Securing Location in Iot Enabled LTE Network Based on CoAP

Midhukrishna K
Dept of Computer science and Engineering
Thejus Engineering College

Abstract- *The authentication framework uses in LTE is an extensible authentication format. A method that in EAP uses the Authentication and Key Agreement (AKA) mechanism based on challenge-response mechanisms, EAP-AKA is used in the 3rd generation mobile networks then modified and it is inherited to 4th generation mobile networks. Evolved Packet System Authentication and Key Agreement (EPS-AKA) mechanism is using nowadays in LTE networks. But it is not suitable for IoT enabled networks. EPS-AKA vulnerabilities are disclosure of the user identity, Man in the Middle attack and Denial of Services (DoS) attacks so a robust authentication protocol and a new secure middleware is needed for proper and efficient internet access. In this project, a new authentication protocol along with a secure middle layer is introduced. The new mechanism provides security not only at one end but also at the other end also. For this, a new scheme called CoAP is developed for this purpose that gives security and better efficiency than the current ones. Nowadays location based security services are running immensely. Security is the main challenge in such services also. Hence through the project, securing location based on CoAP.*

Keywords- CoAP, EPS-AKA protocol, IoT, LTE network

I. INTRODUCTION

The Internet of Things or IoT, a network that connects remote objects (Object can be any physical devices, actuators, sensors, home appliances etc.) introduced by the concept of allowing communication and data exchange between various devices. Each thing in the network can be identified by its embedded computing system but it can operate only with an internet infrastructure. IoT devices are controlled by a remote internet infrastructure. Nowadays applications of IoT mainly include smart homes (In a smart home, for example, suppose a user into a house and his car starts a communication with garage to open the door, once the user enter into the home, the temperature inside the room and light intensity will be automatically adjusted as per some environmental conditioned.), wearables, smart grids, smart city, industrial internet, connected car, Smart retail and so many. As already mentioned, Each IoT device identified by a unique object id and communication among objects made possible only by using this id. For initiating a device to device communication or person to device communication or person to person communication, objects have the capability to transmit data and relevant information. For the next generation networks, D2D communication is an innovative feature. It operates between public networks safety and commercial networks. One example for such network is LTE. LTE stands for long term evolution which is a part of evolved packet system. Figure 1.1 shows the LTE network evolution from GSM. High data rate, high efficiency are the main requirements of an LTE network.

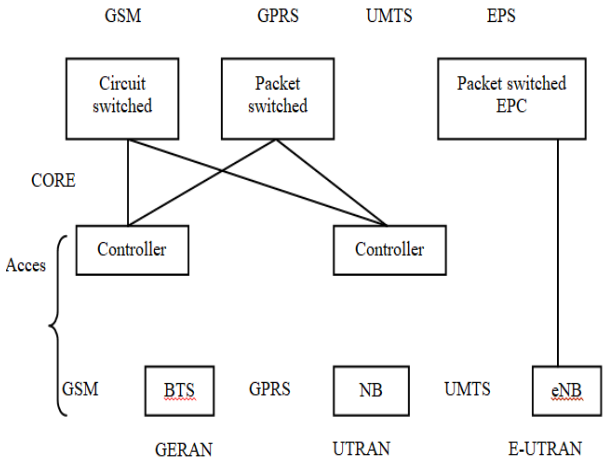

Fig 1.1 GSM to LTE

1.1 Architecture of LTE:

Fig. 1.1.1 shows a general security architecture of E-UTRAN (Evolved Universal Terrestrial Radio Access Network). It is the major portion of an LTE network and EPS-AKA is the protocol using in LTE. Architecture shows only some basic elements of the protocol. Each user in the network should create their account in a home subscriber server with their subscription. With the help of a user interface user connect with evolved node B (eNB) using his/her mobile device or any user device. eNB is the one who provide user interface. eNB is connected with MME (mobile management entity) using S1-MME interface and uses S1-U interface for connecting with serving gateway. MME is the one who authenticate the user by initiating a communication with HSS

(home subscriber server). For getting authentication information MME communicate with HSS through S6a interface. There are two sections for security among user entity among user entity and E-UTRAN. First one is AS(Access stratum). It protects radio resource control and user plane. Another layer is called a non-access stratum that enables security between UE and MME.

