International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 07 | July 2019 www.irjet.net p-ISSN: 2395-0072

Security Analysis and Improvements to IoT Communication Protocols - CoAP

Vinod Kumar Singh[1], Hari Om Sharan[2]

[1]Research Scholar - CSE, Rama University, Mandhana, Kanpur, UP, India
[2]Assistant Professor and Head of Department – CSE, Rama University, Mandhana, Kanpur, UP, India

---

Abstract - *IOT security is the key aspects in the modern days of smart devices and its data communication. Day by day, Data is being crucial to make secure from the unintended threats. IOT devices must be secure enough to protect data from such threats. In this reference, communication security is the first point to consider. In the IOT communication – CoAP protocol is provided with DTLS security is considered enough in most of the scenario. However, it's still not enough to protect your data with volume. So other aspects of CoAP protocol security analysis and proposed solution are discussed and defined in this paper.*

Internet of Things (IoT) is the interconnection of physical entities to be combined with embedded devices like sensors, actuators connected to the Internet which can be used to communicate from human to things for the betterment of the life. Information exchanged among the entities or objects, intruders can attack and change the sensitive data. The authentication is the essential requirement for security giving them access to the system or the devices in IoT for the transmission of the messages. IoT security can be achieved by giving access to authorized and blocking the unauthorized people from the internet. When using traditional methods, it is not guaranteed to say the interaction is secure while communicating. Digital certificates are used for the identification and integrity of devices. Public key infrastructure uses certificates for making the communication between the IoT devices to secure the data. Though there are mechanisms for the authentication of the devices or the humans, it is more reliable by making the authentication mechanism from X.509 digital certificates that have a significant impact on IoT security. The digital certificates have the ability to perform hashing, encryption and then signed digital certificate can be obtained that assures the security of the IoT devices. When IoT devices are integrated with X.509 authentication mechanism, intruders or attackers will not be able to access the system, that ensures the security of the devices.

***Key Words*: IOT Security, IoT, Privacy, Internet of Things, CoAP, MQTT, DTLS, Denial of Service.**

1. INTRODUCTION

As per Wiki definition - The Internet of Things (IoT) is the inter-networking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, smart grids, and other items embedded with sensors, electronics, actuators, software, and network connectivity which enable these smart devices/objects to collect and exchange data [1].

The Internet of Things, abbreviated as IoT, refers to the connection of smart and/or small devices (other than typical fare such as computers and smartphones) to the Internet. Cars, kitchen appliances, home appliances, traffic systems and even heart monitors can all be connected through the Internet of Things. This list of devices is growing rapidly and estimated to grow millions of devices in the next few years [2].

- Client/external communications - Web/Portal, Dashboard, APIs
- Event processing and analytics (including data storage)
- Aggregation/bus layer – ESB and message broker
- Relevant transports – MQTT / HTTP / XMPP / CoAP / AMQP, etc.
- Devices

The cross-cutting layers are

- Device manager
- Identity and access management

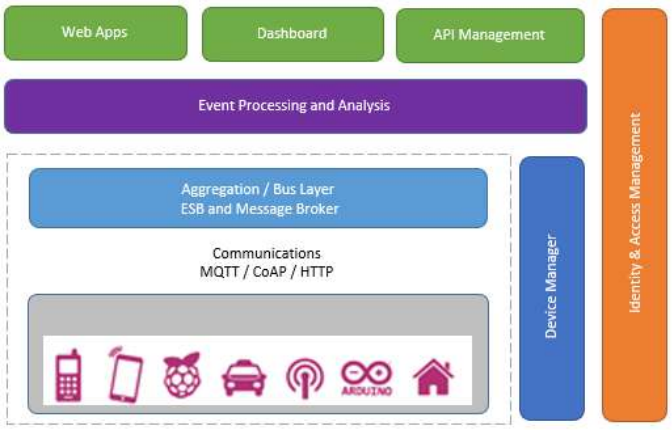

Fig -1: IOT Layers

Rather than trying to fit all of the IoT Protocols on top of existing architecture models like OSI Model, these are categorized into the following layers to provide some level of organization [3]:

