Secure and Efficient CoAP Based Authentication and Access Control for Internet of Things (IoT)

Mohsin B Tamboli, Dayanand DAmbawade

Abstract—**Internet of Things (IoT) is growing as an attractive system paradigm. There is a lot of hype around the internet of things (IoT) and it continues to evolve as we move beyond humans talking to machines. IoT has interconnections through the physical, cyber and social spaces. Things used in IoT are sensors and actuators, mechanical devices and network- ing includes gateways, wireless infrastructure. Most of devices among them are resource constrained. During the interaction betweendevices,IoTgetssufferedfromseveresecuritychallenges. Complicated network produces potential vulnerabilities referred to heterogeneous devices, sensors and backend systems. So to realize the dream of internet of things secured device to device communication is expected. Security of resource constrained networks becomes prime important. Many existing mechanisms gives security and protection to networks and systems but they are unable to give fine grain access control. In this work, we focused on CoAP based framework to give service level access control on resource constrained devices. It gives fine grain access control on a per service basis. ECDSA is used to improve privacy of the system. Performance of CoAP based framework is compared and analyzed with existing security solutions. Test results are presented which shows that communication overhead and authentication delay are less than the existing system. Hence security performance of system gets improved. The goal is to present comprehensive security framework for low power networks consist of resource constrained devices.**

Keywords—CoAP, Internet of Things, Ticket, Security.

I. INTRODUCTION

The Internet of Things (IoT) is the next paradigm shift, where devices are connected via internet, which gather and share data directly with each other, collect and analyze that data to make our planet intelligent, interconnected and more instrumented [3]. Many areas are going toimplementIoTinfrastructure in order to collect and access information in a real time. Areas include home automation, healthcare,environ- mental monitoring, structural monitoring, industrialmonitoring etc[2].

Internet of Things systems consists of miniature wireless devices which act as sensors or actuators forming wireless sensor networks. Varieties of objects are involved inIoT such as sensors, RFID devices, mobiles, short range wireless connectivity etc. Low power short rangewirelesstechnologyfor these devices is the key part of IoT architecture [8]. Due to weaker characteristics of wireless sensors as resource constrained devices, security of network becomes more Sensitive[2].IoT involves communication system where data serversconnected to physical world through ubiquitous wirelessresource con-strained devices. These devices comes Sensor networks. Generally sensing devices and embedded computingdevices deployed within IoT are expected to be with common featuresof limited processing capability, constrained energy resources,real time nature of applications, limited memory, vulnerableradio conditions and no direct human interaction. So such re-source constrained device may violets the security of network.It becomes necessary to take action to make network secure.

As IoT is a complex environment, there are some legislations related to data privacy. Reliance on connected devices in business context brings a lot of risk, especially with large amount of personal data and proprietary information that is being collected. IoT is still an evolving technology where new standards, protocols and legislations are continuously arising. So it is important to be aware of this changing landscape and identify and manage these security risks efficiently in order to thrive in a big connected network in future.

Services provided by networks are distributed in nature and depends on communication channel. So they are inherently vulnerable to security threats. They can be protected using communication protocols along with strong encryption schemes such as IPSec, DTLS. Regarding security,useofIPSec was increased during last years. But IPSecneedsashared password to encrypt and decrypt messages. If these passwords are static could be compromised after some thou- sand number of messages [5]. IPSec requires comparatively large processing power which causes higher processor loads. There is possibility that vulnerabilities in IP layer in remote network could be passed to corporate network through IP tunnel. So IPSec becomes less efficient in case of resource constraineddevices.

Datagram Transport Layer Security (DTLS) used toprotect UDP packets which add an extra layer of protection. DTLS increases packet size. It is fully integrated in CoAP protocol. Use of it could achieve a per service access control, but this would require a large number of different key pairs. So management and administration of such large number of keys would be difficult task [5]. Application layer usually employs HTTP to provide web services but HTTP has high computation complexity, comparatively low data rate and high energy consumption. Therefore IETF has developed several lightweight protocols. Out of them constrained application protocol (CoAP) is best approach. This paper proposes a framework based on CoAP which provide fine grain access control. Resource constrained de- vices are key components of network for internet of things. This framework focused on low overhead on these devices. The proposed solution uses another authentication and access control system like Kerberos along with the CoAP protocol. Optimized version of ECDSA is implemented within smartthings which provides efficient privacy.This paper structured as follows: Section II presents re

