Ubiquitous computing IoT Application Layer (Restful) Protocols- Survey

Geeta Pawar[#1]and JayashreeAgarkhed[*2]
[#]Research Scholar, Department of Computer Science and Engineering, PDA College of Engineering, Kalaburagi, India
[*]PhD,Department of Computer Science and Engineering, PDA College of Engineering, Kalaburagi, India

***Abstract*—The Internet of things (IoT) is the next wave of ubiquitous computing. IoT is the network of physical devices, vehicles, home appliances and other items embedded with electronics, software, sensors, actuators, and network connectivity which enables these objects to connect and exchange data. The objective of the research behind this paper is to establish a state of the art in the development of IoT protocols in Application layer, Transport layer, Internet layer and Physical/Link layer. In specific, here we evaluate the IoT Application layer protocols CoAP(RESTFUL), MQTT, AMQT, XMPP with respect to the type of architecture and security support in those protocols. The focus was made on Constrained Application Protocol (CoAP)and corresponding security protocol DTLS. Gaps in the security of CoAP protocols are identified and presented.**

***Index Terms* -ubiquitous computing , Internet of Things (IoT), IoT Protocols, CoAP, MQTT, AMQT, XMPP, DTLS, RESTFUL. Ubiquitous computing**

I. INTRODUCTION

The growing evolution of information and communication technology (ICT) systems is moving beyond the big desktop computers and tends to increasingly smaller and more powerful devices providing enhanced computing capabilities and multiple heterogeneous wireless communications interfaces. These devices, such as personal digital assistants (PDAs) and smartphones, enable a new class of advanced services characterised by being available anywhere, at any time and for anyone.

internet of things (IoT) is the network of physical devices, vehicles, buildings and other items embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data. In 2013 the Global Standards Initiative on Internet of Things (IoT-GSI) defined the IoT as "the infrastructure of the information society"[1]. The IoT allows objects to be sensed and controlled remotely across existing network infrastructure[2], creating opportunities for more direct integration of the physical world into computer-based systems, and resulting in improved efficiency, accuracy and economic benefit[3] ; when IoT is augmented with sensors and actuators, the technology becomes an instance of the more general class of cyber-physical systems, which also encompasses technologies such as smart grids, smart homes, intelligent transportation and smart cities[4-9]. Each thing is uniquely identifiable through its embedded computing system but is able to interoperate within the existing Internet infrastructure. Experts estimate that the IoT will consist of almost 50 billion objects by 2020 [10].

The Internet of Things (IoT) has undergone rapid transformation since the term was first coined in 1999 by Kevin Ashton. Since the variety - and the number - of devices connected to the Internet has increased exponentially in recent years, IoT has become a mainstream technology with a significant potential for advancing the lifestyle of modern societies. Typically, IoT is expected to offer advanced connectivity of devices, systems, and services that goes beyond machine-to-machine (M2M) communications and covers a variety of protocols, domains, and applications [11]. The interconnection of these embedded devices (including smart objects), is expected to usher in automation in nearly all fields, while also enabling advanced applications like a grid, and expanding to the areas such as smart cities[12-15].

"Things," in the IoT sense, can refer to a wide variety of devices such as heart monitoring implants, biochip transponders on farm animals, electric clams in coastal waters, automobiles with built-in sensors, DNA analysis devices for environmental/food/pathogen monitoring or field operation devices that assist firefighters in search and rescue operations [16][17]. Legal scholars suggest to look at "Things" as an "inextricable mixture of hardware, software, data and service"[18]. These devices collect useful data with the help of various existing technologies and then autonomously flow the data between other devices [19]. Current market examples include smart thermostat systems and washer/dryers that use Wi-Fi for remote monitoring [20].

The aim of this article is to make a general survey of the state of the art in the development of IoT protocols in Application layer, Transport layer, Internet layer and Physical/Link layer as in figure 1. In specific, here we evaluate the IoT Application layer protocols CoAP, MQTT, AMQT, XMPP with respect to the type of architecture and security support in those protocols. The focus was made on Constrained Application Protocol (CoAP) and corresponding security protocol DTLS. Gaps in the security of CoAP protocols are identified and presented.

Layer	Protocols
Application Layer	CoAP, MQTT, XMPP, AMQP, RESTFUL, Websockets
Transport Layer	UDP, DTLS
Internet Layer	RPL, 6LoWPAN
Physical/Link Layer	IEEE 802.15 Series, IEEE 802.11 Series

Fig.1: IoT Protocols

II. LITERATURE REVIEW

Internet of Things (IoT) is emerging technology. Show in previous section inside of IoT describe as protocols. By studying paper regarding IoT and IoT protocol related IETF standards

paper show application layer protocols focus basically on message exchange between applications and the internet [21]. Most of paper summarizes some the most important standard that provide different stander organizer. It also provides a discussion of different IoT challenges including mobility, scalability. In other survey paper show different layer like transport layer used or provide security in application layer protocols. Internet layer protocols like RPL (Routing for low power and lossy network) and 6LoWPAN (IPv6 over Low Personal Area Network). 6LoWPAN used in application layer as providing IP address to devices for communication. Physical layer protocols like IEEE 802.11 series, IEEE 802.15 series, zigbee and Adriano. Those physical layer protocols used at application layer to manage sensor and actuators. Application layer work with other layer like transport layer, Internet layer and physical layer. In this paper our aim to provide comprehensive survey to describe all main six application layer protocols and also provide newly arising standards protocols and their architecture.