1.2 *Background*

LTE is one among the most popular cellular technology that evolved from 3rd generation partnership 3GPP. It provides better security when compare with GSM. Even though LTE architecture is developed from GSM, it is entirely different from GSM's procedures and services. At the various levels of LTE, some integrity protection systems has been done via set of keys.

The current protocol using for a LTE communication EPS-AKA (evolved packet system authentication and key agreement) doesn't support in IoT communications a new authentication protocol is introduced [1].

The rest of the paper lies as follows. Next section provides an overview of LTE networks and different security mechanisms exist. Section III includes the newly adopted methodology for developing this system. Finally an analysis has been generated based on some performance parameters and concluded at V.

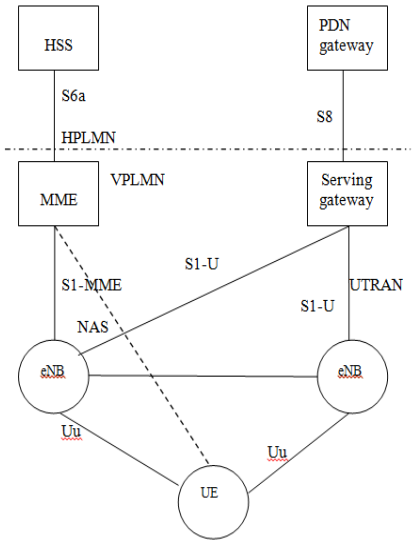

Fig 1.1.1 LTE System architecture

II. RELATED WORKS

The evolved packet system based key agreement protocol (EPS-AKA) that is using currently in LTE networks doesn't support the IoT concept due to some of its security issues. Each object or device in an IoT network is identified by its id. The main security problem or challenge arising in IoT is keeping this object identity safe. Some other problems arising in the EPS-AKS is its large overhead, limited identity privacy, synchronization. Hence a better solution adopted in "Authentication protocol for IoT enabled LTE networks" [1] which introduces a new secure and efficient AKA protocol that mainly aims in reducing synchronization problems in existing ones and makes object id safe. It uses a 4 step based authentication protocol which include protocol setup, secret creation, protocol initiation and execution. As it doesn't support sequence number, it can prevent the need for synchronization. But instead of this, this protocol uses MAC for verification purpose. A security analysis generated at the final stage which show that the protocol is secure, efficient and privacy preserved and reduces bandwidth consumption during authentication stage. Also AKA protocol maintains collision free MAC, identity privacy and theft, session unlink ability and also confidentiality. The protocol also prevents attacks such as MITM, Replay, Redirection attack etc.

A "Mutual entity authentication for LTE" [2] describes the EPS-AKA protocol using in LTE systems. It introduced a new architecture which is a 3rd generation partnership project version of 4th generation. For an online authentication protocol, An advancement to EPS-AKA protocol has been done. This paper proposes a mutual authentication between user entity and home subscriber server. As a design restriction we retain the challenge-response sequence and the AV concept, but permit ourselves to include new message elements and redefine the authentication token. One necessary change is the introduction of new subscriber module, the ESIM, which replaces the USIM.

In "A review paper on advanced network parameter in LTE 4G" [3] generates a study of different parameters that affects the performance of LTE networks By a brief explanation about QOE concepts in LTE, IMS network is introduced. It also gives an overview on an architecture called Diffserv that is used in the transport network for classification of different services like voice, FTP etc. It concludes with the explanation on the various scheduling strategies that will be used in the transport network.

