Indian Institute of Technology (Indian School of Mines), Dhanbad

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

PROJECT REPORT

Session : (2021-22)
VIII Semester

Topic: Handover Authentication for next Generation Mobile Network using Blockchain

Submitted to:
Guide: Dr. Ansuman Battacharya

Submitted by:
Name : Satyavart
Admission No : 18JE0746

Certificate

This is to certify that Satyavart (18JE0746) has satisfactorily submitted the project progress report till now on topic "Fast ans Secure Authentication using Blockchain". This Project report is submitted to the Department of Computer Science and Engineering of Indian Institute of Technology (ISM) Dhanbad in partial partial requirement for the degree of Bachelor of Technology with Master of Technology in Computer Science and Engineering during academic year 2021-22.

Dr. Ansuman Battacharya
Assistant Professor
Department of Computer Science and Engineering
IIT (ISM) Dhanbad

Declaration of Originality

I, Satyavart (18JE0746) hereby declare that this research "Handover Authentication for next Gen Network using Blockchain" represents my original work carried out as a student of Indian Institute of Technology (Indian School of Mines), Dhanbad and, to the best of my knowledge, it contains no material previously published or written by another person unless cited. Any contribution made to this research by others, with whom I have worked with explicitly acknowledged in the plan. Work of their authors cited in this report have been duly acknowledged under the section "References"

12 May, 2022
IIT(ISM) Dhanbad

_____
Signature

Acknowledgement

I would like to express heartfelt gratitude and regards to my project guide Dr. Ansuman Battacharya and specially to scholar Prasanta Kumar Roy. I convey a humble thanks to them for their valuable cooperation, support and suggestion throughout the project work which made this project successful.

Abstract

The next generation mobile cellular communication and networking system (5G) is highly flexible and heterogeneous. It integrates different types of networks, such as 4G legacy networks, Internet of Things (IoT), Vehicular Ad-hoc Network (VANET) and Wireless Local Access Network (WLAN) to form a heterogeneous network. This easily results in continual vertical handovers between different networks. On the other hand, substantial deployment of small/micro-cell Base Stations (BSs) brings frequent horizontal handovers within a network. The continual handovers among BSs and various networks expose Mobile Equipment(ME) to risk of security and privacy threats.

Nevertheless, there still lacks a thorough algorithm for fast authentication of the ME during the handover which is invulnerable to attacks. In this project, I have worked on the algorithm that will authenticate the ME with secure and fast way furthermore verify the user with blockchain.

Contents

List of Figures

List of Tables

Chapter 1

Introduction

With the continuous increase of data and devices in wireless networks, existing wireless networks have been facing difficulty to withstand increasing traffic load. Consequently, the next generation of mobile cellular communication and networking system (5G) has emerged to meet these intense demands via innovative technologies, e.g. Network Function Virtualization (NFV), Software-Defined Network (SDN), Device-to-Device (D2D) communications, etc. Enhanced Mobile Broadband brings 100 times higher data rates than that of 4G that can reach 10 gigabits per second. Massive Type Communications require a Base Station (BS) to manage an enormous number of devices that are designed for Internet of Things (IoT) in general.

5G is highly flexible and heterogeneous with numerous communication networks involved. According to International Telecommunication Union (ITU), low penetrability of high-frequency signals adopted in 5G and networks consist of a large number of small Access Points (AP) to provide high data access rates and available network bandwidth.

1.1 Handover

Mobile handover technology, which underpins the continuity of mobile network service, allows ME to move seamlessly between different base stations (BSs) or access points (APs) equipped with different access technologies. Handover or Handoff is an important element in planning and deployment of cellular networks. The deployment of small APs brings frequent horizontal handovers in the cellular network.

1.2 Classification of Handover

There are many taxonomies to classify handover, for instance, based on the carrier frequency, handover can be classified into inter/intra-frequency handover. But according to the proposed solution in chapter 4, we will talk about Intra/Inter Mobililty Management Entity (MME) handover.

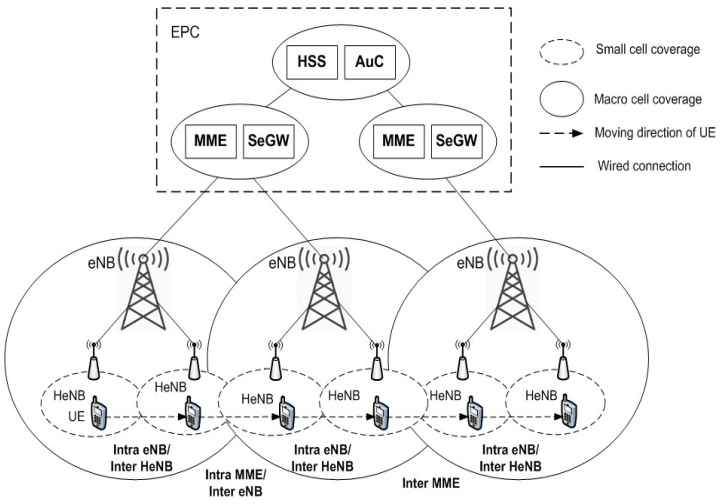

Figure 1.1: Intra/Inter MME handover

1.2.1 Inter MME Handover

In this, two MMEs are involved in handover, source MME and target MME. The source MME (S-MME) is in charge of the source eNodeB and target MME (T-MME) is in charge of target eNodeB.
Inter MME Handover occur from source eNodeB to target eNodeB.

