International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 10 | Oct 2020 www.irjet.net p-ISSN: 2395-0072

Internet of Things- Ecosystem, Architecture, Protocols: A Survey

Pranjal Upadhyay[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 survey state-of-the-art methods, protocols, and applications in this new emerging area. This survey paper proposes some applications that have the potential to make a striking difference in human life, especially for the differently abled and the elderly. As compared to similar survey papers in the area, this paper is far more comprehensive in its coverage and exhaustively covers most major technologies spanning to applications. This paper discusses different standards offered by IEEE, IETF and ITU to enable technologies matching the rapid growth in IoT. These standards include communication, routing, network and session layers of the networking stack that are being developed just to meet requirements of IoT. As well as in this paper we discuss different architecture of Internet of Things.*

Key Words: IoT, Internet of Things, IoT Ecosystem, IoT Architecture, Protocols, RPL, 6LoWPAN

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.

The Internet of Things (IoT) is envisioned to grow rapidly due the proliferation of communication technology, the availability of the devices, and computational systems. Hence, IoT security is an area of concern in order to safeguard the hardware and the networks in the IoT system. However, since the idea of networking appliances is still relatively new, security has not been considered in the production of these appliances.

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 paralyze the physical domain or the physical devices may be tampered or compromised, affecting the supervisory control system.

We are now entering an era of even more pervasive connectivity where a very wide variety of appliances will be connected to the web. We are entering an era of the "Internet of Things" (abbreviated as IoT). This term has been defined by different authors in many different ways. Let us look at two of the most popular definitions. Vermesan et al. define the Internet of Things as simply an interaction between the physical and digital worlds. The digital world interacts with the physical world using a plethora of sensors and actuators.

Sensors and actuators are devices, which help in interacting with the physical environment. The data collected by the sensors has to be stored and processed intelligently in order to derive useful inferences from it. Note that we broadly define the term sensor; a mobile phone or even a microwave oven can count as a sensor as long as it provides inputs about its current state (internal state + environment). An actuator is a device that is used to effect a change in the environment such as the temperature controller of an air conditioner.

2. Application of IoT

All IoT applications need to have one or more sensors to collect data from the environment. Sensors are essential components of smart objects. One of the most important aspects of the Internet of Things is context awareness, which is not possible without sensor technology. IoT sensors are mostly small in size, have low cost, and consume less power. They are constrained by factors such as battery capacity and ease of deployment. Schmidt and Van Laerhoven provide an overview of various types of sensors used for building smart applications.

2.1 Mobile Phone Based Sensors

The mobile phone, which is ubiquitous and has many types of sensors embedded in it. In specific, the smartphone is a very handy and user-friendly device that has a host of built in communication and data processing features. With the increasing popularity of smartphones among people, researchers are showing interest in building smart IoT solutions using smartphones because of the embedded sensors. Some additional sensors can also be used depending

upon the requirements. Applications can be built on the smartphone that uses sensor data to produce meaningful results. Some of the sensors inside a modern smartphone are as follows.

1. The accelerometer senses the motion and acceleration of a mobile phone. It typically measures changes in velocity of the smartphone in three dimensions. There are many types of accelerometers.

2. The gyroscope detects the orientation of the phone very precisely. Orientation is measured using capacitive changes when a seismic mass moves in a particular direction.

3. The camera and microphone are very powerful sensors since they capture visual and audio information, which can then be analysed and processed to detect various types of contextual information. For example, we can infer a user's current environment and the interactions that she is having. To make sense of the audio data, technologies such as voice recognition and acoustic features can be exploited.

4. The magnetometer detects magnetic fields. This can be used as a digital compass and in applications to detect the presence of metals.

5. The GPS (Global Positioning System) detects the location of the phone, which is one of the most important pieces of contextual information for smart applications. The location is detected using the principle of trilateration. The distance is measured from three or more satellites (or mobile phone towers in the case of A-GPS) and coordinates are computed.

