International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 11 | Nov 2020 www.irjet.net p-ISSN: 2395-0072

A Survey on Routing Attacks in Internet of Things (IOT)

Rushabh Vaghela[1], Prof. Deepak Upadhyay[2]

[1]*Dept. of Computer Engineering (Cyber Security), GTU – Graduate School of Engineering and Technology, Gujarat, India*
[2]*Dept. of Computer Engineering (Cyber Security), GTU – Graduate School of Engineering and Technology, Gujarat, India*

Abstract – *In this paper, we discussed the Internet of things architecture, Internet of things security, as well as all the current architecture in IoT Networks. We discussed network layer of IoT in detail, all the Protocols and the details of that protocols. Attack on RPL Networks and Details about individual RPL attack (How it works) and Countermeasures on RPL as well as 6LoWPAN.*

Key Words: IoT, Internet of Things, RPL, 6LoWPAN, IoT Architecture, Countermeasures, Routing Attacks.

1. INTRODUCTION

The Internet of things (IoT) describes the network of physical objects "things" that are embedded with sensors, software, and other technologies for the purpose of connecting and exchanging data with other devices and systems over the Internet.

Some examples of existing IoT systems are self-driving vehicles (SDV) for automated vehicular systems, microgrids for distributed energy resources systems, and Smart City Drones for surveillance systems. A microgrid system represents a good example of a cyber physical system: it links all distributed energy resources (DER) together to provide a comprehensive energy solution for a local geographical region. However, a microgrid IoT system still relies on traditional Supervisory Control and Data Acquisition (SCADA). The integration of the physical and cyber domains actually increases the exposure to attacks: cyber-attacks may target the SCADA supervisory control and paralyse the physical domain or the physical devices may be tampered or compromised, affecting the supervisory control system. On the other hand, the drone market is moving quickly to adopt automation techniques and can be integrated into firefighting, police, smart city surveillance, and emergency response. As municipalities and citizens begin to rely on such a system, it will become critical to keep the system secure and reliable.

Today the Internet has become ubiquitous, has touched almost every corner of the globe, and is affecting human life in unimaginable ways. However, the journey is far from over. We are now entering an era of even more pervasive connectivity where a very wide variety of appliances will be connected to the web.

opez et al. defines the Internet of ´ Things as a paradigm in which computing and networking capabilities are embedded in any kind of conceivable object. We use these capabilities to query the state of the object and to change its state if possible. In common parlance, the Internet of Things refers to a new kind of world where almost all the devices and appliances that we use are connected to a network. We can use them collaboratively to achieve complex tasks that require a high degree of intelligence.

2. IoT security

Due to the diversity of the devices and multitude of communication protocols in an IoT systems, and also various interfaces and services offered, it is not suitable to implement security mitigation based on the traditional IT network solutions. In fact, the current security measures which are applied in a conventional network may not be sufficient. Attack vectors as listed by Open Web Application Security Project (OWASP) concern the three layers of an IoT system, which are hardware, communication link and interfaces/services. Hence, the implementation of IoT security mitigation should encompass the security architecture at all IoT layers, as presented in Fig. 2 1. Radio Frequency Identification (RFID) and Wireless Sensor Network (WSN) are considered as part of an IoT network

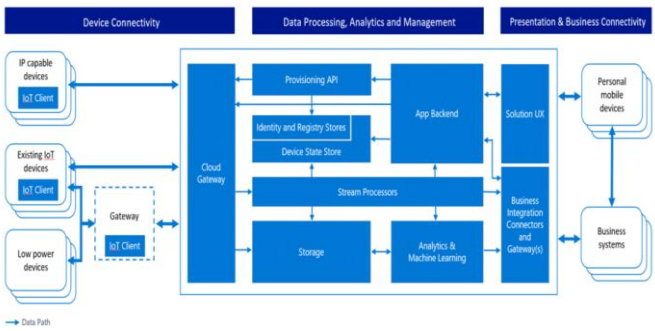

Figure 2 1: IoT Security Architecture

3. Internet of Things Architecture:

There is no single consensus on architecture for IoT, which is agreed universally. Different architectures have been proposed by different researchers.