1.2.2 Intra MME Handover

In this, only one MMEs is involved in handover. The same MME is the charge of the source eNodeB and target eNodeB.
Inter MME Handover occur from source eNodeB to target eNodeB.

1.3 What is blockchain

A blockchain is a distributed database that is shared the various nodes of a laptop community. As a database, a blockchain stores data electronically in digital layout. Blockchains are first-rate known for his or her important position

in cryptocurrency structures, such as Bitcoin, for maintaining a relaxed and decentralized record of transactions. The innovation with a blockchain is that it ensures the accuracy and security of a document of records and generates agree with without the need for a trusted 3rd party.

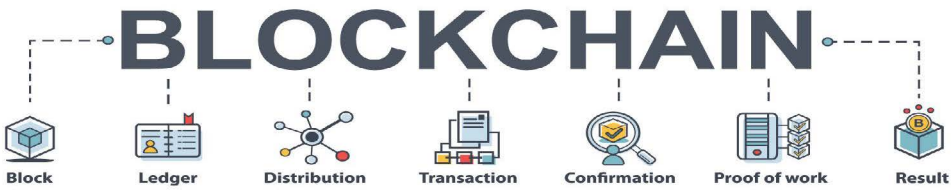

Figure 1.2: Key Component of Blockchain

According to a study, it is proved that cell shrinking and low penetrability of millimeter-wave make the handover happens every 11.6 seconds. So, smoothly supporting mobility among the eNBs is big challenge while maintianing security of the mobile network.

By keeping this concept in mind, I have worked on building a network model which is fast and secure enough.

Chapter 2

Survey

2.1 LTE-A Network Architecture

The high-level network architecture of LTE is comprised of following three main components:

- The User Equipment (UE).
- The Evolved UMTS Terrestrial Radio Access Network (E-UTRAN).
- The Evolved Packet Core (EPC).

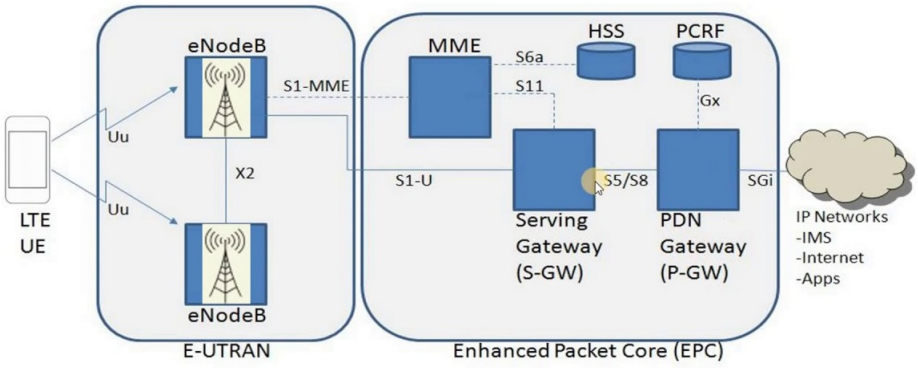

Figure 2.1: LTE-A Network Model for Authentication

2.1.1 User Equipment (UE)

The internal architecture of the user equipment for LTE is identical to the one used by UMTS and GSM which is actually a Mobile Equipment (ME). The

mobile equipment comprised of the following important modules:

- **Mobile Termination (MT) :** This handles all the communication functions.
- **TTerminal Equipment (TE) :** This terminates the data streams.
- **Universal Integrated Circuit Card (UICC) :** This is also known as the SIM card for LTE equipments. It runs an application known as the Universal Subscriber Identity Module (USIM).

A USIM stores user-specific data very similar to 3G SIM card. This keeps information about the user's phone number, home network identity and security keys etc.

2.1.2 The E-UTRAN

The E-UTRAN handles the radio communications between the mobile and the evolved packet core and just has one component, the evolved base stations, called eNodeB or eNB. Each eNB is a base station that controls the mobiles in one or more cells. The base station that is communicating with a mobile is known as its serving eNB.

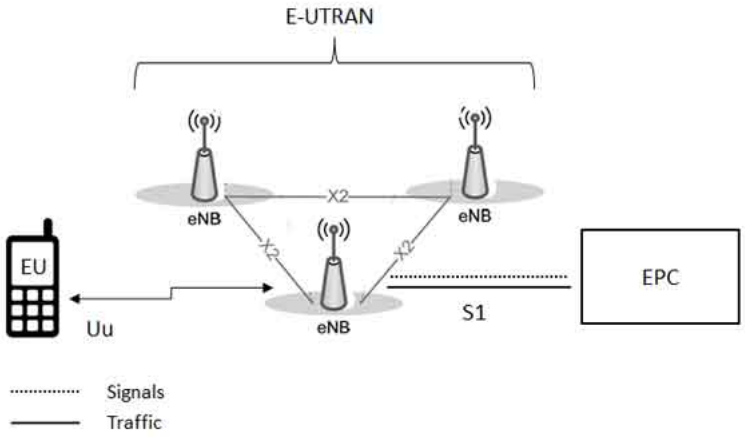

Figure 2.2: E-ULTRAN (Access Network)

2.1.3 The Evolved Packet Core (EPC)

The EPC represents the Core of an LTE network. It is formed by multiple nodes, the main ones being MME, SGW, PGW and HSS.
It has following functionality:

- Makes the LTE core network function

- Authenticates subscribers
- Determines the subscribers' access to the network
- Helps to locate the UE
- Essentially aids mobility management