"LTE authentication protocol (EPS-AKA) weaknesses solution "[4] is a modified Evolved Packet System Authentication and Key Agreement (MEPS- AKA) protocol which is mainly based on a Simple Password Exponential Key Exchange. A symmetric key cryptography method is proposed to solve these problems by performing an authentication procedure to generate dynamic keys at every instant that a user

access to the network. Also each and every message sent will be confidentially protected. A new tool Scyther tool used to verify the efficiency of the proposed protocol. Using C, EPS-AKA and MEPS- AKA are simulated. Each algorithms execution time is calculated using this. The proposed protocol is a 2 step schema. The first step is the exchange of five messages between (UE, MME), where the messages are exchanged in the first step. The second step is the exchange of two messages between (MME, HSS)

"Enhancing user identity privacy in LTE" [5] discusses how LTE architecture solves the problem of keeping object identity safe. Also it describes by which solutions the security made better. But the problem found is that the user identity vulnerability found in the existing networks also exists in the LTE networks. For solving this problem proposed system provides end to end user id privacy to LTE users. In this method, identity of the user is restricted to only UE and HE. The id is not transmitted throughout the network, hence relaxes security needs otherwise the intermediates of the network.

Enabling D2D communications over LTE-A networks suggests a method that has some benefits in terms of its throughput, energy consumption, traffic load, and so on. It enables a location based mechanism. "Secure device-to-device communication in LTE" [6] focuses on an overview of the security architecture, threads, and requirements. By reusing the existing systems different solutions have been proposed. Initially the paper divides LTE-A D2D into three types based on the availability of a network and the presence of a user application based on the need of user. These types actually manage the network that results in the security requirements of network that chosen. [6] Introduced a new security architecture and analyse the security requirements for these 3 types. For these three types an authentication and key management solutions have been proposed also.

"TinyCoAP" [7] gives the implementation and description of constrained application protocol for TinyOS, called TinyCoAP. CoAP works same as a normal HTTP protocol. CoAP basically has low overhead and simple design. While the designing of a CoAP based application, wireless sensor networks needs a special attention. It can be achieved by a native library called TinyOS. It already includes implementation of CoaP known as CoAPBlip. The evaluation of Tiny CoAP and CoAPBlip in terms of measuring memory consumption, energy consumption and latency and finally evaluates the goodput.

LTE networks are designed by 3rd generation partnership project 3GPP. LTE networks designed mainly at the aim of low overhead, scalable bandwidth, less delay and high latency. With the emergence of LTE network applications, the need of securing LTE networks also made important part. Authentication of LTE networks is very important due to various security attacks in network. Attackers try to authenticate in LTE network as an authorized person. The basics of Extensible Authentication Protocol-Authentication and Key Agreement (EAP-AKA) are used in LTE AKA protocol which is called Evolved Packet System AKA (EPS-AKA) protocol to secure LTE network, However it makes different vulnerabilities such as user identity issue, overhead, storage issues etc. In this paper, an Efficient EPS-AKA protocol (EEPS-AKA) is proposed to overcome such problems. "An efficient authentication and key agreement protocol for 4G (LTE) networks" [8] provide solution by using a simple password exponential key exchange (SPEKE) protocol. When compare with existing ones, the new sheme is faster and uses secret key that is a certification based. The size of messages that is transmitted reduced. Also this scheme reduces low overhead and storage overhead.

Enhancements on AKA protocol called "Enhancement Mobile Security and User Confidentiality (EMSUCU) for UMTS" [9] introduced to overcome problems related to user id disclosure and secret key exposure. The user identity encrypts using EMSUC. Instead of encryption keys and functions, the proposed protocol uses some hash functions. It faster the working of method and increasing security by using security function f11. F11 generate the key Kc and protects exchanged message of AKA protocol.

"A Security Enhanced Authentication and Key Agreement (SE-EPS AKA) based on Wireless Public Key Infrastructure (WPKI)" [10] has been proposed. The method ensures the safety of user identity in IoT network and the messages exchanged in a very low energy. For this purpose a scheme called Ellipse curve cipher encryption is used. Th disadvantage of the method is that it is vulnerable to brute force attack.

