Survey of Networking Protocol for IoT

Trupti Pithva, Deepak Upadhyay
Student of cyber security at GTU-GSET, Professor At GTU-GSET

Department of Masters of Engineering in cybersecurity at GTU-GSET Ahmedabad India.

Abstract : : Internet of Things (IoT) is a typical pattern that has gained more popularity in recent years. IoT refers to the interaction among our everyday devices such as smartphones, tablets, laptops, personal computers, and other devices. These devices now communicate smartly [1] to each other. The goal of IoT is to be connected anytime and anywhere using a network or internet. In this paper, different types of network layer prototype and they include communication with the network. The discussion includes.

Index Terms **- IOT, Encapsulation, Routing.**

I. Introduction

IoT and its protocol are widely used nowadays. IoT is the most recent trend in academic and industrial fields. They are used in hardware and software-based work to implement the device to communicate with network and handheld devices. According to analysis, the IoT devices are the most usable device compare to other devices and they are the most money-making technology being invested in the digital market. Billions of dollars are being invested by investors on IoT enabling technologies and research while much more is expected to come in the upcoming years in this era.

In this paper some of the standard protocol and non-standard protocol that is used for network encapsulation and routing in IoT applications. the encapsulation layer that forms the packet and in the routing layer it handles the transfer of the packet from source to destination.

II. Characteristics of Internet of Things (IoT)

Some information about IOT that communicate with a different type of physical devices. Devices work a very important role in IoT technology.

- Self-Organization: self-organize is it works to restore the information or services provided by the device. It also takes care of the information with network connectivity.
- Optimized energy solution: we must able to know about low power devices and owners to be accessible to almost optimal outcomes and used information.
- Localization and tracking capabilities: it must be able to track the device information and locate them within a less duration.
- Information and knowledge management: in IoT information does not need to instruct machines every time. All devices are well-known with information to make a decision and find the solution.
- Ubiquitous data exchange: ubiquitous sensors are more powerful so it gathers the information through the input in IoT device.
- Scalability: IoT network has scalability with a strong network and all the devices are must be identified uniquely and tags properly.

III. Applications of Internet of Things (IoT)

The world of IoT includes a wide variety of devices and applications with wireless communication. Most of the users were used applications in our daily life.

- Traffic Management: in traffic management, people are don't require the manual signal and lights, IOT applications used for traffic management to avoid accidents.
- Agriculture and Breeding: using the IoT people are use the high qualified technology for farming and breeding to support the improvement of the system with drone technology in agriculture.

- Transportation Industry: in the transportation industry people are avoiding the stop and pay at toll gate through IoT. Also using at buses and train fairs in the token system.
- Environment Monitoring: Using the RFID chip and sensor to check the weather and air pollution in the environment.
- Retail and Marketing: The use of IoT in marketing and the retail field is very useful. Information about the stock and availability of the merchandise through RFID tags.
- Independent Living: IoT applications can be useful for people to remember their activities at that time and give to support their lives.
- Connected Medicine: Patients are using the facilities over the IoT using health tracker and get the information regarding any kind of symptoms. Doctors can monitor the patient from the hospital itself.
- Driverless Cars: using IoT people are don't want to require a driver in a car, they used sensors to control automatically and navigate the passenger to the destination
- Earthquake Detection: Disasters like an earthquake, tsunami snowfall can be identified before it's going to happen through IoT sensors or devices.

IV. Challenging Issues

In, regular life several technical issues of IoT ware pointed out. All new challenges and issues identified in the current internet scenario require the effort to change the era.

- Data management in a regular day's people are used lots of data and lots of information transferred from one device to another. Which data transmitted in which place and how to be placed in data management know all kinds of information using IoT.
- Security: In IoT, two major issues are privacy (user-related information) and security about the sensed data and business processes. The heterogeneity in IoT nodes, the large scale of deployment, resource constraints, and their mobility make it harder to secure the network. There are a large number of techniques for ensuring confidentiality. Security providing might be difficult as the automation of the devices has been increased which created new security issues.

Security is a critical component for adopting the IoT at a global level, and without any guarantee, regarding authenticity, confidentiality, integrity, and non-repudiation the related party is unlikely to adopt on a large scale.