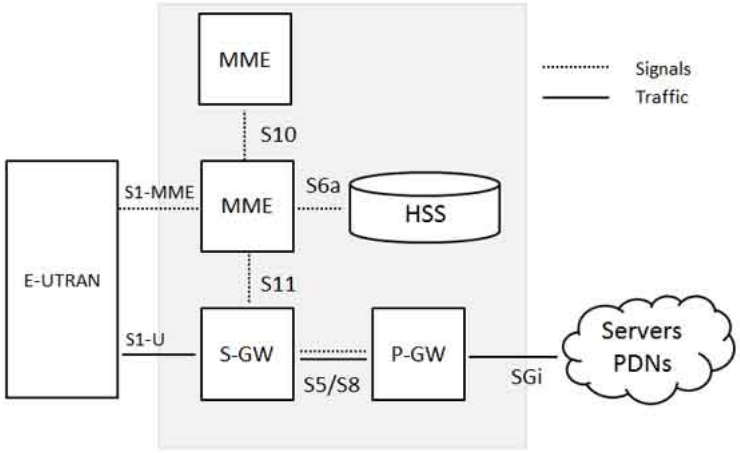

Figure 2.3: EPC (Core Network)

2.2 Increasing Network Capacity

In time, as more customers use the mobile network, traffic may build up so that there are not enough frequency bands assigned to a cell to handle its calls. A number of approaches have been used to cope with this situation, including the following:

- **Adding new channels:** Typically, when a system is set up in a region, not all of the channels are used, and growth and expansion can be managed in an orderly fashion by adding new channels.
- **Frequency borrowing:** In the simplest case, frequencies are taken from adjacent cells by congested cells. The frequencies can also be assigned to cells dynamically.
- **Cell splitting:** In practice, the distribution of traffic and topographic features is not uniform, and this presents opportunities of capacity increase. Cells in areas of high usage can be split into smaller cells. Generally, the original cells are about 6.5 to 13 km in size. The smaller cells can themselves be split; however, 1.5 km cells are close to the practical minimum

size as a general solution. To use a smaller cell, the power level used must be reduced to keep the signal within the cell. Also, as the mobile units move, they pass from cell to cell, which requires transferring of the call from one base transceiver to another. This process is called a handoff. As the cells get smaller, these handoffs become much more frequent.

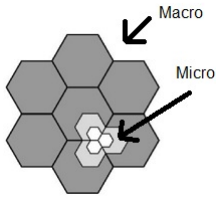

Figure 2.4: Cell Spliting

- **Cell sectoring:** With cell sectoring, a cell is divided into a number of wedgeshaped sectors, each with its own set of channels, typically 3 or 6 sectors per cell. Each sector is assigned a separate subset of the cell's channels, and directional antennas at the base station are used to focus on each sector.

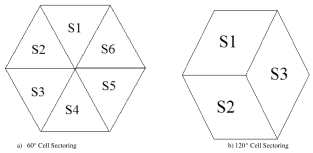

Figure 2.5: Cell Sectoring

- **Microcells:** As cells become smaller, antennas move from the tops of tall buildings or hills, to the tops of small buildings or the sides of large buildings, and finally to lamp posts, where they form microcells. Each decrease in cell size is accompanied by a reduction in the radiated power levels from the base stations and the mobile units. Microcells are useful in city streets in congested areas, along highways, and inside large public buildings.

2.3 5G Network Architecture

In 5G network, spectrum will come from frequency bands above 24 GHz. Due to high frequency, it will propagate over much shorter distances which is suitable for smaller cells as the interfere between densely deployed cell will be less. This will significantly increase the number of base stations. As the earlier network

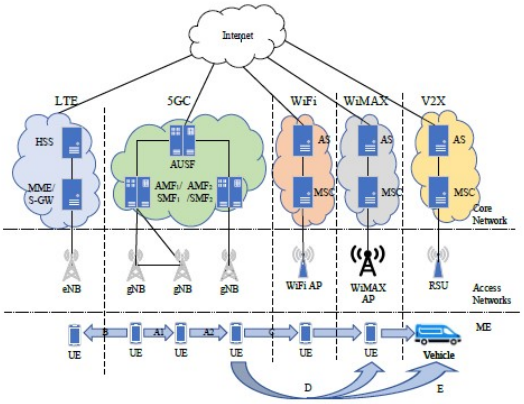

Figure 2.6: Handover scenarios in 5G networks

generation 5G should coexist with previous generation networks.
5G network mainly consists of two parts, named Core Network (CN) and Radio Acess Network (RAN) as shown in the above fig. 2.4.

2.3.1 Core Network

CN mainly contains Access and Mobility Management Function (AMF), User Plane Function (UPF), Session Management Function (SMF), and Authentication Server Function (AUSF).

- The Access and Mobility Management Function (AMF) acts as a single-entry point for the UE connection.
- The User Plane Function (UPF) transports the IP data traffic (user plane) between the User Equipment (UE) and the external networks.
- The Authentication Server Function (AUSF) allows the AMF to authenticate the UE and access services of the 5G core.
- Other functions like the Session Management Function (SMF), the Policy Control Function (PCF), the Application Function (AF) and the Unified Data Management (UDM) function provide the policy control framework, applying policy decisions and accessing subscription information, to govern the network behavior.

2.3.2 Radio Access Network

In RAN, there are g-Node Base Stations (gNB) which communicate with MEs. If a ME wants to connect to the 5G CN, AMF would firstly represent AUSF to perform mutual authentication with the ME.

