International Journal of Computational and Electronic Aspects in Engineering
Volume 3, Issue 4, December 2022, pp 76 - 83
https://doi.org/10.26706/ijceae.3.4.2211616

Improved Security and Handover Technique in (4G) LTE

Alhakam Ayad Salih

College of Art, Tikrit University, Iraq

Correspondence: alhakam.a.allawie@tu.edu.iq

Abstract :Mobile communications play a significant role in our daily lives and are receiving greater attention from researchers as a result of the information and network technologies' quick growth. To meet the public's need for high speed, the 3GPP organization suggested the LTE mobile system. The LTE employs a hierarchical key management to enhance secure data transmission. However, the existing system lacks backward security and is susceptible to attack during the X2 handover procedure. We suggest an improved security feature by group key to address the mentioned problems and guard against malicious base stations and malicious attacks during the LTE x2 handover operation.

Keywords: eNB, X2 Handover, Security, LTE.

Article – Peer Reviewed
Received: 2 Dec 2022
Accepted: 16 Dec 2022
Published: 22 Dec 2022

Cite this article: Alhakam Ayad Salih, "Improved Security and Handover Technique in (4G) LTE", *International Journal of Computational and Electronic Aspects in Engineering*, RAME Publishers, vol. 3, issue 4, pp. 76-83, 2022.

https://doi.org/10.26706/ijceae.3.4.2211616

1. Introduction

Mobile wireless communications are becoming more and more common and necessary for daily life. The Third Generation Partnership Project (3GPP) Group suggested the advanced mobile technology, LTE (4G), to transfer multimedia data with greater speed service [1]. Its structure is shown in Figure 1, which offers a service that is more reliable, low-latency, and secure. The 4G offers several key management features to achieve secure connection.

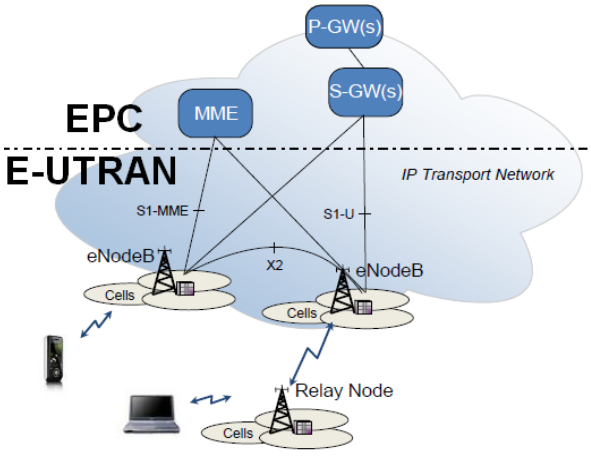

Figure 1. LTE Architecture

The base station is known as eNB, and the MME entity is responsible for charging for mobility management as shown in Figure 1. Two different handover processes exist. The MME must communicate the most recent parameters to the target base station in order for it to generate the session key during the S1 vertical handover. In the case of the X2 horizontal handover, the source base station delivers the necessary data directly to the target eNB. Since the source eNB and mobile user (UE) are not authorized by the target eNB, the X2 handover process is susceptible to attack.

In articles [2], the backward security problem and de-synchronization attack were discussed. In this assault, the series keys for target stations are generated from of the key generation sequence, and if the source node key is stolen, this poses a challenge for privacy. In the next part, we are going to talk about the holes in the security. The deployment of a group key in order to maintain a secure communication between these stations and also the MME entity is discussed [3]. After that, we will conduct a security analysis, and then we will draw a conclusion. This is done so that the security features can be improved.

2. X2 Handover

2.1 X2 Protocol

Compared to the legacy 3GPP technologies, handover architecture, deployment, and implementation have completely changed. The Radio Network Controller (RNC), a component of the network that is responsible for handling any handover signaling capabilities, was supplied by Universal Mobile Telecommunications System (UMTS) technology. RNC has been eliminated in LTE Evolved Packet System (EPS), and intelligence is now stored on the eNB side, which is in charge of handover [4]. For eNBs to signal with one another for handovering, a link must be established. This is controlled by the X2 Application Protocol interface (X2-AP).

