SURVEY ON DEVICE MANAGEMENT IN IoT

Meenu muraleedharan [1], Merin K J [2], Nijisha Jose [3], Dr.Vince Paul [4]
B.Tech CSE, Sahrdaya college of engineering & technology, Kodakara, Kerala, India ,Head of Department[2],Department of Computer Science and Engineering

Abstract: ***The Internet of Things (IoT) is the next wave of innovation that promises to improve and optimize our daily life based on intelligent sensors and smart objects working together. Through Internet Protocol (IP) connectivity, devices can now be connected to the Internet, thus allowing them to be read, controlled, and managed at any time and at any place. Security is an important aspect for IoT deployments. However, proprietary security solutions do not help in formulating a coherent security vision to enable IoT devices to securely communicate with each other in an interoperable manner. This paper gives an overview of the efforts to design a protocol which standardize security solutions for the IoT ecosystem. We first provide an in-depth review of the communication security solutions for IoT, specifically the standard security protocols to be used in conjunction with the Constrained Application Protocol (CoAP) or Message Queing Telemetry Transport (MQTT), an application protocol specifically tailored to the needs of adapting to the constraints of IoT devices.This paper also discusses efforts to adapt MQTT embedded in REST for IoT applications. This paper also includes device to device communication (D2D) in wireless wide area network in addition to the fundamental requirements of energy efficiency, reliability, and Internet connectivity. We also develop a enhanced LTE standard for reducing complexity of communication between smart phone and IoT devices.***

Keywords: Communication security, compression scheme,end-to-end security, Internet of Things (IoT), machine-tomachine Communication, standardization. High-speed packet access (HSPA), and long-term evolution (LTE). Constrained Application Protocol (CoAP)

I. INTRODUCTION

The notion of Internet of Things (IoT) has been recognized by media and industrial leaders as the next wave of innovation, and spreading into our daily life [1], [2]. Sensors around us are increasingly becoming more attempts and pervasive to fulfill end user's needs, these are easy to use in our everyday activities. Devices deployed in everywhere are now interconnected with the Internet.ie, households, industrial automation, and smart city infrastructures. This interconnection provides a whole range of data ,ie,environmental context, device status, energy usage, etc. that can be aggregated, collected and then shared in an efficient, secure, and privacy-aware manner. As these devices are connected to the Internet, they can be managed and reached at anytime and at any place. Now the IoT is filled with a very diverse range of wireless communication technologies, such as IEEE 802.15.4, Bluetooth Low Energy (BTLE), WiFi, and various other cellular communication technologies. Actually, gadgets utilizing distinctive physical and connection layers are not interoperable with each other. Through an Internet Protocol (IP) switch, these gadgets are, be that as it may, ready to speak with the Internet. When the differences in the protocol stack extend beyond the link layer and phisical layer, protocol translation needs to be performed by a gateway device. This damages the deployment of IoT devices because the deployment becomes more perplexing and costly with various middleboxes along the end-to-end communication path. In order to ensure seamless connectivity between various devices deployed in the market, a convergence toward all IP-based communication stacks is necessary.

A long time back, the Internet Engineering Task Force (IETF) has institutionalized IPv6 over Low-Power Wireless Personal Area Networks (6LoWPAN) [3], Routing Over Low-power and Lossy networks (ROLL) [4], and Constrained Application Protocol (CoAP) [5] to equip constrained devices with low memory footprint and computational capabilities to run IPv6 over low-power wireless networks. The ZigBee IP standard [6], which principally focuses the smart energy domain, expands on top of the 6LoWPAN stack [7], [8], [9]. IEEE 802.15.4-based devices used in other industry domains are expected to adopt the 6LoWPAN concept as well, since it gives the premise to running IPv6 over low-power radios through an adaptation layer, profiling of the IPv6 neighbor discovery mechanism, and compression schemes. Comparative adjustments are given to BTLE [10] and Digital Enhanced Cordless Telecommunications (DECT) Ultra Low Energy [11], the two other short-extend radio innovations. Then, numerous IoT gadgets are utilizing WiFi and are as of now running the full IP protocol stack. IP protocol can be viewed as the paste to interconnect these heterogeneous wireless networks togetherThe pervasive device connectivity to the Internet also postures concealed security risks, namely, eavesdropping on the wireless communication channel, unauthorized access to devices, altering with devices, and privacy risks. The inherent characteristic of constrained devices means that the state-of-the-art cryptographic algorithms and protocols are difficult to deploy on such devices and even more hard to stay the software up-to-date. The capacities to connect, manage, and control a device from anyplace and at whatever time requires appropriate authentication and authorization measures.

