*International Journal of Latest Trends in Engineering and Technology*
*Vol.(10)Issue(1), pp.134-137*
*DOI: http://dx.doi.org/10.21172/1.101.21*
*e-ISSN:2278-621X*

# A SURVEY ON MECHANISMS FOR DETECTING SINKHOLE ATTACK ON 6LOWPAN IN IOT

Melancy Mascarenhas[1], Prof. Vineet Jain[2]

**Abstract- IPv6 over low power wireless personal area network (6LoWPAN) is used in wireless sensor network as it has ability to transmit IPv6 packet with low bandwidth and limited resources. Routing protocol for low power and lossy network (RPL) is routing protocol which is used by 6LoWPAN network. RPL can be exposed to various routing attacks that can damage the network. A sinkhole attack being most destructive routing attack that could affect the network by preventing communication across network devices. This paper aims to survey the existing mechanisms for detection of sinkhole attack on RPL based 6LoWPAN network in IoT.**
**Keywords – 6LoWPAN, Internet of Things, RPL, Security, Sinkhole attack**

## 1. INTRODUCTION

The Internet of Things (IoT) that consists of the conventional Internet and networks of constrained devices connected together using IP protocol in which all different types of objects like smart phones, laptops or smart sensors can connect to the Internet. Nowadays, the number of devices connected to Internet is increasing continuously; it is expected to reach from 30 to 80 billion devices by 2020 [1]. Internet of Things is a technology consisting of many smart objects. Smart objects are devices deployed in the real world which are capable to collect informative data from the real world with the help of their sensors and execute necessary actions. IPv6 with its potentially unlimited address space can connect billion or even trillion of these devices with the IoT. For this purpose, the IETF defined IPv6 on LoWPAN networks to extend these smart devices on the Internet. This definition has given birth to the protocol: 6LoWPAN [13], thereby, integrating IPv6 into Wireless Sensor Networks (WSN).

The exchanged data may contain critical information which belongs to devices like home sensors, medical devices, and industrial devices. Thus, a large number of devices connected to each other and also to the internet which requires high level of security. So, it is very much important to address security issues so that confidential data is not affected. IPv6 over low power wireless personal area network(6LoWPAN) [3], which is a low throughput wireless network comprising low cost and low-power devices. 6LoWPAN uses Routing protocol for low power and lossy network(RPL) as its routing protocol to route the data. RPL can be attacked by various routing attacks which can lead to network damage. Sinkhole attack is most destructive type since it prevents communication among network devices and it is important to detect and mitigate such attack. This paper aims to investigate and survey different existing mechanisms used to detect and mitigate sinkhole attack in RPL for 6LoWPAN network in IoT.

### *1.1 6LoWPAN*

The network working group in [2] presented 6LoWPAN, which is a low throughput wireless network comprising low cost and low-power devices. The network works together to connect the physical environment to real-world applications, such as WSNs. Furthermore, the physical and MAC layers are compatible with the IEEE 802.15.4 standard, which enables the IPv6 to run over the IEEE 802.15.4 network by fragmenting the IPv6 packet into 128 bytes instead of 1280 bytes in a typical network. 6LoWPAN network supports the following characteristics:

(i) Small packet size
(ii) 16-bit short or IEEE 64-bit extended media access control addresses
(iii) Low bandwidth 250/40/20 kbps
(iv) Typically, battery operated, relatively low cost, and low power
(v) Networks are ad hoc, and devices have limited accessibility and user interfaces
(vi) (vi)Unreliable due to the nature of devices in the wireless medium

### *1.2 RPL*

The IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) [3] is a standardized routing protocol for the IoT. RPL is primarily used in a 6LoWPAN network. RPL creates a destination-oriented directed acyclic graph (DODAG) between the

[1] Department of Computer Science Engineering, Goa college of engineering, Goa, India
[2] Department of Computer Science Engineering, Goa college of engineering, Goa, India

nodes in a 6LoWPAN. It supports unidirectional traffic towards a DODAG root and bidirectional traffic between 6LoWPAN devices and between devices and the DODAG root (typically the 6BR). There may exist multiple global RPL instances for a single 6LoWPAN network, and a local RPL DODAG can be created among a set of nodes inside a global DODAG. In Figure 2 an RPL DODAG [5] is shown where each node has a node ID (an IPv6 address), a list of neighbors, and a parent node. Each node in a DODAG has a rank that indicates the position of a node relative to other nodes and with respect to the DODAG root. Ranks strictly decrease in the up direction towards the DODAG root and strictly increase from the DODAG root towards nodes.