6. The light sensor detects the intensity of ambient light. It can be used for setting the brightness of the screen and other applications in which some action is to be taken depending on the intensity of ambient light. For example, we can control the lights in a room.

7. The proximity sensor uses an infrared (IR) LED, which emits IR rays. These rays bounce back when they strike some object. Based on the difference in time, we can calculate the distance. In this way, the distance to different objects from the phone can be measured. For example, we can use it to determine when the phone is close to the face while talking. It can also be used in applications in which we have to trigger some event when an object approaches the phone.

8. Some smartphones such as Samsung's Galaxy S4 also have a thermometer, barometer, and humidity sensor to measure the temperature, atmospheric pressure, and humidity, respectively

2. IoT Ecosystem

4 Key Elements: 1. Device, 2. Network, 3. Platform, 4. Agent.

Figure 2 a : Ecosystem of internet of Things

1. IoT devices:

   a. As we said earlier, there are many scenarios in which IoT can be employed and they all require different devices. Here, at the most basic level, we can speak of sensors (i.e. devices that sense things, such as temperature, motion, particles, etc.) and actuators (i.e. devices that act on things, such as switches or rotors).

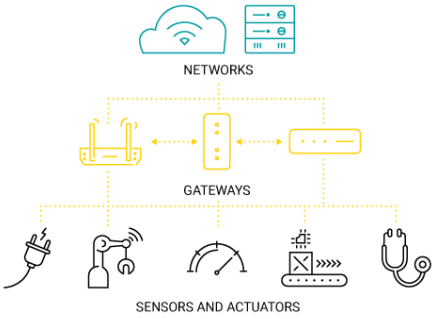

Figure 2 b: Devices

2. Networks:

   a. Based on what you read before, you may think: "Well, if an automatic door senses my presence and opens itself, is that IoT?" Obviously, it is not, because while that door has sensors and actuators, it is not connected to much else. And, as the name suggests, the Internet of Things requires

both things and the Internet (although there are cases of data delivery without the use of the Internet Protocol). Arguably, the real power of this concept lies in the connectivity.

b. Again, based on your deployment needs, there are plenty of different IoT connectivity options, starting with the "classics," such as Wi-Fi or Bluetooth, to more specialized and field-oriented technologies, such as Low-Power Wide Area Networks (LPWAN). They all differ in range and speed of data transfer, making them more or less appropriate for particular deployments. Consider, for example, smart cars that require both high data speed and long range and juxtapose them with the smart farms we've mentioned that don't necessarily need either.

3. IoT platform:

a. Whether they are in the cloud or not, IoT platforms are always the binder for any IoT ecosystem. They are the quiet administrators that take care of device lifecycle management, so that you don't have to worry about them. They are also the hub that collects and aggregates the data, allowing you to make sense of it. With the variety of platforms offered on the market and the breadth of claims their providers make, the choice of the "ideal" IoT platform for a deployment is arguably the most significant, yet also the most difficult to make. It shouldn't be taken lightly, as it determines whether the IoT ecosystem will thrive or wither into oblivion.

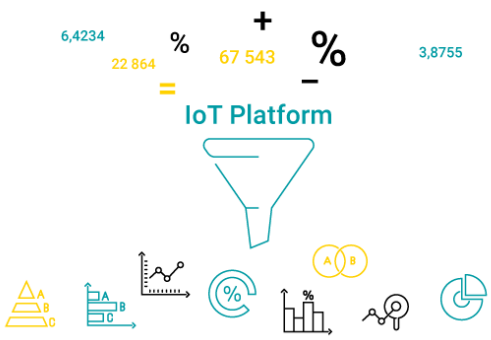

Figure 2 c: Platform of IoT

4. Agents:

a. Agents are all the people whose actions affect the IoT ecosystem. These may be the engineers who devise IoT deployments and design the platforms, it can also be the platform operators. But probably, most importantly, it's the stakeholders, who ultimately reap the results. After all, IoT deployments aren't just art for art's sake. These complex ecosystems are put in place for a reason: to drive efficiency and improve the quality of life. And it is the agents who decide on how to use the devices, networks and platforms to achieve these results. This is where technology and business converge, because it's business goals that very much shape the IoT ecosystem.

