A Survey : Attacks on RPL and 6LoWPAN in IoT

Pavan Pongle
Computer Engineering Department,
Sinhgad College of Engineering,
Pune, India
pavanpongle@gmail.com

Gurunath Chavan
Computer Engineering Department,
Sinhgad College of Engineering,
Pune, India
gt.chavan@gmail.com

Abstract— **6LoWPAN (IPv6 over Low-Power Wireless Personal Area Networks) standard allows heavily constrained devices to connect to IPv6 networks. 6LoWPAN is novel IPv6 header compression protocol, it may go easily under attack. Internet of Things consist of devices which are limited in resource like battery powered, memory and processing capability etc. for this a new network layer routing protocol is designed called RPL (Routing Protocol for low power Lossy network). RPL is light weight protocol and doesn't have the functionality like of traditional routing protocols. This rank based routing protocol may goes under attack. Providing security in Internet of Things is challenging as the devices are connected to the unsecured Internet, limited resources, the communication links are lossy and set of novel technologies used such as RPL, 6LoWPAN etc. This paper focus on possible attacks on RPL and 6LoWPAN network, counter measure against them and consequences on network parameters. Along with comparative analysis of methods to mitigate these attacks are done and finally the research opportunities in network layer security are discussed.**

Keywords: 6LoWPAN, Attacks, Internet of Things, RPL, Security.

I. Introduction

With the introduction of 6LoWPAN compressed IPv6 in WSNs, resource constrained devices can be connected to the Internet. This hybrid network of the Internet and the IPv6 connected constrained devices form the IoT (Internet of Things). Devices are mostly resource constrained and extremely heterogeneous. An IoT device can be sensor node, PC or household appliances connected to the internet, smart meters, a powerful server machine or even a cloud. Hence the number of potential devices that can be connected to the IoT are in hundreds of billions.

A. 6LoWPAN

6LoWPAN integrates IP-based infrastructures and WSNs by specifying how IPv6 packets are to be routed in constrained networks such as IEEE 802.15.4 networks. Due to the limited payload size of the link layer in 6LoWPAN networks, the 6LoWPAN standard also defines fragmentation and reassembly of datagram. The IEEE 802.15.4 frame size may exceed the Maximum Transmission Unit (MTU) size of 127 bytes for big application data, in that case additional fragment(s) are needed. 6LoWPAN networks are connects to the Internet through the 6BR (6LoWPAN Border Router) that is analogous to a sink in a WSN. The 6BR preforms compression/decompression and fragmentation/assembly of IPv6 datagrams.

B. RPL

RPL stands for Routing Protocol for low power and lossy network. It basically designed for the multipoint to point communication, but it can also support the point to point and point to multipoint communication. RPL topology forms the DODAG (Destination Oriented Directed Acyclic Graph) tree, which contain only 1 root. 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 rank value may be depend on the distance from the root node, energy of link etc. The network owner can decide the rank value calculation parameters. The nodes continue to broadcast the DIO message and form the tree topology.

The rest of the paper is organized as follows: Section II discuss the attack on RPL along with their consequences on network and existing solution for these attack. Section III gives discussion on IDS system for 6LoWPAN and RPL based network. Section IV discuss the attacks on 6LoWPAN protocol. Section V is on research areas in RPL network. Section VI concludes the paper.

II. Attacks on RPL Topology

A. Selective Forwarding Attack

This attack takes place by selectively forwarding packets. With this attacks DoS (Denial of Service) attack can be launched. The purpose of attack is to disrupt routing paths and filter any protocol. In RPL attacker could forward all RPL control messages and drop the rest of the traffic. Solution on this attack can be creating the disjoint path or dynamic path between parent and children. Other solution is by using encryption technique in which attacker will not able to identify the traffic flow. Heartbeat protocol [1] basically used for detection of the disruption in network topology but also can be used as defend against selective forwarding attack. IDS solution [2] given the End to End packet loss adaptation algorithm for detection of selective forwarding attack. Such attacks need to detect and removed, RPL self-healing [1] does not correct the topology.