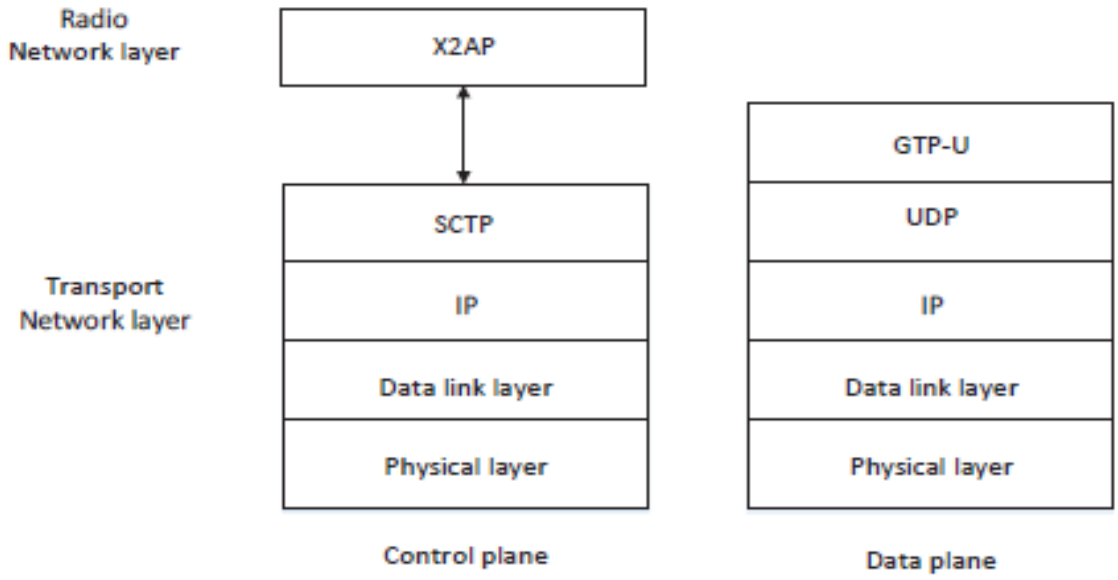

Figure 2. Control-plane and data-plane eNB X2 protocol stack

One eNB can establish an X2 interface with its neighbors in order to exchange the data needed. As a result, unlike the S1 interface, which has a star topology, full mesh topology, is just not required. Additionally, the protocol structure over the X2 interface includes a same data and control planes protocol stack as illustrated over the S1 interface in Fig 2. Both X2 topology and X2-AP structure both offer benefits for the data forwarding operation, Handover can be carried out via MME utilizing the S1 interface in the event that the connection is banned or the X2 interface is not setup. [5], we note the handover mechanism in simple way in fig 3.

The Automatic Neighbor Relation Function (ANRF) or configuration-based neighbor identification phase is where the initialization of the X2 interface begins. After then, the neighbor's TNL address is used to set the Transport Network Layer (TNL). The X2 setup procedure can be launched once the TNL is formed in order to share the application-level data required for two eNBs to function properly via the X2 interface. Figure (3) show simple call flow in LTE, the X2 Setup Request is sent specifically from the source eNB (i.e., the starting eNB to which the UE is attached) to a targets eNodeB. (i.e i.e., the prospective eNB that the UE intends to transfer) [6]. The X2 Setup Response is returned by the destination eNB.

