Intrusion Detection System for Detecting Rank Attacks in RPL based 6LoWPAN Networks

R. Stephen[1], A. Dalvin Vinoth Kumar [2], Dr. L.Arockiam[3]
Research Scholar[1], Research Scholar[2], Associate Professor[3]
Department of Computer Science,St. Joseph's College (Autonomous), Tiruchirapalli, India.

Abstract:

The 6LoWPAN networks are connected to small and constrained devices. They raise more security concerns due to the nature of devices accessible at anywhere from theinternet. Hence,they are vulnerable. The 6LoWPAN network devices are vulnerable to various attacks from inside and outside the network that are aimed to disrupt the network performances.This paper proposes an architecture for intrusion detection in 6LoWPAN networks.

Keywords - **Internet of Things, RPL, Rank attack, 6LoWPAN network.**

I. Introduction

In Internet of Things, the constrained devices are connected with IPv6 address based over the Low Power and Lossy Networks using standard routing protocol. Nowadays, IoT becomes an emerging technology in a wide range of applications [1]. These include home automation, city management, healthcare, environmental monitoring etc. But, the major problem of IoT is connected with unreliable networks due to limited storage, memory and process.

Routing in LoWPAN is divided into static and dynamic [2]. The distance vector protocols are used in dynamic environment and RPL is used in static environment. RPL is an IP-based routing protocol for low power and lossy networks. It is primarily designed for the Internet of Things [3]. In IoT, the sensor nodes are connected and transfer the information towards the root (sink)node as shown in figure 1.

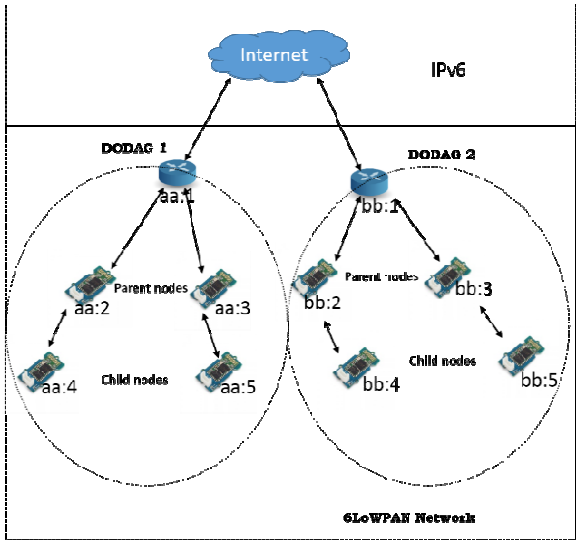

Figure 1: The interconnection of 5LoWPAN network with Internet

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. In this case, sinkhole attacker acts as a parent node to broadcast fake rank value to its neighbor nodes. The nodes which select the sinkhole node become a compromise node to route the traffic through it. The sinkhole attacks create more harmful effects in the LLN when united with selective forwarding and black hole attacks. It is a challenging task to detect and mitigate the sinkhole attacks. This paper proposes a mechanism against

sinkhole attacks in RPL based Internet of Things.

II. Related works

ShahidRaza et al. [4] proposed the real time intrusion detection system in the Internet of Things. This intrusion detection system is called as SVELTE which detects sinkhole attacks and selective forwarding attacks. This IDS achieved 90% true positive rate against sinkhole attacks but it decreased in larger networks. The simulation is tested against routing attacks with energy and memory consumptions.Faiza et al. [5] proposed a Trust-based intrusion detection system architecture for mobile RPL based networks. This architecture has three modules which are identity management, mobility management and intrusion detection. The authors proposed a mechanism to detect Sybil attack in mobility and analysed on network overhead, energy cost and packet delivery ratio.

Anhtuan et al. [6] aimed at detecting the attacks on the RPL based network topology. The authors used a specification based intrusion detection system to detect the sinkhole attack, the rank attack, the local repair, the DIS attack and the neighbor attack. The detection metrics TPR and FPR are used by IDS module against the attacks.Anthea et al. [7] classified the attacks in RPL based Internet of Things. These attacks targeted on network resources, network topology and network traffic. The authors described these attacks, analyzed and compared their properties. Mahmood et al. [8] reviewed the existing mechanisms for detecting sinkhole attacks on RPL and tabulated the drawbacks of each mechanism.Heiner et al. [9] used two mechanisms to provide authentication in RPL. These are VeRA for rank attacks and TRAIL for topology authentication. Divya et al. [10] classified the routing attacks against RPL in IoT and analyzed the techniques and mechanisms to handle them.Anthea et al. [11] articulated the impact of RPL DODAG version attacks. The authors tested the impact of version attacks by using Contiki operating system, such as impact on delivery ratio, high packet loss, overload and a higher path length. Xiyuan et al. [12] focused on the performance analysis of RPL in multi-hop networks with large scale. Particularly, the authors provided an overview of RPL's key features, metrics and objective functions.