B. Sinkhole Attack

In sinkhole attacks attacker node advertises beneficial path to attract many nearby nodes to route traffic through it. This attack does not disrupt the network operation but it can become very powerful when combined with another attacks. The IDS system [2] give the solution to detect this attack. To

978-1-4799-6272-3/15/$31.00(c)2015 IEEE

defend against sinkhole attack [3] evaluated parent fail-over and a rank authentication technique. The rank authentication technique relies on one way hash technique. The root begins to generate hash value by picking random value, and broadcast it in DIO message. All node calculate the hash value using previous received one and again broadcast it using DIO message. Assumed that malicious node doesn't calculate the hash value, it simply broadcast received DIO message. Each node stores the hash value received by its parent along with number of hops in the path. When root node broadcast random number securely, then node can verify its parent rank using that intermediates hops number. Parent fail-over technique uses UNS (unheard nodes set) field in DIO message indicating that the nodes are in sinkhole compromised path. If the node receives the DIO message containing its ID in UNS then it adds its parent in black list. RPL does not have the self-healing capacity against the sinkhole.

C. Sybil Attack

Sybil attack is similar to a clone ID attack, malicious node uses several identities on the same physical node. Using this attack large parts of a network can be taken under control without deploying physical nodes. Author [4] in his work categorized Sybil attacks in social domain of Internet of Things and stated defense against these attack. Sybil attack on RPL is not evaluated yet.

D. Hello Flooding Attack

For joining the network node broadcast initial message as HELLO message. Attacker can introduce himself as neighbor node to many node by broadcasting Hello message with strong routing metrics and enter in network. In RPL, DIO messages refereed as Hello message, which is used to advertise information about DODAG. This attack can be mitigated by using the link-layer metric as a parameter in the selection of the default route [1]. If it fail to receive link-layer acknowledgements then different route is chosen. Another solution can be by using the geographical distance, node should not select the nodes which are beyond their transmission range. This attack cannot exist for long time in RPL network, as RPL's Global and Local repair mechanism removes this attack. If this attack combines with the other attacks then RPL's Global and Local repair mechanism does not remove it.

E. Wormhole Attack

RPL can undergo the wormhole attack [1]. The main purpose of this attack is Disrupt the network topology and traffic flow. This attack can takes place by creating tunnel between the two attackers and transmitting the selective of all traffic through it. Wormhole attack can be prevented using the construction of Markle tree authentication [5]. In RPL the tree construction starts from root to leaf nodes and Markle tree construction starts from leaf node to root. It uses ID of node and public key for calculation of hash. Each parent is identified by its children. Authentication of any node begins with the root node up to the node itself. If any node failed to authenticate, then children nodes avoids the wrong parent selection.

F. Clone ID Attack

Attacker node clones the identity of other node to gain access to traffic destined to victim node or through victim node. Clone ID attack is possible in RPL network [1]. This attack can be minimized by using tracking number of instances of each identity and this could able to detect cloned identities. If geographical location of the nodes with their identity stored at 6BR, using this we can identify the original node and cloned/malicious node. Other distributed technique is by using distributed hash table (DHT).

G. Blackhole Attack

In the Black Hole attack, similar to a hole which sucks in everything, attacker node drops all data packets silently. In this way, all packets in the network routing through that node are dropped. Author [6] in his work tested the Black hole attack on 6LoWPAN network. For this contikiRPL is used in Cooja simulator. The attack test bed consist of 3 scenarios 1. Network topology with no attack in it. 2. A selective forwarding attack (which is special case of Black Hole attack) in network. 3. Pure Black hole attack in network. For simulating malicious activity modifications are made in Contiki OS such that data packets from neighboring nodes are completely dropped by the malicious node. Malicious node continues to take part in the route formation by sending consistent DIO packets. During the case study author concluded the followings,

1) Increased number of DIO messages reflect instability in the network.
2) Scenario with malicious node sending self-generated data packets showed 8% increase in total number of DIO packets exchanged amongst nodes.
3) While scenario with malicious node not generating any data packets had less number of DIO messages exchanged.
4) Data packets suffer delay in presence of malicious activity in the network.
5) The delay for data packets generated by malicious nodes was 4.3 times higher than to data packets from clear network.

