International Journal of Advance Research in Science and Engineering
Volume No.07, Special Issue No.03, April 2018
www.ijarse.com
IJARSE
ISSN: 2319-8354

A Survey on Security Attacks and Countermeasures in RPL for Internet of Things

Ruchi Mehta[1], M.M.Parmar[2]

[1,2]Electronics and Telecommunication Department,
Sardar Patel Institute of Technology, Mumbai, (India)

ABSTRACT

Internet of Things is attracting a lot of attention in the modern world and has become a part of daily life leading to a large scale of distribution of Low power and Lossy Networks (LLN). These networks have been deployed in the world of home automation, manufacturing, life sciences, agriculture, military, etc which form a network of IoT devices, embedded sensors and their interconnection to the Internet. For such networks constrained by low power and storage, an open standard routing protocol, RPL (Routing Protocol for Low Power and Lossy Networks) has been proposed by IETF. However this protocol is vulnerable to a number of attacks which may degrade the performance and resources of the network leading to incorrect output. In this paper we propose to establish taxonomy of the attacks against RPL protocol and shall discuss the existing counter measures and their usage against these attacks. The paper shall also highlight the recent usage of Trust based mechanism to detect and mitigate topology attacks.

Keywords: Internet of things, LLN, RPL, security

I. INTRODUCTION

Internet of Things (IoT) is a dynamic global ecosystem where billions of small devices with data capture and communication capabilities are seamlessly integrated into the information network. These devices have self-configuring capabilities based on interoperable communication protocols. These devices have physical and virtual identities, physical attributes, virtual personalities and use intelligent interfaces which facilitate interactions with "smart things" over the internet. IoT devices are a part of everyday living linking the real world data with the virtual world thus enabling anytime anyplace connectivity for anything like social processes, healthcare, automotive, security, manufacturing, services, energy, agriculture and many other areas. However these devices have limited data storage and processing capabilities. To add the devices have limited power stored in tiny batteries. Hence security challenges with regards to data, privacy, confidentially, identification and access control are pertinent. The existing protocols are not capable of dealing with above mentioned constraints [1]. Hence the IEEE 802.15.4 standard protocol for the communication layers in wireless personal area networks (WPAN) and the 6LowPAN protocol which defines encapsulation and header compression mechanisms between IPv6 and 802.15.4. have been developed. The RPL (Routing Protocol for Low and Lossy Networks) have been proposed at the routing layer based on IPv6 [2]. However this protocol is vulnerable to a number of attacks [3]. The tight energy and processing constraints of IoT devices make the likes of traditional

cryptographic method for protection against various routing attacks inoperable. Many researches have been conducted on security issues regarding mobile ad-hoc networks [4], [5] and wireless sensor networks [6]. The ROLL working group study provides a complete insight into the RPL security issues. The CIAA model (confidentiality, integrity, authentication and availability) classifies these attacks. The study [7] provides guidelines and recommendations to counteract these attacks but lacks to detail how the attacks are quarantined using RPL protocol. In [8] only three attacks regarding RPL protocol have been taken up while studying the security in 6LowPAN networks. The survey [9] of some existing attacks against RPL protocol and the 6LowPAN protocol have been done without any classification and discussed different types of IDS like [10] and [8]. The research in [10, 11, 12, 13] also highlights some attacks targeting RPL protocol but their main contribution is to detect these attacks using an intrusion detection system (IDS). Authors of [14] presented a detailed classification of attacks against RPL and authors of [15] further added some more attacks but it does not include recent countermeasures based on trust based mechanism.

In this paper, our objectives are the identification and categorization of different attacks against the RPL protocol while providing details on how those attacks can take place and the existing countermeasures against those attacks. The paper shall also highlight the recent usage of Trust based mechanism to detect and mitigate topology attacks.

II. RPL PROTOCOL

RPL means Routing Protocol for Low power and Lossy network, is a proactive protocol which operates by discovering routes once the RPL network starts. DODAG (Destination Oriented Directed Acyclic Graph) tree is formed by RPL topology, which contains only one root also known as Sink node. Upon broadcasting the DIO (DODAG Information Object) messages the sink node start creating network topology. Fig. 1 illustrates a network containing many DODAG graphs which operates one or more RPL instances. A set of metrics or constraints determine as association of an objective function to each RPL instance which is accountable for computing the best path. Several instances are joined at the similar time by the RPL node, but it can only connect to one (such as nodes 13 and 17) DODAG graph per instance as in Fig.1.

