoT

1Introduction

Internet of Things (IoT) is a looming technology in the modern era which connects everything in the world via Internet. The connected things in an IoT system have distinct ID to communicate with each other. These things can be accessed by computers, smartphones and IoT equipped devices through Internet [10 -13]. IoT provides automated services in all fields such as home automation, agriculture, smart city, smart health care, etc. The sensitive data which are collected by the IoT system from these fields are needed to be secured from the intruders. Network security plays a major role for securing data in IoT [14-16]. RPL based network security is the most predominant issue. RPL is designed for low power lossy network (LLN). RPL is the most used protocol for routing in Internet of Things. Rank attack is very harmful attack in RPL based IoT network. Rank attack changes the legitimate rank value into illegitimate. The rank attack reduces packet delivery ratio, throughput and energy. Rank attack is categorized into two types such as rank increased attack which increases the rank of the node illegitimately in the network and rank decreased attack which decreases the rank of the node illegitimately in the network. The proposed LEACE technique identifies and mitigates the rank attack based on the number of hops in the network [17,18].

Further, the paper is divided into four sections such as literature review, methodology, results and discussions and conclusion. Literature review section examines the related work of IoT and rank attack. Methodology section expounds the proposed technique. The result and discussions section explicates the experimental work and comparisons of the proposed work with existing technique. Ultimately, the conclusion gives the key idea of the proposed technique.

2. Review of Literature

In[1], IoT challenges, security and privacy issues were entailed. The context of the paper was detailed into two aspects such as layer-wise attack and taxonomy of the attacks. It explicated the most predominant issues in IoT. The attack tabulation in the paper gave the better comprehension of various attack in IoT.

Charles Wheelus et al.[2] analyzed security crises in Internet of Things. The authors explained the security threats which provoked a security crises in IoT system. The authors were able to shed some light on the characteristics for securing the IoT environment. The framework for deploying secured IoT was proposed.

Ch Sandeep et al.[3] delved into IoT architecture, elements of IoT and security in IoT. The authors specially expounded the momentous role of security for IoT architecture and its development. The significant roles of security in each layer were explored. The attacks in Internet of Things were mooted by the authors.

The article [4] examined the portrayal of RPL attacks by simulating them in Cooja simulator. The impacts of RPL on resources, topology and data traffic in IoT were analyzed. The article was concluded that energy and packet loss ratio were the major parameters to be analyzed for detecting attacks in RPL protocol.

Mahammad et al.[5] explicated the topological vulnerabilities such as version number attack and rank attack. Authors introduced proficient scheme to counter these attacks. The scheme used online and offline signature process to scout out the predominant attacks in RPL. The scheme was compared with existing techniques namely TRAIL and VeRA. It achieved better results than the compared techniques in term of authentication.

In [6], diverse techniques and methods were spotlighted which were used to get wind of rank attacks in RPL based Internet of Things. These techniques were looked over their key ideas behind finding and mitigating the rank attack in RPL. Friedman test was conducted to compare the impacts of rank attack, selective forwarding attack and IP spoofed attack on RPL.
Aditya Tandon et al.[7] recommended enhanced trust based method to secure IoT routing against sybil and rank attacks. The method solved the destructive situation in IoT which was generated by simultaneous occurrence of sybil and rank attacks. It was compared with Sec-Trust protocol in terms of detection accuracy, energy consumption and throughput.
Abd Mlak Said et al.[8] suggested anomaly based rank attack detection system using support vector machine in IoT network. The system was deployed in healthcare field to secure patients' sensitive data. The system provided better detection accuracy.
Majula et al.[9] proposed multiple intrusion detection system to identify detrimental attacks such as rank attack, wormhole attack, selective forwarding attack and denial of service attack in wireless sensor network. The proposed intrusion detection system was simulated using Cooja simulator on Contiki operating system with 10, 40 and 100 nodes. Different parameters like energy consumption, detection accuracy and false positive rate of malicious nodes were considered for evaluating the proposed system.

3. Methodology

In RPL based IoT network, the network is established in different form according to the objective function. The proposed technique "Level based Rank attack detection technique" uses hop count as objective function. In hop count based RPL construction, the node which has less hop count compared with other nodes in the network is selected as parent. The rank of a parent node is required to be less than its child/ children nodes. All the nodes in the network are divided into levels according to the rank of the nodes. The nodes which are having the same rank value are placed in same level. Each node is corresponded with its rank and level in the network. The levels of the nodes are stored in the root node. The levels are updated periodically. Before changing a rank of a node, it has to verify its level for detecting rank attack. If a node is not in the level with its corresponding rank then the node is considered as malicious node which is affected by rank attack. If the level of a node is less than its corresponding rank, it is affected by rank decreased attack. And if the level of a node is higher than its corresponding rank then it is affected by rank increased attack. The malicious node is isolated from the network. After isolating the affected node, the network is reconstructed.