Many of the wide-area applications for IoT [12] are enterprise-centric and offer an appealing market opportunity to wireless operators who are looking to improve their incomes by entering the IoT market. Because of the expected boom in IoT with power grid management, smart cities and such wide-area applications, there is a strong interest in developing wide-area solutions within the Third Generation Partnership Project (3GPP) and in forums such as OneM2M [13]. For IoT devices, in addition to the desired property of low power/energy consumption, the hardware must be inexpensive and reliable and have a long lifetime. In many cases, it must be capable of operating in rugged environments. Convenience is another important factor for IoT devices, with minimal or no alignment or synchronization requirements. IoT devices must have the capacity to endure frequency/time drift within a predetermined range and also support simple subscriber identification (ID).Furthermore, the traffic properties of IoT devices are wide ranging, from static, delay tolerant, infrequent and small packets to mobile, delay sensitive, frequent, and large packets. As said before, it is clear that the prerequisites to support IoT communications are substantially different from the design paradigm for current

macrocellular networks enhanced for human communications.The difficulties in conveying current macrocellular networks [e.g.,high-speed packet access (HSPA), general packet radio service (GPRS), and long-term evolution (LTE)] for IoT are the tight synchronization necessity and high signaling overhead not suited to energy-constrained devices.Therefore, the necessities for IoT communications might be best upheld by a new architecture and lightweight protocol structure rather than an evolution of the current cellular architecture and protocols. Besides, research has addressed the requirement for a simplified protocol stack for supporting IoT transmissions in widearea networks. The utilization of the LTE smartphone as a gateway to IoT devices is proposed, with constrained application protocol (CoAP) as the session layer protocol alongside client datagram protocol (UDP) at the transport layer. CoAP is intended to suit the energy constraints and the low handling power of IoT devices. CoAP is a protocol with low message overhead, along with support for retransmissions, multicast , and congestion control.

This paper gives an overview of the efforts to design a protocol which institutionalize security solutions for the IoT ecosystem. We first give an in-depth review of the communication security solutions for IoT, particularly the standard security protocols to be utilized as a part of conjunction with the Message Queing Telemetry Transport (MQTT) or Constrained Application Protocol (CoAP), an application protocol particularly tailored to the needs of adapting to the constraints of IoT devices.This paper also discusses efforts to adapt MQTT embedded in REST for IoT applications. This paper also includes device to device communication (D2D) in wireless wide area network in addition to the fundamental prerequisites of energy efficiency, reliability, and Internet connectivity. We also develop a enhanced LTE standard for reducing complexity of communication between smart phone and IoT devices.

II. IoT

The Internet of Things (IoT) is a novel paradigm that is rapidly quickly making progress in the situation of present day wireless telecommunications.The essential thought of this idea is the pervasive presence around us of a assortment of things or items – for example, Radio-Frequency IDentification (RFID) tags, sensors, mobile phones,actuators, etc. – which, through unique addressing schemes, are able to interact with each other and cooperate with their neighbors to achieve common goals [14]