H. Denial of Service Attack

Denial of service or Distributed denial of service attack is attempt to make resources unavailable to its intended user. In RPL this attack can be bring using the IPv6 UDP packet flooding. Many malicious nodes by coordinating can bring the Distributed denial of service attack, in this attack it is difficult to identify the malicious nodes. However IDS system in [7] proposed the framework for detection of DOS attack in 6LoWPAN. The architecture integrates the IDS into the network framework developed within the EU FP7 project ebbits. At the security layer of ebbits Dos protection module is added. IDS probe nodes located in the network which sends periodically the traffic in 6LoWPAN through wired connection to IDS system. Dos protection manager receives the alerts from IDS system. It takes the network related information from other modules of network manager layer to confirm the attack. IDS sends the jamming information of attack to Dos protection manager. The presence of jamming information at the modules of network manager of ebbits indicated the presence of attack.

I. Alteration and Spoofing Attack

1) Rank attack: In RPL rank value increases from root to child node. By changing Rank value, an attacker can attract child node for selecting as parents or improve some other metric, and can attract large traffic going toward the root. The variation of rank attack [8] based on the attack existing duration (continuous or discontinuous) and update or no update of DIO information into four types and evaluated in RPL environment against network QOS parameters. The consequences of rank attack are as follow,

1) Formation of un-optimized path [9]
2) Formation of loop without any detection.
3) Optimized path exist in the topology but never be used.
4) Decrease in packet delivery ratio with slight change in end to end delay [10] when number of attacker increases.
5) The topology around the malicious node is also expected to change. If they update the routing information in the DIO, their neighbors will have to update their topology as well, so more control overheads will be created.

To defend Rank attack VeRA (Version number and Rank Authentication) [11] a new security service for preventing the misbehaving node from decreasing Rank values for attack purpose. VeRA prevents publishing an illegitimate decreased Rank by generating the hash chaining using random number chosen by root node. New hash chain is generated is a nothing but the rank. Attacker cannot change the rank value as it require the previous hash chain value to generate new one. For rank authentication is used which is provided by root node consisting of MAC (Message Authentication Code) over the max rank hash value and next version number as key. Further VeRA schema goes under two attacks [12] Rank hash chain forgery attack and Rank replay attack. As VeRA is only 2-backward-secure, hence it is vulnerable to rank chain forgery. To mitigate this backward-secure approach [12] is proposed in which simple challenge-response procedure is followed and provided authentication of the rank hash chains using an encryption chain instead of MACs. In each rank update, VeRA discloses the cryptographic credentials needed for verifying the advertisements from parents to each node. This attack is mitigated using the Challenge-Response Scheme [12].

TRAIL (TRust Anchor Interconnection Loop) [12], a generic scheme for topology authentication in RPL. It detects and prevents topological inconsistencies by enabling each node to validate its upward path to the root and also detects the rank spoofing on it. TRAIL also minimize network message exchanges and node resource consumption.

2) Version Attack: This attack takes place by publishing the higher version number of DODAG tree. When nodes receive the new higher version number DIO message they start the formation of new DODAG tree. This can cause the generation of new un-optimized topology and brings inconsistencies in topology. The loops and rank inconsistencies created by the attack are generally located around the neighborhood of the attacker. VeRA schema prevents this attack by providing verification to version number using digital signature and MAC. The attack increases control overhead 18 times [13], impacts energy consumption and channel availability. It also reduce the delivery ratio of packets by up to 30% and nearly double the end-to-end delay in a network. An attacker located at large distance from the root causes the highest increase in overhead, and the higher packet loss.

3) Local Repair Attack: In local repair attack, attacker without any problem with link quality periodically sends the local repair message. This causes the local repair around the nodes which hears the local repair message. Local repair attack creates more impact on delivery ratio than any other kind of attack [10], generates more control packets and increases the end to end delay. While constructing the packet dropping occurs from previous topology. Also exhaust the energy of node unnecessarily.

4) Neighbor Attack: In this attack the malicious node broadcast DIO messages that it received without adding information of himself. The node who receives this type of messages may think that new neighbor node send this DIO message. The victim nodes try to select the node which is not in range as parent node and change the route to the out range neighbors. This attack is similar to the wormhole attack with special case of selective forwarding of DIO message only. This attack affects network QOS parameter [10] as no change in packet delivery ratio, slightly increases the end to end delay, slight change in network topology, negligible control overhead. When combined with other attack can be dangerous.