III. APPLICATION LAYER PROTOCOLS: REVIEW

This section reviews standards and protocols for message passing in IoT application layer proposed by different standardization. All-most web-based application and IoT application are IP based and they use TCP and UDP for transport. However, there are several message distribution functions that are common among many IoT applications; it is desirable that these functions be implemented in an interoperable standard way by different applications. Those protocols are:

A. *MQTT*

MQTT (Message Queue Telemetry Transport) was develop by or introduce by IBM in 1999 and standardized by OASIS in 2013 to target come up with lightweight M2M communication [22]. It is publish/subscribe protocol architecture similar to client/server protocol show in figure below. The importance of MQTT protocol is due to its simplicity and the no need of high CPU and memory usage (reason is the lightweight protocol) [23]. MQTT supports a wide range of different devices and mobile platforms. At transport layer TLS/SSL security provide to MQTT.

B. *AMQP*

The Advanced Message Queuing Protocol (AMQP) is a protocol that across from the financial industry. Security is managing with the use of the TLS/SSL protocols. It run over TCP. AMQP protocol follow publish/subscribe communication protocol for messaging. AMQP is same like MQTT but the advantage of AMQP is, it stores data and then forwards it, and this feature is used at the time of network disruptions which ensures reliability. As shown in figure below a broker divides into two-part exchange and queue. Exchange responsibility to receive publishers' messages and distribute to queue. Queues is based on pre-define roles and condition and it's basically send message to subscribers who subscribe those data.

C. *XMPP*

Extensible Messaging and Presence Protocol (XMPP) is a messaging protocol that was designed originally for chatting and message exchange applications. It was standardized by IETF more than a decade ago. In all application layer protocols only XMPP protocol support publish/subscribe and request/response model and it depend on application developers to develop application which model they use [24]. It does not provide any quality of service guarantees and, hence, is not practical for M2M communications. XMPP is rarely used in IoT but has gained some interest for enhancing its architecture in order to support IoT applications.

D. *RESTFUL SERVICES*

Representational State Transfer (RESTFUL Services) is an architectural style for networked hypermedia applications that gives web administrations which permit correspondence and information trade between various gadgets utilizing HTTP in IoT condition [25]. REST utilizes the HTTP strategies GET, POST, PUT, and DELETE to give an asset arranged informing framework where all activities can be performed essentially by utilizing the synchronous request/response HTTP commands.

RESTful services use the secure and reliable HTTP which is the proven worldwide Internet language. It can make use of TLS/SSL for security.

E. *CoAP*

CoAP (constrained application protocol) is used for low power and low memory embedded devices where it can be used for communication instead of HTTP. Currently there is HTTP protocol available with request/response paradigm but HTTP has many features and more footprint [25]. HTTP runs over TCP where TCP will need more resources due to three-way handshake and many more complex mechanisms. Now for low power embedded devices, there is no need of this heavy protocols and we can optimize it to run over TCP.

As CoAP is a Restful web transfer protocol for use with constrained networks. CoAP uses client/server model of approach same as HTTP. It is designed for constrained

IV. SECURITY IN COAP

CoAP is now becoming the standard protocol for IoT applications. Security is important to protect the communication between devices. In the following part, a security protocol DTLS is introduced. Also, one of CoAP application, Smart Homes, is described in this section.

There are three main elements when considering security, namely integrity, authentication and confidentiality. DTLS can achieve all of them [26]. DTLS solves two problems: reordering and packet lost. It adds three implements: 1 packet retransmission. 2 assigning sequence number within the handshake. 3 replay detection.

Unlike network layer security protocols, DTLS in application layer as in figure 2 protects end-to-end communication. No end-to-end communication protection will make it easy for attacker to access to all text data that passes through a compromised node. DTLS also avoids cryptographic overhead problems that occur in lower layer security protocols.

Application (CoAP, XML)
Security (DTLS)
Transport (UDP)

Network (IPv6)

Figure 2: DTLS in protocol stack

V. CHALLENGES

A. SEQURITY

Sensors will sense the data and send it to network so confidentiality of information is very important where we can use some standard encryption/decryption to encrypt the data and send over network and other device can decrypt it. That's why application layer security.

B. RELIABILITY

The main challenge in IoT is reliability. When one IoT node send data to more than one server, if one of the server will crash or goes down then it is very hard to get original file. If file will be deleted at server side it cannot be reconstructed so, data will be lost.

C. LOW POWER

The one of the main challenge for IoT is low power of devices as embedded devices used in IoTs are deployed at many places and that has limited power capacity in this case it's very important to save power whenever its possible [27]. So there is need of mechanism where we can power off the devices when there is no need of power and can power up again whenever needed.

D. NETWORK CAPABILITY

The challenge regarding network capability is there are many sensors and devices connected with network and the data from sensor device will be sent through wired or wireless interface. The transmission system or network should be able to collect all the data from sensors and make sure that no data loss occur due to network congestion.