Three- and Five-Layer Architectures. The most basic architecture is a three-layer architecture as shown in Figure

3 a 1 and figure 3 a 2. It was introduced in the early stages of research in this area. It has three layers, namely, the perception, network, and application layers.

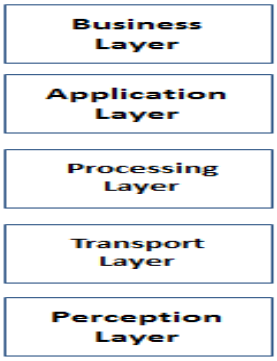

Figure 3 a 1: IoT Five-layer Architecture

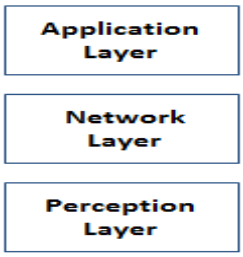

Figure 3 a 2: IoT Three-layer architecture

The perception layer is the physical layer, which has sensors for sensing and gathering information about the environment. It senses some physical parameters or identifies other smart objects in the environment.

The network layer is responsible for connecting to other smart things, network devices, and servers. Its features are also used for transmitting and processing sensor data.

The application layer is responsible for delivering application specific services to the user. It defines various applications in which the Internet of Things can be deployed, for example, smart homes, smart cities, and smart health.

The three-layer architecture defines the main idea of the Internet of Things, but it is not sufficient for research on IoT because research often focuses on finer aspects of the Internet of Things. That is why, we have many more layered architectures proposed in the literature. One is the five-layer architecture, which additionally includes the processing and business layers. The five layers are perception, transport, processing, application, and business layers (see Figure 3 a 1 and figure 3 a 2). The role of the perception and application layers is the same as the architecture with three layers. We outline the function of the remaining three layers.

The transport layer transfers the sensor data from the perception layer to the processing layer and vice versa through networks such as wireless, 3G, LAN, Bluetooth, RFID, and NFC.

The processing layer is also known as the middleware layer. It stores, analyzes, and processes huge amounts of data that comes from the transport layer. It can manage and provide a diverse set of services to the lower layers. It employs many technologies such as databases, cloud computing, and big data processing modules.

The business layer manages the whole IoT system, including applications, business and profit models, and users' privacy. The business layer is out of the scope of this paper. Hence, we do not discuss it further.

3.1 Cloud and Fog Based Architectures:

In particular, we have been slightly vague about the nature of data generated by IoT devices, and the nature of data processing. In some system architectures the data processing is done in a large centralized fashion by cloud computers. Such a cloud centric architecture keeps the cloud at the centre, applications above it, and the network of smart things below it. Cloud computing is given primacy because it provides great flexibility and scalability. It offers services such as the core infrastructure, platform, software, and storage. Developers can provide their storage tools, software tools, data mining, and machine learning tools, and visualization tools through the cloud.

Often the terms "fog computing" and "edge computing" are used interchangeably. The latter term predates the former and is construed to be more generic. Fog computing originally termed by Cisco refers to smart gateways and smart sensors, whereas edge computing is slightly more penetrative in nature. This paradigm envisions adding smart data pre-processing capabilities to physical devices such as motors, pumps, or lights. The aim is to do as much of pre-processing of data as possible in these devices, which are termed to be at the edge of the network. In terms of the system architecture, the architectural diagram is not appreciably different from Figure 3 a 3. As a result, we do not describe edge computing separately.