Mohsin B. Tamboli Dept. of Electronics and Telecommunication, Sardar Patel Institute of Technology Andheri(W), Mumbai, India. (mohsintamboli95@gmail.com)

Dayanand D. Ambawade, Dept. of Electronics and Sardar Telecommunication Patel Institute of Technology Andheri(W), Mumbai, India. (dd_ambawade@spit.ac.in)

978-1-5090-0774-5/16/$31.00 © 2016 IEEE

lated work, section III gives brief information about proposed framework, next section IV gives security analysis, section V gives results from our experiments. Finally in section VI we end with some conclusions.

II. RELATEDWORK

In this section, goal behind this work has been described. Description of CoAP protocol along with some other protocols is given used in proposed framework.

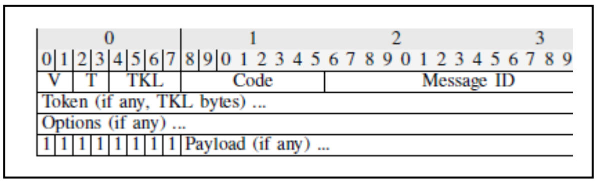
A. *Industrial Networking andsecurity*

Industrial control includes monitoring and controllingman- ufacturing and other operations. Networking becomes domi- nant part for automation throughout all the industrial control. IoT itself is a large network. According to experts, 20.8 billions devices will gets connected under IoT by 2020 [12]. Networking growing rapidly with connected devices.Withthisincrement, connected device might be vulnerable to internet and security threats. Many efforts have been done to prevent the network fromattacks.

In case of networks consist of resource constrained devices some specific protocols becoming more useful. Some of the most efficient ones from the security point of view are de- scribed below.

B. *CoAP (Constrained ApplicationProtocol)*

CoAP is one of the latest application layer protocol de- veloped by IETF for smart devices to connect to Internet. As many devices and networks exist with constrained resources, it leads a lot of variation in power computing, communication bandwidth etc. Thus lightweight protocol CoAP is intended to be used. CoAP is a specialized web transfer protocol designed to provide web services to constrained nodes [9]. It is used for low power networking. Protocol supports a request/response interaction that utilizes both synchronous and asynchronous responses and satisfying REST protocol to sup- port URI (Uniform Resource Identifier).CoAPeasilyinterfaceswith HTTP and uses the HTTP commands GET, POST, PUT, and DELETES to provide resource-oriented interactions in client-server architecture [10]. CoAP support multicast com- munication, runs over the UDP, very low overhead. It has two types of messages: Confirmable message (CON) - A request message that requires an acknowledgement (ACK). The response can be sent either synchronously (within the ACK) or if it needs more computational time, it can be sent asynchronously with a separate message. The other typeisNonConfirmable Message (NON) - A message that does not need to be acknowledged. CoAP also support blockwisetransfer of big messages in which it splits messages and send them with reference order. For that it uses stop and wait mechanism [5].



<table>
<tr><td colspan="8">0</td><td colspan="8">1</td><td colspan="8">2</td><td colspan="6">3</td></tr>
<tr><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td><td>0</td><td>1</td><td>2</td><td>3</td><td>4</td><td>5</td><td>6</td><td>7</td><td>8</td><td>9</td></tr>
<tr><td colspan="2">V</td><td colspan="2">T</td><td colspan="4">TKL</td><td colspan="8">Code</td><td colspan="14">Message ID</td></tr>
<tr><td colspan="30">Token (if any, TKL bytes) ...</td></tr>
<tr><td colspan="30">Options (if any) ...</td></tr>
<tr><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td>1</td><td colspan="22">Payload (if any) ...</td></tr>
</table>

Fig. 1: CoAP Message Format

The CoAP message format (see Figure 1) has a maximum length of 1400 bytes, but the header has a length of 32 bits (2 for the version control, 2 for message type, 4 for token length, 8 for the message code and 16 for the message ID) [5].

