ISSN No:-2456-2165

Advance Approach for DTLS using Authentication Technique with COAP based on Internet of Things in Smart Grid Application

[1]Vinitha .V
Department of Master of Computer Application
AMC Engineering College Bangalore
University VTU

[2]Velantina .V
Department of Computer Science Engineering (M.Tech)
C.B.I.T Kolar
University VTU

Abstract:- The IOT is an emerging trend that evolves to make a thing's information safely and securely available on a global scale, when the information is needed by an aggregation points. A smart grid component consists of control of production, electronic power conditioning and distribution of electricity. This smart grid is an electrical grid which as varieties of operations consists of smart meter. As the power system is evolved vastly into a smarter and most flexible state. We selected Constrained Application Protocol (CoAP) with DTLS Protocol enhanced which is based on Restful environment as the M2M protocol. As in traditional grid system is growing that the electricity demand keeps on increasing, the departments have decided to focus on smart grid to implement this technology.

Keywords:- *Internet of Things, Smart Grid, Security.*

I. INTRODUCTION

Smart grid (SG) acts as bidirectional communication network which tries to balance the amount of electricity generation and utilization. SG uses network which uses Internet of Things (Iot) application which is used for Information and Communication Technology framework to automate the existing traditional electricity network. The basic scenario is to switch the smart grid that allows the power generated from different distributed sources. That consist of traditional power plants, renewable solar and wind as well as plug-in electric vehicles and energy storage.

II. EXISTING SYSTEM

The existing system was a power grid system that was operated manually by people leading to various issues and problems. Hence there was a need in automation of the power grid by using the emerging technologies like IOT automation, where the operations and process can be operated and managed automatically and remotely. An interconnection of various elements in the grid was built with synchronous machines, power transformers, and transmission lines that are located far from the power consumption area and the power was transmitted through long transmission channels called lines. This power distribution process through transmission lines was a one way communication and lead to several problems, hence the system was automated with smart technologies.

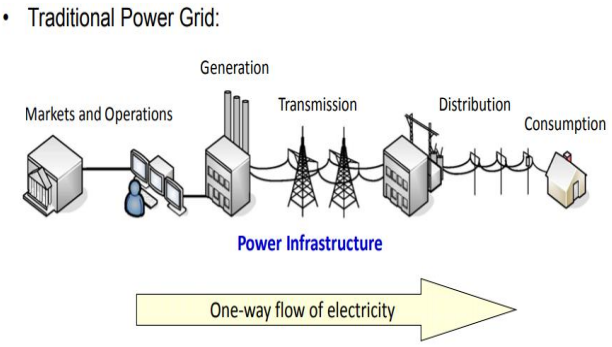

Fig 1:- Traditional Power Grid

➢ *Some of the Disadvantage Is:*
- Privacy Problems
- Volatility of the grid

III. PROPOSED SYSTEM

The modernization of grid and digitalization in the process is called as smart grid. The grid is smarter because of the technologies used like sensing devices, embedded processing and digital communication. The smart grid has the property of self-healing, interactive, optimized, secure, predictable and distributive nature.

The conventional grid had electromechanical arrangements which were highly inefficient and there was false tripping and power failures frequently. The smart grid can do automatic fault restoration by using sensors in transformers and transmission lines. The two ways communication process takes place in smart grid with sensors throughout, self healing and self monitoring.

➢ *Components of smart grid*

- **Sensing and measurement:-** How much electricity we are using and how much it is costing us in rupee per hour should be analyzed, So this can be can done using Smart meter. The automated meter infrastructure performs the following functions:

- **Smart meter: -** It satisfies the two way by smart connect/disconnect operations and the power flow is monitored, the energy that is consumed is also been determined and a awareness message/alert of energy consumption is sent to the user. The smart relays the

information to central monitoring stations, the traditional meters are replaced.

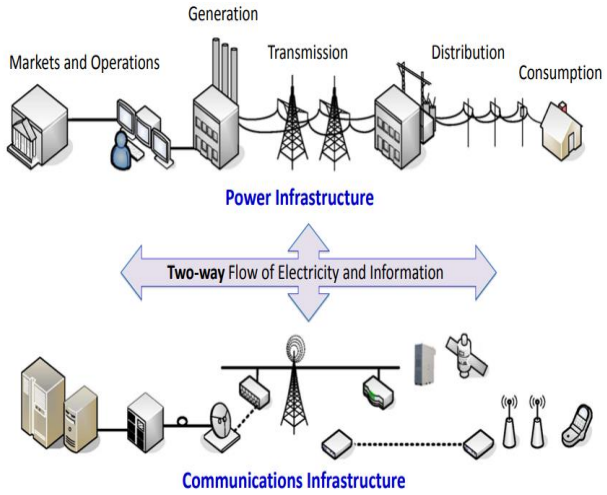

Fig 2:- Future Smart Grid

❖ *Advantages*

- Managing the energy in better way.
- Reduce carbon emissions.