- Storage management: As there is a large amount of data generated. When the devices are being connected there would be a large amount of multimedia data which is being transferred they occupy a large amount of data and the other kind is random files where it contains data regarding the devices these files doesn't occupy a huge amount of space but they are large in number they must be accessible very quickly whenever necessary.
- Energy: Many of the IoT nodes runs on battery-operated power and energy efficiency is most crucial for availability and proper functionality of the network. Most of its nodes are running on non-chargeable energy sources and communication between heterogeneous nodes [2] is more energy-consuming.
- Insecure authentication/authorization: We generally provide authentication to provide permission for the user to access the information and authorization is used to editing or change the data for that particular application and permission will be given by the administrator.
- Server technologies: as the number of devices over the network area increases the request and the number of responses of the device also increases at the same time it depends on the server where we are running the interface. The response of the server to the request of the device should be done quickly. There should be no delay in the response to the client.

V. Network layer encapsulation protocol

Encapsulation is a process by which a lower-layer protocol receives data from a higher-layer protocol and then places the data into the data portion of its frame. Thus, Encapsulation is the process of enclosing one type of packet using another type of packet.

Ericsson (2011) estimated that up to 2020 there will be 50 billion devices on the Internet, so to support the unique addressing mechanism IPV6 protocol is used on its network.

IoT data link frame format relatively small to store IPV6 addresses. Therefore, to handle this kind of situation IETF (Internet Engineering Task Force) working on a set of standards to enclose the IPV6 datagram's into IoT [2] data link layer frames.

VI. Encapsulation with 6LowPAN

- **6LowPAN**

Low-power Wireless Personal Area Network (6LowPAN) is defined by the IEEE standard [3][4][5]. Could be applied to the smallest devices and those low-power devices with limited processing capabilities. It efficiently encapsulates IPv6 long headers in IEEE802.15.4 PHY (only support frame up to 127 bytes) small packets [5]. Realizing IPv6 communication on wireless networks composed of low-power wireless modules. Includes packet compression and other optimization mechanisms, which are used for effective use of the routing of IPv6 packets. From a security point of view, 6LowPAN suffers from several attacks that aim to directly damage the network. 6LowPAN is vulnerable to spoofing attacks, selective forwarding, Sybil attacks, wormhole attacks, and sinkhole attacks. These attacks can be internally initiated by malicious code or intrusion and externally by unauthorized devices or users.

- **6TiSCH**

Ipv6 over the time-slotted channel hopping mode of IEEE 802.15.4e (6TiSCH): It builds document and higher standard based architecture [3]. Highlight best practices and standardize missing components of the archive industries and great performance ex latency, scalability, reliability, and low power operation. Such devices communicate following a time division multiple access (TDMA) schedule. So it allocates unit of the bandwidth of time slot between neighbor nodes. It will allow the programming of predictable transmissions and also based on RPL protocol. The development of the 6TiSCH protocol is in process. 6TiSCH's IoT stack is used in a wide range of applications such as forest fire detection, home automation, and smart city.

- **6lo**

A newly assigned IETF group called IPv6 over networks of resource-constrained nodes (6Lo) is working to propose a set of standards on the transmission of IPv6 frames on various data links [3]. Even though 6LowPAN and 6TiSCH were developed for encapsulation purposes, it became clear that more standards are needed to cover all data link standards. Therefore, 6Lo was formed by IEFT for this purpose.

Most of the 6Lo specifications have not been finalized and are in various stages of drafts.

1. Network layer routing protocol

1. Identity the path from sender to receiver.
2. Two nodes communicate in a bi-directional manner. If and only if they are within the communication range of each other.
3. The neighbors can communicate directly but A and C want to communicate then must seek help from B.

   a. We are adding node D then more possibilities to exchange data from A to C.
   b. A-B-C, A-D-C, A-D-B-C, A-B-D-C.
   c. The whole scenario gets even more complicated with the increase of the number of nodes in the network.
   d. Only neighbor information is not enough.

VII. Categories of routing protocol

1. Proactive routing protocol- each node maintain routing
2. Reactive routing protocol- do not maintain all routing into at all node
3. Hybrid routing protocol-combination of proactive and reactive protocol

   a. For proactive protocol and For reactive protocol
   b. Dijkstra algorithm and the bellman-ford algorithm used to find the shortest path.