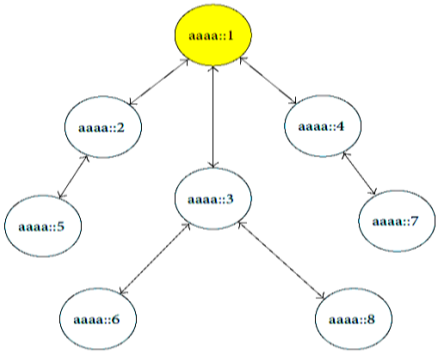


Fig1.RPL DODAG

The root node is also called as the sink node. Root node starts the formation of the topology by broadcasting the DIO (DODAG Information Object) messages. Nodes receiving the DIO message selects the parent to sender, with rank value calculated with respect to the parents rank value and other parameters. The network owner can decide the rank value calculation parameters. The nodes continue to broadcast the DIO message and form the tree topology. The node could join multiple DODAGs within the same RPL instance. DODAG ID is the IPv6 address of the root, and the DODAG version is the current version of the DODAG. Therefore, when a new DODAG is computed with the same root, its version increments. RPL has three main control messages. The first message is the DODAG information object (DIO), which multicasts downward in the RPL instance, and allows other nodes to discover the RPL instance and join it. The second message is the DODAG information solicitation (DIS), which is considered as the link local multicast request for DIO neighbor discovery. The third message is the destination advertisement object (DAO), which flows from the child toward the parents or the root.

*1.3 Sinkhole Attack*

This survey mainly focuses on the attacks that affects the topology of the DODAG graph in RPL, particularly the sinkhole attack [5] that occurs in two steps occurs in two steps. First, the malicious node can attract considerable traffic by advertising falsified information data for parent preference by the other nodes. Then, the malicious node may modify or drop it after receiving the traffic illegally. Sinkhole attack prevents communication between the network devices which can further damage the network. Sinkhole attack can be coupled with other attacks and can cause significant damage for RPL based 6LoWPAN network.

The paper is organized as follows. Section II provides a brief explanation for the recent mechanism and the IDS that are used to detect a sinkhole attack. Section III discusses the drawbacks of each mechanism. The paper is concluded in Section IV.

## 2. RELATED WORK

Dvir et al. [6] proposed an encryption mechanism for version number and rank authentication (VERA). The nodes should be able to change the rank field of a DIO message as it passes through the other nodes. The rank field specifies the favorability of a node that is close to the root and neighbors. Therefore, this field can be forged by a node executing a sinkhole attack. In [6], VERA prevents the attacking nodes from obtaining lower rank than true rank by implementing a one-way hash chain, which is used to ensure the strict increase of ranks from the DODAG root to the constrained nodes. Although the VERA approach can successfully mitigate a version number attack, it is still weak against two topology attacks. First is rank spoofing, which allows an attacker to pretend like any rank in the DODAG. The second is the rank replay attack, which allows a malicious node to claim one level closer to the root by replaying the rank of its parents.

TRAIL [7] was proposed to fix VERA issues in the incompleteness of the message rank authentication in VERA. Then, TRAIL presents enhancements to VERA for repair, and finally discovers and isolates bogus nodes while these nodes attack the RPL routing hierarchy. TRAIL also have a problem, in which a child node chooses an attacking node as its parent since a child node cannot determine whether its parent node is an attacking node. Therefore, Iuchi et al. in [7] proposed a secure parent solution to ensure that child nodes select a legitimate node as their parent. Each child node can select a legitimate node as its parent. In addition, each node selects a parent after excluding the best candidate if multiple parent nodes are offered.

In [9], the authors present SVELTE, an IDS that handle different attacks, including sinkhole, selective forwarding. The centralized system defines three modules: mapping (6Mapper), intrusion detection and a mini-firewall to routing attacks. In [12], the authors describe Ebbits, a system that uses a component to monitor the network traffic in order to perform an

analysis and detect misbehaving nodes. Ebbits detects DoS (denial of service) attacks in 6LoWPAN networks. Although, Ebbits fits to most of the IoT features, it does not consider node mobility and it presents limitations in analyzing node behaviors. Moreover, SVELTE and Ebbits result in high resource consumption, producing low network and system performance. The specification-based IDS was conducted by Le et al. [11] to fix issues in the SVELTE approach, such as providing low false positive rate and low resource consumption. The specification cluster approach solves the synchronization issue that causes the high false positive during the message exchange between the nodes in the previous approach by adding the sequence number information in the DIO and DIS messages.

## 3. ANALYSIS AND COMPARISON OF EXISTING MECHANISMS

The mechanisms based on rank encryption, such as VERA, TRAIL, and secure parent approaches [6,7,8], implement high-level encryption methods and provide rank check in each node to prevent decrease rank attacks. However, these mechanisms are complex in terms of implementation. Each approach only works effectively when combined with the other two approaches Furthermore, the parent fail-over approach alone is insufficient in mitigating a sinkhole attack.

Distributed-based IDS, such as SVELTE and INTI [8], [9] places an agent on both sides of the RPL. The first agent in the host node is for reporting, and the second agent in the DODAG root is for analyzing. These mechanisms have two drawbacks. First, the false positive detection due to the DODAG root has to report the information of the attacking node to each node. However, the information may pass through malicious nodes, which similarly perform as normal nodes; thus, the delivered information is ineffective. The second drawback is high resource consumption due to the agent overhead processing, which is placed in each node.