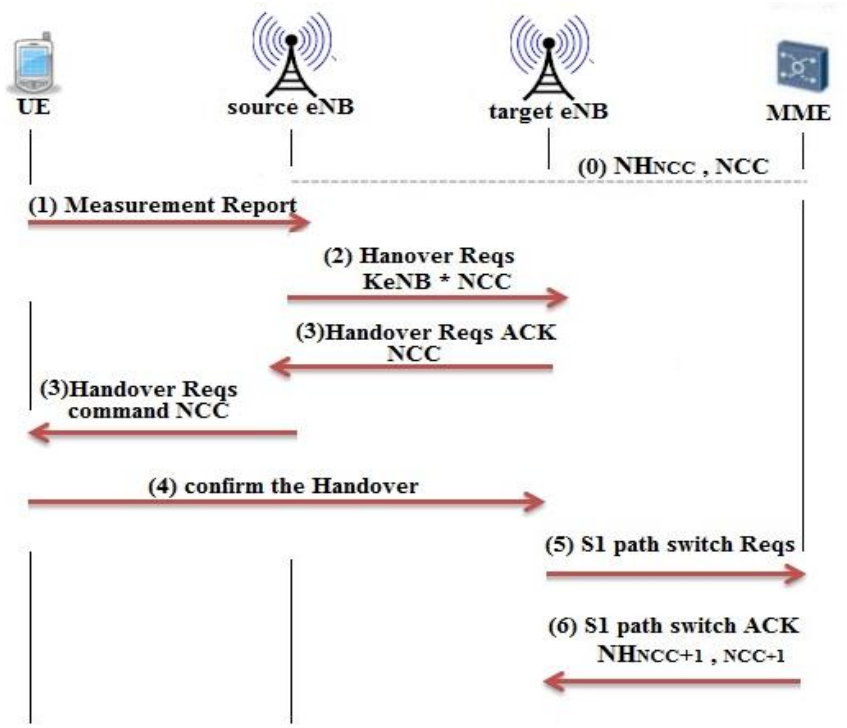

Figure 3. default diagram for X2 handover

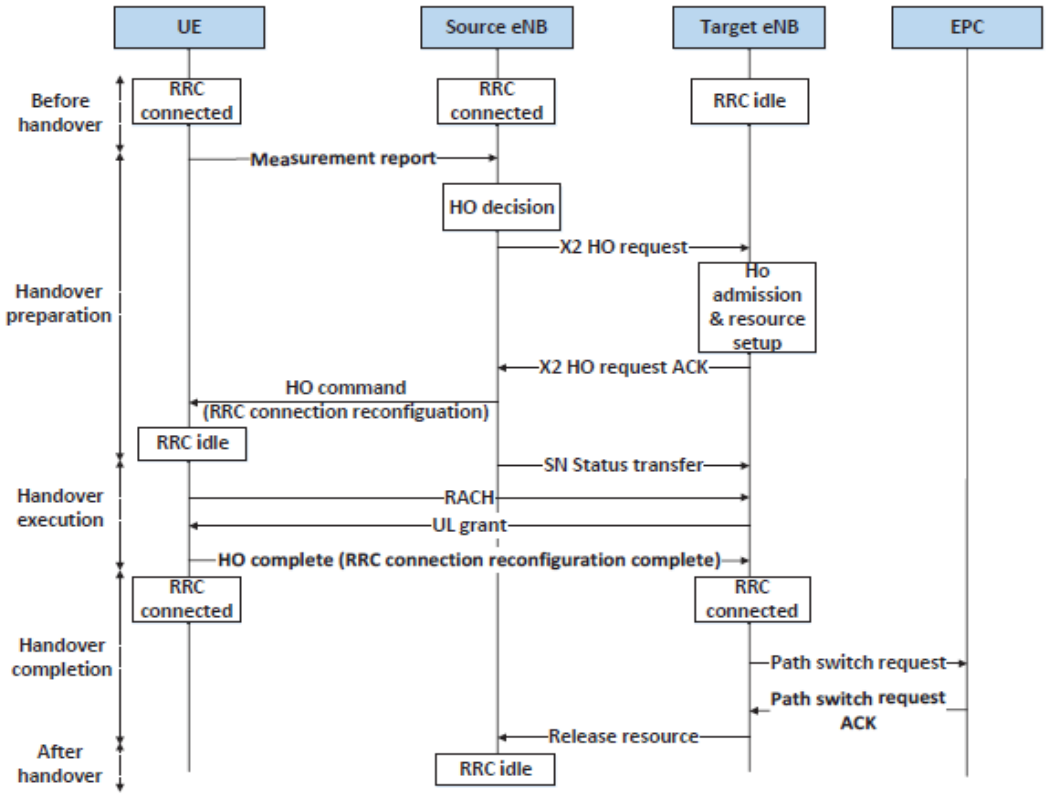

Figure 4. LTE X2 handover Procedure.