VIII. Routing with RPL

Routing protocol for low-power and lossy networks (RPL) is a distance-vector protocol designed at IETF for routing in the IoT system. Message confidentiality and reliable message delivery are cared for by RPL. The router is usually limited in terms of processing power, battery, and memory. RPL traffic pattern could be p2p, p2mp, mp2p. The RPL enabled with features of low data rate and communication with high throughput. Security will be the major challenge of RPL enabled IoT devices.

IX. RPL topology

DODAG topology used in RPL[6] DODAG is a destination-oriented directed acyclic graph. It is acyclic means top-down and bottom-up possibilities are there. DODAG is a DAG rooted at a single destination. The DODAG root has no outgoing edges. DODAG is uniquely identified by a combination of RPL instance ID and DODAG ID. Node rank defines the node individual position relatives to other nodes concerning a DODAG root. RANK strictly increase in the down direction and strictly decrease in the up direction. DODAG root is the DAG root of the DODAG. May act as border router and aggregate routers in the DODAAG and may redistribute DODAG routes into other routing protocols.

X. Challenges of RPL Protocol

- If any node fails then anyhow packet reaches the server node.
- Upward path is so common (mp2p) all children not traversing possible Downward path is optional mainly for p2p and p2mp.
- DODAG are disjoint (no shared node) link properties are (reliability, latency)
- Node properties powered on not.
- RPL instance has an optimization objective.
- Multiple instances with different optimization objectives can coexist.

XI. Collection Tree Protocol (CTP)

CTP is a distance-vector routing algorithm that was developed as a solution to routing in WSNs. It stands as a predecessor to RPL and was considered the de-facto routing standard for TinyOS. It builds a tree-based topology with the root at the sink of the network, CTP uses an adaptive beaconing mechanism to broadcast routing control messages. Moreover, CTP relied on specific link-layer technology for topology formation, CTP was earlier known for its efficient energy consumption and high Packet Reception Ratio (PRR).

Lightweight on-demand ad hoc distance-vector routing protocol-next generation LOADng: The Lightweight on-demand ad hoc distance-vector routing protocol-next generation or LOADng is a lightweight variation of AODV for LLNs.[1] It is designed based on the idea that LLNs are idle most of the time. Hence instead of adopting a proactive approach that would generate unnecessary overhead, LOADng follows a reactive approach in which routes are established towards destinations only when there is some data to send. LOADng is a reactive routing protocol and is found suitable for a more general traffic pattern. It does not have any node that performs special functions like the root and is hence not subjected to the subsequent problems that arise due to such a consideration. Also, due to its compressed and flexible data format, there is no possibility of fragmentation. It does not impose any strict source routing rules, hence it can accommodate applications that require a fixed MTU. However, LOADng might have a higher delay in the route discovery phase and might have higher control traffic overhead if the traffic flows are predominantly P2P.

- **CORPL**

Cognitive and Opportunistic RPL (CORPL) is the extension of RPL. Specifically designed for Cognitive networks and uses DODAG topology generation [3]. CORPL utilizes opportunistic forwarding to forward the packet by choosing multiple forwarders. And coordinates between the nodes to choose the best next-hop to forward the packet to the same way as RPL. The process of opportunistic forwarding uses the local network information for deciding on dynamically forwarding the data to its neighboring node.

- **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 [3]. 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 networks. In data forwarding, the packet is routed from the sensor to the sink in a hop-by-hop fashion. Each next hop is determined independently. The main problem with CARP is that it does not support the reusability of previously collected data. Since it is not standardized and just proposed in the literature, it is not yet used in other IoT applications.