5) DIS Attack: DIS (DODAG Information Solicitation) message used by new node to get the topology information before joining the RPL network. In this attack malicious nodes periodically sends the DIS messages to its neighbors. When the DIS messages broadcast by attacker, the receiver nodes upon receiving DIS message reset the DIO timer assuming something went wrong with the topology around it. When attacker unicast the DIS message the receiver node in return send the DIO message indicating that sender is willing to join the network. Both way of sending DIS message adds the consequences in network as no impact on delivery ratio [10] but DIS multicast attack showed most increase in end to end delay. This attack helps to generate more control overhead and hence energy exhausting.

Table I gives the summery of attack on RPL and their effect on topology along with method used to defend.

III. IoT AND IDS

The intrusion detection system, network security approaches which collects the network data by monitoring network parameters and identify the attacks and attackers. IoT contains the resource constrained devices, so Hybrid IDS architecture [14], [2] is mostly suitable for it. The centralized module can be put on 6BR and small modules in computational aspect which collects the network data can be install on sensor nodes. The IDS system are categorized as follow depending upon the method used for detection of attack.

A. *Event detection based IDS*

IDS architecture based on event detection captures the event triggered in network and by analyzing events raises alarm for attack detection. The IDS architecture [15] uses event based method. When the event occurs the stream of event data if first filtered and stored in databases. The malicious event pattern are defined and stored in database using SQL and EPL (Event Processing Language). When occurred event pattern matches with the stored patterns then alarm raises for attack. This is just a framework designed but not evaluated for any kind of attack detection.

TABLE I: SUMMERY OF ATTACKS ON RPL

Attack	Effect on network parameters	Method to counter measure	Comments on method
Selective forwarding	Disrupt routing path	Heartbeat protocol [1], End to end packet loss	Both techniques only detects the existence of attack
Sinkhole	Large traffic flows through attacker node	IDS solution [2], parent fail-over, rank authentication technique[3]	& IDS solution, parent fail-over detects the attack, Rank authentication technique avoids the attack
Hello flooding	Route formation through attacker node	RPL's Global and Local repair mechanism removes attack	This attack cannot exist for long time in RPL network
Wormhole	Disrupt the network topology and traffic flow	Markle tree authentication [5]	Prevention technique
Sybil and Clone ID	Routing traffic unreachable to victim node	No technique evaluated yet	-
Denial Of Service	Make resources unavailable to Intended user	IDS based solution [7]	not compactable to general network architecture
Blackhole	Packet delay and control overhead	No technique evaluated yet	-
Rank	Packet delay, delivery ratio and generation of Un-optimised path and loop	IDS based solutions [2],[16], VeRA [11], TRAIL[12]	IDS based solutions detects the attack and Vera, TRAIL prevents the Rank attack
version number	control overhead, delivery ratio, end to end delay	VeRA [11]	VeRA prevents attack from occurring
Local Repair	Control overhead, Disrupt routing and traffic flow	IDS based solution [9]	Attack detection mechanism
Neighbor and DIS	Packet delay	No technique evaluated yet	-

B. *Signature detection based IDS*

In signature based IDS system, signature patterns in packets are matched with stored signature of malicious activity or code. If match founds then alarm is raises for attack. RIDES (Robust Intrusion DEtection System) [16] is signature based IDS for resource constrained sensor network connected to IP network. It is a hybrid IDS which uses the features of both signature based and Anomaly based IDS. A novel coding schema used to implement signature based IDS on resource constrained nodes. The sensor nodes runs Bloom filters and Network anomaly detector module, whereas sink stores Signature Database and run the module anomaly based analyzer. At sensor node, the payload of packet is passed through Bloom filter, further processing over the packet is stopped if match founds and alert signal is sent to sink node along with signature code. Author also stated that it is the first kind of signature based IDS for resource constrained devices. This IDS is not evaluated for the attack seen on RPL in section II. As signature matching is done on sensor node this may cause exhaustion of energy of node.

C. *Host based IDS*

This type if IDS system uses the Hybrid architecture model in which centralized and distributed modules cooperates for detection of attack. SVELTE [2] is novel host based Intrusion detection system for IoT running on RPL. This system uses hybrid approach for placement of modules. Two centralized modules 1. 6Mapper which builds the RPL topology and maps it with IDS parameters, 2. Firewall which protects the sensor system from internet attacks. And every sensor node has 3 client modules 6Mapper, Firewall and Packet loss calculator. This system detects rank attack, inconsistency in RPL topology, sinkhole attack and selective forwarding attack. For simulation RPL instance on Contiki os is used and Tmote sky node as sensor nodes. This IDS system can be extend to detect more attacks like wormhole, local repair, Sybil etc.