The steps that make up the finished X2 technique are depicted in Figure 4. the UE is connected to the source eNB before to handover. Through the established Dedicated Radio Bearers (DRBs) and Signaling Radio Bearers, UL/DL communication is transmitted between both the source eNB and the UE (SRBs).

The user equipment (UE) keeps all of the resources that have been allocated to it by E-UTRAN and EPC, and it maintains its state as Radio Resource Control (RRC)-Connected, EMM-Registered, and ECM-connected with respect to a eNB which is its source, after that the handover Prepping stage was started, the UE sends the source eNB the periodic measurement report, which includes details about the surrounding cells. Based on the reported measurement findings [7], the source eNB initiates the handover and selects the UE's top-reported target cell. Next, the source eNB contacts the target eNB with an X2 handover ask. The required information for the handover was contained in this signal, including the Target Cell ID, Radio Access Bearer (RAB) context, and UE context information. The target eNB executes call admission control while taking into account the QoS in the RAB context, and if it is able to provide the new UE with the requested resources, it sends a handover (HO) request acknowledgment (ACK) to the source via the X2 direct tunnel configuration. The source eNB receives this message in a transparent container that also contains the RRC Connection Reconfigure- ration message and also the GTP-U tunneling setup for every radio access data radio bearer, which the source eNB must then send to the UE.

An RRC packet contains L1/L2 information that are delivered to the UE, so that it can synchronize with the target eNB. The source eNB then sends the HO command message [8], which contains the RRC Connection Reconfiguration message to the UE, An X2 failure message is returned to the source eNB by the destination eNB if it is unable to accept the Ho request (because of load or the necessary configuration). The UE states are unaffected at this phase.

The third stage is the handover implementation, after receiving the RRC Connection Reconfiguration message, the user equipment (UE) transitions to the RRC idle state, which causes the source eNB to be detached. The Sequence Number (SN) status transfer signal, which comprises the PDCP sequence numbers, is transmitted from the source eNB to the target eNB over the X2 interface. This message is sent by the source eNB. First data item that was missing from UL has been added, and the subsequent sequence number is going to be assigned to DL. After the user equipment (UE) has completely finished the handover to the destination eNB, it will sync with the destination and according to settings that have been specified, after that the HO Confirmation signal is sent, with the RRC Connection modification final provided, as a consequence of this, with respect to the target eNB, the UE moves from the RRC disconnected state to the RRC connected state. In terms of UE synchronization, If a dedicated random access preamble has been received in the RRC Connection Reconfiguration message, the UE is not required to perform the random access procedure, widely known as contention free Random Access Channel (RACH) process. Otherwise, the UE employs the common random-access method described in [9].

Completing the handover process is phase four. The RRC message triggers the route switch procedure in both the destination eNB and MME/S-GW. Prior to any fresh packets arriving from the Supplying Gateway (S-GW), the aim eNB begins passing all information received from the X2 interface to the UE, following receipt of the destination eNB's UE release context message, the source eNB's UE context is then released.

At this time, the S1 bearer that was initially established between the source eNB and the UE is likewise released. The UE is connected to the target eNB following the Handover. The DRB and SRB are established, and UL/DL traffic is transmitted in the same manner like in the first step.

2.2 Handover Criteria and Parameterization

In theory, the LTE network configuration takes hexagonal architecture for eNB deployment into account. Let B represent the quantity of deployed eNBs, and let rdBm[k] represent, in dBm scale, the Reference Signal Received Power (RSRP) from each base station (BS) at time k 2 for each I I = 1,... B. The radio resource control (RRC) layer employs an Exponential Moving Average (EMA) filter to average data in order to smooth out any sudden RSRP fluctuations [10]. (i.e., L3 filtering). Because they are filtered away, high frequency fluctuations can be disregarded. The filtered signal is represented by the following dBm value:

$$r_i^{-dBm}[k] \triangleq (1-\alpha) r_i^{-dBm}[k-1] + \alpha r_i^{dBm}[k] \qquad \ldots\ldots (1)$$

in which, 2q/4, and q 2 F 3. A set of handover parameters are used during the handover process. Here, we make reference to both their definitions and the fields they are associated with in the respective RRC layer structures, i.e., Report Config EUTRA, Meas Object EU- TRA, and Quantity Config EUTRA; see also [11]. The parameters that could be changed are, specifically:

- Hysteresis (hys): This event's hysteresis parameter, i.e. hysteresis as defined in Report Config EU- TRA.
- OFN : the neighbor cell frequency's frequency-specific offset , i.e., offset Freq as defined in Meas Object EUTRA.
- OFS : the serving cell frequency's frequency-specific offset, i.e., offset Freq as defined in Meas Ob- ject EUTRA.
- OFF : This event's offset parameter, i.e., a3-offset as defined within Report Config EUTRA for this event.
- L3 Filtering coefficient RSRP/Reference Signal Received Quality (RSRQ) (q): This parameter, which is defined under Quantity Config EUTRA, is for the EMA filter as defined in equation (1).

A very well handover category is based on the RSRPs test method, which includes hysteresis and handover offsets, and is frequently employed in conventional HO decision algorithms for mobile communication systems (also used in 3GPP LTE). In particular, the A3 occurrence and its situation, which serves as a factor for cell choosing, are the subject of this research. The standard is as follows:

$$r_n^{-dBm}[k] + ofn + ocn > r_s^{-dBm}[k] + ofs + ocs + hys + off \quad \text{…. (2)}$$

with n 2 I s and stands for the neighbor cells and s 2 I represents the serving cell. Finally, the above-described definitions are applied to the handover parameters that are part of Eq. (2).

The aforementioned inequality is understood to mean that when a neighbor cell's RSRP (calculated as the total of the near RSRP and offsets, rdBmn [k] + ofn + ocn) exceeds that of the serving BS (calculated as the total of signal strength and offset, rdBms [k] + ofs+ ocs), and the distinction is larger than the value of off, the handover buffer between the source and the destination cell is represented by the term "hysteresis" (hys). The disparity can finally be condensed as follows:

$$r_n^{-dBm}[k] + S > r_s^{-dBm} \quad \text{…….. (3)}$$

where S equals ofn plus ocn, which then becomes ofs, ocs, hys, and off. The S may be calculated by adding up all of .the offsets, including the consequences of all the offsets on the process of triggering the handover condition

2.3 Handover Delay

The delay that occurs during the changeover may be broken down into two main classifications:

1. 1-the protocol delay, which accounts for the processing time and handover signaling delay.
2. 2-the transport delay, which accounts for the transmit process time across the physical medium of the X2 link, for those interested in a further level of specificity [12], The following is a definition of what constitutes an average delay estimate for a handover:

$$Delay_{Ho} = T_{Before\_Ho} + T_{Ho\_Preparation} + T_{Ho\_Exccution} + T_{Ho\_Completion} + T_{Margin} \quad \text{…… (4)}$$

From equation 4 we found :

While $\boldsymbol{T_{Before\_Ho}}$ is the amount of time needed to look for and locate the target cell's identification. This only applies to handovers that are initiated by the network (such as load-balancing); otherwise, it is 0.

When the RRC Connection Reconfiguration message is received from the source eNB, the UE transitions from the RRC connected state to the RRC idle state during the $\boldsymbol{T_{Ho\_Preparation}}$ period.

This delay, which is set to 10 ms, comprises the processing and transportation for X2-AP. The $\boldsymbol{T_{Ho\_Exccution}}$ parameter, which is set to 35 ms for contention-based random access with a very low probability of collision, represents the time to acquire the random access (contention-free or contention-based) and receive an uplink resource grant for

sending the RRC Connection Reconfiguration complete message. Given that the UE is already in the target eNB's RRC connected state, $T_{Ho\_Completion}$ Delay for the UE is 0. The implementation-dependent margin time with an upper bound of 20 ms is known as T_{Margin}. The whole handover delay budget is therefore calculated to be 65 ms.