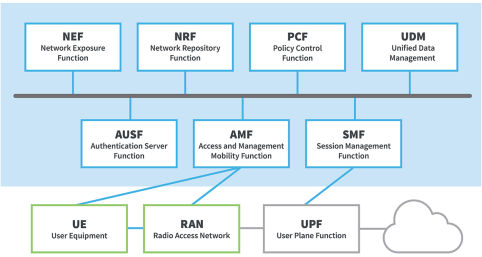

Figure 2.7: Key Component of 5G Core Network

2.4 Threat Model

According to a survey, which have analised 34 types of attacks which are analysed and prevented by authentication and privacy preserving schemes for 4G and 5G cellular networks. They have divided these attacks in 4 types as shown in the fig.

- Attacks against privacy
- Attacks against integrity
- Attacks against availability
- Attacks against authentication

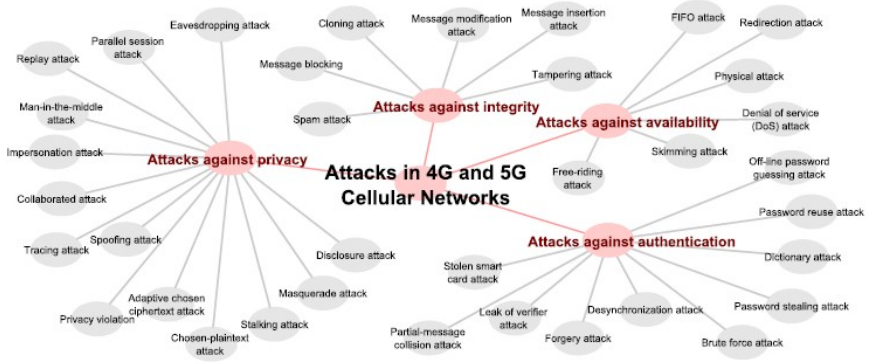

Figure 2.8: Classification of Attack in 4G/5G Network

2.5 Security Requirement

It describe functional and non-functional requirements that need to be satisfied in order to achieve the security attributes of a network.

It has divided into 6 parts:

2.5.1 Mutual Authentication and Authorization

Authentication is the most important part of the handover security. It is the process of determining whether someone or something is, in fact, who or what it says it is.An ME should be successfully authenticated by both its source network and its target network whenever a handover occurs. On the other hand, the ME must confirm the validity of the target network before accessing it. After the success of mutual authentication, subscribed services should be negotiated and authorized for the ME. The requirements on mutual authentication and authorization mainly prevent the handover in 5G networks from attacks against authentication, e.g., impersonation attacks, spoofing attacks, and MitM attacks.

2.5.2 Confidentiality

Confidentiality is the ability not to disclose information to unauthorized persons, programs, or processes. It relates to information security because it requires control over access to protected information. Confidentiality requires measures to ensure that only authorized persons have access to information, and while unauthorized persons are denied access to them. Simply put, confidentiality means that something is secret and should not be passed on to unintentional persons or organizations. If confidentiality is compromised, this can lead to loss of privacy and disclosure of confidential information to the public or other persons.

2.5.3 Integrity

Integrity means that protection against improper modification and destruction of information, ensuring that information cannot be changed undetected, and ensuring the integrity of the information. This means that a cyber threat or vulnerability to cyber-attack can be measured by compromising one or more of its principles. Integrity is based on encryption and hashing to ensure the best possible protection against cyber attacks and cyber threats such as cyber espionage.

This is a basic security requirement for the 5G networks, naturally also for handover. Correspondingly, ME and the network should agree on a session key after the handover in order to achieve confidentiality and integrity in each communication session against both passive attacks, such as eavesdropping, and active attacks, such as message blocking attacks, message modification attacks, and tampering attacks.

2.5.4 Availability

Availability means that the network is available for legal users in any situation even under common attacks. The services should be robust anytime and anywhere even under DoS or DDoS attacks. Since 5G is an open environment, an adversary can attack ME or BS from different networks by raising various kinds of attacks.

2.5.5 Resistent to active and passive attacks

Active attack: An Active attack attempts to alter system resources or affect their operations. Active attacks involve some modification of the data stream or the creation of false statements.

Passive attack: A Passive attack attempts to learn or make use of information from the system but does not affect system resources. Passive Attacks are in the nature of eavesdropping on or monitoring transmission. The goal of the opponent is to obtain information that is being transmitted.

2.5.6 Session Key Secrecy

A session key is an encryption and decryption key that is randomly generated to ensure the security of a communications session between a user and another computer or between two computers.
Securing session is also very important. It contains 3 parts:

Forward/Backward Secrecy

- **Forward Secrecy:** It is a feature that for an entity with knowledge of session key K_m between the entity with a second entity, it is infeasible to predict any future K_{m+n} (n>0) used between a third entity and the second entity. Forward secrecy protects future communications from the threat of current keys leakage. In the context of handover, forward secrecy refers to the property that, for a gNB with knowledge of a K_{gNB}, shared with a UE, it is computationally infeasible to predict any future K_{gNB} that will be used between the same UE and another gNB.

- **Backward Secrecy:** Contrary to FWS, Backward Secrecy (BWS) is a feature that for an entity with knowledge of session key K_n, it is infeasible to predict any previous K_{n-m} (n>m>0) from which K_n is derived. Backward secrecy protects previous communications from the threat of current keys leakage. In the context of handover, backward secrecy refers to the property that, for a gNB with knowledge of a KgNB, shared with a UE, it is computationally infeasible to predict any previous K_{gNB} that has been used between the same UE and a previous gNB.