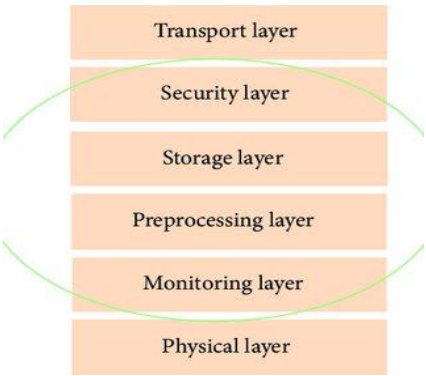

Figure 3 a 3: Fog Computing

3.2 Social IoT:

Let us now discuss a new paradigm: social IoT (SIoT). Here, we consider social relationships between objects the same way as humans form social relationships. Here are the three main facets of an SIoT system:

The SIoT is navigable. We can start with one device and navigate through all the devices that are connected to it. It is easy to discover new devices and services using such a social network of IoT devices. A need for trustworthiness (strength of the relationship) is present between devices (similar to friends on Facebook).
We can use models similar to studying human social networks to also study the social networks of IoT devices.

4. Network layer in brief:

In this section, we discuss some standard and non-standard protocols that are used for routing in IoT applications. It should be noted that we have partitioned the network layer in two sublayers: routing layer which handles the transfer of the packets from source to destination, and an encapsulation layer that forms the packets. Encapsulation mechanisms will be discussed in the next section.

4.1 Network Layer Routing Protocol

RPL:
Routing Protocol for Low-Power and Lossy Networks (RPL) is distance-vector protocol that can support a variety of data link protocols, including the ones discussed in the previous section. It builds a Destination Oriented Directed Acyclic Graph (DODAG) that has only one route from each leaf node to the root in which all the traffic from the node will be routed to. At first, each node sends a DODAG Information Object (DIO) advertising itself as the root. This message is propagated in the network and the whole DODAG is gradually built. When communicating, the node sends a Destination Advertisement Object (DAO) to its parents, the DAO is propagated to the root and the root decides where to send it depending on the destination. When a new node wants to join the network, it sends a DODAG Information Solicitation (DIS) request to join the network and the root will reply back with a DAO Acknowledgement (DAO-ACK) confirming the join. RPL nodes can be stateless, which is most common, or stateful. A stateless node keeps tracks of its parents only. Only root has the complete knowledge of the entire DODAG. Hence, all communications go through the root in every case. A stateful node keeps track of its children and parents and hence when communicating inside a sub-tree of the DODAG, it does not have to go through the root.

CORPL:
An extension of RPL is CORPL, or cognitive RPL, which is designed for cognitive networks and uses DODAG topology generation but with two new modifications to RPL. CORPL utilizes opportunistic forwarding to forward the packet by choosing multiple forwarders (forwarder set) and coordinates between the nodes to choose the best next hop to forward the packet to. DODAG is built in the same way as RPL. Each node maintains a forwarding set instead of its parent only and updates its neighbor with its changes using DIO messages. Based on the updated information, each node dynamically updates its neighbor priorities in order to construct the forwarder set.

CARP:
Channel-Aware Routing Protocol (CARP) is a distributed routing protocol designed for underwater communication. It can be used for IoT due to its lightweight packets. It considers link quality, which is computed based on historical successful data transmission gathered from neighboring sensors, to select the forwarding nodes. There are two scenarios: network initialization and data forwarding. In network initialization, a HELLO packet is broadcasted from the sink to all other nodes in the network. In data forwarding, the packet is routed from sensor to sink in a hop- by-hop fashion. Each next hop is determined independently. The main problem with CARP is that it does not support reusability of previously collected data. In other words, if the application requires sensor data only when it changes significantly, then CARP data forwarding is not beneficial to that specific application. An enhancement of CARP was done in E-CARP by allowing the sink node to save previously received sensory data. When new data is needed, E-CARP sends a Ping packet which is replied with the data from the sensor nodes. Thus, E-CARP reduces the communication overhead drastically.

Summary:
Three routing protocols in IoT were discussed in this section. RPL is the most commonly used one. It is a distance vector protocol designed by IETF in 2012. CORPL is a non-standard extension of RPL that is designed for cognitive networks and utilizes the opportunistic forwarding to forward packets at each hop. On the other hand, CARP is the only distributed hop-based routing protocol that is designed for IoT sensor network applications. CARP is used for underwater communication mostly. Since it is not standardized and just proposed in literature, it is not yet used in other IoT applications.