2.4 Security Weakness

The horizontal X2 and the vertical S1 handovers are the two types of handovers that the 4G EPC is capable of supporting [13]. In this work, our primary focus is on the security flaw associated with the X2 handover as well as key management. Because the target eNB doesn't authenticate the source eNB and UE during the X2 handover, it leaves itself open to the possibility of an attack [14]. The following are the several weak points:

2.4.1 Methods and Materials

An LTE key management method includes a key-chaining design. With this architecture, the current eNB is able to generate new keys for subsequent target eNBs using the present key together with parameters that are unique to the target eNB. As can be seen in Figure 2, the source station initiates a handover request and then transmits it to the target eNB [15] , using the formula KeNB* = KDF(KeNB, PCI, EARFCN-DL). After a threat actor has successfully compromised the source eNB, the KeNB* may be acquired. It is possible to deduce directly from KeNB* the following session keys that will be used between a UE and the target eNB. This architecture of handover key-chaining will not be successful in achieving backward security.

2.4.2 Attacks through de synchronization

As shown in Figure 2 (x2 handover) Suppose for the sake of this argument that an unauthorized base station may successfully mimic the capabilities of an authorized base station. The malicious eNB gives the attacker the ability to thwart the update of the NCC value.

The MME will either send the NCC to the target eNB (signal number 0 or between the eNBs signal number 2), or at signal (6), the MME will send the S1 path switch acknowledgement message. Because of this scenario, the updated value of NCC will cause de-synchronous value to be stored in UE [16]. This will require the targeted eNBs to only complete horizontal handover key derivation, which will leave future session keys susceptible to being hijacked.

2.5 The Suggested Design

Here we suggest a technique based on group key to enable quick and secure changeover mechanisms in the present 4G LTE protocol. This can be done without requiring large modifications to the existing architecture.

The key hierarchical structure is depicted in Figure 5, and it demonstrates how the source eNB and the destination eNB re able to authenticate one another and create a secure connection when the share key KMGK is pre-distributed to all of the eNBs. Because our plan does not include any third parties in the handover method, the amount of time needed for verification is cut down significantly.

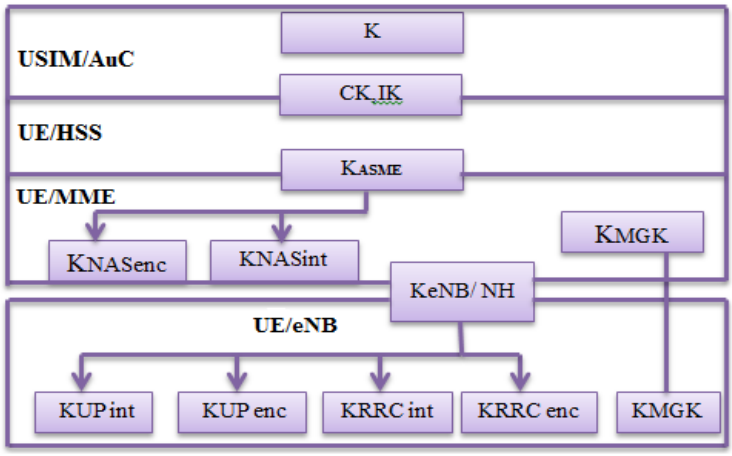

Figure 5. Key hierarchy

2.5.1 Initial Environment Settings

An Authentication and Key Agreement (EPS-AKA) takes place between a User Equipment (UE) and a Mobile Network Entity (MME) on behalf of the Home Subscriber Server (HSS)/Authentication Center whenever a UE establishes a connection to the EPC over the E-UTRAN (AuC). Following the completion of an initial AKA process, an MME and a UE are required to derive a KeNB and a Next Hop parameter (NH) using the KASME. The generated KeNB can then be used in the secure communication that takes place between a mobile user UE and an eNB.