The smart grid has environment impact by reducing the green house gases and millions of devices that are evolving could be deployed in various platforms in the future.

The Constrained application protocol is an IoT protocol. CoAP is defined in RFC7252.The main features of CoAP protocols are:

- Asynchronous message exchange between the nodes.
- It has a property to perform parsing.

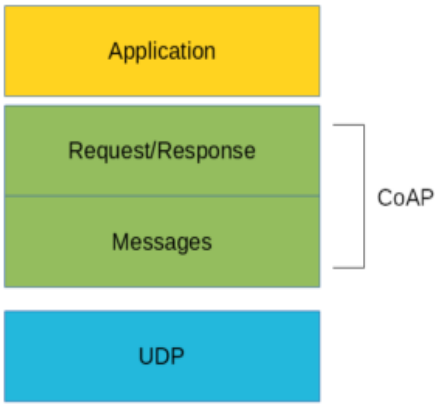

Fig 3:- Constrained application protocol layers

This protocol is very similar to HTTP and it is much optimized in performing the tasks. The layers are Messages and Request/Response layer. The CoAP defines an end point that is an entity that participates in the protocol with a host. Client is an entity that sends request and where in the server that receives a request from the client and sends back a response to the client.

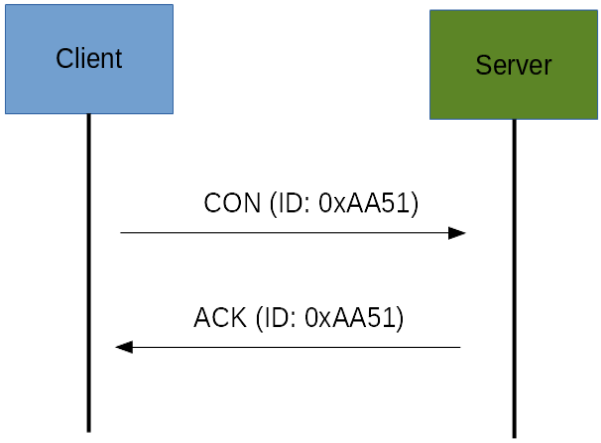

Fig 4

➢ *Constrained application protocol message model*

In this model there is an exchange of UDP messages between the end points. As we know the messages are of four types, as shown in Fig 4, the messages are reliable at two end points. The Client is very sure that the message will arrive at the server as it provides the guarantee. The Acknowledgement message contains the same message ID for the confirmable message. The server can send back a Rest message (RST) instead of Acknowledgement while managing the requests as shown in Fig 5.

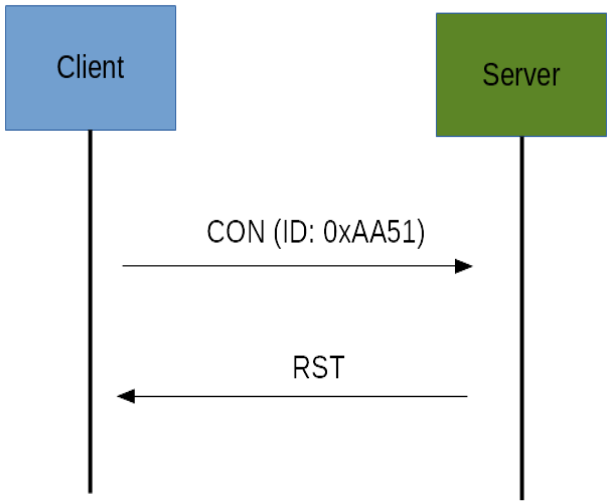

Fig 5

➢ *Request and Response model of Constrained application Protocol*

The second layer in CoAP is the abstraction layer that performs operation using confirmable and Non-Confirmable message. The confirmable message is used in order to respond immediately to the request by the server, if any error occurs it is indicated by the error code messages, by sending these messages to the client as an acknowledgement, the server will initiate the client.

ISSN No:-2456-2165

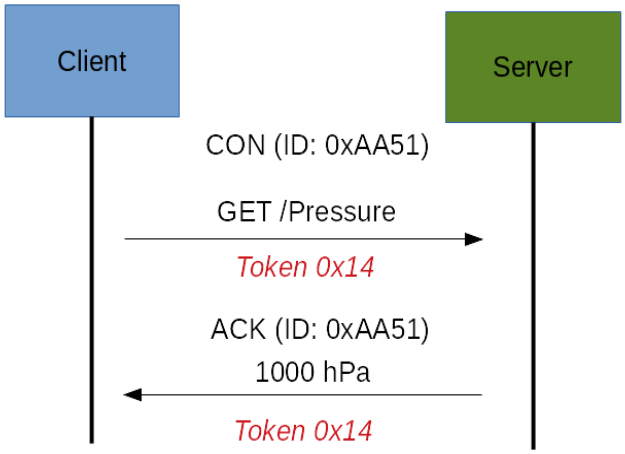

Fig 6

As shown in Fig 7, when the response is available then the server sends a new confirmable message to the client. If the request is coming from client carrying a non-confirmable message, the client sends back an acknowledge message.