Cluster-based IDS proposed in [11] adopted SVELTE and overcame its problems by proposing cluster-based IDS. However, the cluster-based IDS can fail due to centralization. By contrast, when the IDS agent in the cluster head goes down due to power or attack, the IDS will no longer be functional. The following table provides a comparison among the mechanisms and IDS that are used to detect sinkhole attacks.

| Mechanisms | Detection method | Disadvantages |
|---|---|---|
| VERA [6] | DIO message rank encryption using SHA | Complex, causes node overhead, resource consumption, and ineffective |
| TRAIL [7] | Analysis algorithm for fixing VERA issues | Based on VERA, the child node may choose the sinkhole node as a parent |
| Secure parent [8] | Selection algorithm presenting a threshold value to solve the parent selection issue in TRAIL | Only provides a symptom solution for parent selection, wherein other issues still exist |
| SVELTE [9] | IDS agent placed in the host node and the main root | High false positive, resource consumption |
| INTI [10] | IDS classifies the node to different categories to inform to the root and support node mobility | Reduced the false positive and resource consumption for SVELTE; however, the limitation of both works in which a few critical QoS metrics were overlooked |
| Specification cluster-based [11] | Cluster-based IDS centralizes the agent in the middle of the node graph to reduce the overhead on the nodes and the root | Solves the resource consumption issue and the false positive issue in SVELTE and INTI; however, it introduces a high probability of IDS failure due to centralization |

Table 1. Summary of mechanisms used to detect sinkhole attack on RPL

## 4. CONCLUSION

This Survey aims to provide a brief understanding related to the type of internal attacks and the influence of sinkhole attacks on RPL. Moreover, the recently proposed various mechanisms and IDS were concluded to detect sinkhole attacks. Further, each mechanism was analyzed and studied, and their advantages and drawbacks with regard to false positive rate and resource consumption was discussed. Finally, a brief comparison was provided in the given table, which shows different detection mechanisms to detect sinkhole attack.

## 5. REFERENCES

[1] Dave Evans. The Internet of Things How the Next Evolution of the Internet Is Changing Everything. https://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FI AL.pdf/, 2011. [Online; accessed 04-May-2015].

[2] [2] K. Kim, S. D. Park, G. Montenegro, S. Yoo, and N. Kushalnagar,"6LoWPAN ad hoc on-demand distance vector routing (LOAD)," Network F. Gonzalez and J. Hernandez, " A tutorial on Digital Watermarking ", In IEEE annual Carnahan conference on security technology, Spain, 1999.

[3] T. Winter, P. Thubert, A. Brandt et al., "RPL: IPv6 routing protocol for low-power and lossynetworks," RFC 6550, March 2012.

[4] A. Mayzaud, R. Badonnel, and I. Chrisment, "A Taxonomy of Attacks in RPL-based Internet of Things," International Journal of Network Security, 2016.
[5] L. Wallgren, S. Raza, and T. Voigt, "Routing Attacks and Countermeasures in the RPL-based Internet of Things," International Journal of Distributed Sensor Networks, vol. 2013, 2013.
[6] A. Dvir, L. Buttyan, and others, "VeRA-version number and rank authentication in RPL," in 2011 IEEE Eighth International Conference on Mobile Ad-Hoc and Sensor Systems, 2011, pp. 709–714.
[7] H. Perrey, M. Landsmann, O. Ugus, T. C. Schmidt, and M. Wählisch,"TRAIL: topology authentication in RPL," arXiv preprint arXiv:1312.0984,2013.
[8] I. Kenji, T. Matsunaga, K. Toyoda, and I. Sasase, "Secure parent node selection scheme in route construction to exclude attacking nodes from RPL network," IEICE Communications Express, vol. 4, no. 11, pp. 340–345, 2015.
[9] S. Raza, L. Wallgren, and T. Voigt, "SVELTE: Real-time intrusion detection in the Internet of Things," Ad hoc networks, vol. 11, no. 8, pp. 2661–2674, 2013.
[10] C. Cervantes, D. Poplade, M. Nogueira, and A. Santos, "Detection of sinkhole attacks for supporting secure routing on 6lowpan for internet of things," in 2015 IFIP/IEEE International Symposium on Integrated Network Management (IM), 2015, pp. 606–611.
[11] A. Le, J. Loo, K. K. Chai, and M. Aiash, "A Specification-Based IDS for Detecting Attacks on RPL-Based Network Topology," Information, vol. 7, no. 2, p. 25, 2016.
[12] P. Kasinathan, C. Pastrone, M. A. Spirito, and M. Vinkovits, "Denial-of service detection in 6lowpan based internet of things," in Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on. IEEE, 2013, pp. 600–607.
[13] Antonio J. Jara, David Fernandez, Pablo Lopez, Miguel A. Zamora and Antonio F. Skarmeta " Lightweight MIPv6 with IPSec support ,A mobility protocol for enabling transparent IPv6 mobility in the Internet of Things with support to the security,