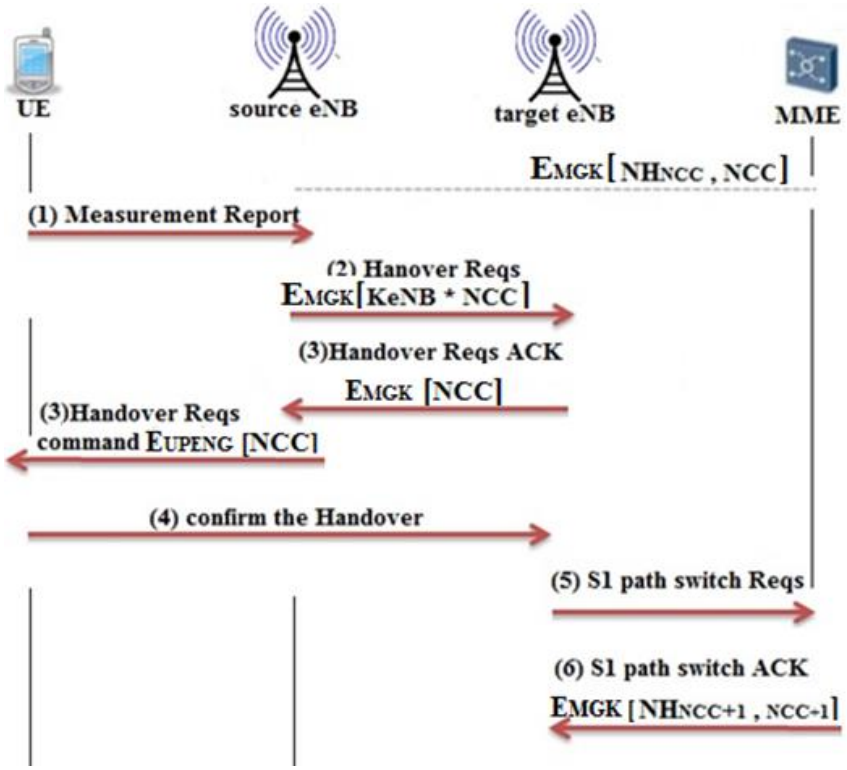

Figure 6. The Suggested X2 handover

In addition, every eNB and MME has a group key known as KMGK that all of them share [17]. This key can be used by eNBs to authenticate one another in preparation for an upcoming X2 handover operation.

2.5.2 The proposed X2 handover

The associated eNB (As show in figure 6) is able to acquire new key parameters from the MME. Those parameters are NHNCC and NCC. There are two primary factors that contribute to its formation. One is for the handover in the horizontal direction, the first one is:

$$K_{eNB}^{*} = KDF\ (K_{eNB}, PCI, EARFCN\text{-}DL) \quad \ldots. (5)$$

The second handover in the vertical direction, and the key generation goes as :

$$KeNB^{*} = KDF\ (NHNCC, PCI, EARFCN\text{-}DL) \quad \text{where} \quad NHNCC = KDF(KASME, NHNCC\text{-}1) \quad \ldots. (6)$$

When the source eNB does not contain a correct NH value, the KeNB* is produced from the currently active KeNB. This is referred to as a horizontal key. This could occur in the event that the "NH, NCC" does not arrive in time before the X2 transfer is carried out.

The KeNB* is formed from the NH parameter, and this derivation is known as a vertical key derivation. This derivation occurs only when the source eNB has a newly generated NH key accessible. Figure 5 shows that the source eNB is equipped with a new NH key that was obtained from the MME. Because NHNCC is generated from the previous NH value as well as KASME, only MME and UE have the ability to derive NH.

The Initial stage Perform the X2 handover procedure when the source eNB receives the signal measurement from the UE and the signal noise ratio (Signal Noise Ratio) is lower than anticipated. As seen in Fig. 4, it will transmit the encrypted EMGK [KeNB*, NCC] pair to the target eNB, in Step two the source eNB sends the target eNB the handover request using EMGK [KeNB*, NCC].

The session keys between the target eNB and the UE are acquired, namely KeNB* and NCC. in third step t the encrypted EMGK [NCC] is returned to the UE by the target eNB via the source eNB. The UE will verify that the value it received from the NCC matches the value it has stored in order to synchronize. The UE runs the new KeNB*= KDF, the vertical handover key derivation (NHNCC, PCI, EARFCN-DL). The security link is then established with the target eNB, after that the target eNB receives a confirmation of handover from UE, during the next step the t Targeted eNB transmitted an S1 path switch request message to MME, in final step, KDF is used to compute the NH key's fresh value (NHNCC+1) (KASME, NHNCC), In preparation for the subsequent X2 handover, MME sent "NHNCC+1, NCC+1" back to the Target eNB encrypted using KMGK.