C. *Kerberos*

Kerberos [4] is network authentication protocol. It gener- ates a ticket by observing communication between the Au-thentication Server (AS) and the client. Ticket will be used in future for accessing different services on Service Servers (SS). It provides mutual authentication. Kerberos is able to run over UDP or TCP. Ticket generation process uses different types of encryption methods [5].

D. *ECDSA (Elliptical Curve Digital Signature Algorithm)*

ECDSA stands for Elliptical Curve Digital Signature Al- gorithm, uses elliptic curve cryptography. It is used to create a digital signature of data (a file for example) in order to allow youtoverifyitsauthenticitywithoutcompromisingitssecurity. Size of key used in ECDSA is only160 bit which is very small as compared to normal DSA. This reduces the communication overhead and improves the privacy of communication.

Currentlyusedprotocolsandsystemsarenotmuchefficientt o provide security. Protocols like IPSec does not suit to resources constrained environment. DTLS, HTTP becomes comparatively complex. So secure and scalable framework is necessary in order to cope with the inherent security require- ment of IoTnetwork.

III. FRAMEWORK

In this section, proposed architecture is explained along with authentication and access control mechanism.

A. *Requirements*

Our objective is to improve the authentication and to get fine grain access control. Communication overhead, authenti- cation delay, computational complexity of the security system should be low to improve security performance. Ticket system is useful to distinguish authenticated user from intruder. So only valid devices should be allowed to communicate with accesscontrolservices.Inordertoenhancetheprivacyofcom- munication, advanced encryption schemes should be used. Ac- cess methods and rules could be changing with authentication policies. These can be changes according to conditions like position, sensor data, power source, time, quantity,complexity etc. The goal is to present comprehensive security framework and to give fine grain access control per services.

B. *ProposedArchitecture*

Proposed framework uses CoAP, Kerberos and ECDSA solutionstocreatelowpowersecurityplatformformainserver. Architecture is shown in Figure2.

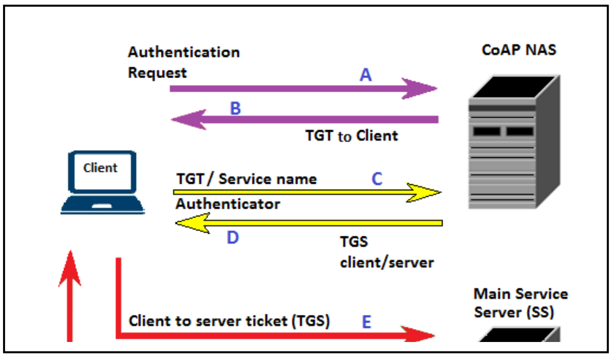


Fig. 2:Proposed Framework Architecture

In Fig. 2, the client wants to access services on Main server. So it has first undergone security check at CoAP NAS. New user has to make registration first. Existing user made login and ready to get ticket if login details matched with the stored one (A). Ticket (TGT) is send back to client (B). Now client send request to access particular services along with ticket (TGT) to CoAP NAS (C). If it has valid ticket then CoAP NAS grant the request and returns ticket (TGS) for requested service. Using TGS, client send request for service access situated on main server (E). After verifying TGS, main server gives reply to Client (F). Whole process is explained briefly in subsection C and D of section III.

RMI (Remote Method Invocation) is used here to start the services. Kerberos approach provide authentication by generating ticket for valid user. Authentication service [.well-known/auth] must exist on CoAP server [11]. CoAP server must be able to perform login and logout correctly. On successful login it should generate ticket and on logout should deleteit.

C. AuthenticationProcess

The proposed solution performs two processes, one is authentication and other is access control. Authentication is a procedure to verify that received messages come from the alleged source and have not been altered. This checks the validity of user. If new user comes then he has to first make registration on database at CoAP server. Users login name, password, shared key or other validator are stored. When user sent request for authentication, its identity will be checked against stored data. If data matched, this process will inform CoAP server about authenticity of user. So CoAPNAS generate the valid ticket (TGT) for this user with timeout as shown in Fig. 3. TGT is ticket to get ticket used for authentication. User now allowed entering the system. If above processfailsthenauthentication becomesunsuccessful.