Key Escrow Freshness

Key escrow is a method of storing important cryptographic keys. Each key stored in an escrow system is tied to the original user and subsequently encrypted for security purposes. Much like a valet or coat check, each key is stored in relation to the user that leverages it, and then returned once queried. By using key escrow, organizations can ensure that in the case of catastrophe, be it a security breach, lost or forgotten keys, natural disaster, or otherwise, their critical keys are safe.

Ephemeral Secret Leakage

If ephemeral secrets are compromised, an adversary can reveal the private keys of clients and the session key would turn out to be known from the eavesdropped messages. This phenomenon is called Ephemeral Secret Leakage (ESL) attacks.

2.5.7 Privacy

Conditional Privacy

Although it is quite significant to preserve user privacy, some sensitive information is requested to be provided in order to offer some services in certain situations. For example, when a user falls into a dangerous situation and needs help, his/her location should be conditionally available to ambulancemen. Thus, conditional privacy should be offered in the 5G handover.

Non Traceability

To distribute pseudonyms to the mobile user is a good way to achieve anonymity, but the adversary is able to trace users by linking a number of fixed pseudonyms between different sessions. Therefore, it is necessary to ensure non-traceability in handover.

Anonymity

In many handover scenarios in 5G networks, user identity privacy preservation is a significant requirement. Mobile users prefer to enjoy seamless mobile network services without using their real identities and exposing locations or other personally sensitive information. The real identity of an ME must be hidden from visiting networks or other MEs, and no attacker can link specific conversations to the real identity so that the user's privacy can be well protected from various attacks against privacy.

2.6 Possible Solution of Security Requirement

2.6.1 Mutual Authentication

Mutual Authentication is a security process in which entities authenticate each

other before actual communication occurs.

2.6.2 Proper Key agreement

Key exchange protocols enable two or more parties to establish a shared encryption key that they can use to encrypt or sign data that they plan to exchange. Key exchange protocols typically employ cryptography to achieve this goal. Different cryptographic techniques can be used to achieve this goal.

In order for two parties to communicate confidentially, they must first exchange the secret key that will be used to encrypt and decrypt messages. This initial exchange of the encryption key is called the key exchange.

A proper key exchange protocol is to be designed to establish confidentiality without letting unauthorized party to intercept, infer or otherwise obtain the key.

2.6.3 Dynamic Key

In traditional cryptosystems a specific cipher is chosen thus security of the system relies on the frequency of key changes and the key agreement scheme. Dynamic Encryption enhance such a system by defining a set of ciphers such that not only the key but also the cipher changes on every new data transaction.

2.6.4 Desynchronization Resistant

A connection should be maintain even after any type attack

2.6.5 Dynamic Pseudonym

Identity protection is considered to be important for authentication and key agreement protocol design in single-server and multi-server architectures. For that Dynamic Pseudonym should be used.

2.6.6 Short-term and Long-term Key

If Alice and Bob are going to speak securely, they don't need to keep the shared secret key around for a long time. They only need it for as long as they're speaking. And they don't want someone who records their conversation to be able to learn what they said. If they agree on a temporary key, one that lasts only as long as their conversation, that is a session key.

A session key is one that is not intentionally stored, and is not re-creatable. Session keys are used only for communications protocols, never for storage purposes. In computer protocols like SSL, the session key is generated randomly, exchanged securely with the other computer (using a key exchange protocol like DH), and remains in each computer's memory only for the duration it is needed

(a session.) When the session is ended, both sides wipe their copies of the key from memory.*

A long-term key is one that is deliberately stored somewhere, either on a computer disk, flash memory, or even printed on paper. The key is intended to be used at multiple points in time, such as "I will use this key to encrypt this secret file today, and use it again to decrypt my secret next week." A long term key can be used for any purpose, including stored information as well as transient communications.

Chapter 3

Problem Statement

With the increase in population and mobile equipments, existing wireless networks have been facing difficulty to withstand increasing traffic load. Thats why, 5G network is designed in such a way that it will meet these intense demands in addition to security and seamless communication. As explained in chapter 2, types of ways to increase the capacity of a network. 5G network is aimed to use microcells concept. In this a cell is divided into microcells of aprrox. radius of 200m which was 30km in 4G networks. Due to decrease in cell size, high-frequency signals of low penetrability is adopted as 5G networks consist of a large number of small Access Points (AP) to provide high data access rates and available network bandwidth. High frequency signal will not interfere with other cells frequency.

But to decrease in the cell size, handover between the Base Station (BS) and mobile equipment become very frequent. According to a study, it is said that on an average it will take 11.6sec to have a handover for a mobile equipment (ME) in 5G network. During handover we have use a secure way to authenticate the ME and acess point. And handover process should be resistant to any type of attack. But as well as with providing security we should also make the it fast to provide the seamless connection to the mobile equipment.

So, we should find a fast and secure way for authentication during the handover.

Chapter 4

Proposed Method

Handover in 4G network occurs when a ME move from one cell to another cell. And during authentication base station as to confirm ME identity from HSS which increase time of handover by twice of propogation delay, twice of transmission delay and computation delay $(2 * T_p + 2 * T_t + T_c)$.

In the 4G network, the only part that is wireless is connection between base station and ME and range to few kms only. Whereas rest of the connections like BS with MME, MME with HSS is wired and can be thousands of kms appart. Due to which T_p play a important role in seamless communication.