- Infrastructure (ex - 6LowPAN, IPv4/IPv6, RPL)
- Identification (ex - EPC, uCode, IPv6, URIs)
- Discovery (ex - Physical Web, mDNS, DNS-SD)
- Transport (ex - Wifi, Bluetooth, LPWAN)
- Data Protocols (ex - CoAP, MQTT, AMQP, Websocket, Node)
- Semantic (ex - JSON-LD, Web Thing Model)
- Device Management (ex - TR-069, OMA-DM)
- Multi-layer Protocol Frameworks (ex - Alljoyn, IoTivity, Weave, Homekit)

1.1 CoAP Protocol

CoAP stands for Constrained Application Protocol. It is specified in RFC 7252[4]. It is open IETF standard very efficient RESTful protocol. It is easy to proxy to/from HTTP and Embedded web transfer protocol (coap://). It uses asynchronous transaction model. UDP is binding with reliability and multicast support. GET, POST, PUT and DELETE http methods are used to construct this protocol. It is URI is supported and having small header as just of 4 bytes. It supports binding to UDP, SMS and TCP. For security, it uses DTLS based PSK, RPK and certificate security. It has in-build discovery mechanism and uses subset of MIME types and HTTP response codes.

1.2 CoAP Architecture

CoAP is a document transfer protocol like to HTTP. Unlike HTTP, it is designed for the needs of constrained devices.

CoAP packets are much smaller respective to HTTP TCP flows. Bitfields and string mappings to integers are extensively used to save space. Data packets are simple to generate and can be parsed in-place without consuming extra RAM in constrained devices.

CoAP runs over UDP, not TCP. That means clients and servers communicate through connectionless datagrams. Retries and reordering of data packets are implemented in the application stack. Removing the need for TCP may allow full IP networking in small microcontrollers and its supported devices. CoAP allows UDP multicast and broadcast to be used for addressing.

CoAP follows similar to client/server model. Clients make requests to servers; servers send back responses and acknowledgements. Clients may use GET, PUT, POST and DELETE resources.

CoAP is designed to interoperate with HTTP and the RESTful web services at large through simple proxies.

CoAP is datagram or UDP based, it may be used on top of SMS and other packet-based communications protocols [5].

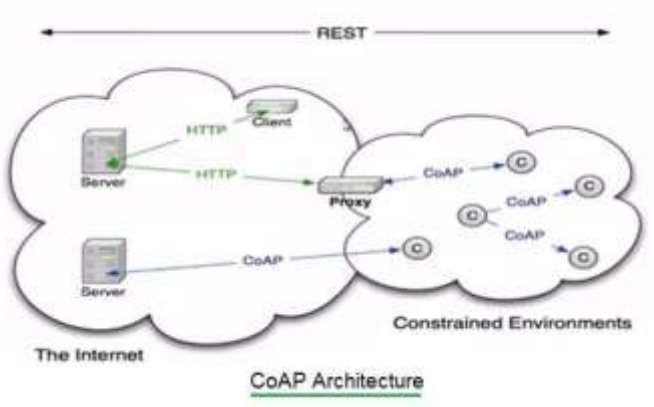

Fig -2: CoAP Architecture

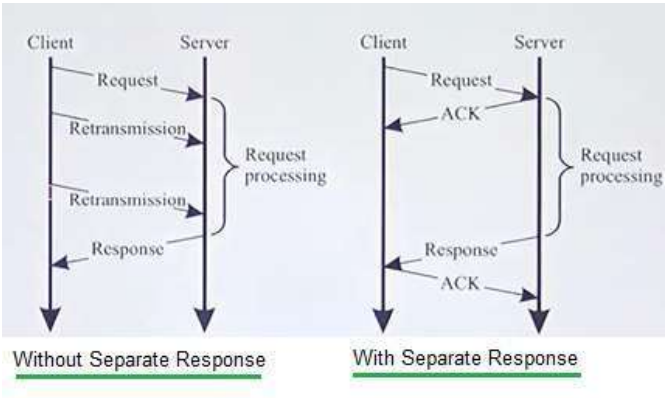

Fig -3: CoAP Message Exchange

1.3 Security

CoAP is built on top of UDP not TCP, so SSL/TLS are not available to provide security. DTLS (Datagram Transport Layer Security) [6] provides the same assurances or security as TLS but for transfers of data over UDP. Most commonly, DTLS capable CoAP devices are able to support RSA and AES or ECC and AES.

