RESEARCHERID
THOMSON REUTERS

[COTII- 2018]

ISSN 2348 – 8034
Impact Factor- 5.070

GLOBAL JOURNAL OF ENGINEERING SCIENCE AND RESEARCHES

IMPROVING MESSAGE SECURITY OVER IOT USING COAP

Prateek Singhal, Puneet Sharma, Vineet Singh & Sheenu Rizvi
Department of Computer Science and Engineering,
Amity University, Uttar Pradesh, India

ABSTRACT

Internet of things and universal computing requires an everyday object to be IP addressable and internet accessible which are most recent trends. The opportunities to connect the world we should manage and visualize the thing that helps to increase rapidly and to make known physical world. A promising technology revolution is made by IoT (Internet of Things) which provide the infinite benefits to groove the innovation and knowledge which is associated by visualizing the things of physical world. IoT is an interconnection of physical devices, actuators, sensors and embedded electronics from one to another (M2M) communication over an internet that enables to collect or gather the information or exchange data. In IoT the main important is security which helps to secure the information while exchanging or also known as web of things (WoT). Moreover, to perform routing in 6LoWPAN network, RPL is used that is destination-oriented DAG (DODAG) between the different IPv6 nodes. We can also interface the CoAP and 6LoWPAN through RPL using UDP protocol for various constrained nodes in Contiki OS. There are the various protocols which help to prevent the attack while data exchanging over an internet. In this paper we focus on the proposed project are CoAP (Constraint application protocol) that falls under a software component at application layer. The DTLS security is provided by the CoAP protocol and also gives the unicast messages because DTLS not support multicast. The proposed solution to make a multicast message is distributing session key using key distribution center. This is used to encrypt or decrypt the multicast message then design and improve the cryptography algorithm. We have implemented this proposed work on the Contiki OS with the framework using Cooja Simulator.

Keywords: *IoT; CoAP; DTLS; Security; Cooja simulator*

I. INTRODUCTION

In every communication the main problem is faced is Security. Many different types of attacks such as application layer attack, data notification, man-in-middle, IP spoofing, eavesdropping, password based and sniffer attack to make a interruption in the communication between the various devices (M2M). There are many range of IoT based devices such as microchip, power administration gadget, semiconductor advancement and sensors with a proper framework that can communicate (M2M) devices. The IPv6 availability and low power gadgets are contained by IoT.

Application layer protocols included by the IoT protocol stack (XMPP, CoAP, AMQP, MQTT), transport layer include (DTLS, UDP), Internet layer include (6LoWPAN, RPL) and last but not least Network layer include (IEEE 802.11 and IEEE 802.15 series) [1]. The application layer that inclined toward the web-based protocol using CoAP and its security DTLS. To monitor the various applications such as home management, parking sensors and health-care we use a CoAP protocol because it usage multicast systems.

Table. 1. Stack protocol in IoT [1]

Layers	Protocols
Application layer	CoAP, Websocket, XMPP, RESTFUL, AMQP, MQTT
Transport layer	UDP, DTLS

Internet layer	RPL, 6LoWPAN
Link layer	IEEE 802.11 and IEEE 802.15 series

The inter connection of physical devices, sensors, actuators, embedded devices and network connectivity which permit to gather data or exchange data over internet known as IoT (Internet of Things) [3]. The communication can be done between M2M with help of IoT at anywhere anytime.

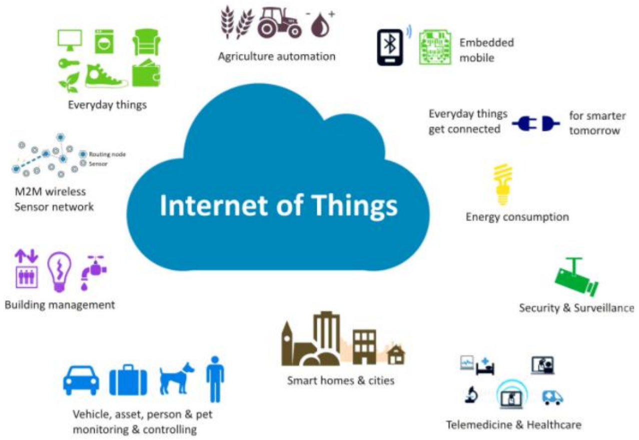

Fig.1. Internet of Things

In a precise the IoT means the interconnection of devices to a physical to virtual world with help of objects or data exchanging or things as a smart call of IoT. Security is the main feature or need while communicating thus we have encrypt or decrypt the message through cryptography algorithm. IoT needs the low complexity, power and constraints algorithm.