The authentication system should allow a system adminis- trator to create user accounts, including login name, password, and appropriate roles and permissions authorizations. Server must be able to identify valid user and send that information to the CoAP NAS. In the proposed solution, public login service is created on CoAP NAS by using Kerberos.

- Ticket is unique per user and service.
- Ticket has particular timeout, after that it becomes invalid.
- Ticket length could be configurable according to the requirement.

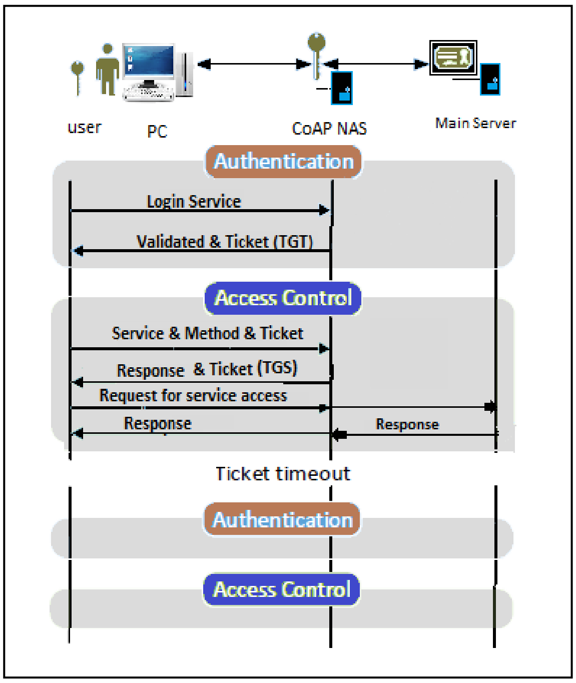


Fig. 3: Authentication Process [5]

D. Access ControlProcess

Access control is second process. When user requestfor service access, CoAP NAS checks the validity of ticket (TGT) user got during authentication along with the service name,Message ID. Server keeps the IP address and port numberof message packet. For each service access request, servermust verify ticket timeout, username, Message ID. If ticketis expired, user request will not be proceed and he will notbe allowed to access the services on main server. With allthis information server is able to verify the user and givepermission to access service. All the user data is stored ondatabase at CoAP server. On successful verification server,creates one more ticket (TGS) for requested service as shown in Fig. 3. This is ticket for granting service. This ticket hasalso timeout. By using this ticket user can access requiredservice on main server. If the ticket is wrong or there is noticket on the packet, the server must send an error message toinform the user that he has not permissions to use that service. When ticket timeout is over, ticket becomes invalid, so neither authentication nor access control is performed as shown in Fig. 3.

Generally,whenpacketssendonnetworkduetoencryption their size gets increased which increases complexity. Here

CoAP protocol provides communication with low overhead packets. In this framework ECDSA encryption scheme isused. Due to this normal size of packet does not increase too much and improves the privacy. Ticket option makes the access controlprocesssuperiorandfine.Tickethasfollowingfeatures:

- Ticket is unique per user and service.
- Ticket has particular timeout, after that it
- Ticket could be encrypted to avoid attack on it.

IV. SECURITY AND PRIVACY ANALYSIS

In this section security feature of proposed solution is shown.

1) Confidentiality: We want toachieveconfidentialityto

prohibit privacy threat and eavesdropping attacks. CoAP is efficient to provide confidentiality. Encryption method keeps the message packet secure from attackers. So information can not bedisclosedtounauthorizedparty.

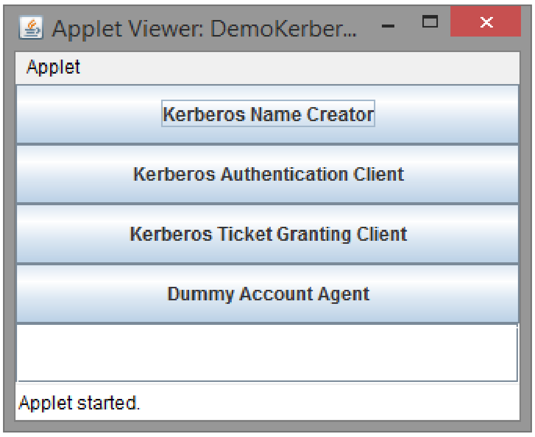
2) Data Integrity: ECDSA scheme used in proposed solution gives protection to data packet and ticket generated. So no one can alter the messageandticket.This helps to keep the integrity of communication.
3) Non-repudiation:Ticketisgeneratedforvaliduserforeach transaction. So once message sent, user cannot deny having sent a transaction.
4) Man in middle attack: Proposed system will encrypt the data and will use timeout for each ticket and connection. So it becomes difficult to identify password and to retrieve the message.
5) Replaying attack: CoAP add the header with unique value to message packet. Also ticket attached with each request is unique. So replaying of message can beavoided.