3.1 Theoretical analysis of the proposed LEACE technique

For analyzing the proposed technique, forty nodes are taken and proved that the technique detects the rank attack in RPL based IoT network. Fig 1 shows the legitimate network with nodes' rank and corresponding levels.

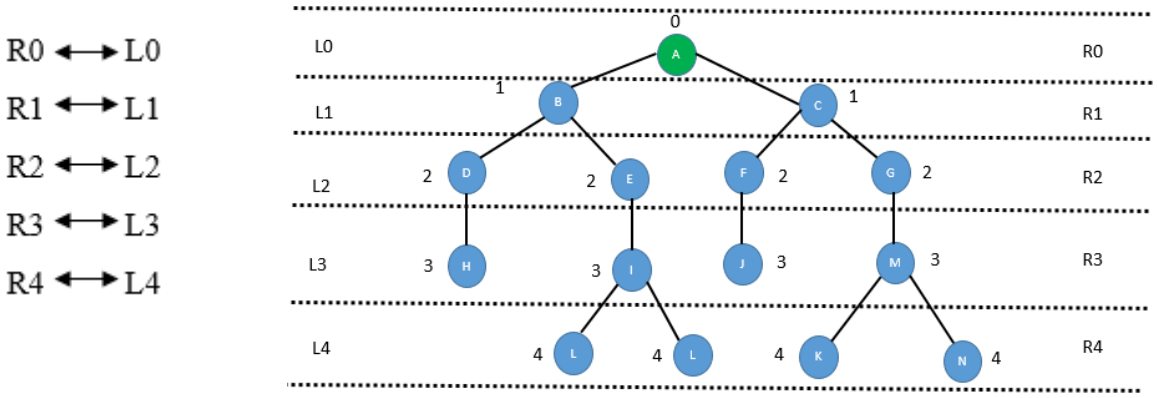

Fig 1 Level of each nodes

In right side of the fig 1, the nodes' rank is given and left side the nodes' level is displayed. R represents the rank of the nodes. L represents the level of the nodes. The correspondence of the rank and level are indicated with double side arrow which is given below.

Table 1 Nodes' Level and Rank

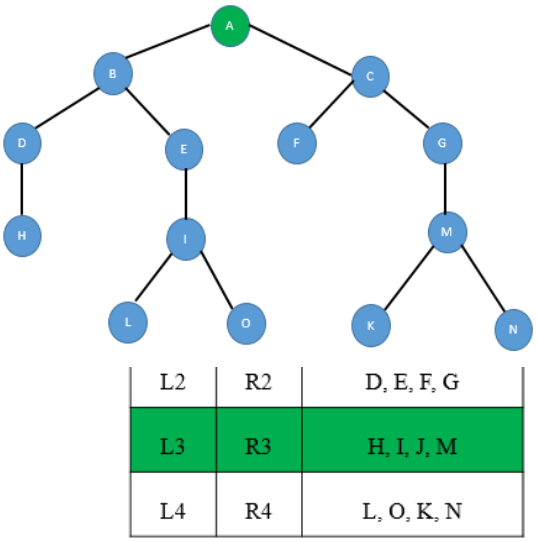

Fig 2 Network with rank attack

Table 1 shows the nodes which are stored levelwise in the root table. The levels of the nodes' are checked by using this table. Let the node J be affected by rank attack which changes its rank into one in the given network.

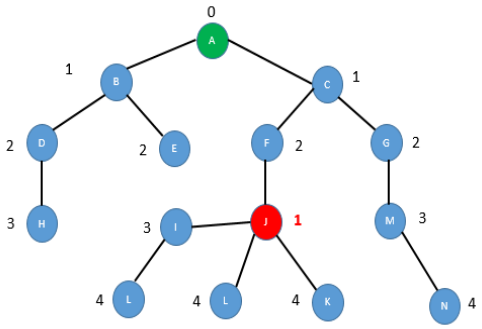

Fig 3 Reconstruction of the network

Now, the level of the node has to be verified from the table which is stored in the root node. From the table 1, the rank of node J is one but the corresponding level for node J is four. So, the rank of the node J does not correspond with its level. It is declared that there is no corresponding matches with rank and level for node J. So, node J is affected by the rank attack. Node J has to be isolated from the network.
Fig 3 shows the reconstruction of the network. The node J is isolated from the network and network is reconstructed with the legitimate nodes. After reconstructing the network, the nodes' level table is updated with current rank and level for the available nodes in the network.