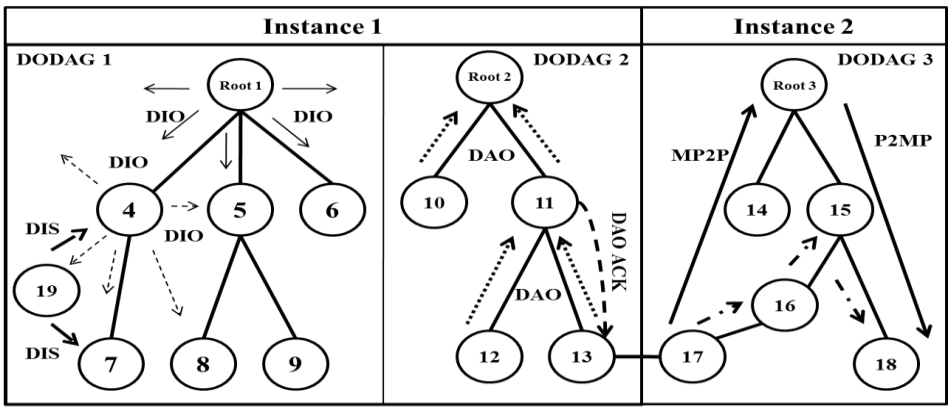

Fig. 1 RPL DODAG

2.1 DODAG Formation

Step by step the DODAG is constructed as depicted in Fig1. A DIO message (DODAG Information Object) is broadcasted originally by the root node. Upon receiving DIO message, RPL node finds its instance and selects a parent. After adding sender to its parent list, node determines its rank by inferring to the objective function present in the DIO message. The parents rank must be lesser than the rank of the child node to assure the acyclic nature of graph. The node sends all the packets to the sink node using its parent which act a gateway for that node. Using trickle timer algorithm the DIO messages are sent at regular intervals to optimize the number of the control messages transmission. Existing network can be joined by a new node by sending a (DODAG Information Solicitation) DIS message. Using the (Destination Advertisement Object) DAO messages downward routes are built. The router nodes manage the routing tables based on the mode of operation specified by the root in DIO messages. DAO-ACK messages are the acknowledged messages of the DAO messages. In this way network topology is created in RPL protocol by exchanging four control messages. Like any other wireless protocol this protocol is also prone to topology attacks like wormhole and grayhole which are explained in next section.

III. CLASSIFICATION OF ATTACKS

The RPL protocol is vulnerable to a number of attacks. The attacks can be classified as attacks targeting network resources, attacks modifying the network topology and attacks related to network traffic.

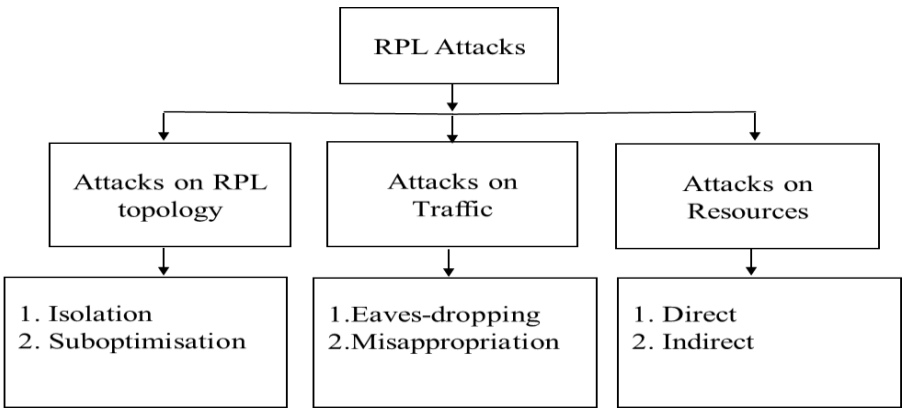

Fig. 2: Broad classification of RPL attacks.

3.1 Attacks on RPL Topology

Network topology can be targeted by attacks against RPL protocol. There are two main categories: suboptimisation attack and isolation attack.

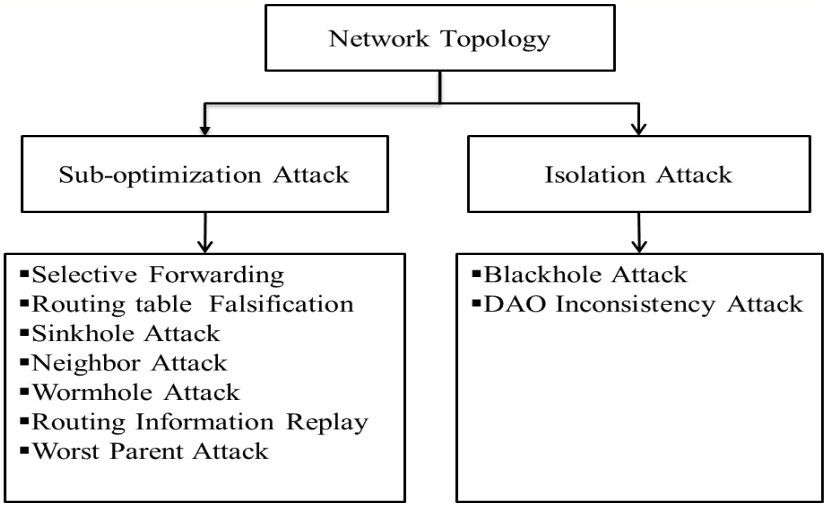

Fig. 3 Network Topology Attack Classification

3.1.1 Sub-optimization Attacks:

These attacks does not let network converge to an optimal path which degrades the performance of the network.

3.1.1.1 Routing Table Falsification Attacks in Storing Mode

To advertise falsified routes to different nodes in a routing protocol, it is likely to forge or modify routing information. By using enhancing or forging DAO control messages, this attack can be accomplished in the RPL network in order to build fake downward routes. This can only be finished when the storing mode is enabled. As an example, a malicious node displays routes toward nodes that aren't in its sub-DODAG. Sub-optimization network is caused when the targeted nodes have wrong routes in their routing table. Longer inducing delay, packet drops or network congestion can be caused by this path.