1.4 Security Protocol & Application for CoAP

CoAP is most common and now becoming the standard protocol for IoT applications. Security is an important aspect to protect the communication between IoT end-node devices. In the following part, a security protocol DTLS is introduced to secure the CoAP and other UDP based protocol. Also, one of CoAP application, Smart Homes, describes to the case study.

2. LITERATURE REVIEW

2.1 Security issues in perception layer

It is a lowest level of IoT construction. Perception layer is the base source of access to information throughout the IoT. IoT cannot provide itself a security protection system and it is vulnerable to the attack due to diversity, energy limited,

simple and weak protective capability of sensing node which affects the security of Wireless Sensor Network (WSN), Radio-frequency Identification (RFID) and Machine to Machine (M2M) terminals. The security issues in Perception layer include the physical security of sensing devices and security of information collection. The RFID includes security problems such as information leakage, information tracking, replay attacks, tampering, cloning attacks and man-in-the-middle attacks. The security problems faced in perception layer includes capture gateway node, unfair attacks, physical capture, congestion attack, DoS attacks, node replication attack and forward attack.

2.2 Security issues in physical layer

The physical layer performs different functionalities such as selection and generation of carrier frequency, modulation and demodulation, encryption and decryption, digitization, transmission and reception of data. This layer is attacked mainly through:

Jamming: This DoS (Denial of Service) [7] attack occupies the communication channel between the nodes and prevents them from communicating with each other. It exploits the transmission of radio signal to interfere with radio frequencies that used by sensor network. It can be performed either in continuous way or in an isolated way. In both the cases network will suffer from damage and communicate breakout.

Node tampering: Extracting sensitive information from the end device is known as node tampering.

2.3 Security issues in network layer

Internet of things faces some risks in the network like illegal access, virus attack, confidentiality, data eavesdropping, integrity, DoS attacks, destruction, man-in-the-middle attack and so on. IoT sensing into a large number of devices means to a variety of formats of the data collected, and the data information has a massive, multi-source and heterogeneous characteristics. It will also cause network security issues like data transfer needs of large number of nodes leading to network congestion, resulting in DoS attacks. The function of the network layer is data routing to the intended recipients. The DoS attacks always take place in the network layer:

- ***Message Flooding Attack:*** It causes high traffic in channels by congesting the channel with a high number of useless messages unusually. Message is replayed by the attacker to create a high traffic by sending useless message to a node.

- ***Homing:*** In Homing attack, a search is made in the traffic for cluster heads and key managers which having the capability to shut down the entire network.

- ***Selective forwarding:*** In selective forwarding, a compromised node sends false data to few selective nodes instead of all the nodes. The selection of the node is based on the requirement of the attacker to achieve his malicious objective and thus such node does not forward packets of data.

- ***Sybil:*** In this attack, the attacker replicates a single node and then presents it with multiple identities to the other nodes to pretend to be part of devices.

- ***Wormhole:*** Wormhole attack causes relocation of bits of data from its original position to other position. While passing bits of data over a low latency link, the relocation of data packet is carried out to node to node.

- ***Acknowledgement flooding:*** When routing algorithms are used, the acknowledgements are required at times in sensor networks. In Acknowledgements flooding attack, a malicious node spoofs the false acknowledgements to the destined neighbouring nodes.

2.4 Security issues in application layer

The security issues in application layer include eavesdropping and tampering of the data in communication. This layer carries out the responsibility of data-traffic management. It also provides software for different application domains which carries out the translation of data into a comprehensible form or helps in collection of information by sending request/queries. A DoS attack is initiated in application layer by stimulating the sensor nodes to create a huge traffic in the route towards the base station.