Kevin et al. [13] demonstrated two techniques, parent fail-over and rank authentication to mitigate the effects of sinkholes on an RPL network. The combination of these two techniques was more effective than either one of the techniques. Surendar et al. [14] proposed intrusion detection model for detecting sinkhole attacks, using constrain based specification technique. This work has shown improvement on many critical QoS metrics over the existing scheme. Christian et al. [15] proposed an intrusion detection system called INTI to identify sinkhole attacks. This system combined watchdog, reputation and trust strategies and its effectiveness in terms of attack detection rate, number of false positives and false negatives. Abdul et al. [16] proposed a mechanism to handle rank attack using objective function in RPL for low power and lossy networks. This attack used objective function to change the rank value to affect network performance, such as decrease the packet delivery ratio and end-to-end packet delay. The most frequent attacks in RPL and the affecting parameters are tabulated in table 1.

Table 1: RPL Attacks with Affecting Parameters

Attacks	Affecting parameter	Author
Rank Attack	Packet rate, Packet Delivery Ratio, packet loss rate	Cabarcas [18]
Sinkhole attack	Hop count, packet forward rate, packet arrival rate	Pongle [19]
Worm Hole attack	RSS, Tx power,	Khan [20]
Selective Forwarding attack	Packet sending ratio, PDR, power Loss rate	Wallgren [21]
Clone ID	DIO Traffic, control over head	Wallgren [21]

III. RPL DODAG Construction

The routing protocol for Low Power and Lossy Networks (RPL) designed by the IETF working group, is based on the construction of a Destination Oriented Directed Acyclic Graph (DODAG).In RPL topology, the source nodes send the packets towards the root node (6BR), which is directly connected with the internet. The child nodes select the preferred parent node based on the Rank. The rank value must be in an increasing order from the root towards the child node. Objective function (OF) is used to calculate rank value. The OF0, OF1 are the default Objective Functions used in RPL. There are also other metrics like energy, transmission range etc [17]that are used in RPL to calculate the rank. RPL uses four types of control messages in DODAG construction: (i) DODAG Information Solicitation (DIS), (ii) DODAG Information Object (DIO), (iii) Destination Advertisement Object (DAO) and (iv) Destination Advertisement Object Acknowledgement (DAOAck).

The root node initiates DIO transmission to construct the DODAG. The neighboring nodes receive DIO from root node and send DAO to root node. The root node accepts the node as child node by sending DAOAck as shown infigure 2.

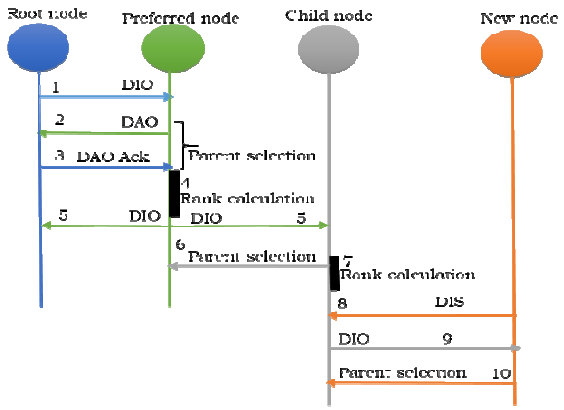

Figure 2: RPL DODAG construction

IV. Impact of Sinkhole Attack or Rank attack in RPL

The RPL is an IP- based routing protocol which is primarily designed for Internet of Things. IoT is connected with constrained devices with limited power, memory and processing. Due to constrained resources, the intruder launches different attacks to disrupt the routing path in the network. This paper works on sinkhole attacks due to its effectiveness in the RPL based Internet of Things. In sinkhole attacks, a malicious node attracts the neighbor nodesto route the traffic through it by using fake routing metrics. In RPL, an intruder launches a sinkhole attack by propagating its rank as a better rank to make nodes as compromised by selecting it as a preferred parent node. Hence, when the data packets are routed through the malicious node either it drops orit selectively forwards the information to the base station. In figure 3, the node J is a malicious node and it attracts the nodes H, I, K and L by sending fake rank value. The nodes H and I choose node J as a preferred parent by believing the fake rank value.