3.1.1.2 The Sinkhole Attack

The malicious node will create its rank with a good value, usually the same rank of the sink. Its neighbors will select it as their preferred parent and send traffic to that malicious node. The Sinkhole attack is often combined with the Selective Forwarding attack to drop all the traffic attracted. In RPL networks, the attack can be easily performed through the use of the rank value. Because of this falsified advertisement, the malicious node is more often chosen as a preferred parent by the other nodes, while it does not provide better performance. Thus, the routes are not optimized for the network. The topology is modified and the network performance degrades due to the attack.. Besides, if the attacker decides to drop all the traffic, it also performs a black hole attack. The authors in [12] and [10] proposed an IDS after studying Sinkhole attack. A functionality of this IDS is to build a global view of the network and as a result, the possibility to detect incoherence's in the network such as sinkholes. In [16], the authors investigated defense techniques against sinkholes. The first technique is called Rank verification and restricts the possibility for the attacker to decrease its rank value. This allows legitimate nodes to check if another node along the path has a fake rank. The second technique is called parent fail-over and operates as an end-to-end acknowledgment. In a DIO message field, node address is added, when a root node does not receive enough traffic from a node. The node blacklists its parent and selects another one when it

node receives the DIO message with its own identity. The authors show that a combination of these two techniques provides efficient results in an RPL network.

3.1.1.3 Selective Forwarding Attack

By selectively forwarding packets DoS (Denial of Service) attack can be launched with the purpose of disrupting the routing paths and filtering any protocol. The attacker could forward all RPL control messages and drop the rest of the traffic in RPL. Creating the disjoint path or dynamic path between parent and children can be one solution. Using encryption technique in which attacker will not be able to identify the traffic flow can be another solution. Heartbeat protocol [12] basically used for detection of the disruption in network topology but it can be also used as defence against selective forwarding attack. IDS solution [10] gives the End to End packet loss adaptation algorithm for detection of selective forwarding attack. Such attacks need to be detected and removed as RPL self-healing [12] does not correct the topology.

3.1.1.4 Routing Information Replay Attacks

An RPL node can also perform routing information replay attacks. An RPL node records valid control messages from other nodes and forwards them later in the network. In the case of dynamic networks, this attack is quite damaging because the topology and the routing paths are often changed. These attacks cause nodes to update their routing tables with outdated data resulting in a false topology. The RPL protocol uses some sequence counters to make certain the freshness of the routing information such as the Version Number for DIO messages or the Path Sequence present in the Transit Information option of DAO messages [2]. Routing information replay attack is studied in [13] however the authors neither study the consequences of such attack nor explained how it can take place in RPL networks.

3.1.1.5 The Neighbour Attack

The malicious node will replicate any DIO messages that it receives and broadcast them again when this attack is triggered. Upon receiving this type of messages the victims may think that it has a new neighbour, which is not in range. Moreover, the victims may request it as the preferred parent if the new neighbour advertises a good rank and change the route to the out range neighbours.

3.1.1.6 Worst Parent Attacks

"Rank attack" as described in [18] chooses as per the objective function, the worst preferred parent. The resulting path is not optimized which induces poor performance. This attack cannot be easily tackled because children node relies on their parent to route packets and this attack cannot be monitored by neighbours. Using a security solution which rebuilds a global view of the graph based on nodes information should detect this attack such as the proposed solution in [10].

3.1.1.7 Wormhole Attacks

RPL protocol is attacked by Wormhole attack [12] with the purpose to disrupt the network topology and traffic flow. This attack takes place by creating tunnel between the two attackers and transmitting selective traffic through it. Merkle tree authentication [19] can prevent the construction of Wormhole attack. In RPL the tree construction starts from root to leaf nodes and Merkle tree construction starts from leaf node to root. The wormhole attack uses public key and ID of node for calculation of hash. Each parent is identified by its children

and authentication of any node begins with the root node up to the node itself. The children nodes avoids the wrong parent selection if any node failed to authenticate. The authors of [20] have used RSSI received signal strength indicator for detecting wormhole attack and attacker which is resource friendly as it doesn't impose undue overhead on the network.

3.1.2 Isolation Attacks

These attacks isolates a part of the network as a result the nodes present in that part are not able to communicate with the parent nodes as well as other nodes.

3.1.2.1 Black hole attack

A malicious attacker drops all the packets that it is supposed to forward in a black hole attack. The blackhole attack when combined with a sinkhole attack causes the loss of a large part of the traffic which can be seen as a type of denial-of-service attack. It can isolate several nodes from the network, if the attacker is located at a strategic position in the graph. When the attacker only discards a specific subpart of the network traffic it is called a grayhole attack (or also selective forwarding attack). The author Chugh et al. [21] studied the consequences of black hole attacks in RPL networks through a set of Cooja simulations. They highlighted different indicators to detect these attacks such as rate and frequency of DIO messages, packet delivery ratio, loss percentage, and delay. The IDS SVELTE proposed in [10] was designed to detect selective forwarding attacks in such networks.

3.1.2.2 DAO Inconsistency Attacks in Storing Mode

DAO inconsistencies occur when a node has a downward route that was previously learned from a DAO message, but this route is no longer valid in the routing table of the child node [2]. RPL gives a mechanism to improve this inconsistency, called DAO inconsistency loop recovery. This optional mechanism allows RPL router nodes to exclude the outdated downward routes using the Forwarding-Error 'F' flag in data packets which indicates that a packet cannot be delivered by a child node. In order to use another neighbor node the packet with the 'F' flag is sent back to the parent. The packet should normally never go up again, once a packet is transmitted downward. When it happens the router sends the packet to the parent node that passed it with the Forwarding-Error 'F' bit set and the Down 'O' bit left. When the parent node receives the packet with 'F' set it removes the identical routing state by clearing the 'F' bit, and attempt to transmit the packet to another neighbour. If the other neighbour still has an inconsistent state the process reiterates.