V. EXPERIMENT AND RESULT

In this experiment, client configuration involves IP address 192.168.1.1 for hostname kdc-client.foobar.com and 192.168.1.101 for corresponding hostnamekdc.foobar.com.The main configuration file is /etc/krb5.conf which mainly used by the Kerberos library to configure any kerberized client requiring access to KDC. Some packages needed to be installed in order to be compatible with server and to integrate the ticket management [11]. Eclipse Indigo tool is used to perform coding in JAVA/J2SE language. User friendly Graphical User interface is created.

GUI windows are shown below. Fig.4 shows the different steps performs in the experiment. The first button 'Kerberos Name Creator' is used to create registration of new user. When second button 'Kerberos Authentication Client' is pressed, it opens login Menu as shown in Fig. 5. Here registered user make login to system. On successful login user receives ticket (TGT)

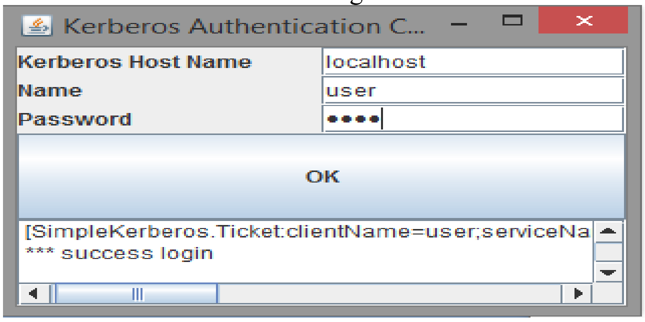
successful login user receives ticket (TGT).


Applet Viewer: DemoKerber...
Applet
Kerberos Name Creator
Kerberos Authentication Client
Kerberos Ticket Granting Client
Dummy Account Agent

Applet started.

Fig. 4: Main Window

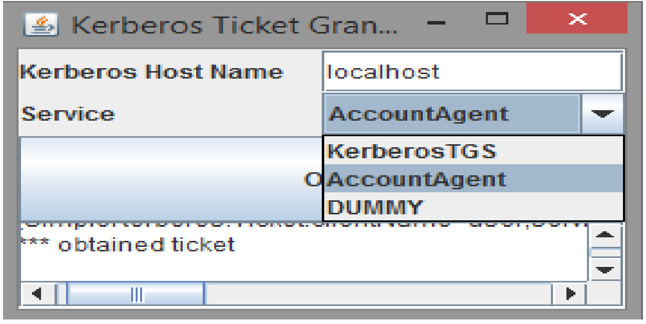
When third option 'Kerberos Ticket Granting Client' is pressed, it opens window as shown in Fig. 6. Here usermake selection of service to be accessed and send request along with TGT. On successful verification of TGT, he gets another ticket TGS. Fourth button opens the window in Fig. 7 where user can send the message to main server



Kerberos Host Name	localhost
Name	user
Password	••••

```
[SimpleKerberos.Ticket:clientName=user;serviceNa
*** success login
```

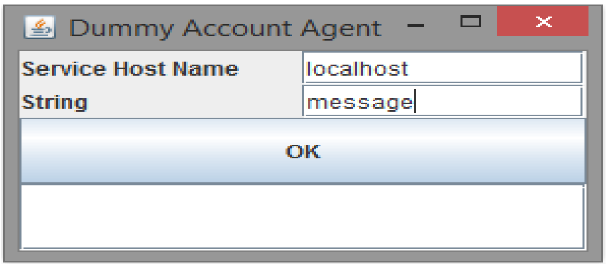
Fig. 5: Login Menu



Kerberos Host Name	localhost
Service	AccountAgent

```
*** obtained ticket
```

Fig. 6:Ticket(TGS) Generation



Service Host Name	localhost
String	message

Fig. 7: Service Access

.