There are three main elements when considering security, named as integrity, authentication and confidentiality. DTLS can achieve all of them. IETF modifies TLS to develop another security protocol DTLS [6]. DTLS employ on TCP/UDP, which is too complex. DTLS solves two problems: reordering and packet lost. It adds three implementations: 1 packet retransmission. 2 assigning sequence number within the handshake. 3 replay detection.

DTLS stays in application layer (Fig. 4) and protect end-to-end communication just like network layer security protocols. It's not easy for attackers to access any data from end-to-end communication where data passes through a compromised node. DTLS also avoids cryptographic overhead problems with some exception that usually occurs in lower layer security protocols.

There are two layers in DTLS. The bottom one contains Record protocol. The upper one includes three protocols which are Alert, Handshake and application data, in some condition Change Cipher Spec protocol may replace one of them. The Change Cipher Spec message is used to notify

Record protocol to protect subsequent records with just-negotiate cipher suite and keys.

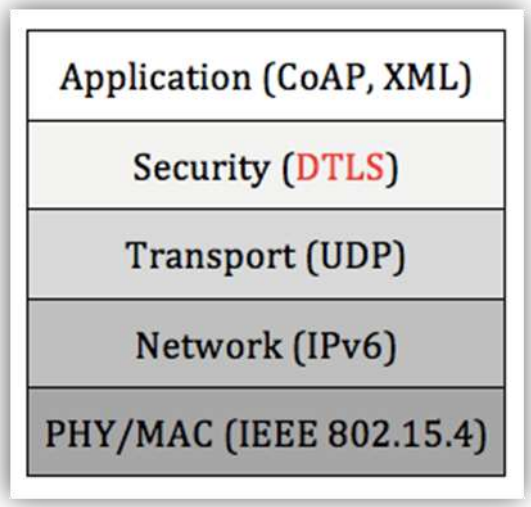

Fig 4: DTLS in protocol stack

Record protocol protects application data by using keys generated during Handshake. For outgoing messages, protocol divides, compress, encrypt and apply Message Authentication Code (MAC) to the messages. For incoming message, protocol reassemble, decompress, decrypt and verify them based on various algorithm used on source and destination. Record header is made of two parts, one is content type and another is fragment field. Content type decides what data or content is going to be contained in fragment field. It could be a handshake protocol, alert protocol or an application data. In the Comparison with DTLS Record, Handshake protocol is rather a complex one which involves a lot of exchange steps. Individual messages are grouped into message flights. Fig -5 shows the process of Handshake [8].

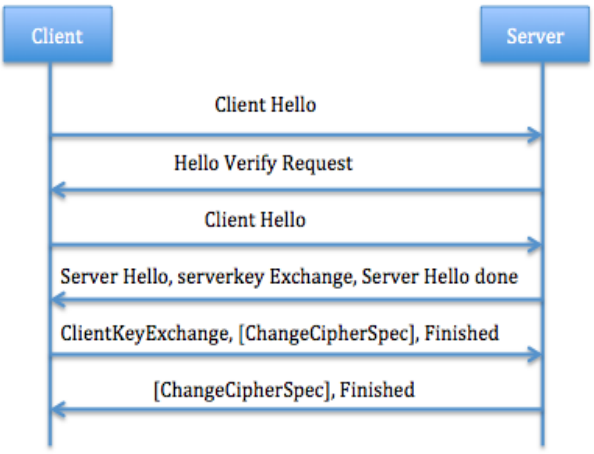

Fig -5: Process of Handshake

3. OBJECTIVE

DTLS is available make security of it, but with increase of payloads and encryption tools, it becomes heavier for CoAP protocol. This always leaves the scope for improvements for security architecture of CoAP. This research will be to analyze the deficiencies of available CoAP security mechanisms and design a solid approach that will be able to make CoAP protocol faster, reliable and secure in constrained environments.

I. Security design and structure analysis of network, transport and application layers.
II. Encryption mechanism at application and network layers.
III. Cryptographic Algorithms evaluation and appropriate selection.
IV. Key-cert security process analysis.
V. Analyze a security and interoperability level which can provide a measurement to security level.
VI. Analysis of various layers of communication in the respect to security.
VII. Communication security.
VIII. Evaluation of existing and new implementation.