3.2 Attacks on Traffic

The attacks targeting the RPL network traffic are included in this category. It includes eavesdropping attacks and misappropriation attacks.

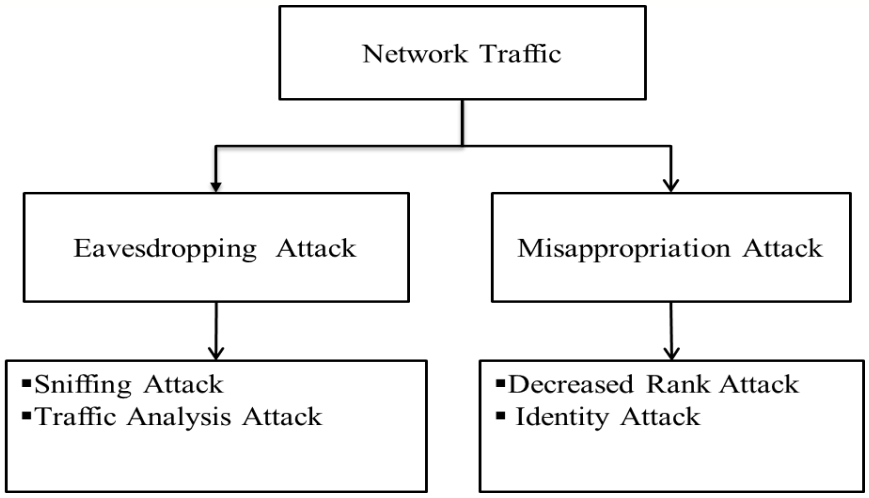

Fig. 4 Network Traffic Attack Classification

3.2.1 Eavesdropping Attacks:

This is a passive attack where attacker performs activities like sniffing and analyses of network traffic.

3.2.1.1 Sniffing Attacks

A sniffing attack entails listening of the packets which are transmitted over the network. Various information can be obtained from the packet which is sniffed like routing and topology information and data content. In RPL networks an attacker can access information such as DODAG ID, Version Number, ranks of the nodes by sniffing the control messages. When an attacker sniffs the data packets it not only discover packet content but also have a local view of the topology in the eavesdropped area by looking at source/destination addresses. This attack becomes difficult to detect as it is passive in nature. Encryption of messages is the only way to prevent sniffing when the attacker is external. Even if RFC 6550 mentions encryption of control messages as an option its implementation is difficult as the technical details are left out from the specification making.

3.2.1.2 Traffic Analysis Attacks

The objective of this attack is to gather routing information about the RPL network such as a partial view of the topology by using the characteristics and patterns of the traffic on a link. A malicious node can possibly perform other attacks along with this attack with the gathered information. Even when the packets are encrypted this attack can be performed The effects of the attack depends on the rank of the attacker. When the node is located close to the root node it can analyse a large amount of traffic and can gather more information as compared to when the attacker node is on the verge of a sub-DODAG.

3.2.2 Misappropriation Attacks

In this category the identity of a genuine node is seized or performance is over claimed. These attacks does not damage the network so much but they are usually chosen as first step to perform other attacks. They permit the attacker with a better understanding of the network and its topology, allow better access or to capture a large part of the traffic.

3.2.2.1 Decreased Rank Attacks

In a DODAG graph, the closer the node is to the root, the lower the rank is and this node has to manage more traffic. When a node maliciously advertises a lower rank value, it claims to over perform because of which

many legitimate nodes connect to the network via the attacker and results in the association of a large part of the traffic. Through the falsification of DIO messages an attacker can change its rank value in RPL network. The solutions proposed like VeRa [22] and the Rank verification method [16] are able to resolve this issue. However authors in [29] proposed an improvement called TRAIL over VeRa as they were not sure regarding rank authentication. Decreased rank attack can also be detected by SVELTE [10] as it can detect sinkhole attacks.

3.2.2.2 Identity Attacks

Identity attacks include both spoofing and Sybil attacks. When a malicious node pretends to be a genuine existing node than a spoofing attack also called Clone ID attack happens. An attacker may sniff the network traffic to identify the root node, as root node helps in building and maintaining the network topology by sending routing information. Once the malicious node is able to identify the DODAG root it can spoof the root address and can take the entire control of the network. During Sybil attacks [23], one malicious node uses several identities on the same physical node. Authors of [24] categorised various Sybil attacks and stated defense against these attacks. Sybil and Clone ID were studies in [12] and the authors showed that there is no self-healing mechanism in the RPL protocol against these attacks and proposed to consider geographical location of nodes to detect such attacks.

3.3 Attacks against Resources

This category of attacks aims at consuming node energy, memory or processing by making legitimate nodes perform unnecessary processing. This attack effect the availability of the network and shortened the lifetime of the network. The two subcategories of attacks includes Direct and Indirect attacks

3.3.1 Direct Attacks:

In direct attacks, the attacker is directly accountable for exhausting the resources. This is done by either launching flooding attacks or by performing routing tables overloading when the storing mode is active.