In this system we have compared parameters of proposed system with existing system which uses normal encryption methods like DSA. Proposed system uses ECDSA encryption scheme along with CoAP protocol. We have calculatepropogation time and communication overhead for both the systems and compared them graphically. Table 1 shows values of authentication time, ticket granting time and communication overhead.

TABLE I. COMPARISION OF PARAMETERS

Parameter	Existing System	Proposed System
Avg. Authentication Time Computation	102 ms	49 ms
Avg. Ticket Granting Time Computation	27 ms	8 ms
Avg. Comm. Overhead	60 byte	48 byte

Graphs give the comparison of parameters for proposed and existing system.

In plot shown in Fig. 8, x axis contains number of server round trip and y axis shows authentication time in millisecond.

Plot shows that authentication time required for proposed system is less than that of existing system

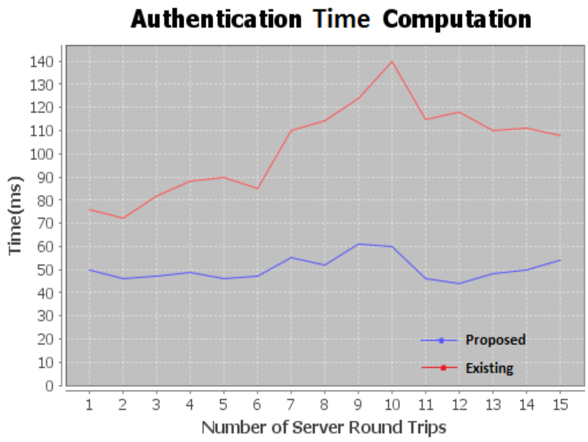


Fig. 8: Plot of Authentication Time

Plot in Fig. 9 shows Ticket granting time computation. Here x axis contains number of time request send for ticket granting to get TGS and y axis contains time in ms.This plot showsthat ticket granting time taken by proposed system is less than existing system.

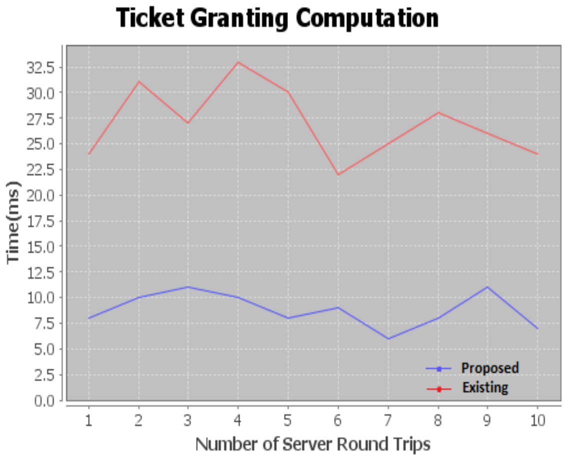


Fig.9: Plot of Ticket Granting Time

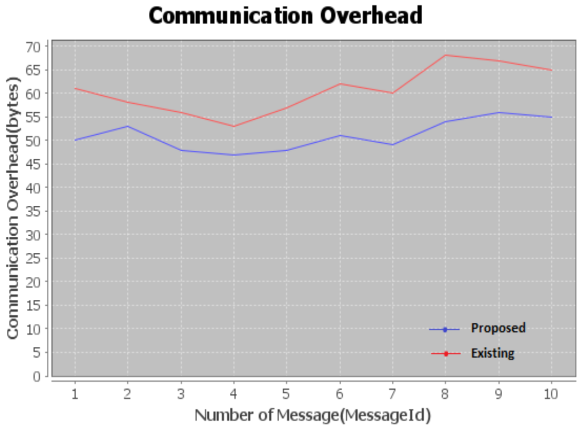


Fig. 10: Plot for Communication Overhead

Plot in Fig. 10 shows communication overhead. Here x axis contains message ID and y axis contains message packet size in bytes. message packet size reduces in proposed system which reduces communication overhead.