4. METHODOLOGY

The proposed study is about to analysis the existing security methods for COAP IOT protocol. For meaningful analysis and for making valid recommendations, study should be based on the findings of the comparative data and analysis. This study will consist about security techniques and mechanism of CoAP protocol and do the evaluation based on data throughput, memory usage, performance, communication consistency etc. These techniques will be achieved through setup of some IOT devices using CoAP protocol specifications and implementations [9], its execution and results comparison.

Analytical Research Methodology will be used to analyze the existing research methods, develop the new formulae with adjusting the memory, data size, throughput, etc.

Authentication and Authorization techniques [10] will also be used on Application layer security analysis.

Various Performance Evaluation techniques [11][12] will be used to compare the existing and new data stats.

5. OUTCOME

The objective of this research is to provide an approach to defend our IOT data in connection establishment, data transfer, and device management using most common IOT communication protocol – CoAP. It will provide all the communication aspects between IOT devices includes the security, privacy, performance, comparative study of existing mechanism and evolved the working and the technical

specifications. The main focus of this research will be on to find the most accurate and appropriate security system on application and transport layer for most used IOT protocol CoAP.

6. CONCLUSION

CoAP protocol security is currently based on DTLS security that is based on TLS security for HTTP. DTLS security becomes bulky and CPU intensive in bigger data payloads and frequent data acquisitions. This is all going to be analyzed and propose a better solution to handle security for CoAP protocol in terms of Point to Point or End to End.

REFERENCES

[1] Angelo Capossele, Chiara Petrioli, Gianluca De Cicco and Valerio Cervo, "Security as a CoAP resource: An optimized DTLS implementation for the IoT", https://ieeexplore.ieee.org/document/7248379

[2] Paul Fremantle, "A reference architecture for the internet of things", https://wso2.com/whitepapers/a-reference-architecture-for-the-internet-of-things

[3] Simon Ford, "IoT Standards and Protocols", https://www.postscapes.com/internet-of-things-protocols

[4] Z. Shelby, K. Hartke, C. Bormann, "The Constrained Application Protocol (CoAP)", https://tools.ietf.org/html/rfc7252, P.10.

[5] Xi Chen, Prof. Raj Jain, "Constrained Application Protocol for Internet of Things", https://www.cse.wustl.edu/~jain/cse574-14/ftp/coap/index.html, P.8-12.

[6] E. Rescorla - RTFM, Inc., N. Modadugu - Google, Inc., "Datagram Transport Layer Security Version 1.2", https://tools.ietf.org/html/rfc6347

[7] Int. J. Ad Hoc and Ubiquitous Computing, Vol. x, No. x, xxxx, "Jamming and Anti-jamming Techniques in Wireless Networks: A Survey", https://www.cs.montana.edu/yang/paper/jamming.pdf

[8] "What is CoAP IoT protocol | CoAP Architecture, message header", https://www.rfwireless-world.com/IoT/CoAP-protocol.html

[9] Carsten Bormann, "CoAP Specification and Implementation", http://coap.technology/

[10] Pablo P Pereira, Jens Eliasson, Jerker Delsing, Dept. of Computer science, Electrical and Space Engineering, Lulea University of Technology, Lulea, Sweden, "An Authentication and Access Control Framework for CoAP-based Internet of Things", https://www.researchgate.net/publication/278847085_An_Authentication_and_Access_Control_Framework_for_CoAP-based_Internet_of_Things

[11] Mariusz Slabicki, Krzysztof Grochla, "Performance Evaluation of CoAP, SNMP and NETCONF Protocols in Fog Computing Architecture", https://www.researchgate.net/publication/301694346_Performance_evaluation_of_CoAP_SNMP_and_NETCONF_protocols_in_fog_computing_architecture

[12] Waqas Rahman, Young-Seok Choi, Kwangsue Chung, "Performance Evaluation of Video Streaming Application Over CoAP in IoT", https://www.researchgate.net/publication/332220067_Performance_Evaluation_of_Video_Streaming_Application_Over_CoAP_in_IoT

BIOGRAPHIES

Vinod Kumar Singh, Research scholar, Rama University, Mandhana, Kanpur, Uttar Pradesh, India