4.2Network Layer Encapsulation Protocols

One problem in IoT applications is that IPv6 addresses are too long and cannot fit in most IoT data link frames which are relatively much smaller. Hence, IETF is developing a set of standards to encapsulate IPv6 datagrams in different data link layer frames for use in IoT applications. In this section, we review these mechanisms briefly.

6LoWPAN:
IPv6 over Low power Wireless Personal Area Network (6LoWPAN) is the first and most commonly used standard in this category. It efficiently encapsulates IPv6 long headers in IEEE802.15.4 small packets, which cannot exceed 128 bytes. The specification supports different length addresses, low bandwidth, different topologies including star or mesh, power consumption, low cost, scalable networks, mobility, unreliability and long sleep time. The standard provides header compression to reduce transmission overhead, fragmentation to meet the 128-byte maximum frame length in IEEE802.15.4, and support for multi-hop delivery. Frames in 6LoWPAN use four types of headers: No 6loWPAN header (00), Dispatch header (01), Mesh header (10) and Fragmentation header (11). In No 6loWPAN header case, any frame that does not follow 6loWPAN specifications is discarded. Dispatch header is used for multicasting and IPv6 header compressions. Mesh headers are used for broadcasting; while Fragmentation headers are used to break long IPv6 header to fit into fragments of maximum 128- byte length.

6TiSCH:
6TiSCH working group in IETF is developing standards to allow IPv6 to pass through Time Slotted Channel Hopping (TSCH) mode of IEEE 802.15.4e datalinks. It defines a Channel Distribution usage matrix consisting of available frequencies in columns and time-slots available for network scheduling operations in rows. This matrix is portioned into chunks where each chunk contains time and frequencies and is globally known to all nodes in the network. The nodes within the same interference domain negotiate their scheduling so that each node gets to transmit in a chunk within its interference domain. Scheduling becomes an optimization problem where time slots are assigned to a group of neighboring nodes sharing the same application. The standard does not specify how the scheduling can be done and leaves that to be an application specific problem in order to allow for maximum flexibility for different IoT applications. The scheduling can be centralized or distributed depending on application or the topology used in the MAC layer.

6Lo:
IPv6 over Networks of Resource-constrained Nodes (6Lo) working group in IETF is developing a set of standards on transmission of IPv6 frames on various datalinks. Although, 6LowPAN and 6TiSCH, which cover IEEE 802.15.4 and IEEE 802.15.4e, were developed by different working groups, it became clear that there are many more datalinks to be covered and so 6Lo working group was formed. At the time of this writing most of the 6Lo specifications have not been finalized and are in various stages of drafts. For example, IPV6 over Bluetooth Low Energy Mesh Networks, IPv6 over IEEE 485 Master-Slave/Token Passing (MS/TP) networks, IPV6 over DECT/ULE, IPV6 over NFC, IPv6 over IEEE 802.11ah, and IPv6 over Wireless Networks for Industrial Automation Process Automation (WIA-PA) drafts are being developed to specify how to transmit IPv6 datagrams over their respective datalinks [6Lo]. Two of these 6Lo specifications "IPv6 over G.9959" and "IPv6 over Bluetooth Low Energy" have been approved as RFC and are described next.

IPv6 over G.9959:
RFC 7428 defines the frame format for transmitting IPv6 packet on ITU-T G.9959 networks. G.9959 defines a unique 32-bit home network identifier that is assigned by the controller and 8- bit host identifier that is allocated for each node. An IPv6 link local address must be constructed by the link layer derived 8-bit host identifier so that it can be compressed in G.9959 frame. Furthermore, the same header compression as in 6lowPAN is used here to fit an IPv6 packet into G.9959 frames. RFC 7428 also provides a level of security by a shared network key that is used for encryption. However, applications with a higher level of security requirements need to handle their end-to-end encryption and authentication using their own higher layer security mechanisms.