VI. CONCLUSION

The Internet of things (IoT) is the next wave of ubiquitous computing. Current work concentrate on IoT application layer protocol with special focus on CoAP application layer protocol. Having light weight and consume low energy, CoAP is used on many applications of IoT. To secure data transferred, CoAP used DTLS protocol named as Datagram Transport Layer Security protocol as the security agent. Gaps in the security of CoAP protocols are identified and presented. Further we focus on specific implementations of security in application layer protocols, their limitations and proposal with new security solutions to address them.

REFERENCES

[1]. "Internet of Things Global Standards Initiative". ITU. Retrieved 26 June 2015.
[2]. "Internet of Things Global Standards Initiative". ITU. Retrieved 1 June 2016.
[3].https://hbr.org/resources/pdfs/comm/verizon/18980_HBR_Verizon_IoT_Nov_14.pdf
[4]. http://www.internet-of-things research.eu/pdf/Converging_Technologies_for_Smart_Environments_and_Integrated_Ecosystems_IERC_Book_Open_Access_2013.pdf
[5].http://www.cisco.com/web/solutions/trends/iot/introduction_to_IoT_november.pdf
[6].http://cordis.europa.eu/fp7/ict/enet/documents/publications/iot-between-the-internet-revolution.pdf
[7].http://www.vs.inf.ethz.ch/publ/papers/Internet-of-things.pdf
[8].http://www.cognizant.com/InsightsWhitepapers/Reaping-the-Benefits-of-the-Internet-of-Things.pdf
[9]."The Supply Chain: Changing at the Speed of Technology". Retrieved18 September 2015.
[10]. Dave Evans (April 2011). "The Internet of Things: How the Next Evolution of the Internet Is Changing Everything" (PDF). Cisco. Retrieved 15 February 2016.
[11]. Wood, Alex. "The internet of things is revolutionizing our lives, but standards are a must". theguardian.com. The Guardian. Retrieved 31 March 2015.
[12]. J. Höller, V. Tsiatsis, C. Mulligan, S. Karnouskos, S. Avesand, D. Boyle: From Machine-to-Machine to the Internet of Things: Introduction to a New Age of Intelligence. Elsevier, 2014,ISBN 978-0-12-407684-6.
[13]. O. Monnier: A smarter grid with the Internet of Things. Texas Instruments, 2013.
[14].https://www.itu.int/dms_pub/itu-t/oth/0b/15/T0B150000153301PDFE.pdf
[15]. "IEEE Xplore Full-Text PDF:". Retrieved 26 June 2015.
[16]. "Molluscan eye". Retrieved 26 June 2015.
[17]. Erlich, Yan iv (2015). "A vision for ubiquitous sequencing". Genome Research 25(10): 1411–1416. doi:10.1101/gr.191692.115. ISSN 1088-9051.
[18]. I. Wigmore: "Internet of Things (IoT)". TechTarget, June 2014.
[19]. Noto La Diega, Guido and Walden, Ian, contracting for the 'Internet of Things': Looking into the Nest (February 1, 2016). Queen Mary School of Law Legal Studies Research Paper No. 219/2016. Available at SSRN:http://ssrn.com/abstract=2725913
[20]. Hendricks, Drew. "The Trouble with the Internet of Things". London Datastore. Greater London Authority. Retrieved 10 August 2015.
[21]. Jayavardhana Gubbi et al. "Internet of Things (IoT): A vision, architectural elements, and future directions". In: Future Generation Computer Systems 29.7 (2013), pp. 1645–1660. ISSN: 0167-739X. DOI: http://dx.doi.org/10.1016/j.future.2013.01.010. URL: http://www.sciencedirect.com/science/article/pii/S0167739X13000241
[22]. Xi Chen. "Constrained Application Protocol for Internet ofThings".URL: https://www.cse.wustl.edu/~jain/cse57414/ftp/coap/.
[23]. Sangyoon Oh, Jai-Hoon Kim, and Geoffrey Fox. "Real-time Performance Analysis for Publish/Subscribe Systems". In: Future Gener. Comput. Syst.26.3 (Mar. 2010), pp. 318–323 ISSN: 0167-739X. DOI: 10.1016/j.future.2009.09.001. URL: http://dx.doi.org/10.1016/j.future.2009.09.001
[24]. Stan Schneider.Understanding the Protocols Behind TheInternetOfThings.URL: http://electronicdesign.com/iot/understandingprotocols-behind-internet-things
[25]. IoT Messaging Protocols. 31 march 2015.URL: https://iotprotocols.wordpress.com/.
[26]. [Kothmayr12] A DTLS Based End-To-End Security Architecture for the Internet of Things with Two-way Authentication Thomas Kothmayr, Corinna Schimitt, Wen Hu, Michael Bruning. 2012 http://kothmayr.net/wp-content/papercite-data/pdf/kothmayr2012dtls.pdf

[27]. Xi Chen. “Constrained Application Protocol for Internet ofThings”.URL:https://www.cse.wustl.edu/~jain/cse57414/ftp/coap/.