From the plot we can say that overall propogation time reduces in proposed method which gives fast communication. Proposed system gives low communication overhead than previous one. Proposed method increases the performance of security system and system can be made efficient for resource constrained networks.

V.CONCLUSION

In this paper we proposed a security model based on challenge-response architecture that uses lightweight protocols to mutually authenticate the CoAP client and server to setup a secure communication channel. The paper discusses the proposed authentication scheme as well as explains the contribution of CoAP and other protocols. CoAP arises as best alternative to recently used security protocols. Proposed Solution uses Kerberos protocol along with CoAP. This reduces authentication time and ticket granting time. Hence overall authentication delay reduces in proposed method. This gives quick access to system. To access different services on server, special ID called ticket is generated. This ticket is unique per service. This makes the access control fine and superior. ECDSA retains the privacy of communication and gives better security from attacker. It adds less number of bits to original message as compared to recently used encryption schemes. This reduces packet size and in turns decreases the communication overhead. These parameters show that security performance is improved. Test results and graphs support the usability and reliability of proposed solution. SoitcanbeastrongoptiontoIPSec, DTLS based security systems. Thus this framework can be a good security solution for resource constrained networks.

ACKNOWLEDGMENT

The author would like to thank Sardar Patel Institute of Technology, India for providing the necessary facilities for carrying out this work.

REFERENCES

[1] Balandina E., Balandina S., Koucheryavy Y., Mouromtsev D., "IoT Use Cases in Healthcare and Tourism," IEEE 17th Conference on Business Informatics, Year:2015

[2] A. Rghioui, A. Laarje, F. Elouaai, M. Bouhorma, "The Internet of Things for Healthcare Monitoring: Security Review and Proposed Solution," Information Science technology (CIST), 2014 IEEE 3rd International Colloquium.

[3] E. Poenaru, C. Poenaru, "A Structured Approach of the Internet-of-Things eHealthUseCases,"4thIEEEconferenceonE-HealthandBioengineering Year:2013

[4] L. Zhu, K. Jaganathan, and S. Hartman, "The Kerberos Version 5 Generic Security Service Application Program Interface (GSS-API)," Mechanism: Version 2, Network Working Group, RFC Editor, RFC 4121, July2005. [Online] Available: http://tools.ietf.org/rfc/rfc4121.txt

[5] P. P. Pereira, J. Eliasson, J. Delsing, "An Authentication and Access Control Framework for CoAP-based Internet of Things," Industrial Elec- tronics Society, IECON 2014 - 40th Annual Conference of the IEEE,Year: 2014 ,Pages: 5293 - 5299.

[6] Olivier FLAUZAC,Carlos GONZALEZ, Abdelhak HACHANI, Florent NOLOT, "SDN based architecture for IoT and improvement of the security," 29th International Conference on Advanced Information Net- working and Applications Workshops.Year:2015

[7] Antonio F. Skarmeta, Jose L. Hernandez-Ramos, M. Victoria Moreno, "Decentralized approach for Security and Privacy challenges in the Internet of Things," 2014 IEEE International Conference on World Forum on Internet of Things (WF-IoT).

[8] Adarsh Kumar, Krishna Gopal, Alok Aggarwal, "Simulation and Anal- ysis of Authentication Protocols for Mobile Internet of

Things(MIoT)," Parallel, Distributed and Grid Computing (PDGC), International Confer- enceYear:2014

[9 Xi Chen, "Constrained Application Protocol for Internet of Things,"April2014,http:/www.cse.wustl.edu/jain/cse57414/ftp/coap/index.html.

[10] Angelo P. Castellani, MattiaGheda, Nicola Bui, Michele Rossi, Michele Zorzi, "Web Services for the Internet of Things through CoAPand EXI," IEEE International Conference on Communications Workshops (ICC),5- 9 June 2011, pp. 1-6.

[11] Jean-Yves Migeon (2008, July) "The MIT Kerberos Administrators How- to Guide Protocol, Installation and Single Sign On" [Online]. Avaliable: http://www.kerberos.org/software/adminkerberos.pdf

[12] Gartner Report (2015, November) [Online].Avalaible:http://

www. gartner.com/newsroom/id/3165317. Access Date: 15 April

2016