An IoT device can be characterized by its functionalities or "features." For the purpose of description, this paper defines a feature as a specific input or output "capability" of the IoT device. For example, a wearable ring with a temperature sensor has the input device feature (IDF) called "temperature" (abbreviated as T-IDF). A couple ofwearable glasses with the optical head-mounted display has the output device feature (ODF) called "display" (abbreviated as D-IDF). An IoT device might be associated with the network (i.e., Internet) utilizing wireless communications directly or indirectly through an advanced mobile phone. Assuming this is the case, the relating software called network application is created and executed by a server in the network side, which gets or sends the messages from/to the IoT device. When the values of the IDFs are overhauled, the IoT device will inform the network application to take few actions, and the network application may send the outcome to the ODF of an IoT device. With this view, the IoT devices connect with each other through their features, and we say that the network application "maps" the IDFs to the ODFs.. Fig. 1 illustrates five IoT devices D1, D2, D3, D4, and D5, where the left-hand side of the figure shows the IDFs of the devices and the right-hand side of the figure shows the ODFs of the devices. The wearable ring D1 has three input device features H-IDF (humidity), G-IDF (gravity), and T-IDF. The smart phone D2 has four input device features T-IDF, G-IDF, M-IDF (microphone), and C-IDF (camera) illustrated in the left-hand side of Fig. 1, and three output device features: D-ODF, V-ODF (vibration), and S-ODF (speaker) illustrated in the right-hand side of Fig.2.1The wearable glasses D3 have two input device features M-IDF and C-IDF, and one output device feature D-ODF. The bulb D4 has an output device feature L-ODF (luminance). The tail D5 has one output device feature V-ODF (vibration). This special device is the Silver Medal Award artwork "transparent organ" in Salon International Des Invention [16]. The tail of this device was based on the vibration strength received from its V-ODF

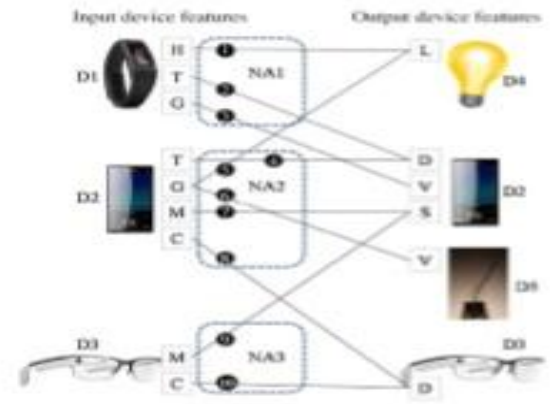

Fig 2.1 IoT devices, device features, and the network applications.Connections among D1, D2, D3, D4, and D5.

In an IoT-enabled environment, things or physical objects becomes responsive. They are connected to the Internet and embedded with processing and communication capabilities. Wireless Sensor Networks (WSNs) decide a key building block of IoT technologies. Typically, sensors are considered resource-constrained devices with restricted battery power and computation capabilities(e.g.low CPU clock and memory footprints) [16]. Therefore, it is more effective and efficient to pass on multicast messages to a gathering of devices rather than sending energy consuming unicast messages to individual devices in various copies. Securing the group key establishment incline to form the key functionality to give integrity, authentication, and confidentiality for message transmissions in these multicast groups [15]. Besides, group key establishment protocols have to support device and network characteristics in IoT-enabled WSNs such as resource constraints, dynamic group formation , and scalability.

The field of applying multicast is as manifold as the application area of IoT itself, including smart homes, smart cities, environmental monitoring, and healthcare For a better understanding of major necessities for a multicast support the following usecase is resolved. It is intended for the control of lightbulbs in a smart building [17] (Figure 2.2). The environmental monitoring network collects information about light intensity, temperature, and population of all rooms in the building and conveys accumulated information to a central entity. In view of information got, the central entity can empower synchronous operations (e.g., giving commands for on, off, or dim-level) among a group of light bulbs in a floor or room to achieve a visual synchronicity of light effects on the client

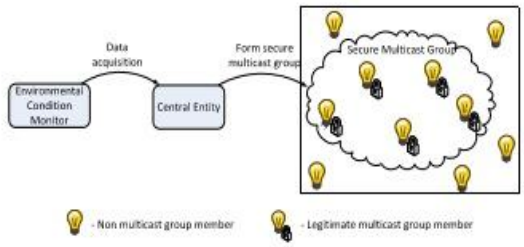

Fig2.2 Multicasting for light bulbs

III. IoT PROTOCOL

To provide communication between devices and services several protocols are used in IoT.Some of these are MQTT,CoAP,SOAP,REST etc.There are three types of commnicatications-Device to Device(D2D),Device to Server(D2S),and Server to Server(S2S).Devices must communicate with each other (D2D). Device data then must be collected and sent to the server infrastructure (D2S). That server infrastructure needs to share device data (S2S), perhaps giving it back to devices, to analysis programs, or to people.the protocols used to provide secure interaction can be described as:

- MQTT: a protocol for collecting device data and communicating it to servers (D2S)
- XMPP: a protocol best for connecting devices to people, a special case of the D2S pattern, since people are connected to the servers
- DDS: a fast bus for integrating intelligent machines (D2D)
- AMQP: a queuing system designed to connect servers to each other (S2S)Each of these protocols is widely adopted. There are at least 10 implementations of each. All four claim to be real-time publish-subscribe IoT protocols that can connect thousands of devices. And it's true, depending on how you define "real time," "things," and "devices."

Nonetheless, they are very different .Today's Internet supports hundreds of protocols. The IoT will support hundreds more. It's important to understand the class of use that each of these important protocols addresses[18]

A. MQTT

MQTT, the Message Queue Telemetry Transport, targets device data collection(Fig 3.1 As its name expresses, its fundamental object is telemetry, or remote monitoring. Its goal is to collect data from numerous devices and transport that data to the IT infrastructure. It targets huge networks of small devices that should be monitored or controlled from the cloud.

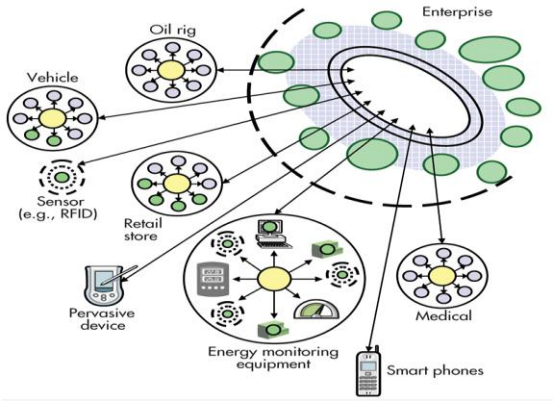

Fig 3.1 MQTT

MQTT makes little attempt to enable device-to-device transfer, nor to "fan out" the data to many recipients. Since it has a clear, compelling single application, MQTT is simple, offering few control options. It also doesn't need to be particularly fast. In this context, "real time" is typically measured in seconds.

A hub-and-spoke architecture is natural for MQTT. All the devices connect to a data concentrator server, like IBM's new MessageSight appliance. You don't want to lose data, so the protocol works on top of TCP, which provides a simple, reliable stream. Since the IT infrastructure uses the data, the entire system is designed to easily transport data into enterprise technologies like ActiveMQ and enterprise service buses (ESBs).

MQTT enables applications like monitoring a huge oil pipeline for leaks or vandalism. Those thousands of sensors must be concentrated into a single location for analysis. When the system finds a problem, it can take action to correct that problem. Other applications for MQTT include power usage monitoring, lighting control, and even intelligent gardening. They share a need for collecting data from many sources and making it available to the IT infrastructure.

B. CoAP

Constrained Application Protocol (CoAP) is a software protocol intended to be used in very simple electronics devices, allowing them to communicate interactively over the Internet. It is particularly targeted for small, low-power sensors, switches, valves and similar components that need to be controlled or supervised remotely, through standard Internet networks. CoAP is an application layer protocol that is intended for use in resource-constrained internet devices, such as WSN nodes. CoAP is designed to easily translate to HTTP for simplified integration with the web, while also meeting specialized requirements such as multicast support, very low overhead, and simplicity Multicast, low overhead, and simplicity are extremely important for Internet of Things (IoT) andMachine-to-Machine (M2M) devices, which tend to be deeply embedded and have much less memory and power supply than traditional internet devices have. Therefore, efficiency is very important. CoAP can run on most devices that support UDP or a UDP analogue[19].