An "Ensured confidentiality authentication and key agreement (ECAKA)"[11] has been proposed to achieve the user's confidentiality. By the scheme, using an encryption function all the AKA messages are fully protected. Then it can prevent the disclosure of user identity. Mutual authentication and secure communication between UE and HSS can be ensure due to the usage of public-key based protection mechanisms. But it cause a large number of computational costs, storage costs communication costs for mobile devices.

A new modified version of the EPS-AKA protocol has been proposed in [12]. The modified scheme generates a

subscriber module instead of USIM. It provides a direct online mutual authentication link between the ESIM and the MMEIHSS to solve the dis advantages of the EPS-AKA protocol. It has only slight variations on the the access security architecture. Because of the use of a new USIM it may create some problems in the LTE networks. Hence the home subscriber identity needs to participate in each and every authentication setup for each user entity. It may generate a large number of communication and computation delays and thus signaling congestion arises at the communication side.

Another solution has been provided in [13], proposed a new authentication method by improving the existing EPS-AKA for LTE networks. The new method uses an authentication mechanism which is based on a proxy signature. The proxy signature system prevents the issues in the basic handover mechanism like multi key management services. Also the delay arising due to handover because of the message exchange in between user entity and mobile management entity. The proposed method includes two phases, First phase is an attach phase which prepare to the next handover authentication and the next phase is the uniform handover authentication that complete mutual authentication between user entity and eNB.

In [14], An analysis is done which is based on the disadvantages of EPS-AKA protocol such as disclosure of user identity, replay attacks, redirection attacks and MITM attack. The main issue is that the communication channel in between mobile management entity and home subscriber identity is not safe. As a result, the authentication vectors will be in a risk. To overcome from these problems, an enhanced mechanism called Security Enhanced Authentication and Key agreement (SE-EPS AKA) has been proposed based on Wireless Public Key Infrastructure (WPKI) and ECC (Ellipse Curve Cipher) encryption method. Using a verification model the model has been proofed. To make the user id safe, the IMSI (International mobile subscriber identity) is encrypted using the public key of HSS.

III. METHODOLOGY

The basic of system is given in the figure. Initially a user enters into a network by browsing internet. Then it will browse to FAC portal and submit user login information. If the login was successful FAC deliver the login message to client. Then client login and access request will be accepted and assign guest permissions. Later the user is authorized and gets internet access. If the session timeout, user no longer can exist in the network.

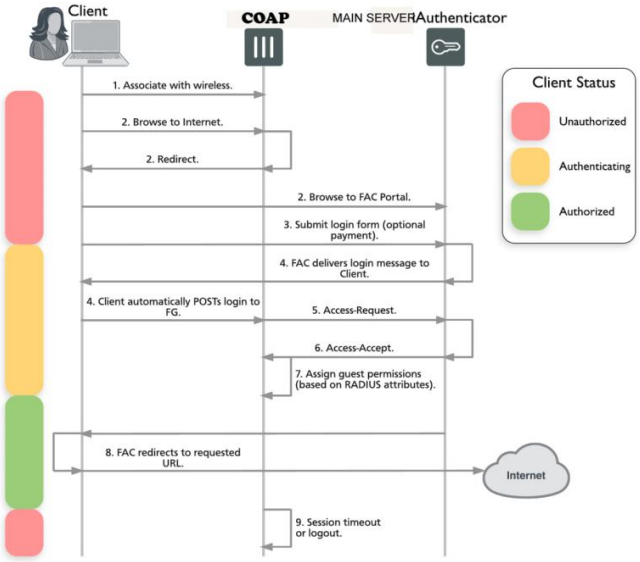

Fig 3.1 Captive portal communication

3.1 *Authentication*

In the authentication module, a user will be entered onto a network by giving username and password. Captive portal is using as authentication medium. RADIUS protocol is used to authenticate and provide access to a network remotely. Nowadays in a wide area of research RADIUS is using at server side. It is a client server protocol with browser as a client and RADIUS as server. If any browser uses RADIUS as server for connection it will follow the following steps