3.3.1.1 Flooding Attacks

When a node wants to join the network it broadcast initial message as HELLO message. By broadcasting Hello message with strong routing metrics attacker can enter in the network. DIO messages are refereed as Hello message in RPL network. By using the link-layer metric as a parameter in the selection of the default route [2] this attack can be mitigated. RPL self-mechanism is able to remove this attack so this attack cannot stay for long in the network but if is it combined with other attack than it cannot be removed.

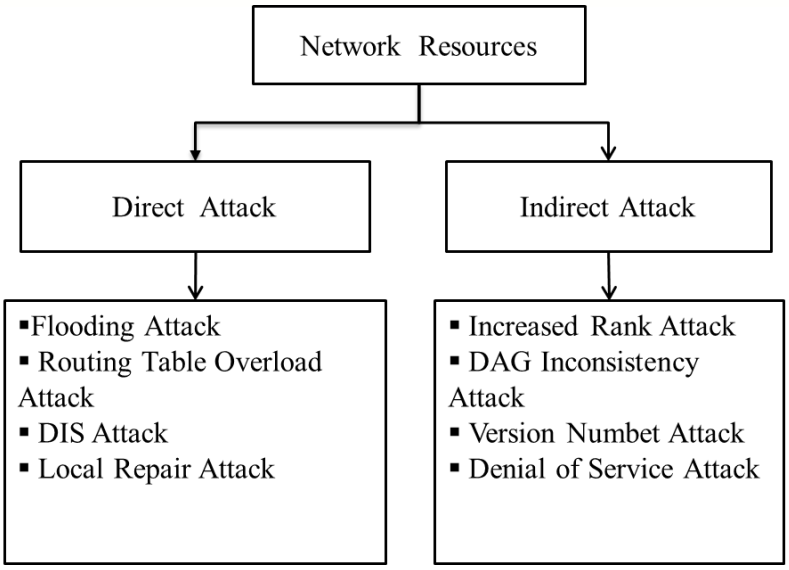

Fig. 5 Network Resource Attack Classification

3.3.1.2 Routing Table Overload Attacks in Storing Mode

By overloading the RPL routing tables it is possible to implement direct attacks against resources. Being a proactive routing protocol, RPL maintains routing tables. This attack works by announcing fake routes using the DAO messages, which saturate the routing table of the targeted node. This overload prevents the building of new legitimate routes and impacts network functioning, which results in memory overflow.

3.3.1.3 DIS Attack

When a new node wants to join the network, solicitation message DIS are used to get the topology information. In this attack, the DIS messages are send periodically by malicious nodes to its neighbours. This attack can be launched by unicast DIS message or by broadcasting DIS message in both cases the neighbouring nodes have to reply with DIO message which leads to network congestion and saturation of nodes. This attack generates more control overhead but the there is no effect on delivery ratio.

3.3.1.4 Local Repair Attacks

In this attack, attacker periodically sends the local repair message even when there is no problem with link quality. This leads to the local repair around the nodes which hears the local repair message. This attack creates a lot of impact on delivery ratio as compared to any other kind of attack [1], creates more control packets and upsurges the end to end delay as a result the energy of nodes is exhausted needlessly.

3.3.2 Indirect Attacks

Indirect attacks are those attacks where the malicious node targets other nodes to create an overload for the network. This attack includes increased rank attacks, DAG inconsistency attacks, and version number attacks.

3.3.2.1 Increased Rank Attack

The rank attack comprises of maliciously increasing the rank of an RPL node in order to create loops within the network. These attacks have been studied in [25] through ns-2 simulations. Each node in RPL network is associated with a rank which shows its position with respect to root node and rank value increases from root to leaf nodes to preserve the acyclic nature of DODAG graph. If a node wants to change its rank value, it has to

first update its parent's list by eliminating the nodes having a rank higher than its new rank. A malicious node advertises a higher rank to attract traffic. Loops are formed only if the attacker does not use loop avoidance mechanisms and when its new parent was in its prior sub-DODAG. With the limitation of the maximum rank value advertised for a DODAG the count to infinity problem is avoided. This attack is more damaging in the second case as more routing loops are built in the neighbourhood. In that case many DIO messages are sent for the loop repair mechanism which takes long time to converge. As number of affected nodes increases convergence time also increases. To avoid this attack, the DODAG graph should observe the number of times an RPL node increases its rank value to determine if a node can be considered as malicious. However a node can legitimately increase its rank value if it cannot manage the amount of received traffic or when the objective function no longer matches. But in that case it can wait for a new version of the DODAG graph or it must use the loop prevention techniques.

3.3.2.2 DAG Inconsistency Attacks

DAG inconsistency is detected when the node receives a packet with a Down 'O' bit set from a node with a higher rank and vice-versa [2]. To control this problem the Rank-Error 'R' bit flag is used. Two scenarios are possible when an inconsistency is detected by a node: (i) if the Rank-Error flag is not set, the node sets it and the packet is forwarded. (ii) if the 'R' bit is already set, the node discards the packet and the timer is reset . As a result more control messages are sent. A malicious node has to just alter the flags or add new flags to the header. The direct outcome of this attack is to the reset DIO trickle timer of the targeted node due to which this node starts to transmit DIO messages more often creating local instability in the network. This depletes the battery of the nodes and effects the link availability. Moreover, the malicious node can discard all the packets by modifying legitimate traffic which leads to black hole and isolates network segments. To mitigate this attack authors of [26] proposes to limit the rate of trickle timer resets to no greater than 20 resets per hour. Authors of [28] [27] have proposed two solutions instead of a fixed threshold. The first solution is an adaptive threshold [27] which is improved in dynamic approach [28] where specific node parameters are used. They showed that these approaches are more effective as it results in preserving energy consumption of the nodes.