II. RELATED WORK

Now days the emerging technology is IoT and in this paper there are regarding about IoT protocols and IoT that most probably focusses on the message exchanging or sharing between the application devices via internet. The main focus on the CoAP protocol in the application layer while transferring the data or sending messages and for the CoAP security we have uses DTLS which is in transport layer [2] [5].

The CoAP is defined as a RESTFUL (Representational State Transfer) in a web exchange pact for use with compiled system. As the HTTP approach is there same as the CoAP approach utilizes the request/respond model for communicating. HTTP is improved by the convention of CoAP and CoAP runs on the UDP because before transmission it avoids having a costly TCP handshake between them. The RESTFUL protocol is very efficient, asynchronous transaction model, URL support, easy to proxy to/from HTTP, security binding to DTLS, the minimal header format of CoAP to saves the energy consumption in the IoT systems or devices comparing to the running HTTP constraints nodes or devices. CoAP used DTLS security with PSK and support reliability and multicast [4].

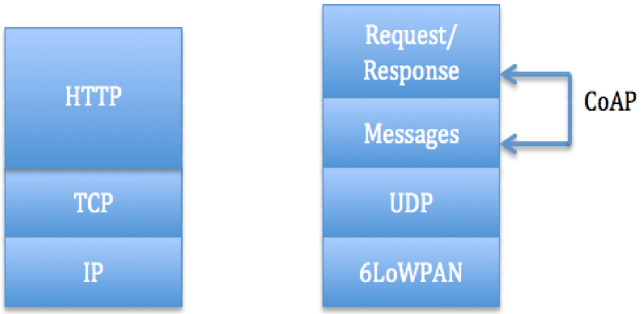

Fig.2. HTTP and CoAP protocol Stack

To solve the problem of monitoring health care, ECG, level of glucose or oxygen, heart rate application through web-based we can resolve it by the CoAP protocol. The communication between sensors and server having many problems in the applications to over come these problem by the help of CoAP [11] [12] because it can communicate with remotely through wireless on web. Communication between the server is being done over a 6LoWAPN network due to data protection. Secure end-to-end communication, hardware and may other devices. The DTLS security only provide the unicast protection to the message while communicating from one to another. The DTLS cryptography algorithm. The message incoming or outing are protected or secured by the DTLS security in the CoAP protocol [10]. Cryptography algorithm is non-blocking algorithm which exist in the unicast message security scenario for end-to-end communication.

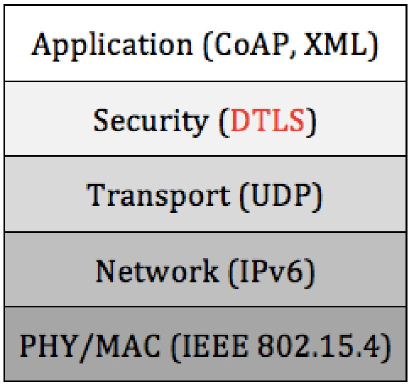

Fig.3. DTLS protocol Stack

III. PROPOSED WORK

The multimedia is the best example of multicast communication [8] [9]. The HTTP model where the CoAP is bit similar to it for the multicast communication between the devices (M2M). CoAP is request/response model where the client sends the multiple request to server node and server responses to client. For the protection of the message we have use the DTLS security in CoAP and have a DTLS handshake [10].