D. *Specification based IDS*

This type of IDS also known as software engineering based [9] or Finite state machine (FSM) based IDS. IDS [17] is Finite state machine based IDS. This IDS detects Rank attack and Local repair attack. The FSM consisting states are start, topology setup, sending receiving of DIO, Invalid topology and attack states. The system consist of a backbone node and many monitoring nodes. Each node is covered under at least one monitoring node. The rank attack can be detected by monitoring node by listening DIO message from malicious node comparing its parent and its rank value. The Local repair attack generating node is detected by using number of times the topology changed by node compared with threshold value. The FSM can be extended by adding states for detecting other RPL attack, and it can enhance the detection range of large number of attack.

Table II gives the summery of existing IDS system, method used to detect the attack and placement of IDS in network.

TABLE II: SUMMERY OF EXISTING IDS IN IOT

IDS	Method	Attack detection	Placement
RIDES [16]	Signature based IDS, uses Bloom filter for signature matching	No	Hybrid
[7]	DOS detection IDS architecture on ebbits	DOS	Hybrid
[17]	Finite state machine based IDS system	Rank and local repair	Distributed
SVELTE [2]	Topology construction at 6BR, Host based IDS system	Sinkhole, DODAG inconsistency, Rank, selective forwarding	Hybrid
[15]	Complex Event Processing based IDS system	No	Centralized

IV. Attacks on 6LoWPAN

6LoWPAN provides the connectivity between IPv6 network and resource constrained devices. It acts as adaptation layer. As devices are resource constrained so the maximum MTU size is 127 bytes only, however IPv6 minimum MTU size is 1280 bytes due to this the fragmentation is done. 6LoWPAN does not support any kind of authentication mechanism this lead to fragmentation attack.

A. Fragmentation Attack

In this attack the attacker may put his own fragments in fragmentation chain as there is no authentication mechanism at receiver side for checking that received fragment is not a spoofed or duplicated fragment. To mitigate this attacks, author [18] propose two mechanisms, split buffer approach and content chaining scheme. The content chaining scheme uses cryptography to verify that received fragments belong to the same packet or not, on a per-fragment basis.

Attacker can attack on the receiver buffer allocation as the receiver waits for all fragments to receive for reassembly. Attacker can take advantage of this fact to perform attack. Split buffer schema [18] promote direct competition between original senders and an attacker for reassembly buffer resources.

B. Authentication Attack

6LoWPAN does not authenticate the node before joining the network. Due to this any attacker node can easily joins the network. To authenticate the nodes author [19] presents a mechanism that can be used to control the nodes that have access 6LoWPAN network. This method is based on administrative approval, which controls the third party nodes from using the network to communicate with regular nodes. The mechanism comprises of four steps node presence detection, node authorization, authorized node list propagation and data filtering. The border router contains the list of nodes in the network with their layer 2 address. Using this address the presence of node is determined. And authorized to only those nodes which are in the list. The data filtering is done by decision process based on the address of nodes and flow of data between authorized and regular nodes.

C. Confidentiality Attack

Providing confidentiality or encryption mechanism in 6LoWPAN can help to mitigate the various attacks including eavesdropping, man in middle, spoofing kinds of attacks etc. 6LoWPAN extension for IPsec [20] provide the End-to-End (E2E) secure communication between IP enabled sensor networks and the traditional Internet. The extension supports both IPsec's Authentication Header and Encapsulation Security Payload. Using this communication endpoints are able to check the integrity of messages, encrypt and authenticate using standardized and established IPv6 mechanisms.

Crypto hardware can be used within existing IEEE 802.15.4 for 6LoWPAN/IPsec [21] for getting more speed in generation of encrypted packets. IPsec scales better than linklayer security when the data size and the number of hops grow, results in time and energy savings.

The author [22] examined implementation of Moving Target IPv6 Defense (MT6D) in 6LoWPAN. The MT6D is basically designed to defend against network attacks such as Denial-of-Service and Man-In-The-Middle. In MT6D the nodes continuously changes their address in deterministic fashion such that attacker will not able to perform the attack on specific node.