Figure 2 d: Agents for IoT

Now another Ecosystem for Internet of things based on the Layers of the IoT.

A 7-layer model of IoT ecosystem. At the bottom layer is the market or application domain, which may be smart grid, connected home, or smart health, etc. The second layer consists of sensors that enable the application. Examples of such sensors are temperature sensors, humidity sensors, electric utility meters, or cameras. The third layer consists of an interconnection layer that allows the data generated by sensors to be communicated, usually to a computing facility, data center, or a cloud. There the data is aggregated with other known data sets such as geographical data, population data, or economic data. The combined data is then analyzed using machine learning and data mining techniques. To enable such large distributed applications, we also need the latest application level collaboration and communication software, such as, software defined networking (SDN), services-oriented architecture (SOA), etc. Finally, the top layer consists of services that enable the market and may include energy management, health management, education, transportation etc. In addition to these 7 layers that are built on the top of each other, there are security and management applications that are required for each of the layers and are, therefore, shown on the side.

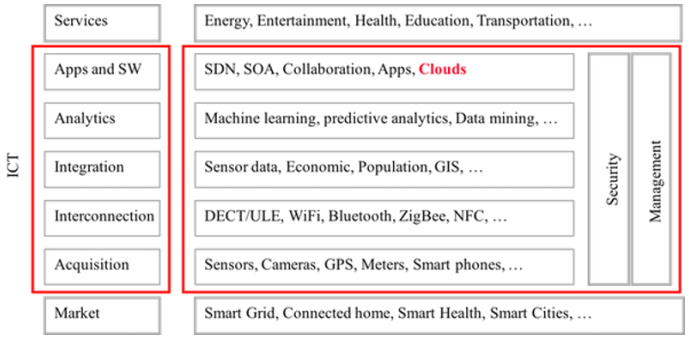

Figure 2 e: 7-layer ecosystem of IoT

3. Internet of Things Architecture:

Three- and Five-Layer Architectures. The most basic architecture is a three-layer architecture as shown in Figure 3 a 1. It was introduced in the early stages of research in this area. It has three layers, namely, the perception, network, and application layers.

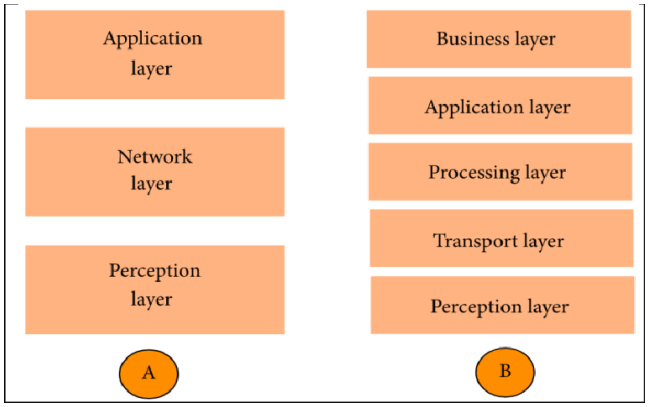

Figure 3 a 1 : Three Layer and Five Layer Architecture

- 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). 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.

Another architecture proposed by Ning and Wang is inspired by the layers of processing in the human brain. It is inspired by the intelligence and ability of human beings to think, feel, remember, make decisions, and react to the physical environment. It is constituted of three parts. First is the human brain, which is analogous to the processing and data management unit or the data center. Second is the spinal cord, which is analogous to the distributed network of data processing nodes and smart gateways. Third is the network of nerves, which corresponds to the networking components and sensors.