Labels used in the Technique
NHC – Number of hop count
L - Level of a node
CU – Current node
RT – Root node
NR – Neighbor nodes
RK –Rank of a node
PA – Parent node
Ch – Children
AN – All nodes in the network

3.2 Proposed "LEACE" technique

Input ***:*** *RPL Control messages, L, RK*
Output: *Rank attack detection*
1: RT multicasts the DIO messages
2: NR receives DIO messages and send DAO to RT
3: Compute
RK (CU) = RK(PA (CU)) + HC(CU, PA)
4: Children unicast DAO to their selected parents.
5: PA sends DAO_ACK message to CH then the DODAG is constructed.
6: Compute Level of each node from RT to AN based on RK of nodes
for i=0; i++; i<=n-1 // i is Index of Level, n is total number of nodes in the network
{
$L_i = i+0;$
}

7: Do corresponding process of nodes' rank with nodes' level
L_i RK_j ⟷
8: Rank attack detection process
If L (CU) = RK (CU)
CU is an legitimate node
If L (CU) < RK (CU)
CU is affected by rank increased attack
If L (CU) > RK (CU)
CU is affected by rank decreased attack
10: Isolate the affected nodes
11: Reconstruct the network

4. Experimental Result

For implementing level based rank attack detection technique, Cooja simulator is used over the Contiki operating system. Forty nodes have been taken for the testing process. The sky mote is used to simulate the proposed work.

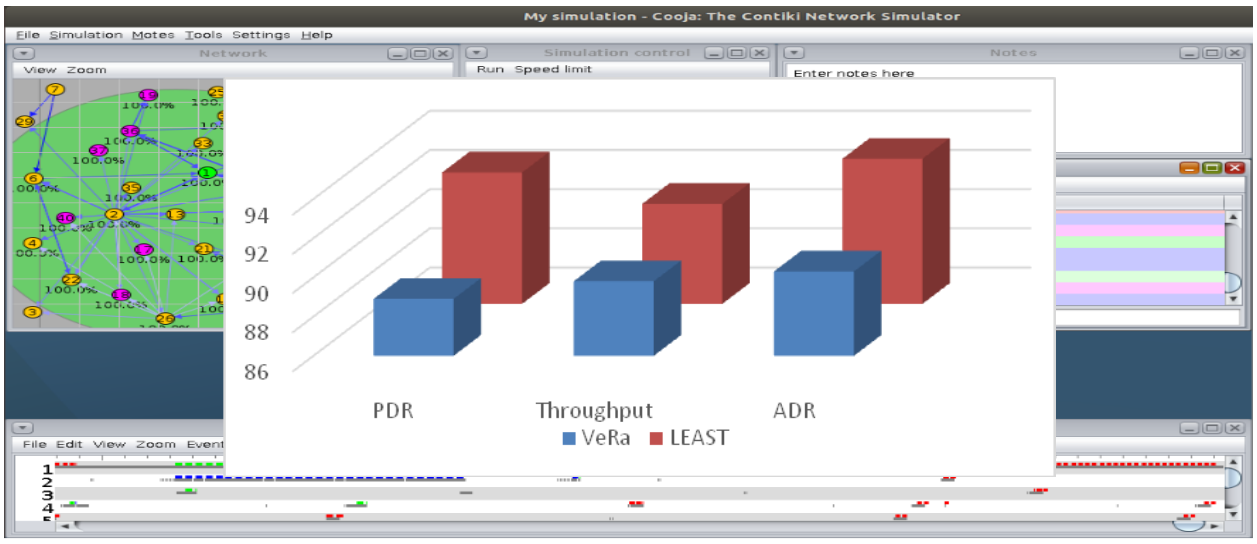

Fig 4 Rank Attack identification

Fig 4 exposes the rank attack detection process. The node which is in green colour is the root node. The yellow colour nodes are legitimate nodes in the network. The pink colour nodes are malicious nodes which are affected by the rank attack. The nodes which are detected as malicious nodes are specified in the mote output.

Fig 5 LEACE vs VeRa

Fig 5 depicts the comparison of the proposed work. The proposed work is compared with the existing technique VeRa in terms of packet delivery ratio, throughput and attack detection rate. The values for Packet delivery ratio (PDR), Throughput and Attack Detection Ratio are given in percentage. The proposed LEACE technique has performed better than the VeRa technique.

5. Conclusion

The proposed technique is a proficient technique to detect rank attack in RPL based Internet of Things. It identifies rank attack using the level of the nodes in the network. Each node is corresponded with rank and level in the network. The proposed work outperformed the existing technique VeRa in terms of packet delivery ratio, throughput and attack detection accuracy. In future, the work will be tested for other attacks such as block hole attack, sinkhole attack, version number attack and hello flood attack in Internet of Things environment.