- User authenticate using port 4100 or by HTTP connection with IPsec. Then the device read the username and password
- Device then sent an access request message to server
- If the server is configured correctly it will respond by a an accept or reject message
- If the server accepted, it will check the client identity and whether the request is from a trusted authority, if yes, it will check for the authentication method
- If the authentication type is known to the client (Here it is CoAP), server will move on to the username and password verification mechanism.
- Radius server will check whether the given information matches or not. If any policy match fond, server sent the corresponding response.
- If any of the above conditions fail, server will sent an access reject message to the client else sent access accept message

3.2. *Verification*

Verification process is just like a normal username and password verification schema. That means, the data that has been entered by the user will be verified in this section. It will be checked at the sql server. If a match found, it will give access and the corresponding information will be sent onto the CoAP which is the core part or middleware that handles everything related to it. The authentication and verification part is actually occurring using radius server and database.

3.3 *CoAP*

CoAP is a constrained application protocol defined in RFC 7252.CoAP is the one who decides whether internet access has to make avail to the users. Main advantage of using CoAP is that it can provide sessions asper need. Ie; how much time a user can access the internet, how much data he/she can be utilized, and how long. Like that all information will be set as sessions. CoAP also uses in SMS services in mobile networks. It is actually a service layer protocol using in wireless networks. Compare to other web protocols CoAP has very low overhead. In UDP supported machines, CoAP runs efficiently.

For the support of various IoT applications, CoAP is using as intermediate one. It is actually similar to HTTP client server model with two layered structure. Bottom layer is called message layer that manages UDP. Other layer is the request/response layer. Fig 3.3. gives the basic features of CoAP.

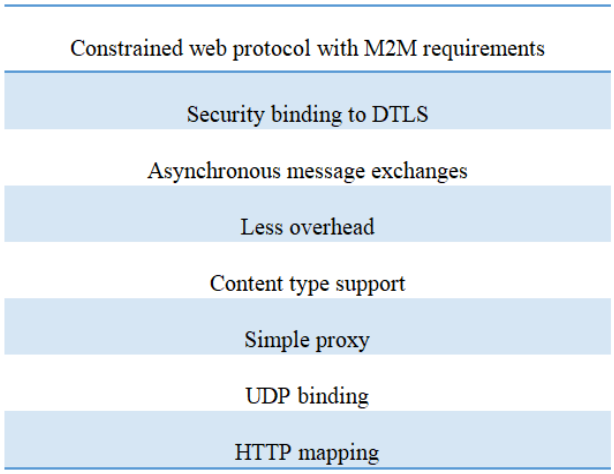

Fig 3. 3.1 Basic CoAP features

Authentication protocol using for the system is [1] explained in some steps.

Protocol setup: In this phase, the basic functions using in the protocols are setup. It uses seven function keys with each having its own functionality and encryption and decryption keys.(f1(),f2(),f3(),f4(),f5(),f6(),f7(), E/D()). For the generation of cipher text, AES-CTR algorithm is using. It has a simcode generation concept. XOR function is designed for this special purpose.

Protocol initiation: In this phase, the intermediate MME key will be sent to MME. By doing this, there is no need of execute the full protocol when resynchronization is needed at any stage. Keys generated are independent of the previous keys.

Protocol execution: Execution is the main part of the project. Initially a user entity will sent a service request to user entity requesting its IMSI (International mobile subscriber identity). Then mobile entity will check whether any connection has been established already with that device. If yes, it will establish session based on the new one. Else it will create a new session using GPRS gateway. Then an authentication data request will be sent to home subscriber server. And verify IMSI through diameter permission range. Later HSS create new authentication vector and sent it to MME. The newly created AV consist of authentication vector set, random number, signed response. On receiving this UE computes RES and compare it with the expected response. If both are same it will be verified. MAC address along with the data gives integrity check.