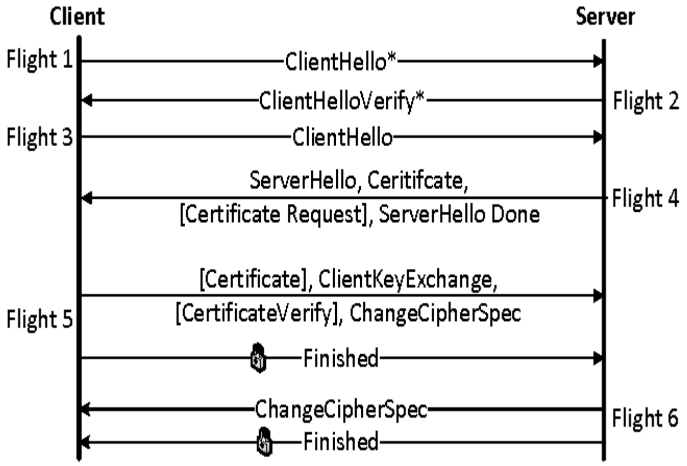
Client
Server
Flight 1
ClientHello*
ClientHelloVerify*
Flight 2
Flight 3
ClientHello
ServerHello, Ceritifcate,
[Certificate Request], ServerHello Done
Flight 4
[Certificate], ClientKeyExchange,
[CertificateVerify], ChangeCipherSpec
Flight 5
Finished
ChangeCipherSpec
Finished
Flight 6

Fig.4. DTLS handshake

The generation of key session is used to protect or secure the message communication in multicast. We have to make KDC (Key Distribution Center) from here the session is generated for the key to every node. This is done due to for encryption the message and same for the session key for decryption the message when we are communicating it. The low complexity, standardization and network capability is needed in the IoT based implementation for algorithm or equipment. The CoAP provide the multicast communication but he DTLS support the unicast communication, so here we use TLS/SSL protocol-based security for the multicast securing communication using cryptography algorithm.

IV. IMPLEMENTATION

Implementing the secure unicast message communication, we have used the Contiki OS with Cooja simulator as an implementation tool. In the Contiki OS the COOJA simulator runs and it is a cross level simulator which provides simulation on network level that can be small or large, OS level and machine code level. In this tool it is purposely used because it is developed or created for low power devise in the constraints environment [6].

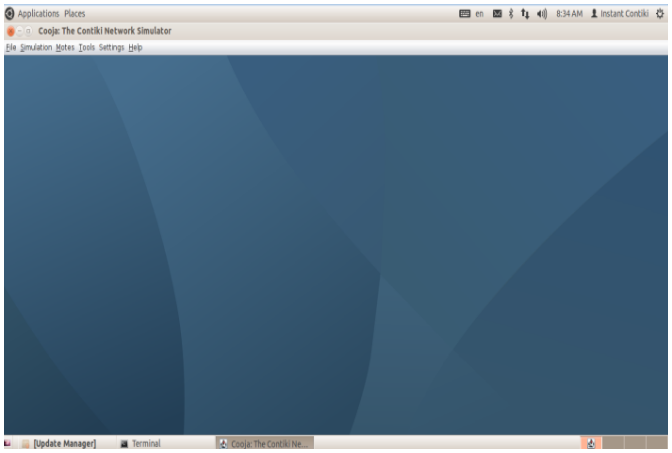
Applications Places
en 8:34 AM Instant Contiki
Cooja: The Contiki Network Simulator
File Simulation Motes Tools Settings Help
[Update Manager]
Terminal
Cooja: The Contiki Ne...

Fig.5. Startup window of Cooja

Now, we create a unicast communication in the simulator with function and front-end interface combination of java codes and C language [7].