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 preprocessing capabilities to physical devices such as motors, pumps, or lights. The aim is to do as much of preprocessing 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 1. As a result, we do not describe edge computing separately.

Finally, the distinction between protocol architectures and system architectures is not very crisp. Often the protocols and the system are codesigned. We shall use the generic 5-layer IoT protocol stack (architectural diagram presented in Figure 3 a 1) for both the fog and cloud architectures.

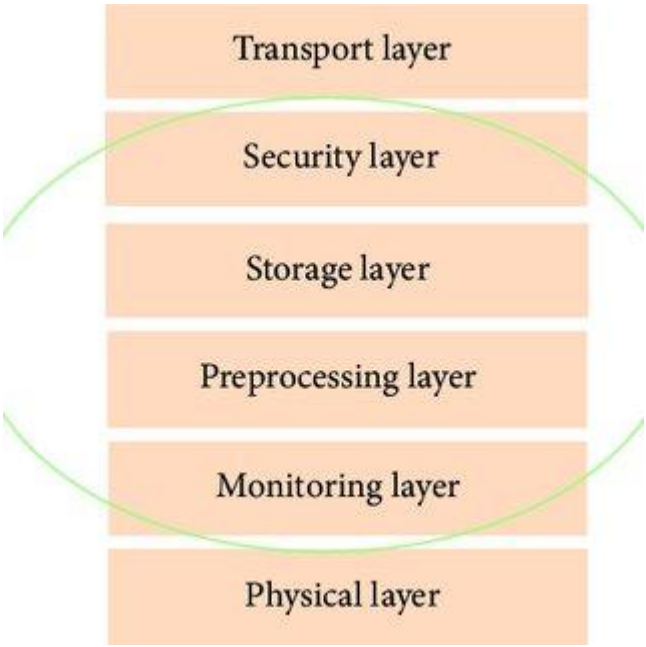

Figure 3 a 2: Fog Computing Architecture

4. Internet of things Protocols

IoT deals with the large amount of information, queries, data analysis paradigms and data mining processes with the help of software architectures that maintain the communication standards such as Hypertext Transfer Protocol (HTTP) and Internet Protocol (IP).The Protocol Stack for LLN Network Communications is depicted in Figure 4 1. Different standardization bodies are developing various protocols that are suitable for LLN networks.

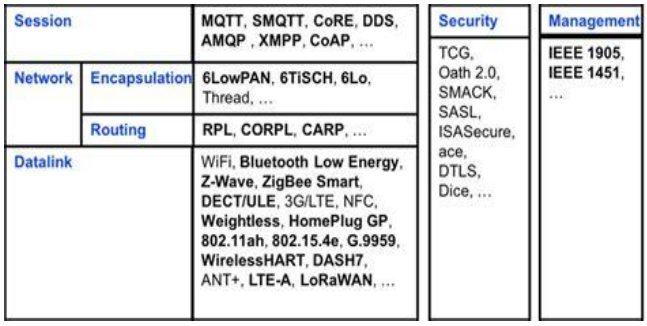

Figure 4 1: Protocol Stack

Low power radio technology IEEE 802.15.4-2006 is the well-known standard for the physical (PHY) layer which would meet the energy efficiency requirements of LLN devices. This standard operates on the worldwide unlicensed frequency band of 2.4-2.485 GHz (ISM Band).

The medium access control (MAC) layer, adopts the newly developed IEEE 802.15.4e. The important features of this protocol time-synchronized channel hopping to combat fading and interference. IEEE 802.11 - Wi-Fi Low Power for WLAN is the standard which will also be part of the MAC layer that assures high energy efficiency and integrates the existing infrastructure with integrated IP compatibility.