3.3.2.3 Version Number Attack

This attack occurs when a malicious node increases the version number which is an important field of each DIO message. Such an attack causes an unnecessary rebuilding of the whole DODAG graph which significantly increases control message overhead, exhausting nodes resources and congesting the network. Dvir et al. [22] proposed a security mechanism called VeRa (Version Number and Rank Authentication) which verifies the version number by using digital signature and MAC. Also, authors of [29] proposed an improvement over VeRa by solving some issues they discovered in VeRA.

3.3.2.4 Denial of Service Attack

Denial of service (DOS) or Distributed denial of service attack (DDOS) attack make resources unavailable to its envisioned user. This attack is launched by flooding the IPv6 UDP packet. Distributed denial of service attack occurs by coordination of many malicious nodes wherein it is difficult to identify the malicious nodes. However the authors of [17] proposed an IDS for the detection of DOS attack in 6LoWPAN. IDS probe nodes located in the network periodically sends the traffic in 6LoWPAN through wired connection to IDS system. IDS send the

congestion information of attack to DOS protection manager. The presence of congestion information at the modules of network manager of ebbits indicated the presence of attack.

IV. TRUST IN IOT ROUTING PROTOCOL

Recently researchers are focusing on the use of Trust-based mechanism which employs a lightweight solution with respect to the limited resources of the nodes, as an interesting solution for the security of RPL routing. In computers, trust between entities can be characterized by trust values. These values can be continuous or discrete. A mature technique is called the Subjective Logic [30]. In subjective logic the trust values are computed from opinion triangles that not only consider trust or distrust but also consider uncertainty about a trustee. An opinion triangle is characterized by the three variables b (belief or trust), d (disbelief or distrust), and u (uncertainty). All the three variables are real numbers having values between0 and 1, and their values must always add to 1. The trust values can be computed from positive and negative experiences with a trustee by metrics like the following [31]

$$b = \frac{p}{p+n+k} \qquad d = \frac{n}{p+n+k} \qquad u = \frac{k}{p+n+k}$$

The variable p expresses the number of positive experiences and the variable n expresses the number of negative experiences and the constant k takes values 1 or 2 and determines how fast certainty about a trustee is built. The aim of this mechanism is to compute a trust value for each node and embed these computed trust values for routing decision. This way it will provide an optimal routing decision while also isolating malicious nodes that may seek to drop control and route packets. The authors of [32][33]have used trust mechanism for securing RPL against black hole and selective forwarding attack where trusted values are arranged in descending order which are then embedded in objective functions of RPL along with Rank and ETX to compute routing paths that will include only trusted nodes thus attack will be quarantine from the network. . The authors of [34] have proposed distributed Trust based detection mechanism for detecting sinkhole, selective forwarding and version attack where Border router computes the aggregate trusted values

V. RESEARCH SCOPE IN RPL PROTOCOL

As discussed in section 3 RPL protocol is vulnerable to various attacks of which some of these attacks have been evaluated. However a few attacks are still to be evaluated like Internet Smurf Attack, Homing Attack, Resource Exhausting Attack, etc. The IDS based solution for detecting Local Repair Attack, Neighbour Attack, DIS, Blackhole, Sinkhole and Version Attack can be a research challenge. Existing IDS solution can be extended for detection of Sybil and Clone ID Attack. Trust based mechanism can be evaluated for wormhole and other attack as a research area. With the number of IoT network on the rise , the need for secure routing protocol is becoming salient. A few secure IoT routing protocol design recommendation for the researchers can be outlined as Secure route establishment, Self stabilization, Effective malicious node identification system, Light weight computation and Location privacy.

Sr. No.	Attacks	Type	Effect on network	Prevention techniques
1	Flooding Attacks	Direct Attack / Attack on Resources	Compromises Availability and effects network performance due to dissipation of sensor battery power	RPL's Self healing mechanism removes attack[12]
2	Routing Table Overload	Direct Attack / Attack on Resources	Compromises Availability and Integrity and leads to Memory/ Battery exhaustion ,making resources unavailable	None
3	Local Repair Attack	Direct Attack / Attack on Resources	Compromises Confidentiality & Integrity and effect the network performance which is due to high control overhead and routing traffic disruption	IDS based solution[36]
4	Neighbor attack	Direct Attack / Attack on Resources	Compromises Confidentiality, Integrity & Availability and effects network performance based on False route, route disruption and resource consumption	No technique evaluated yet
5	Rank Attack	Indirect attack / Attack on Resources	Compromises Availability and effects Packet delay, delivery ratio and generation of Un-optimised path and loop	IDS based solutions [2],[16],VeRA[22], TRAIL[29]
6	DAG Inconsistency	Indirect attack / Attack on Resources	Compromises Availability and Integrity and effects Battery/ Power consumption, unavailability of resources	Limitation of Timer Resets[26]
7	Version Number Attack	Indirect attack / Attack on Resources	Compromises Confidentiality &Integrity and effect the performance of network due to increased control overhead and low packet delivery ratio, high end to end delay	VeRA[22], Trust based IDS[34]
8	Denial of Service attack	Indirect attack / Attack on Resources	Compromises Availability and effects the performance of network depending on unavailability of resources at nodes.	IDS based solution[10]
9	Routing Table Falsification	Sub-optimization Attack/ Attack on topology	Compromises Availability and Integrity and effects Target's Subnet	None
10	Sinkhole Attack	Sub-optimization Attack/ Attack on topology	Compromises Confidentiality & Integrity and effect the network performance due to Compromising huge traffic passing through attacker node	IDS solution[10], parent fail-over[16] rank authentication techinque[22], Trust based IDS [34]