XII. E-CARP Routing Protocol

E-CARP, which is an enhancement upon CARP, to develop a location-free and greedy hop-by-hop routing protocol for forwarding packets from sensor nodes to the sink node in an energy-efficient manner. CARP does not consider the reusability of sensory data collected previously by domain applications in the following time points, which induces sensory data packets [1] forwarding which may not be beneficial to certain applications. Therefore, E-CARP allows the caching of sensory data at the sink node, for avoiding these data packets forwarding in the network. CARP requires to reply to a PONG control packet whenever receiving a PING control packet when selecting the most appropriate relay node for packet forwarding. This PING-PONG strategy may not be mandatory when the network topology is relatively steady. This observation drives us to improve the relay node selection strategy in CARP, and the relay node adopted previously is given a higher priority to be reused at this moment. Simulation results validate that our E-CARP can decrease the communication cost and increase the network capability to a large extent, especially when the ratio of packet size between control packets and sensory data packets is relatively large. E-CARP does not differentiate the priority of different attributes. Sensory data of attributes of more importance should be routed to SN with a higher priority. Besides, sensory data of a certain sensor node may vary following a spatial and/or temporal discipline.

XIII. CONCLUSION

This paper surveys some of the standard and nonstandard protocols that are used for network routing in IoT applications. Six routing protocols and also include encapsulation in IoT were studied in this paper. RPL is the most commonly used one. It is a distance-vector protocol. CORPL is a nonstandard extension of RPL that is designed for cognitive networks and utilizes the opportunistic forwarding to forward packets at each hop. 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 the literature, it is not yet used in other IoT applications. E-CARP does not differentiate the priority of different attributes.

XIV. REFERENCES

1) ALAHARI HANUMAT PRASAD, T.HEMA BHARAT “NETWORK ROUTING PROTOCOLS IN IOT”, International Journal of Advances in Electronics and Computer Science, ISSN: 2393-2835, Volume-4, Issue-4, Aprl.-2017
2) Anurag Shukla, Sarsij Tripathi, “A Survey on Next-generation Computing IoT Issues and Challenges”, International Journal of Pure and Applied Mathematics 2018.
3) R Yugha, S Chithra “A Survey on technologies and security protocols: Reference for Future Generation IoT” Elsevier Journal of Network and Computer Applications 2020.
4) Tara Salman, Raj Jain, “A Survey of Protocols and Standards for the Internet of Things” 2017 21st International Conference on Control Systems and Computer Science (CSCS). IEEE conference 2017.
5) Arif Mahmud, Faria Hossain, Tasnim Ara Charity and Faija Juhin, “Simulation and Comparison of RPL, 6LoWPAN, and CoAP Protocols Using Cooja Simulator” Springer Nature Singapore Pte Ltd. Proceedings of International Joint Conference on Computational Intelligence, Algorithms for Intelligent Systems 2020.
6) Nikshepa, Vasudeva Pai, Karthik Pai, Udaya Kumar K Shenoy, “Performance Analysis of IoT Adaption Layer Protocol”, International Journal of Engineering & Technology, Research paper 2018.
7) Baraq Ghaleb, Ahmed Al-Dubai, Elias Ekonomou, and Isam Wadhaj, “A New Enhanced RPL Based Routing for the Internet of Things ”, ICC2017: WS06-Convergent Internet of Things- On the synergy of IoT systems, IEEE International conference July 2017.
8) Ala Al-Fuqaha, Mohsen Guizani, , Mehdi Mohammadi, Mohammed Aledhari, Moussa Ayyash“Internet of Things: A Survey on Enabling Technologies, Protocols, and Applications”, IEEE journal 2015.
9) Basim Ahmad Alabsi, Mohammed Anbar, Selva Kumar Manickam, Omar E. Elejla. ‘DDoS attack aware environment with secure clustering and routing based on RPL protocol operation’ IET journals the institute of engineering and technology in September 2019.
10) Ammara Roohi, Muhammad Adeel, Munam Ali Shah, “DDoS in IoT: A Roadmap Towards Security & Countermeasures”. 19136769 25th International Conference on Automation and Computing (ICAC) 2019.
11) Sharwari Satish Solapure and Harish H.Kenchannavar “RPL AND COAP PROTOCOLS, EXPERIMENTAL ANALYSIS FOR IOT: A CASE STUDY” International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.10, No.2, April 2019.
12) Pratyush Kumar Sinha, E.Suresh Babu, Nipun Gupta, Kazi Afreen Naz, Hameeda Khatoon “IMPLEMENTATION OF COMMUNICATION PROTOCOL STACK FOR 6LOWPAN NETWORK DOMAIN IN INTERNET OF THINGS” International Journal of Pure and Applied Mathematics Volume 115 No. 6 2017, 327-333