The network layer holds the 6LoWPAN protocol which has the responsibility of connecting the LLN devices to the Internet.6LoWPAN connects the Internet with the devices in the LLNs through the IPv6 capabilities such as encapsulation and header compression that allows the IPv6 packets to be transmitted over low-power link layer technologies. The routing issues are very challenging in the case of LLN devices. IETF's RPL protocol is capable of building the routes quickly and transmits the routing information among the nodes with minimum overhead. Adapting to the topological changes is an additional property of the RPL protocol so that it is applied in a wide range of IoT networks such as smart home, smart healthcare and smart grids.

The Transmission Control Protocol (TCP) and User Datagram Protocol (UDP) are adopted by the Transport Layer. The Constrained Application Protocol (CoAP) developed by IETF will be utilized by the application layer that implements the interoperability with HTTP for simple integration.

5. Overview of Routing protocol In IoT:

The Internet Engineering Task Force (IETF) created working groups (WGs) which developed various IoT protocols for IoT devices. We discuss below the routing protocols which have been developed by IETF for the Internet of Things (IoT).

Table -1: Protocol and respected Layers

Layer	Protocols
Application Layer	CoAP
Transport layer	TCP,UDP
Network Layer	IETF RPL, IETF 6LoWPAN
MAC Layer	IEEE 802.15.4e IEEE 802.11 - WiFi Low Power for WLAN
Physical Layer	IEEE 802.15.4

5.1. Routing in IPv6 over low power wireless personal area networks (6LoWPAN):

6LoWPAN is an IETF-standardized IPv6 adaptation layer (data link and cross-layer protocol) that enables IP connectivity over low power and lossy networks. This is observed as the basis for the network build up for the Internet of Things such as smart homes, smart cities and industrial control systems. A large number of applications utilize 6LoWPAN for IP-based communication through an upper layer protocol such as the RPL routing protocol. 6LoWPAN essentially adjusts IPv6 packets into frames of 127 bytes, a frame size requirement that low power sensor devices can utilize among themselves. 6LoWPAN supports the transmission of large-sized IPv6 packets on the data link layer of the IEEE 802.15.4. It further provides fragmentation

support at the adaptation layer involving processes such as buffering, forwarding and processing of fragmented packets which are expensive on these already resource constrained devices. Rogue nodes can send stale, overlapping or duplicate fragments to disrupt the network. At this layer there is no authentication, so the receiving nodes are debilitated in differentiating between legitimate and spurious packets during fragment reassembly. Usually the receiving nodes store up the fragments received in order to re-assemble them. If the entire set of frames making up the packet are not received after a certain timeout they are discarded. This system could also be exploited by malicious nodes which could send false fragments to fill up the nodes store, so it does not receive the legitimate fragments for re-assembly.

5.2. Routing protocol for low-power and lossy networks (RPL):

RPL was developed by the IETF working group [ROLL WG] as routing functionalities in 6LoWPAN were very challenging due to the resource constrained nature of the nodes. RPL operates at the network layer making it capable to quickly build up routes and distribute route information among other nodes in an efficient manner. RPL is a Distance Vector IPv6routing protocol for LLNs, thus network path information is organized as a set of Directed Acyclic Graphs (DAGs) and this is further classified as a set of Destination Oriented Directed Acyclic Graphs (DODAG). A DODAG typically consist of sensor nodes and a sink node which collects data from these nodes. Every DODAG is distinguished by four factors which include: DODAG ID, DODAG version number, RPL instance ID and Rank while every DODAG sink is linked with each other (Winter et al.,2012). Route selection in RPL depends on the DODAG link, cost of information to a node such as workload, throughput, node power, latency or reliability. To produce a route topology, every node selects a set of parents that comprises nodes with equal or better paths towards the sink. The node with the best route link is chosen as the parent. RPL employs three types of control messages in order to form and manage routing of information in the network and these are: I. DODAG Information Object (DIO), used for setting and updating the network topology. ii. DODAG Advertisement Object (DAO) used for broadcasting and advertising destination information upwards during network route updates. DODAG Information Solicitation (DIS) used when a new node seeks topology information while waiting to join the network. DAO and DIS are involved during a topology change process while the DIO message is broadcast and mainly used for the purpose of starting a topology change process. DIO is commonly used to distribute its routing state to other nodes using its rank (rank specifies the link quality to a sink node) and objective function. Every node computes its rank according to the rank of its selected parent and the objective function. A DIO message is sent to all nodes every time a node updates its rank or preferred parent. To prevent the formation of loops, RPL utilizes the rank rule whereby a node in a parent should always have a lower rank than its children. Also, to limit the amount of broadcast, RPL uses the trickle algorithm for scheduling DIO messages to be sent. It does this by setting a counter which observes the network topology and thereby decides when a node has to send a DIO message. For every DIO message received without comparing it with the previous DIO message this will cause the DIO counter to increase and if the DIO counter reaches a threshold value (redundancy value) the node will reset its DIO counter and double the trickle time. This is done to stabilize the network topology over a period of time and avoid the unnecessary frequent route updates which could consume the limited power and bandwidth available. The RPL routing protocol has capacity to incorporate different types of traffic and signaling information swapped among nodes although this depends on the requirements of the considered data flows. RPL supports the Multipoint-to-Point (MP2P), Point-to-Multipoint (P2MP) and Point-to-Point (P2P) traffics.