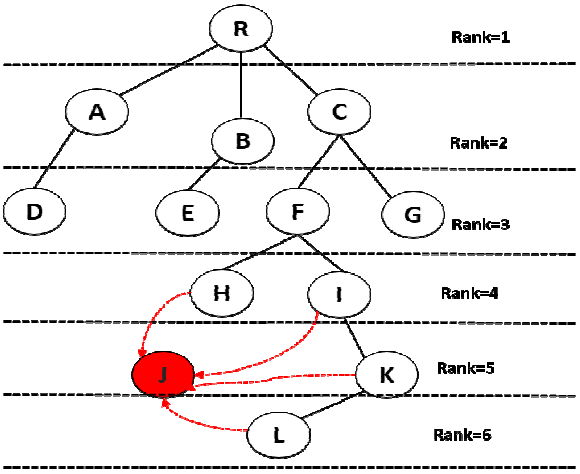

Figure 3: Impact of sinkhole attack

V. Methodology

In RPL, handling routing attacks is one of the key issues. The proposed intrusion detection system handles the rank attack using three phases, (i) rank calculation, (ii) substantiation and (iii) malicious node elimination as shown in figure 4. The attacker node advertises a false rank information to attract its neighbor nodes. This attack is called as rank attack or sinkhole attack.

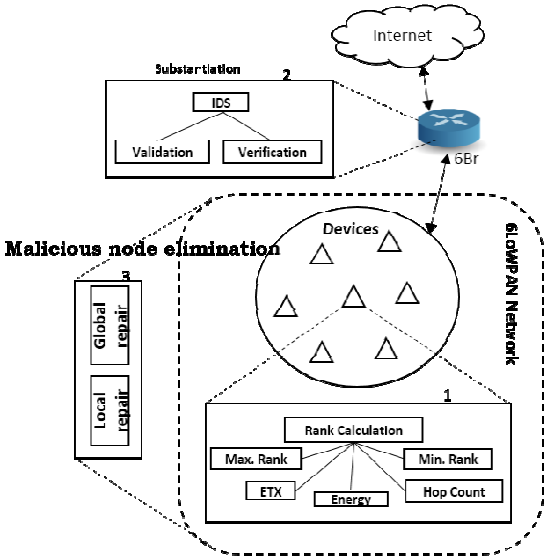

Figure 4: An IoT setup with IDS modules

The following phases explain the proposed architecture:

Phase 1: Rank Calculation based on Energy Metric

In RPL, the network is constructed by forming a destination oriented acyclic graph. The nodes in the RPL network select their preferred parent using rank value. In this phase, two rank calculations are involved namely self-rank and child rank. The self-rank (SR) is the node's own rank. The proposed work concentrates on the energy metric for rank calculation. The self-rank is calculated using the formula given in equation (1). The preferred parent calculates child rank (CR) for all its child nodes. Its initial energy and packets sent by the child nodes are known to the preferred parent. The available energy in the child node is identified by preferred parent using initial energy and spent energy. The CR is calculated as given in equation (2). The SR and CR are used in substantiation phase to identify the attacker node. The parent node maintains the self-energy, child initial energy and expenditure energy as shown in figure 5.

$$SR = PR + Rank_{increase} \qquad (1)$$

Where,

$Rank_{increase} = credit + MinHopRankIncrease$

$$Credit = \frac{Available\ energy}{Initial\ energy}$$

$$CR = PR + Rank_{decrease} \qquad (2)$$

Where ,

$Rank_{decrease} = Expenditure + MinHopRankIncrease$

Expenditure = (packets sent x required energy) + (ideal time x ideal require energy)

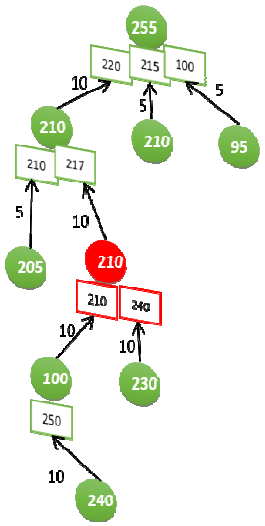

Figure 5: Impact of attacker node with fake energy value

Phase 2: Substantiation

The attacker node is identified in the substantiation phase. The rank information received from neighboring nodes are validated and verified. The validation of child nodes rank is accomplished by cross verification of received rank information. The child rank (CR) is calculated by the preferred parent as explained in phase 1. If the received self-rank and calculated child rank are not identical, then parent node verifies whether the child is an attacker node or not. The identified attacker node is removed from the DODAG by malicious node removal process.