Features:

- Overhead and parsing complexity.
- URI and content-type support.
- Support for the discovery of resources provided by known CoAP services.
- Simple subscription for a resource, and resulting push notifications.
- Simple caching based on max-age
- Instead of addressing each resource individually (e.g. to turn on all the CoAP-enabled lights in a room with a single CoAP request triggered by toggling the light switch).Therefore CoAP can be used to implement group key method of device control which is previously mentioned in this paper.

IV. CONCLUSION

From this survey,we observe that The internet has drastically changed the way we lived, as in scenario all the interaction is done over the internet. The IoT has the potential to add a new dimension to this process by enabling communication between smart objects. IoT should be considered as a part of future internet as everything is going to be connected in a network so there are lots of issues which are to be solved to make this a reality.The main reasons why it has not truly been implemented is the impact it will have on the legal,

ethical, security and social fields. Once implemented successfully, the quality of life is improved because of the reduction of the effort made by humans on unimportant things.

REFERENCES

[1] Cisco. (2014, Jan.). The Internet of Things[Online].

[2] Ericsson, "More than 50 billion connected devices," Ericsson White Paper 284 23-3149 Uen, Feb. 2011.

[3] N. Kushalnagar, G. Montenegro, and C. Schumacher, " IPv6 over low-power wireless personal area networks (6LoWPANs)Overview,assumptionns,problem statement, and goals," RFC 4919, Aug. 2007.

[4] T. Winter et al., "RPL: IPv6 routing protocol for low-power and lossy networks," RFC 6550(Proposed Standard), Mar. 2012.

[5] Z. Shelby, K. Hartke, and C. Bormann,"Constrained application protocol (CoAP)," draft-ietf-core- coap-18, IETF, 2013. [50] T.Winteretal., "RPL: IPv6 routing protocol for low-power and lossy networks," RFC 6550 (Proposed Standard), Mar 2012

[6] Zigbee Alliance, "Zigbee-IP specification," Mar. 2013.

[7] J. Hui and P. Thubert, "Compression format for IPv6 datagrams over IEEE 802.15.4-based networks,"RFC 6282 (Proposed Standard) Sep. 2011.

[8] G. Montenegro, N. Kushalnagar, J. Hui, and D. Culler "Transmission of IPv6 packets over IEEE 802.15.4 networks," RFC 4944, Sep. 2007

[9] Z. Shelby, S. Chakrabarti, E. Nordmark, and C. Bormann, Neighbor discovery optimization for IPv6 over low-power wireless personal area networks," RFC 6775, Nov. 2012.

[10] J. Nieminen et al., "Transmission of IPv6 packets over Bluetooth low energy," draft-ietf-6lowpan-btle-12, IETF

[11] P. PeterMariager, J. Petersen, and Z.Shelby, "Transmission of IPv6 packets over DECTultralow energy," draft-mariager-6lowpan- v6over-dect-ule-03, IETF, 2013

[12] G. Wu, S. Talwar, K. Johnsson, N. Himayat, and K. D. Johnson, "M2M: From mobile to embedded Internet," IEEE Commun. Mag.,vol. 49, pp. 36–43, Apr. 2011

[13] OneM2M. (2012). [Online]. Available: http://onem2m.org/

[14] https://www.elsevier.com/__data/assets/pdf_file/0006/97026/ The-Internet-of-Things.pdf

[15] S. Keoh, S. Kumar, O. Garcia-Morchon, E. Dijk, and A.Rahman. (Feb. 2014). DTLS-Based Multicast Security for Low-Power and Lossy Networks (LLNs).

[16] J.ZhangandV.Varadharajan,''Wirelesssensor networkkey management survey and taxonomy,'' J. Netw. Comput. Appl.,vol. 33, no. 2, pp. 63–75, 2010.

[17] Rahman and E. Dijk. (Oct. 2014). Group Communication for the Constrained Application Protocol (CoAP). [Online]. Available: https://tools.ietf.org/html/rfc7390

[18] http://electronicdesign.com/iot/understanding -protocols-behind-internet-things

[19] https://en.wikipedia.org/wiki/Constrained_Application_Protocol