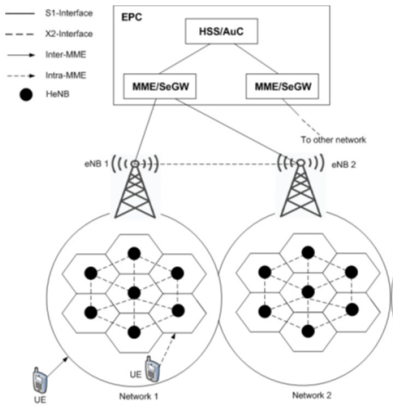

Figure 4.1: 4G Network Deployment Model

4.1 Assumption Model

The solution for the above problem is given but with few assumption as listed below.

- Only HSS can insert a block in the ledger.
- A block is only inserted in the case of intra MME handover.
- During intra MME handover U_i will receive a group key to participate in the inter MME handover.
- During inter MME handover, user authentication will be done based on on the last entry in blockchain as well as the group key.
- Once verified user will receive a positive acknowledgement from the visited network (BS).

By keeping this in mind, a solution is proposed in this project. Instead of contacting HSS everytime a ME move from one eNB to another eNB. We will only contact HSS in only 2 cases:

- When a ME move from one MME to another MME.
- If ME dont move from between MME, then after every fixed time interval.

It doesn't mean we dont have to authenticate ME and eNB during handover. But that process of authentication is solely based on the eNB, this method will drastically decrease time delay that happens during handover.

4.2 Fast and Secure Handover

As explained in Chapter 1 for handover will be based on Intra/Inter MME. In case of Intra MME handover that is, when a ME move from eNB of one MME to another eNB of different MME, ME with have a mutual authentication phase with HSS and then HSS will send a handover key to all the eNB in target MME for mutual authentication of ME and eNB. And in case of Inter MME handover, ME stays within the same MME. In this case ME will goes through mutual authentication phase with eNB using the handover key that was generated previously. After the mutual authentication with eNB in both cases, eNB will create a session key.

This whole process will require credentials which can be extracted from 3 steps:

- Registration of user
- Mutual Authentication with HSS
- Mutual Authentication with eNB

In this,step 1 is phase which take place when a SIM is registered to HSS. Step 2 and step 3 is part of handover phase. As result it will provide secure session key for further data communication.

4.2.1 Registration of user

When a user want to access 5G technology, user must advance to technology which are suitable for protocol of 5G network. For that he must register himself in offile mode. That when he will get Subscription Permanent Indentifier (SUPI). But to reduce the threat of information loss we shouldn't use SUPI for communication. If in any case SUPI is compromised it will lead to opening a path for the attacker to various attacks. So we should use dynamic temporary IDs for further communication. In addition to that every new user must register itself with HSS for further authentication. So, for solving these two problem a registration request is send to HSS. Then HSS will create a Temporary ID (TID) and a random number (r) for the further communication. This will be send to user and will be saved in Universal Subscriber Identity Module (USIM).

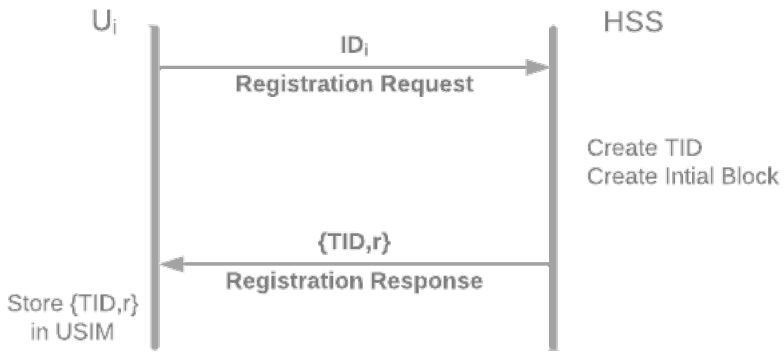

Figure 4.2: Registration of user in HSS

This process can be divied into 3 steps:

- **Step 1:** User ID (ID_i) of user U_i is send in a Registration request to HSS without any encryption as the it send through a trusted channel.
- **Step 2:** Here HSS will have its own secret key (k) which will not be shared with any other entity.

  This following steps will occur here:

  - Collect ID_i
  - Select a random number r
  - Create TID_i as

$$TID_i = E_k[ID_i||r||T_r]$$

, where T_r is the time stamp of registration of user U_i.

- Create Intial Block (B_0) of the blockchain as

$$B_0 = h(ID_i||T_r)$$

- With ID_i store $T_l \leftarrow \phi$, $MME_{id} \leftarrow \phi$, $Blockchain \leftarrow B_0$, where
  T_l is time previous handover is taken place
  MME_{id} is ID of the MME with which U_i was previous connected with.
  Blockchain is the blockchain which will store the new block and verify the previously connected nodes.
- Send TID_i and r to user in Registration Response.

- **Step 3:** Here U_i will recieve the response and save TID_i and r in its USIM. That will be for communication later on.

4.2.2 Mutual Authentication with HSS

Now that registration is complete. Now user will ask for services with service provider. After that whenever user enter a new MME, handover phase will start. It happens in steps:

- **Step 1:** ME will send HSS auth request. To create request these prerequisite is required.
  - Create K_i as,
$$K_i = h(ID_i||r)$$
  - Select another random number r_0
  - Create R_0 as,
$$R_0 = h(K_i) \oplus r_0$$
  - Create V_0 as,
$$V_0 = h(ID_i||r_0||T_u)$$
    where T_u is the current time stamp.
  - Send TID_i, R_0, V_0 and T_u to HSS via target eNB and target MME.

  Format of the message will be as given below.