IPv6 over Bluetooth Low Energy:
Bluetooth Low Energy is also known as Bluetooth Smart and was introduced in Bluetooth V4.0 and enhanced in V4.1. RFC 7668, which specifies IPv6 over Bluetooth LE, reuses most of the 6LowPAN compression techniques. However, since the Logical Link Control and Adaptation Protocol (L2CAP) sublayer in Bluetooth already provides segmentation and reassembly of larger payloads in to 27-byte L2CAP packets, fragmentation features from 6LowPAN standards are not used. Another significant difference is that Bluetooth Low Energy does not currently support formation of multi-hop networks at the link layer. Instead, a central node acts as a router between lower-powered peripheral nodes.

Summary:
In this section, encapsulation protocols for IPv6 in the IoT MAC frame were discussed. First, two standards for IPv6 over 802.15.4 and 802.15.4e were discussed. Such protocols are important as 802.15.4e is the most widely used encapsulation framework designed for IoT. Following that, 6Lo specifications are briefly and broadly discussed just to present their existence in IETF standards. These drafts handle passing IPv6 over different channel access mechanisms using 6LoWPAN standards. Then, two of 6Lo Specifications which became IETF RFCs are discussed in more detail. The importance of presenting these standards is to highlight the challenge of interoperability between different MAC standards which is still challenging due to the diversity of protocols.

5. Attacks on RPL

This one takes into account the goals of the attack and what element of the RPL network is impacted. The taxonomy is

depicted in Figure 5 1 and considers three categories of security attacks. In this paper we have broadly classified the routing attacks in IoT networks in three categories. These are i). Attacks on Network Resources: These include attacks targeting the exhaustion of network resources (energy, memory and power). These attacks are particularly damaging for such constrained networks because they greatly shorten the lifetime of the devices and thus the lifetime of the RPL network. ii). Attacks on Network Topology: These cover attacks aiming at disrupting the RPL network topology. The attackers herein either aim at sub-optimization of the network topology or isolating a set of RPL nodes from the network. iii). Attacks on Network Traffic: This category corresponds to attacks against the network traffic, such as spoofing attacks or deception attacks.

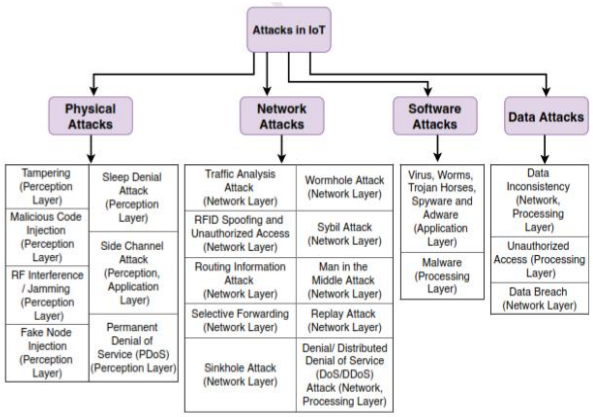

Figure 5 1: Attacks on RPL

5.1 Attacks on Network Topology

Attacks against the RPL protocol can also target network topology. We distinguish two main categories amongst these attacks: sub-optimization and isolation.

Selective Forwarding Attack:
This attack takes place by selectively forwarding packets. With these attacks DoS (Denial of Service) attack can be launched. The purpose of attack is to disrupt routing paths and filter any protocol. The RPL attacker could forward all RPL control messages and drop the rest of the traffic. Solution on this attack can be creating a disjoint path or dynamic path between parent and children. Another solution is by using encryption techniques in which the attacker will not be able to identify the traffic flow. Heartbeat protocol basically used for detection of the disruption in network topology but also can be used as a defense against selective forwarding attack. IDS solution given the End to End packet loss adaptation algorithm for detection of selective forwarding attack. Such attacks need to be detected and removed, RPL self-healing does not correct the topology. Routing Table Poisoning Attacks in Storing Mode: In a routing protocol, it is possible to forge or modify routing information to advertise falsified routes to other nodes. This attack can be performed in the RPL network by modifying or forging DAO control messages in order to build fake downward routes. This can only be done when the storing mode is enabled. For instance, a malicious node advertises routes toward nodes that are not in its sub-DODAG. Targeted nodes have the wrong routes in their routing table causing network sub- optimization. As a result, the path can be longer inducing delay, packet drops or network congestion.