11	Wormhole attack	Sub-optimization Attack/ Attack on topology	Compromises Availability and integrity and disruption of network topology and traffic flow	Merkle tree authentication[19], RSSI based IDS[20]
12	Routing Information Replay	Sub-optimization Attack/ Attack on topology	Compromises Availability and Integrity and effects Attacker's Neighborhood	Using Sequence Number[2]
13	Worst Parent	Sub-optimization Attack/ Attack on topology	Compromises Availability and Integrity and effects Attacker's Subnet	None
14	Blackhole	Isolation Attack/ Attack on Topology	Compromises Availability, Confidentiality & Integrity and effect the network performance based on packets dropped and increased route traffic and control overhead	Trust based mechanism [32][33]
15	DAO Inconsistency	Isolation Attack/ Attack on Topology	Compromises Availability and Integrity and effects Attacker's subnet, corrupt routing tables affecting downward packets	Limitation of discarding routing state[26]
16	Sniffing and Traffic Analysis	Eavesdropping Attack/ Attack on Traffic	Compromises Confidentiality and effects Critical Data disclosure	Lightweight Encryption [2]
17	Sybil and Clone ID	Misappropriation Attack/ Attack on Traffic	Compromises Integrity and makes routing traffic unreachable to victim node	T-IDS[35]
18	Selective forwarding	Sub-optimization Attack/ Attack on topology	Compromises Avaiability&Integrity and effects network performance due to disruption of route path	Hearbeat protocol [2], End to end packet loss , Trust based IDS[34]
19	DIS Attack	Direct Attack / Attack on Resources	Compromises Availability and integrity and effects network performance based on Resource consumption	No technique evaluated yet

TABLE I. Summary of RPL Attacks and Countermeasures.

VI. CONCLUSION

The RPL protocol attacks have been classified in three main categories. The attack against resources reduces network lifetime through the generation of fake control messages or the building of loops. The network not being able to converge to sub optimal configuration and isolation of nodes is caused by these attacks against the topology. Attacks against network traffic leads a malicious node capture and analyze large part of the traffic.

Comparison of the nature of these attacks and discussion of methods like Trust based mechanism and other solutions to remove the attacks form a part of the survey.

However, many security solutions to mitigate the attacks are at a proof-of-concept level. Hence a Intrusion detection and prevention mechanism which can detect and quarantine all possible attacks on RPL network should be the focus of research community. A lightweight and resource friendly mechanism based on Trust can be considered as a possible solution.

REFERENCES

[1] P. Levis, A. Tavakoli, and S. DawsonHaggerty, Overview of Existing Routing Protocols for Low Power and Lossy (RPL) Networks, Internet Engineering Task Force (IETF) Internet Draft: draft-ietf-roll-protocols-survey-07, April, 2009. (http://tools.ietf.org/html/ draft-levis-roll overview-protocols-00).

[2] T. Winter, P. Thubert, A. Brandt, J. Hui, R. Kelsey, P. Levis, K. Pister, R. Struik, J. Vasseur, and R. Alexander, RPL: IPv6 routing protocol for lowpower and lossy networks, RFC 6550, IETF, 2012.

[3] T.Tsao, R. Alexander, M. Dohler, V. Daza, A Lozano, and M. Richardson, A Security Threat Analysis for Routing Protocol for Lowpower and Lossy Networks (RPLs), RFC 7416, Internet Engineering Task Force, 2015.

[4] L. Abusalah, A. Khokhar, and M. Guizani, "Survey of secure mobile ad hoc routing protocols," in the IEEE Communication Surveys & Tutorials, vol. 10, no. 4, pp. 78–93, Oct. 2008.

[5] D. Djenouri, L. Khelladi, and A. N. Badache, "A survey of security issues in mobile ad-hoc & sensor networks," in the IEEE Communication Surveys & Tutorials, vol. 7, no. 4, pp. 2–28, 2005.

[6] Y. Wang, G. Attebury, and B. Ramamurthy, "A survey of security issues in WSN (Wireless sensor networks)," in the IEEE Communications Surveys & Tutorials, vol. 8, no. 2, pp. 2–23, 2006.

[7] O. Gaddour and A. Koubˆaa, "RPL in a nutshell: A survey," Computer Networks, vol. 56, no. 14, pp. 3163–3178, Sept. 2012.

[8] A. Le, J. Loo, A. Lasebae, M. Aiash, and Y. Luo,"6lowpan: A study on Quality of service (qos) security threats and countermeasures using intrusion detection system approach," of the International Journal of Communication Systems, vol. 25, no. 9, pp. 1189–1212, 2012.

[9] P. Pongle and G. Chavan, "A survey attacks on RPL and 6lowpan in IoT," in the International Conference on Pervasive Computing (ICPC'15), pp. 1–6, Jan. 2015.

[10] S. Raza, L. Wallgren, and T. Voigt, "Real time intrusion detection in the internet of things," Ad-Hoc Networks, vol. 11, no. 8, pp. 2661–2674, 2013.