Type	Count	TID	R0	V0	Tu	Path

Table 4.1: Format of HSS auth Request

Here

- Type will define the type of message it is.

- Count will store the jumpt count between the nodes.
- TID, R0, V0, Tu are the values which are calculated before.
- Path will store the path it will follow to reach HSS

- **Step 2:** Now the HSS auth request has reached the HSS. After that following process will take place.
  - Verify T_u with current time stamp. This will help in preventing replay attack.
  - Decrypt TID_i with its own secret key (k), this will give following result
    $$ID_i||r||T_r = D_k[TID_i]$$
    Now ID_i, r and T_r is extracted from here.
  - Check if the user is active user or revoked user. It help to identify if the user should get services or not.
    If
    $$T_u - T_r \leq \Delta_{rev},$$
    then active user
  - Compute K_i with values from 2 steps above, as
    $$K_i = h(ID_i||r)$$
  - Compute r_0, as
    $$r_0 = h(K_i) \oplus R_0$$
  - Verify V_0 by compairing the new V_0 and the V_0 which is received from ME.
  - Verify previous block of Blockchain.
  - Create new block of Blockchain as
    $$B_i = h(B_{i-1}||T_r)$$
  - Create a temporary factor T as,
    $$T = E_k[ID_i||r_i||T_r]$$
    , where r_1 is a new random number
  - Create new TID, as
    $$TID_i^{new} = T \oplus h(K_i)$$
  - Create handover key (hk), as hk is a random hash.
  - Create r^{new}, as
    $$r^{new} = h(ID_i||T||r_i||hk||T_h)$$
    where T_h is current time stamp

- Create HK, as
$$HK = h(K_i) \oplus hk$$
- Update value in ID_i as $T_l \leftarrow T_h$, $MME_{id} \leftarrow MME_{id}^{prev}$, $Blockchain \leftarrow B_i$.

- **Step 3:** Now HSS will send 2 messages

1st : HSS auth Response

HSS auth Response is send to the ME, with the format as shown below.

Type	Count	ETID	ER	Vi	Tnew	HK	Path	Result

Table 4.2: Format of HSS auth Response

- Type will define the type of message it is.
- Count will store the jumpt count between the nodes.
- ETID, ER, Vi, Tnew, HK are the values which are calculated before.
- Path will store the path it will follow to reach HSS
- Result will show if authentication was succeed or not.

2nd : Key Broadcast Request

In this, a key broadcast request is generated in the target MME saying that a new ME with ID_i has enter the network and further handover with this ME will be based on the handover key provided here. The format of the message is shown below.

Type	ID	hk

Table 4.3: Format of Key Broadcast Request

- **Step 4:** At the ME side after recieving HSS auth response, following steps is followed.
  - Calculate K_i, TID_i^{new}, hk, r_i from the message values
  - Using above value verify the V_i.
  - Store the value in USIM as,
$$TID \leftarrow TID_i^{new}, r \leftarrow r_i$$

- **Step 5:** At the MME side who recieved Key Broadcast Request, will send a broadcast message to all of its eNB with some modifications as shown below.
  - Create PID as

    $$PID = h(ID_i||MME_{id}||eNB_{id})$$

    where MME_{id} is ID of current MME and eNB_{id} is the ID of the eNB to which this message is send.
  - Key Broadcast message to every eNB inside itself. The format of message is shown below.

Type	PID	ID	hk

Table 4.4: Format of Key Broadcast message

- **Step 6:** eNB after recieving Key Broadcast message, it will save value of hk and PID under ID_i.

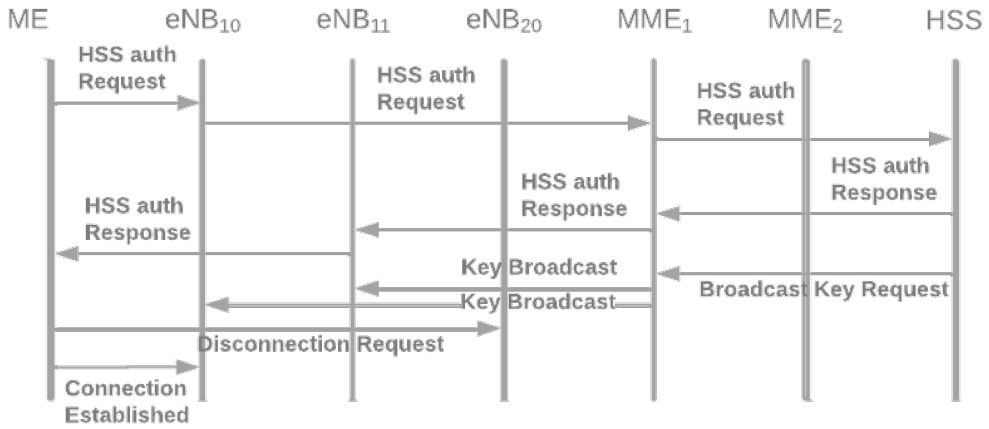

Figure 4.3: Handover from eNB_{20} to eNB_{10})

4.2.3 Mutual Authentication with eNB

The above step will only take place in case of Inter MME handover, but this step will take place in every handover. Here mutual authentication between ME and eNB is designed. For this steps are given below.

- **Step 1:** Firslty ME will generate a eNB auth request, with following steps:
  - Create handover request (H_{req}) as,

    $$H_req = E_{hk}[ID_i||T_c]$$

    where T_c is current time stamp.
  - Select a random number r_2
  - Create V_2, as

    $$V_2 = h(ID_i||T_c||r_2)$$

  - Create R_2, as

    $$R_2 = r_2 \oplus h(ID_i||T_c)$$

  Now a eNB auth message will be send to eNB with the format as shown below.