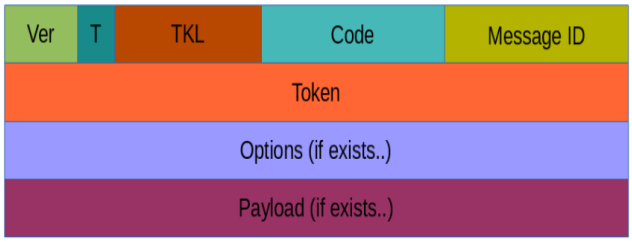

Fig 7:- Constrained application protocol message format

The Constrained application protocol message format consists of several fields like Version, TKL, Code, Message ID etc.

The version field consists of a 2-bit unsigned integer. The type field specifies type of messages as indicated - type:0 confirmable,1 non-confirmable. Token length is the token with 4 bit long. The code response field is of 8 bit in size, the message ID is expressed with 16 bit. The Cipher suites are used to manage the security communication between the devices. Reordering and packet lost problems are handled by the DTLS protocol. The three of its implementations they are:

- Retransmission of packets when there is a loss of packet or failure on communication during transmission.
- During the handshake process the sequence number is assigned to each of the transmissions to uniquely identify and identify the operation.
- The Replay detection is also managed during the transmission process.

Datagram transport layer security in application layer is used to protect end-to-end reliable communication. If there is no end-to-end communication then it is easy for attacker to access all the text data that passes through a compromised node. If we use DTLS protocol the cryptographic overhead problems that occur in lower layer of the security can be managed and avoided. Datagram transport layer protocol combination with constrained application protocol forms a higher level security. The Security consists of three main elements like security, integrity, authentication and confidentiality. These features of enhanced datagram transport layer security protocol made the smart grid system highly secure.

IV. CONCLUSION

As the technologies are evolving with latest trends in today's global environment, the automation in smart grid provides an easy integration and reliable service to the consumers. The grid system is a network based on digital automation technology for monitoring all the operations automatically and remotely within the supply chain. This system can find the solution to the problems very fast and work force is reduced .The sustainable, reliable, safety and quality goals are achieved due to automation in the grid system. In this paper we are describing the wireless protocols like constrained application protocol and datagram transport layer security protocol features and operations, and how the datagram transport layer security protocol plays a vital role in managing the security and privacy of the grid system.

REFERENCES

[1]. Enhanced DTLS with CoAP-based authentication scheme for the internet of things in healthcare application Priyan Malarvizhi Kumar , Usha Devi Gandhi , DOI 10.1007/s11227-017-2169
[2]. Fan Z, Kulkarni P, Gormus S, et al. Smart grid communications: overview of research challenges, solutions, and standardization activities. IEEE Commun Surv Tutor. 2013;15(1):21-38.
[3]. Khurana H, Hadley M, Lu N, Frincke DA. Smart-grid security issues. IEEE Security and Privacy. 2010;8(1):81-85.
[4]. Ericsson GN. Cyber security and power system communication 2014: essential parts of a smart grid infrastructure. IEEE Trans Power Deliv. 2010;25(3):1501-1507.
[5]. Chen PY, Cheng SM, Chen KC. Smart attacks in smart grid communication networks. IEEE Commun Mag. 2012;50(8):24-29.
[6]. Fouda MM, Fadlullah ZM, Kato N, Lu R, Shen X. Towards a light-weight message authentication mechanism tailored for Smart Grid communications. Computer Communications Workshops (INFOCOM WKSHPS). New York: IEEE; 2011:1018-1023.

[7]. Wu D, Zhou C. Fault-tolerant and scalable key management for smart grid. IEEE Trans Smart Grid. 2011;2(2):375-381.
[8]. Xia J, Wang Y. Secure key distribution for the smart grid. IEEE Trans Smart Grid. 2012;3(3):1437-1443.
[9]. Yan Y, Qian Y, Sharif H. A secure data aggregation and dispatch scheme for home area networks in smart grid. Global Telecommunications Conference (GLOBECOM 2011). New York: IEEE; 2011:1-6.
[10]. Lu R, Liang X, Li X, Lin X, Shen X. EPPA: an efficient and privacy-preserving aggregation scheme for secure smart grid communications. IEEE Trans Parallel Distrib Syst. 2012;23(9):1621-1631.
[11]. Wong K-S, Kim MH. Preserving differential privacy for similarity measurement in smart environments. Sci World J. 2014;2014:1-9.
[12]. Hur JB, Koo DY, Shin YJ. Privacy-preserving smart metering with authentication in a smart grid. Appl Sci. 2015;5(4):1503-15