3.4 *Token generation & Encryption:*

Tokens are generated based on the username and password given by the user. For each user , there will be a token. Hence the user will be identified by that key until the particular session finished. Based on the token value, it will be decided that how long the session has to remain, how much mb that can be used by the particular user etc. Hence token generation makes one of the important steps of project.

Next it will be moving onto encryption phase. Encryption is widely used on the internet to protect user information being sent between a browser and a server, including passwords, payment information and other personal information that should be considered private. Organizations and individuals also commonly use encryption to protect sensitive data stored on computers, servers and mobile devices like phones or tablets. Encryption can be done in many ways. Asymmetric and symmetric methods can be adopted. Here symmetric key is using for encryption. That is encryption and decryption done using same key. Here the keys will be generated randomly and using that keys the data will be encrypted and provides security.

3.5 Location sharing

Location based services are becoming very popular. In the location sharing phase, what is happening is that location of a user in the network will be sent onto other person. For that STP (Spatial temporal provenance) is using. It is for generating location proofs and also a semi trusted certificates are using for cryptographic key production.

In STP scheme, there will be a prover, verifier, witness and a certification authority.

Prover: It is a mobile device with the requirement of STP proof at a specific location.

Verifier: Verifier create a proof about the location of a device.
Witness: Witness is the one who creates STP proof when request gets.

Certification authority: It is a server that manage cryptographic credentials

Figure shows the protocol use to implement location sharing system.

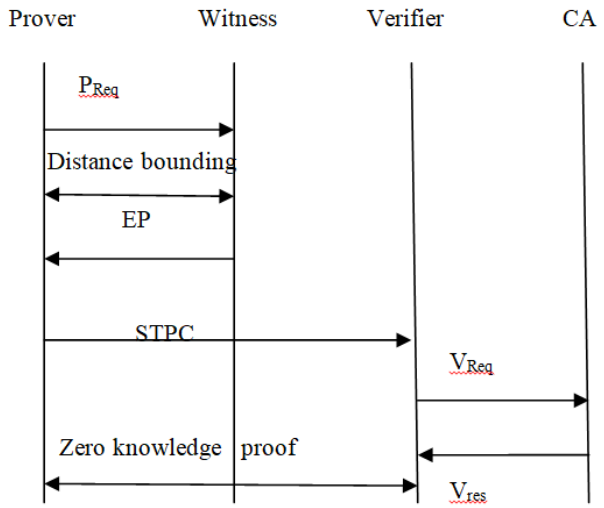

Fig 3.5.1 Location sharing

Location sharing consists of 2 sections mainly. STP proof generation and STP claim and verification. Suppose a prover collects STP information from its neighbors, it is said that the STP proof event has been started by the prover. Initially prover will sent an STP request to witness and tries to enter into STP proof event. While receiving the request, witness will check whether prover is its neighbor or not and enter into distance bounding stage. After that it will jump onto STP claim and verification stage. For that prover will sent a STPC message to verifier and verifier pass this to CA. CA encrypt it using its public key and return to prover itself.

IV. PERFORMANCE ANALYSIS

This section includes the performance of this system in terms of its security measures, overhead and bandwidth.

Overhead: Overhead is an unnecessary computation time, delay, storage in network. In this system, CoAP works as a transparent layer. Ie; It doesn't filter the connection instead of that only watch connections. So communication overhead will be also less. Like that dynamic storing of information are done. Then storage overhead can be reduced.

Bandwidth: Bandwidth of the system is less compared to the existing systems. Because a standard has been kept in the CoAP and there is no individual authentication occurring. Ie; everything is done based on a session. Hence number of packets transmitted will be less. So automatically bandwidth will be reduced.

4.1 Security analysis

Replay attack: Replay attack is a network attack at which the data delayed and resend by an attacker. For solving this issue, the protocol using in this project uses timestamps. Hence replay attack can be prevented easily.