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 gives the solution to detect this attack. To defend against sinkhole attack evaluated parent failover 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 nodes 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 it parent in black list. RPL does not have the self-healing capacity against the sinkhole.

Wormhole Attack:
RPL can undergo the wormhole attack. The main purpose of this attack is Disrupt the network topology and traffic flow. This attack can take place by creating a 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. In RPL the tree construction starts from root to leaf nodes and Markle tree construction starts from leaf node to root. It uses the 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 fails to authenticate, then children nodes avoid the wrong parent selection.

Decreased Rank Attacks:
In a DODAG graph, the lower the rank is, the closer the node is to the root and the more traffic this node has to manage. When a malicious node illegitimately advertises a lower rank value, it over claims its performance. As a result, many legitimate nodes connect to the DODAG graph via the attacker. This results in the attraction of a large part of the

traffic. Thanks to this operation, the malicious node is capable of performing other attacks such as sinkhole and eavesdropping attacks. In the RPL protocol, an attacker can change its rank value through the falsification of DIO messages. The VeRa solution as well as the Rank verification method is able to address this issue. However, authors have shown that VeRa is not sure regarding rank authentication and they proposed improvements to address this issue called TRAIL. They also showed another way to perform this attack by replaying the rank of the attacker's parent which allows it to decrease its rank by one. Since SVELTE can detect sinkhole attacks it can also detect the decreased rank attack. Identity Attacks: Identity attacks gather both spoofing and sybil attacks. In a clone ID attack, an attacker copies the identities of a valid node onto another physical node. This can, for example, be used in order to gain access to a larger part of the network or in order to overcome voting schemes. In a sybil attack, which is similar to a clone ID attack, an attacker uses several logical entities on the same physical node. Sybil attacks can be used to take control over large parts of a network without deploying physical nodes. By keeping track of the number of instances of each identity it is possible to detect cloned identities. It would also be possible to detect cloned identities by knowing the geographical location of the nodes, as no identity should be able to be at several places at the same time. The location of nodes or similar information could be stored either centralized in the 6BR or distributed throughout the network in a distributed hash table (DHT). In an IP/RPL network cloned identities will cause trouble when packets are heading to one of the cloned identities. Packets will be forwarded to one of the cloned identities based on the routing metrics in the network, and the rest of the cloned identities will be unreachable from certain nodes in the network. This however does not affect the network otherwise, and therefore cloned identities on their own, do not cause harm on a 6LoWPAN network.

6. Countermeasures of RPL

In this section, we investigate possible security solutions for the aforementioned threats. The ideal solution is the prevention of the possible threats; however, the specific goal is nearly impracticable, but appropriate countermeasures can mitigate the impact of these threats.

6LoWPAN Security:

Utilizing the IEEE 802.15.4 protocol at the PHY and the MAC sublayers, the Low Power Wireless Personal Area Networks (WPANs) can use only 102 bytes for the transmission of information at next communication layers. However, the value of the Maximum Transmission Unit (MTU) that is needed for the IPv6 requirements is equivalent to 1280 bytes which is considerably higher than the previous number. The purpose of the IPv6 low power WPAN (6LoWPAN) standard is to solve this complication by deploying the interconnection between the IEEE 802.15.4 and IPv6 protocols for WPANs. In particular, it operates as an adaptation layer that utilizes compression, fragmentation and encapsulation mechanisms and transmits the modified IPv6 packets at the MAC sublayer.