D. Security threats from internet side

As 6LoWPAN is directly connected to the unsecured internet can undergo attacks from internet. For avoiding such attack the firewall [2] could be installed on 6BR to control the malicious packets from internet.

V. Research opportunities

6LoWPAN is novel technology designed for resource constrained devices to connect to internet using IPv6. These could go under attack due to vulnerabilities of 6LoWPAN, IPv6 and RPL protocol. 6LoWPAN can undergo attack form internal WSN and external internet environment. Resource constrained devices has limited computational capacity so the traditional security solution could be optimized to light weight design. RPL does not provide the security as the AODV, DSDV protocol. Attacker can take benefit of this to generate attacks. Network layer attack form IPv4 network can be takes place on IPv6 networks. Some of these attacks has been evaluated in RPL and 6LoWPAN environment but lots of attacks yet not. We will discuss these attack as follow.

A. Research on RPL attacks

1) Internet Smurf attack: Internet Smurf attack takes place by spoofing the victim node address and echo message to other node. This could lead the flooding to victim node. RPL has not been evaluated for this attack. If attack exists the defense for this attack, detection of attack using IDS solution can be a research challenge.

2) Homing attack: By traffic analysis attacker can identify the important node for attack being performed. This type of attack is known as Homing attack. Attack can be interested in knowing root node or nodes which are direct child of root node. By exploiting these nodes attacker can bring attack on RPL with more concentration. The defense mechanism and detection of this attack using IDS or cryptographic solution could be a research challenge.

3) Wormhole attack detection: We have discussed in section II about the prevention technique for wormhole attack. The IDS detection technique for wormhole attack and other prevention/detection technique [23] could be a research area.

4) Blackhole attack detection: In section II we have discuss the Blackhole attack and its consequences on RPL. However the detection and prevention mechanism is not evaluated for RPL environment. IDS solution for detecting the Blackhole attack could be a research area.

5) Sybil and Clone ID attack detection: Both Sybil and Clone ID attack has not been evaluated against the network parameter in RPL. Apart from this there is a requirement for the light weight detection and prevention mechanism for these attacks. Existing IDS solutions can be extended for detection of this attack.

6) Sinkhole attack detection: In section II we have seen the defense mechanism against the sinkhole attack. The traditional sinkhole attack detection mechanism can be optimized for RPL network. IDS solution for detecting this attack on 6LoWPAN network could be a research area.

7) Resource exhausting attack: Resource constrained nodes in RPL can exhaust the resource if they have too many missions to do. RPL lacks the mechanism to limit such actions. The attacker can perform this attack using reprogramming node, to start activities such as broadcasting, sending control messages without reason. This behavior of victim nodes also affects the other neighbor nodes. If attack takes place in large scale then, node will exhaust soon and network operations will be downgraded. There is need of mechanism which controls this types of attack and prevent the nodes from getting out of resources by load balancing.

8) RPL based attack: The IDS based solution for detecting local repair attack, neighbor attack, DIS and version attack could be a research challenge. Apart from this using geographical location or distance verification technique [23] neighbor attack can be removed.

B. Research in IDS systems

The IDS based on the event processing [15], signature based [16] can be extended for detection of attacks discussed in section II. In addition the defining the event pattern and signature pattern for these attack on IPv6 network could be a research area. Specification based [17], host based [2] IDS detects only few simple attack based on RPL vulnerability. These IDS can be extended to detect more complex attack like wormhole, Sybil, clone ID, sinkhole etc.

The other type of IDS are not evaluated for RPL network these IDS system are Anomaly based IDS detection, Artificial intelligence based IDS (techniques such as fuzzy logic, game theory, bio inspired, semantic based)[9], Statistical based IDS (techniques such as Hidden marker chain, Bayesian model, Mathematical model), Data mining based IDS. These IDS techniques can be used to detection of attack in RPL based 6LoWPAN network.

VI. Conclusion

This paper concludes that various mechanism are proposed against the attacks on RPL and 6LoWPAN network. Still many attacks has not evaluated on RPL network. Lots of research is needed to counter these attacks. The attacks like Wormhole, Sybil, clone ID, Blackhole etc. need a detection and prevention mechanism based on IDS or other solutions. The effect of attacks on RPL network parameter such as packet delivery ratio, delay etc. are mentioned. Along with this, survey of existing IDS systems are done, and compared with other systems. At last given focus on research area in RPL attack and their solution.