5.3. 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.

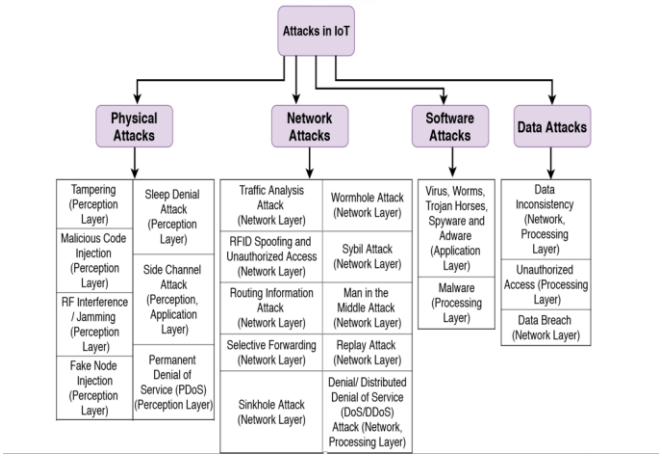

Figure 5 1: Attacks on IoT

Here we provide the Attack, Effect on Network parameter and Method to counter measures in table-2.

Table-2: Attacks and methods to counter measures

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

6. Why RPL is used Instead of 6LoWPAN:

- RPL is a lightweight, rank based routing protocol.
- RPL is the routing protocol developed specifically for low power and lossy networks, in which nodes and routers are expected to be power-constrained.
- So it is made to measure for much of what people have come to believe is (or will be) the Internet of Things.
- RPL runs in power-constrained nodes, it is a reactive protocol. Which means, routes are found when they are needed, rather than routing tables being maintained over time.
- Supporting wifi, 802.15.4, Lora and more in Contiki OS enabled by RPL.
- Like signaling overhead, PDR, latency and energy utilization.
- RPL is a well-suited protocol for LLNs.

7. CONCLUSIONS

In the survey paper we defined all the topics related to the Internet of Things. All the components related to the internet of things in Details. You will get detailed knowledge about the Internet of things ecosystem, Internet of things Elements, Internet of things Architecture. Also we will cover all the internet of things protocols and brief about protocols. In this we will provide the details of attack based on Protocols and at the last we justify why RPL is useful over 6LowPAN in the internet on things network layer.

REFERENCES

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

[2] Pallavi Sethi and Smruti R. Sarangi, "Internet of Things: Architectures, Protocols, and Applications", Journal of Electrical and Computer Engineering, 2016

[3] O. Vermesan, P. Friess, P. Guillemin et al., "Internet of things strategic research roadmap," in Internet of Things: Global Technological and Societal Trends, vol. 1, pp. 9–52, 2011.

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

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