3. Conclusion

The LTE network design has a relatively flat architectural style, making it susceptible to several kinds of threats. It is challenging to guarantee the safety of the LTE x2 handover. In order to defend ourselves from the malicious base station and protect ourselves from the harmful assaults that may occur during the LTE x2 handover procedure. The purpose of this research project is to investigate the feasibility of employing group key go in order to address the concerns regarding the safety of the LTE x2 handover method. The authentication architecture of our scheme has been improved. Our handover strategy is more secured and much more efficient than the 3GPP X2 handover technique. Compare and contrast with that scheme.

Reference

[1] S. Oh, B. Ryu, and Y. Shin, "Epc signaling load impact over s1 and x2 handover on lte-advanced system," in 2013 *Third World Congress on Information and Communication Technologies (WICT)*, Dec 2013, pp. 183–188.

[2] 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, May 2012, pp. 2119-2131.

[3] D. Forsberg, LTE key management analysis with session keys context, *Computer Communications* 33 (16) (2010) 907–1915.

[4] Q. Xiao, W. Zhou, B. Cui, and L. Li, "An enhancement for key management in LTE/SAE X2 handover based on ciphering key parameters," *Proc. - 2014 9th Int. Conf. P2P, Parallel, Grid, Cloud Internet Comput.* 3PGCIC 2014, pp. 256–261, 2014, doi: 10.1109/3PGCIC.2014.73.

[5] M. A. MOHAMED, "Handover Management Optimization over LTE A Network using S1 and X2 handover," no. August, pp. 58–64, 2018, doi: 10.15224/978-1-63248-157-3-11.

[6] S. Oh, B. Ryu, and Y. Shin, "EPC signaling load impact over S1 and X2 handover on LTE-Advanced system," 2013 *3rd World Congr. Inf. Commun. Technol. WICT 2013*, pp. 183–188, 2014, doi: 10.1109/WICT.2013.7113132.

[7] M. Assyadzily, A. Suhartomo, and A. Silitonga, "Evaluation of x2-handover performance based on rsrp measurement with friis path loss using network simulator version 3 (ns-3)," in *Information and Commu- nication Technology (ICoICT)*, 2014 2nd International Conference on, May 2014, pp. 436–441.

[8] I. D. Moscholios, "Evaluation of Multirate Loss Models for the X2 Link of LTE Networks," no. July, 2020.

[9] 3rd Generation Partnership Project; Technical Specification Group Radio Acess Network; Medium Acess Control (MAC); Protocol specification (Release 10); Technical Specification TS 36.321 v10.6.0.[Online]. Available: http://www.3gpp.org

[10] S. Sesia, I. Toufik, and M. Baker, LTE, The UMTS Long Term Evolution: From *Theory to Practice*. *Wiley Publishing*, 2009.

[11] 3GPP. 3rd Generation Partnership Project; Technical Specification Group Radio Acess Network; Radio Resource Control (RRC); Protocol specification (Release 10); Technical Specification TS 36.331 v10.6.0.[Online]. Available: http://www.3gpp.org

[12] 3GPP TR 25.912, "Feasibility Study for Evolved Universal Terrestrial Radio Access (UTRA) and Universal Terrestrial Radio Access Network(UTRAN), Version 12.0.0," Tech. Rep., 2014.

[13] A. Bohk, L. Buttyn, L. Dra, An Authentication Scheme for Fast Handover between WiFi Access Points, in: *Proceeding of ACM Wireless Internet Conference (WICON 2007)*,October 2007, pp.22–24.

[14] D. Forsberg, LTE key management analysis with session keys context, *Computer Communications* 33 (16) (2010)907–1915.

[15] Y. Lin and C. Yang, "Enhanced 4g Lte Authentication And Handover," no. 9, pp. 45–47, 2015.

[16] C.Han and H.Choi, Security Analysis of Handover Key Management in 4G LTE/SAE Networks, *IEEE Transactions On Mobile Computing*, Vol. 13, No. 2, February 2014.

[17] K. Alexandris, N. Nikaein, R. Knopp, C. Bonnet, and A. X. A. Protocol, "Analyzing X2 Handover in LTE / LTE-A," 2016.