1. ***Validation***

This strategy is used to compute the rank value for each node based on energy. It is defined in phase 1. The 6BR has the routing table to maintain the routing information of each node. This information includesnodeId, rank and initial energy.

2. ***Verification***

This strategy is used to verify the rank value of each node. This verification process is based on energy metric. Periodically, the 6BR receives the current energy of a node. The following formula (2) is used to verify the rank value by using energy metric.

V_r= *Initial energy – Current energy* (2)

Phase 3: Malicious Node Elimination

The malicious node elimination is the key feature in intrusion handling mechanism. The change executed in the network by removing the attacker node is termed as network repair or routing repair. In RPL, there are two types of repairs carried out to eliminate the attacker node. They are local repair and global repair. In local repair, the network change impacts a specific part of the network (Sub DAG). In global repair, the removal of attacker node impacts the whole network (DODAG). The global repair is triggered by the root node which involves in additional control overhead.

Local repair

In local repair, the 6BR node detects the particular malicious node and sends the best optimum path to the remaining nodes.

Global repair

In global repair, the 6BR node repairs the entire network in the context of the malicious nodes more effectively.

Mean degree for Attacker nodes

The expected mean degree of the attacker node in the random topology is derived from the random variable X. The expectation $E[X] = \sum x P_r[X=x]$, where $x \epsilon$ random(x). In this core, X is the hops between the source and destination nodes and x is the link between the intermediate nodes .The multiple of probabilities p and q, gives the total number of attacker packets, where p is a number of attackernode, q is a number of non-attacker node.

The probability of a node to be an attacker nodeis P (d) =$\binom{n}{A}$ p^d $(1-p)^{n-d}$.

The expected mean degree of attacker node

$$\sum_{d=0}^{n} d \binom{n}{d} p^d (1-p)^{n-d} = np$$

The value of np can be created using binomial formula to compute the expected mean

$$(p+q)^n = \sum_{d=0}^{n} \binom{n}{d} p^d q^{n-d}$$

By differentiating both sides with the probability (p).

$$n (p+q)^{n-1} = \sum_{d=0}^{n} d \binom{n}{d} p^{d-1} q^{n-d}$$

$$= \frac{1}{p} \sum_{d=0}^{n} \binom{n}{d} p^d q^{n-d}$$

Where p + q =1

q = 1 – p

Substitution q = 1 – p

$$n (p+(1-p)^{n-1}$$

$$= \frac{1}{p} \sum_{d=0}^{n} d \binom{n}{d} (1-p)^{n-d}$$

$$np = \sum_{d=0}^{n} \binom{n}{d} P^d (1-P^{n-d}$$

Mean Degree Analysis for Proposed IDS

N$\binom{n}{A}$ is a random 6LoWPAN topology with n devices and Ais the probability of possible attacker nodes . The number of available attacker node N(n A) is a random variable with the expected value (n) N degree distribution of link between the nodes.

The Probability of attacker node's presence between source and destination have a certain degree (d). It can be represented for intermediate node I that has the value of P [deg(I) = d]. There are$\binom{n}{A}$ possibilities to d nodes as attacker among total n nodes and probability (p^d) that the node be an attacker node.p^d is the probability that a node has link to d nodes . It is the available neighbour link between the nodes whereas there is no link between (n-d) nodes with probability$(1-p)^{n-d}$ as shown in figure 6.