Currently, 6LoWPAN standard does not provide any security mechanism, such as IPsec due to the limitations of IoT devices. However, individual research proposals examine possible solutions to address these constraints, designing compressed security headers for the 6LoWPAN adaptation layer which have the same purpose as the existing Encapsulating Security Payload (ESP) and Authentication Header (AH) of IPsec. Also, some studies consider the incorporation of specific mechanisms in the 6LoWPAN against fragmentation attacks. More specifically, the authors discuss the addendum of a timestamp and a nonce field to the 6LoWPAN fragmentation header in order to address such attacks. In addition, proposes the use of mechanisms that can support the pre fragment sender authentication and prevent messages that are considered as suspicious. Finally, a significant security addition to the 6LoWPAN standard is the key management.as the keys must be regularly renewed in order to assure the principles of confidentiality, integrity and authenticity. For instance, the Internet Key Exchange version 2 (IKEv2) protocol could be adopted, which is appropriate for use in devices with constrained resources. Therefore, as a result, the lack of security mechanisms in the 6LoWPAN standard offer research opportunities for improvements in future versions.

RPL Security:

The RPL protocol was created by the Internet Engineering Task Force (IETF) and is appropriate to route messages in Low Power and Lossy Networks (LLNs). Its operation is based on the creation of a Destination Oriented Directed Acyclic Graph (DODAG) that utilizes an objective function. In more detail, the DODAG consists of a set of nodes, which possess oriented edges in order not to create loops. The creation of a DODAG starts when the root node transmits a DIO message to their neighbors. The neighboring nodes receive the DIO message and take the decision whether they join in the graph. If a node joins the graph, then the corresponding path to the root node is created. Then, using the objective function, the new node of the graph calculates a value which is called rank. This procedure is repeated for each node in the graph. Finally, it is worth mentioning that the nodes have the ability to transmit a DODAG Information Solicitation (DIS) message in order to discover new DODAGs and as well as they can send DODAG Destination Advertisement Object (DAO) messages to advertise a routing path.

The security in the RPL protocol is based on the existence of secure variations of the RPL packets (DIS, DIO, DAO, DAO-ACK) and also the capability to apply three security modes. These variations provide integrity, replay protection, delay protection and optional confidentiality. Specifically, the cryptographic algorithms and the overall security strategy

are identified by the Security field that is analyzed further in the following subfields.

Attack	Effect on network parameters	Method to counter measure
Sinkhole	Large traffic flows through attacker node	IDS solution, parent fail-over, rank authentication technique
Wormhole	Disrupt the network topology and traffic flow	Markle tree authentication
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
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, VeRA, TRAIL

Table 1 1: Attacks and Countermeasures

7. CONCLUSIONS

After reading this paper you have the knowledge of some basic things in the Internet of Things like architectures – three-layer, five-layer, cloud based, and fog. Also, IoT Security and IoT security Architecture. Network layer Protocols and Attack on RPL and Countermeasures on RPL and 6LoWPAN Protocol.

REFERENCES

[1] Tara Salman, "Networking Protocols and Standards for Internet of Things", IEEE Internet of Things Journal, March 2019

[2] IEEE 1905.1-2013, "IEEE Standard for a Convergent Digital Home Network for Heterogeneous Technologies," 93 pp., April 12 2013,

[3] IETF, "IPv6 over Networks of Resource-constrained Nodes (6lo)

[4] Linus Wallgren, Shahid Raza and Thiemo Voigt, "Routing Attacks and Countermeasures in the RPL-Based Internet of Things", International Journal of Distributed Sensor Networks, Volume 2013, Article ID 794326, 11 pages, http://dx.doi.org/10.1155/2013/794326.

[5] T. Winter, P. Thubert, "RFC 6550: RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks," Internet Engineering Task Force (IETF) Request For Comments, March 2010

[6] Mardiana binti , Mohamad Noor, Wan Haslina Hassan "Current research on Internet of Things (IoT) security: A survey", Elsevier, December 2018

[7] Pranjal Upadhyay, Prof. Deepak Upadhyay "Internet of Things- Ecosystem, Architecture, Protocols: A Survey" IRJET, 2020