[11] A. Le, J. Loo, Y. Luo, and A. Lasebae, "Specification based intrusion detection protocol for securing RPL from topology attacks," in Wireless Days, pp. 1–3, 2011.

[12] L. Wallgren, S. Raza, and T. Voigt, "Routing attacks and counter - measures in the RPL based internet of things," in the International Journal of Distributed Sensor Networks, vol. 2013, pp. 1-11, 2013.

[13] A. Rghiout, A. Khannous, and M. Bouhorma, "Denial-of-service attacks on 6lowpan-RPL networks: Issues and practical solutions," Journal of Advanced Computer Science & Technology, vol. 3, no. 2, pp. 143–153, 2014.

[14] Anth´eaMayzaud, R´emiBadonnel, Isabelle Chrisment, "A Taxonomy of Attacks in RPL-based Internet of Things," International Journal of Network Security, Vol.18, No.3, PP.459-473, May 2016.

[15] Divya Sharma, Ishani Mishra, Dr. Sanjay Jain, "A Detailed Classification of Routing Attacks against RPL in Internet of things," in International Journal of Advance Research, Ideas and Innovations in Technology , 2017.

[16] K. Weekly and K. S. J. Pister, "Evaluating sinkhole defense techniques in RPL networks," in the 20th IEEE International Conference on Network Protocols (ICNP'12), pp. 1–6, 2012.

[17] 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.

[18] A. Le, J. Loo, A. Lasebae, A. Vinel, Y. Chen, and M. Chai, "The impact of rank attack on network topology of RPL networks," IEEE Sensors, vol. 13, no. 10, pp. 3685– 3692, 2013.

[19] F. I. Khan, T. Shon, T. Lee, and K. Kim, "Wormhole attack prevention mechanism for RPL based on network," in 5th International Conference on Ubiquitous and Future Networks (ICUFN'13) 149–154, July 2013.

[20] PavanPongle and GurunathChavan," Real Time Intrusion and Wormhole Attack Detection in Internet of Things", International Journal of Computer Applications (0975 - 8887) Volume 121 - No. 9, July 2015.

[21] Chugh, L. Aboubaker, and J. Loo, "Case study of a black hole attack on 6lowpan-RPL," in Proceedings of the SECURWARE Conference, pp. 157–162, Aug. 2012.

[22] A. Dvir, T. Holczer, and L. Butty´an, "Vera - version number and rank authentication in RPL," in Proceedings of Mobile Adhoc and Sensor Systems Conference (MASS'11), pp. 709–714, 2011.

[23] J. R. Douceur, "The sybil attack," in First International Workshop on Peer-to-Peer Systems (IPTPS'01), pp. 251–260, London, UK, 2002.

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

[25] W. Xie, M. Goyal, H. Hosseini, J. Martocci, Y. Bashir, E. Baccelli, and A. Durresi, "Routing loops in dag-based low power and lossy networks," in Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications, pp. 888–895, Washington, USA, 2010.

[26] J. Hui and J. Vasseur, The Routing Protocol for LowPower and Lossy Networks (RPL) Option for Carrying RPL Information in Data-Plane Datagrams, RFC 6553 (Proposed Standard), Internet Engineering Task Force, Mar. 2012.

[27] A. Sehgal, A. Mayzaud, R. Badonnel, I. Chrisment, and J. Sch¨onw¨alder, "Addressing DODDAG inconsistency attacks in RPL networks," in Proceedings of Global Information Infrastructure and Networking Symposium (GIIS'14), pp. 1–8, 2014.

[28] A. Mayzaud, A. Sehgal, R. Badonnel, I. Chrisment, and J. Sch¨onw¨alder, "Mitigation of topological inconsistency attacks in RPL-based low-power lossy networks," International Journal of Network Management, 2015.

[29] M. Landsmann, H. Perrey, O. Ugus, M. W¨ahlisch, and T. C. Schmidt, "Topology authentication in RPL," in IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS'13), pp. 73–74, 2013.

[30] Josang ,"Modelling Trust in Information Security," Phd thesis, Norwegian University of Science and Technology,1997.

[31] Josang and S.J.Knapsog."Metric for Trusted System", in 21st National Security Conference. NSA, 1998.

[32] David Airehrour, Jairo Gutierrez and Sayan Kumar Ray,"Securing IoT routing protocol against Black hole attack using Trust based mechanism",in 2016 International Telecommunication Networks and Applications Conference.

[33] David Airehrour, Jairo Gutierrez and Sayan Kumar Ray," A Trust-Aware RPL Routing Protocol to Detect Blackhole and Selective Forwarding Attacks", Australian Journal of Telecommunications and the Digital Economy, 2017.

[34] Zeeshan Ali Khan and Peter Herrmann," A Trust Based Distributed Intrusion Detection Mechanism for Internet of Things", in 2017 IEEE 31st International Conference on Advanced Information Networking and Applications.

[35] FaizaMedjek, DjamelTandjaoui, ImedRomdhani, Nabil Djedjig," A Trust-based Intrusion Detection System for Mobile RPL Based Networks", in 10th IEEE International Conference on Internet of Things (iThings-2017), AtExeter, UK.

[36] A. Le, J. Loo, A. Lasebae, M. Aiash, and Y. Luo, "6lowpan: A study on QoS security threats and countermeasures using intrusion detection system approach," International Journal of Communication Systems, vol. 25, no. 9, pp. 1189-1212, 2012