ISSN 2348 – 8034
Impact Factor- 5.070

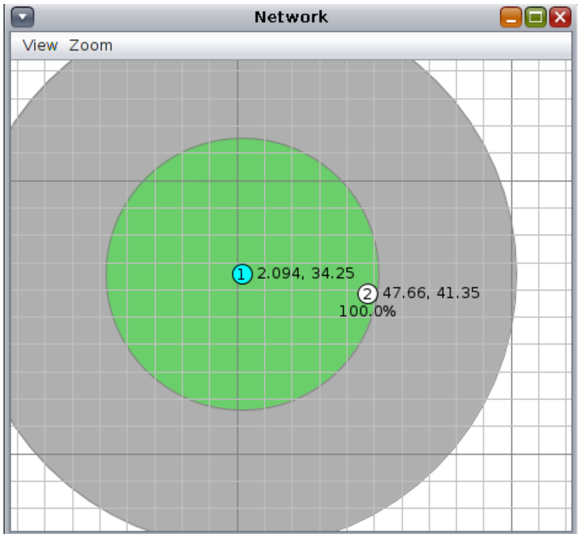

Fig.6. Unicast communication

he cryptography algorithm is applied to the client and server both side for generation of session key that used for encryption and decryption of the message while communication between the devices over internet. It supports the IPv6 and IPv4 standards along with 6LoWPAN, CoAP and RPL.

V. CONCLUSION & FUTURE WORK

The major components for the IoT application are Trust, Security and Privacy. Now days the emerging technology is IoT, but the main focus is on the sending or receiving the message in a secure communication. The main concentration in this paper on CoAP protocol lie in a application layer. It is the lightweight and low energy consumption in the IoT devices. The data should be transferred in a secure manner we use a CoAP with the DTLS security lie under a transport layer. To protect the communication between the object and IoT devices we use heavy weight DTLS security agent. The Random session key is generated for the encryption and same for the decryption the message while communicating. To implementing the various CoAP protocol on the IoT devices lead to the secure message communication. In the future the crypto algorithm can be improve and implement the multicast secure communication between the devices and analysis it.

REFERENCES

1. Makkad Asim "A Survey on Application Layer Protocols for Internet of Things (IoT)" in International Journal of Advance Research in Computer Science. March- April 2017 Volume 8. No.3ISSN No. 0976-5697.
2. S. Kraijak and P. Tuwanut. "A survey on IoT architectures, protocols, applications, security, privacy, real-world implementation and future trends". In: 11th International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM 2015). Sept. 2015, pp. 1–6. DOI: 10.1049/cp.2015.0714.
3. Administration. Internet of Things. 2016 (accessed November 3, 2016). The web link for the topic is URL: https://en.wikipedia.org/wiki/Internetofthings
4. Xi Chen. "Constrained Application Protocol for Internet of Things". The web link for this topic is: https://www.cse.wustl.edu/~jain/cse574-4/ftp/coap/
5. Stan Schneider. Understanding the Protocols Behind the Internet of Things. The web link URL: http://electronicdesign.com/iot/understandingprotocols-behind-internet-things
6. Contiki tutorial – Contiki, 4 November 2014.
7. A. Sehgal, Using the Contiki Cooja simulator, 29 October 2013
8. D. M. Mani, "Secure multicasting for wireless sensor networks, "International Journal of Computer Science and Network Security (IJCSNS), vol. 14, no. 11, p. 70,2014.

9. M. I. D. P. Ishaq I, Hoebeke J, "Experimental evaluation of unicast and multicast CoAP group communication, "Sensors (Basel, Switzerland), 16.7 (2016).

10. R. A. Rahman and B. Shah, "Security analysis of iot protocols: A focus in coap,"in2016 3rd MEC International Conference on Big Data and Smart City (ICBDSC), pp. 1–7, IEEE, 2016.

11. A. Khattak, M. Ruta, E. D. Sciascio, and D. Sciascio, "CoAP-based healthcare sensor networks: A survey," in Proceedings of 2014 11th International Bhurban Conference on Applied Sciences Technology (IBCAST) Islamabad, Pakistan, 14th - 18thJanuary, 2014, pp. 499–503, Jan 2014.

12. D. Ugrenovic and G. Gardasevic, "CoAP protocol for web-based monitoring in iot healthcare applications," in2015 23rd Telecommunications Forum Telfor(TELFOR), pp. 79–82, Nov 2015.