Redirection attack: Redirection attack is in increasing attack strategy in between malicious nodes. Attackers will redirect the path or destination. For resolving this issue, the protocol uses a MAC for integrity check.

V. CONCLUSION

The scheme generates a secure protocol with a securing scheme called CoAP for the public networks. This gives many advantages when compared to a normal Wi-Fi network and also provides an efficient and secure mechanism for making location sharing services protected. Privacy preservation of a user has achieved mainly through the new scheme. The CoAP mechanism and location privacy module generates privacy in the system. Unlike EPS-AKA protocol the new one prevents the synchronization problem by using a message authentication code for verifying valuable information and data. When comparing with the existing techniques, the new method gives the protection not only at the middle layer but also at the security layer. The issues arising during a location sharing service are also solved by CoAP scheme. For the communication among various IoT objects, a safe and better communication scheme is established.

REFERENCES

[1] Saxena, N., Grijalva, S. and Chaudhari, N. (2016). Authentication Protocol for an IoT-Enabled LTE Network. ACM Transactions on Internet Technology, 16(4), pp.1-20.

[2] Koien, G. (2011). Mutual entity authentication for LTE. 2011 7th International Wireless Communications and Mobile Computing Conference.

[3] Varun Das, Shika, "A review paper on advanced network parameter in LTE based 4G", EURASIP journal on wireless communication and networking, 2016, pp.2725-2728.

[4] Abdrabou, M., Elbayoumy, A. and El-Wanis, E. (2015). LTE Authentication Protocol (EPS-AKA) weaknesses solution. 2015 IEEE Seventh International Conference on Intelligent Computing and Information Systems (ICICIS).

[5] Choudhury, H., Roychoudhury, B. and Saikia, D. (2012). Enhancing User Identity Privacy in LTE. 2012 IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications

[6] Alam, M., Yang, D., Rodriguez, J. and Abd-alhameed, R. (2014). Secure device-to-device communication in LTE-A. IEEE Communications Magazine, 52(4), pp.66-73.

[7] Ludovici, A., Moreno, P. and Calveras, A. (2013). TinyCoAP: A Novel Constrained Application Protocol (CoAP) Implementation for Embedding RESTful Web Services in Wireless Sensor Networks Based on TinyOS. Journal of Sensor and Actuator Networks, 2(4), pp.288-315.

[8] Lai, C., Li, H., Lu, R. and Shen, X. (2013). SE-AKA: A secure and efficient group authentication and key agreement protocol for LTE networks. Computer Networks, 57(17), pp.3492-3510.

[9] D.Caragata, S. El Assad, C. Shoniregun, and G. Akmayeva, "Umts security:
Enhancement of identification, authentication and key agreement protocols," in Internet Technology and Secured Transactions (ICITST),

[10] L. Xiehua and W. Yongjun, "Security enhanced authentication and key agreement protocol for L TE/SAE network," in Wireless Communications, Networking and Mobile Computing (WiCOM), 2011 7th international Conference on, 2011, pp. 1-4.

[11] J. B. Abdo, H. Chaouchi, and M. Aoude, "Ensured confidentiality authentication and key agreement protocol for eps," in Broadband Networks and Fast internet (RELABiRA), 2012 Symposium on, 2012, pp. 73-77.

[12] J. Cao, H. Li, M. Ma, Y. Zhang, and C. Lai, "A simple and robust handover authentication between henb and enb in {LTE} networks," Computer Networks, vol. 56, no. 8, pp. 2119 – 2131, 2012.

[13] www.tutorialspoint.com.(2018). LTENetwork architecture.[online]availableat:https://www.tutorialspoint.com/lte/lte_network_architecture.htm [Accessed 16 Mar. 2018].

[14] JkIjsetr.org.(2018).[online]Availableat:http://ijsetr.org/wp content/uploads/2016/08/IJSETR-VOL-5-ISSUE-8-2725-2728.pdf [Accessed 16 Mar. 2018].