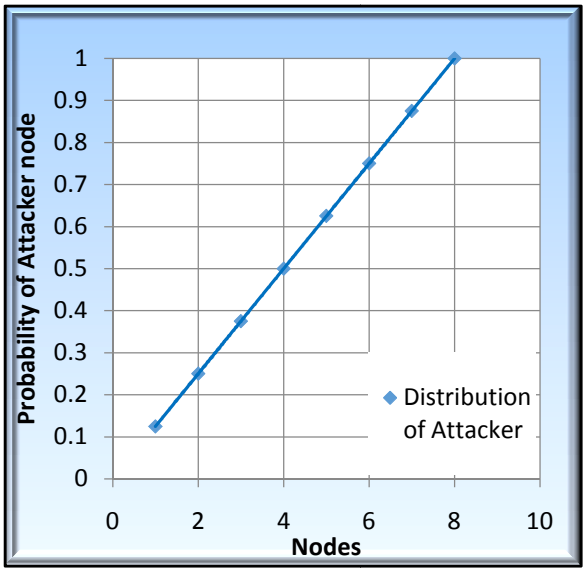

Figure 6: Probability of attacker node distribution

VI. Conclusion

In this paper, an intrusion detection system for Internet of Things is proposed with the energy metric. In RPL, an attacker can exploit the energy metric and launch different attacks by getting a better position in the RPL DAG. To defeat these attacks and also to find the malicious nodes, this

paper has developed energy based intrusion detection module. This IDS module can resist against rank attack and sinkhole attack.

References

[1] Kopetz, and Hermann, "Internet of things",*Real-time systems,* Springer US, 2011, pp.307-323.

[2] C.Mbarushimana, andA .Shahrabi, "Comparative study of reactive and proactive routing protocols performance in mobile ad hoc networks",*InAdvanced Information Networking and Applications Workshops,* Vol. 2, 2007, pp. 679-684.

[3] A. Dalvin Vinoth Kumar, PD Sheba KeziaMalarchelvi, and L. Arockiam. "CALDUEL: Cost and Load overhead reDUction for routE discovery in LOAD ProtocoL",*Advances in Computer and Computational Sciences*. Springer, Singapore, 2017, 229-237.

[4] ShahidRaza, 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.

[5] Hamid Bostani, and Mansour Sheikhan, "Hybrid of anomaly-based and specification-based IDS for Internet of Things using unsupervised OPF based on Mapreduce approach", *Journal on computer communications*, Elsevier, Vol. 98, 2017, PP. 52-71.

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

[7] AntheaMayzaud, RemiBadonnel, Isabelle Chrisment, "A Taxonomy of Attacks in RPL-based Internet of Things", *International Journal of Network Security*, IJNS, Vol.18, Issue. 3, 2016, pp.459 – 473.

[8] MahmoodAlzubaidi, Mohammed Anbar, Samer Al-Saleem, Shadi Al-Sarawi , Kamal Alieyan, "Review on mechanisms for detecting sinkhole attacks on RPLs", *Information Technology (ICIT), 2017 8th International Conference on*. IEEE, DOI: 10.1109/ICITECH.2017.8080028, 2017, pp. 369-374.

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

[10] Sharma Divya, 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. 3, Issue. 1, ISSN: 2454-132x, 2017.

[11] AntheaMayzaud , AnujSehgal , RemiBadonnel , Isabelle Chrisment , and JurgenSchonwalder, "A Study of RPL DODAG Version Attacks", *IFIP International Conference on Autonomous Infrastructure, Management and Security,* Springer, 2014, pp. 92-104.

[12] Xiyuan Liu, Zhengguo Sheng, Changchuan Yin, Falah Ali, and Daniel Roggen, "Performance analysis of Routing Protocol for Low power and Lossy Networks (RPL) in

large scale networks", *IEEE Internet of Things Journal,* 2017.

[13] 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.

[14] Surender M and Umamakeswari, "InDRes: An Intrusion Detection and Response System for Internet of Things with 6LoWPAN", *Wireless Communications, Signal Processing and Networking (WiSPNET), International Conference on*. IEEE, 2016, pp. 1903-1908.

[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] Stephen, R., A. Dalvin Vinoth Kumar, and L. Arockiam. "Deist: Dynamic Detection of Sinkhole Attack For Internet Of Things", International Journal Of Engineering And Computer Science, Vol. 5, Issue.12, 2016, pp. 19358 -19362.

[18] Cabarcas, D., Smith-Tone, D., and Verbel, J. A.,"Key Recovery Attack for ZHFE. In *International Workshop on Post-Quantum Cryptography*, 2017, pp. 289-308.

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

[20] Khan, FarazIdris, "Wormhole attack prevention mechanism for RPL based LLN network",*Ubiquitous and Future Networks*, 2013, pp. 149 -154.

[21] Wallgren, Linus, ShahidRaza, 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, pp.1- 11.