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* 2013 (2013).

[2]. Raza, Shahid, Linus Wallgren, and Thiemo Voigt. "SVELTE: Real-time intrusion detection in the Internet of Things." *Ad hoc networks* 11.8 (2013): 2661-2674.

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

[4]. Zhang, Kuan, et al. "Sybil Attacks and Their Defenses in the Internet of Things."

[5]. Khan, Faraz Idris, et al. "Wormhole attack prevention mechanism for RPL based LLN network." *Ubiquitous and Future Networks (ICUFN), 2013 Fifth International Conference on*. IEEE, 2013.

[6]. Chugh, Karishma, Aboubaker Lasebae, and Jonathan Loo. "Case Study of a Black Hole Attack on 6LoWPAN-RPL." *SECURWARE 2012, The Sixth International Conference on Emerging Security Information, Systems and Technologies*. 2012.

[7]. Kasinathan, Prabhakaran, et al. "Denial-of-Service detection in 6LoWPAN based internet of things." *Wireless and Mobile Computing, Networking and Communications (WiMob), 2013 IEEE 9th International Conference on*. IEEE, 2013.

[8]. Le, Anhtuan, et al. "The Impact of Rank Attack on Network Topology of Routing Protocol for Low-Power and Lossy Networks." (2013): 1-1.

[9]. Le, Anhtuan, et al. "6LoWPAN: a study on QoS security threats and countermeasures using intrusion detection system approach." *International Journal of Communication Systems* 25.9 (2012): 1189-1212.

[10]. Le, Anhtuan, et al. "The impacts of internal threats towards Routing Protocol for Low power and lossy network performance." *Computers and Communications (ISCC), 2013 IEEE Symposium on*. IEEE, 2013.

[11]. Dvir, Amit, Támas Holczer, and Levente Buttyan. "VeRA-version number and rank authentication in rpl." *Mobile Adhoc and Sensor Systems (MASS), 2011 IEEE 8th International Conference on*. IEEE, 2011.

[12]. Perrey, Heiner, et al. "TRAIL: Topology Authentication in RPL." *arXiv preprint arXiv: 1312.0984* (2013).

[13]. Mayzaud, Anthéa, et al. "A Study of RPL DODAG Version Attacks.", 2013

[14]. Kasinathan, Prabhakaran, et al. "DEMO: An IDS framework for internet of things empowered by 6LoWPAN." *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013.

[15]. Jun, Chen, and Chen Chi. "Design of Complex Event-Processing IDS in Internet of Things." *Measuring Technology and Mechatronics Automation (ICMTMA), 2014 Sixth International Conference on*. IEEE, 2014.

[16]. Amin, Syed Obaid, et al. "A novel coding scheme to implement signature based IDS in IP based Sensor Networks." *Integrated Network Management-Workshops, 2009. IM'09. IFIP/IEEE International Symposium on*. IEEE, 2009.

[17]. Le, Anhtuan, et al. "Specification-based IDS for securing RPL from topology attacks." *Wireless Days (WD), 2011 IFIP*. IEEE, 2011.

[18]. Hummen, René, et al. "6LoWPAN fragmentation attacks and mitigation mechanisms." *Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*. ACM, 2013.

[19]. Oliveira, Luis ML, et al. "Network admission control solution for 6LoWPAN networks." *Innovative Mobile and Internet Services in Ubiquitous Computing (IMIS), 2013 Seventh International Conference on*. IEEE, 2013.

[20]. Raza, Shahid, et al. "Securing communication in 6LoWPAN with compressed IPsec." *Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011 International Conference on*. IEEE, 2011.

[21]. Raza, Shahid, et al. "Secure communication for the Internet of Things—a comparison of link-layer security and IPsec for 6LoWPAN." *Security and Communication Networks* (2012).

[22]. Sherburne, Matthew, Randy Marchany, and Joseph Tront. "Implementing moving target IPv6 defense to secure 6LoWPAN in the internet of things and smart grid." *Proceedings of the 9th Annual Cyber and Information Security Research Conference*. ACM, 2014.

[23]. Khan, Zubair A., Saeed U. Rehman, and M. Hasan Islam. "An analytical survey of state of the art wormhole detection and prevention techniques." *International Journal of Science and Engineering REsearch* 4.6 (2013): 1723-1731.