Type	R2	V2	Hreq

Table 4.5: Format of eNB auth Request

- **Step 2:** At eNB after recieving the eNB auth request, it will authenticate the ME and create a session key for communication with the steps shown below.
  - Decrypt H_{req} with hk which was given to eNB from its parent MME, giving

    $$ID_i||T_c = D_{hk}[H_{req}]$$

  - Verify T_c with current time stamp
  - Compute r_2 from ID_i, T_c and R_2, as

    $$r_2 = R_2 \oplus h(ID_i||T_v)$$

  - Verify V_2.
  - Verify PID
  - Select a random number r_3

- Compute R_3, as
$$R_3 = r_3 \oplus h(ID_i||T_{hb})$$
, where T_{hb} is current time stamp.
- Compute $Hres$, as
$$Hres = E_{hk}[ID_i||T_{hb}]$$
- Create session key (SK), as
$$SK = h(r2||r3)$$
- Send the eNB auth response back to ME with the given format.

Type	Hres	R3	Result

Table 4.6: Format of eNB auth Response

- **Step 3:** At ME after recieving eNB auth Response, following steps goes on.
  - Decrypt H_{res} with hk, as
$$ID_i||T_{hb} = D_{hk}[H_{res}]$$
  - Verify T_{hb} with current time stamp.
  - Compute r_3, as
$$r_3 = R_3 \oplus h(ID_i||T_{hb})$$
  - Compute session key (SK), as
$$SK = h(r_2||r_3)$$
- **Step 4:**
- Now ME will disconnect with the previous eNB and communicate with new eNB from now using the session key.

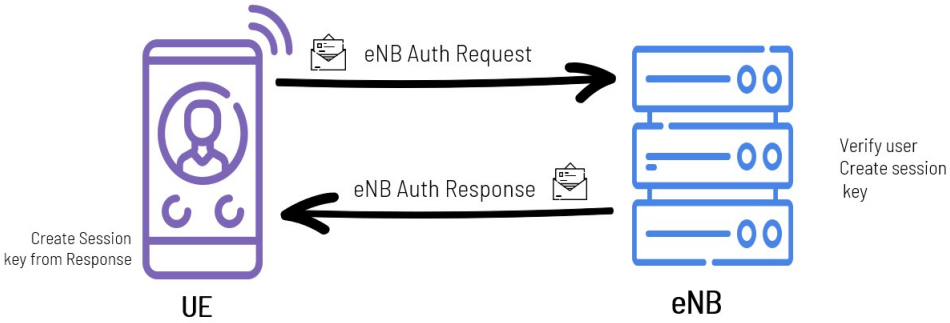

Figure 4.4: Inter MME Handover

Chapter 5

Future Scope

To get the result of simulation from AVISPA tool for security and authentication verification of the current network prototype.

Count of ledgers to be used is undefined for now. Consensus algorithm used by the ledgers to verify the block in unknown. Location of the ledger server is unknown. And who will be assigned ledger part.

Reference

- "Is 5G Handover Secure and Private? A Survey" Dongsheng Zhao, Zheng Yan, Senior Member, IEEE, Mingjun Wang, Peng Zhang, and Bin Song, Senior Member, IEEE
- Security for 4G and 5G cellular networks: A survey of existing authentication and privacy-preserving schemes Mohamed Amine Ferraga,b,∗, Leandros Maglarasc, Antonios Argyrioud, Dimitrios Kosmanosd,
- A. Talukdar, M. Cudak, and A. Ghosh, "Handoff rates for millimeterwave 5G systems," in Proc. 79th IEEE Veh. Technol. Conf. (VTC), 2014, pp. 1–5.
- A. K. Sutrala, M. S. Obaidat, S. Saha, A. K. Das, M. Alazab, and Y. Park, "Authenticated key agreement scheme with user anonymity and untraceability for 5genabled softwarized industrial cyber-physical systems," IEEE Transactions on Intelligent Transportation Systems, 2021
- R. Canetti and H. Krawczyk, "Universally composable notions of key exchange and secure channels," in International Conference on the Theory and Applications of Cryptographic Techniques. Springer, 2002, pp. 337–351
- https://www.digi.com/blog/post/5g-network-architecture
- https://sites.google.com/view/ansuman/wireless-communications-and-networks?authuser=0
- https://www.itu.int/en/mediacentre/backgrounders/Pages/5G-fifth-generation-of-mobile-technologies.aspx
- C.-C. Chang and H.-D. Le, "A provably secure, efficient, and flexible authentication scheme for ad hoc wireless sensor networks," IEEE Transactions on wireless communications, vol. 15, no. 1, pp. 357–366, 2015
- Burrows, M., Abadi, M., Needham, R.M.: A logic of authentication. Proceedings of the Royal Society of London. A. Mathematical and Physical Sciences 426(1871), 233-271 (1989).

- "Desynchronization resistant privacy preserving user authentication protocol for location based services", PK Roy, A Bhattacharya, Peer-to-Peer Networking and Applications 14 (6), 3619-3633
- "A group key-based lightweight Mutual Authentication and Key Agreement (MAKA) protocol for multi-server environment" ,PK Roy, A Bhattacharya, The Journal of Supercomputing, 1-28
- "Secure and efficient authentication protocol with user untraceability for global roaming services ", PK Roy, A Bhattacharya, Wireless Networks, 1-18