References

[1]Dhuha Khalid Alferidah1 and NZ Jhanjhi, "A Review on Security and Privacy Issues and Challenges in Internet of Things", International Journal of Computer Science and Network Security, Volume 20, Issue No.4, 2020, pp. 263-285

[2] Charles Wheelus and Xingquan Zhu, "IoT Network Security: Threats, Risks, and a Data-Driven Defense Framework." IoT,Volume 1, Issue 2, 2020, pp. 259-285.

[3] Bhasha, A. C., & Balamurugan, K. (2019). Fabrication and property evaluation of Al 6061+ x%(RHA+ TiC) hybrid metal matrix composite. SN Applied Sciences, 1(9), 1-9.

[4] Sandeep CH, Naresh Kumar S, Pramod Kumar P,"Significant Role of Security in IoT Development and Iot Architecture", Journal Of Mechanics Of Continua And Mathematical Sciences, Volume 15, Issue 6, 2020, pp 174-184.

[5] Balamurugan, K., Uthayakumar, M., Sankar, S., Hareesh, U. S., & Warrier, K. G. K. (2018). Effect of abrasive waterjet machining on LaPO 4/Y 2 O 3 ceramic matrix composite. Journal of the Australian Ceramic Society, 54(2), 205-214.

[6] Marius Preda and Victor Valeriu Patriciu, "Simulating RPL Attacks in 6lowpan for Detection Purposes", 13th International Conference on Communications (COMM), Bucharest, Romania, pp. 239-245, 2020, doi: 10.1109/COMM48946.2020.9142026.

[7] Mohammad Nikravan, Ali Movaghar and Mehdi Hosseinzadeh, "A Lightweight Defense Approach to Mitigate Version Number and Rank Attacks in Low-Power and Lossy Networks", Wireless Personal Communications, Volume 99, Issue 2, 2018, pp. 1035-1059.

[8] Mohammed Amine Boudouaia, Adda Ali-Pacha, Abdelhafid Abouaissa and Pascal Lorenz, "Security against Rank Attack in RPL Protocol", IEEE Network, Volume 34, Issue 4, 2020, 133-139.

[9] Loganathan, J., Latchoumi, T. P., Janakiraman, S., & parthiban, L. (2016, August). A novel multi-criteria channel decision in co-operative cognitive radio network using E-TOPSIS. In Proceedings of the International Conference on Informatics and Analytics (pp. 1-6).

[10] Aditya Tandon and Prakash Srivastava, "Trust-based Enhanced Secure Routing against Rank and Sybil Attacks in IoT," Twelfth International Conference on Contemporary Computing (IC3), Noida, India, 2019, pp. 1-7, doi: 10.1109/IC3.2019.8844935.

[11] Abd Mlak Said, Aymen Yahyaoui, Faicel Yaakoubi, and Takoua Abdellatif, "Machine Learning Based Rank Attack Detection for Smart Hospital Infrastructure." In International Conference on Smart Homes and Health Telematics, Springer, Cham, pp. 28-40, 2020, doi: 10.1007/978-3-030-51517-1_3.

[12] Manjula C Belavagi and Balachandra Muniyal, "Multiple intrusion detection in RPL based networks", International Journal of Electrical and Computer Engineering, Volume 10, Issue 1, 2020, pp. 467-476.

[13] Loganathan, J., Janakiraman, S., & Latchoumi, T. P. (2017). A Novel Architecture for Next Generation Cellular Network Using Opportunistic Spectrum Access Scheme. Journal of Advanced Research in Dynamical and Control Systems,(12), 1388-1400.

[14] Ranjeeth, S., Latchoumi, T. P., & Paul, P. V. (2020). Role of gender on academic performance based on different parameters: Data from secondary school education. Data in brief, 29, 105257.

[15] Ezhilarasi, T. P., Dilip, G., Latchoumi, T. P., & Balamurugan, K. (2020). UIP—A Smart Web Application to Manage Network Environments. In Proceedings of the Third International Conference on Computational Intelligence and Informatics (pp. 97-108). Springer, Singapore.

[16] Loganathan, J., Janakiraman, S., Latchoumi, T. P., & Shanthoshini, B. (2017). Dynamic Virtual Server For Optimized Web Service Interaction. International Journal of Pure and Applied Mathematics, 117(19), 371-377.

[17] V. A. Jane, Dr. L. Arockiam. (2021). DaRoN: A Technique for Detection and Removal of Noise in IoT Data by using Central Tendency. Annals of the Romanian Society for Cell Biology, 25(2), 3197.

[18] Latchoumi, T. P., & Sunitha, R. (2010, September). Multi agent systems in distributed datawarehousing. In 2010 International Conference on Computer and Communication Technology (ICCCT) (pp. 442-447). IEEE.