International Journal of Cyber-Security and Digital Forensics (IJCSDF) 9(1): 1-11
The Society of Digital Information and Wireless Communications (SDIWC), 2020 ISSN: 2305-0011

GUTI-Based Multi-Factor Authentication Protocol for De-synchronization Attack Prevention in LTE Handovers

Vincent Omollo Nyangaresi[1], Silvance O. Abeka[2] and Anthony J. Rodrigues[3]

[1]School of Information Sciences and Technology, Kisii University, Kenya.

[2,3] School of Informatics & Innovative Systems, Jaramogi Oginga Odinga University of Science & Technology, Kenya.

ABSTRACT

The motivations behind the long term evolution (LTE) networks are low latency, high bandwidths and high data rates. The low latency requirement is tricky and cumbersome to achieve during handovers given that the communication process requires secure and privacy-preserving strategies and hence the introduction of authentication and encryption. Increased latency at cell boundaries leads to packet losses which results in denial of services, and is the reason behind lack of authentication during handover process in some cellular networks such as 2G. Unauthenticated handovers expose cellular communication to attacks such as eavesdropping, illicit modifications and traffic re- direction, all which compromise both confidentiality and integrity of the exchanged data. As such, a number of researchers have developed authentication strategies such as ticketing and group key security. However, these approaches concentrate on the security aspects of the handovers, ignoring the latency issues. In this paper, LTE tracking area partitioning is combined with advance figures of merit measuring and buffering to reduce latencies during the handover process, and hence permitted the incorporation of handover entities authentication. The simulation results indicated that our approach reduced the handover latency from 2.598 seconds for handovers without timing advance to an average latency of 0.048 seconds. In addition, a GUTI based authentication protocol was implemented that was observed to be resistant against attacks such as denial of service, de-synchronization, session hijacking, masquerade and network impersonation.

KEYWORDS: De-synchronization, Handovers, multi-factor authentication, Neuro-fuzzy, low latency, LTE security.

I. INTRODUCTION

In LTE specifications, signaling protocols were strengthened by requiring authentication and encryption (ciphering). However, [1] point out that LTE access network protocol still has several vulnerabilities that facilitate attacks that make LTE devices leak their locations. In their paper, [2] examined handover procedures in LTE and established that there is complexity in achieving seamless handovers, lack of backward security related to complex key management mechanism as well as lack of a uniform procedure structure. During inter- eNB handover, the serving eNB sends authentication parameters with session key to the target eNB though the X2 interface directly with no mutual authentication between the serving eNB and target eNB, making it vulnerable to attacks such as eavesdropping and masquerading attacks through rogue base station.

This is because the authentication parameters are exchanged among the UE, serving eNB and target eNB in clear text [3]. For the case of S1 handovers, MME sends recent parameters as clear text to the serving eNB through S1 to enable it generate a new session key to perform the handover process with the UE [4]. The subsequently capture of these parameters by an adversary using a rogue base station can disrupt and modify the refresh values of the authentication parameters, leading to desynchronizing attack.

In [5], the authors explain that in cellular networks, authentication occurs before any location update or call set up can be permitted into the network. In ideal situations, the authentication process takes 0.5 seconds. The accepted time interval between handover command and handover execution is 0.5 - 1.5 seconds. This means that, if the UE is to authenticate itself to the target eNB during handovers, then the authentication process will be a bottleneck since it may introduce further delays, leading to the dropping of an ongoing call. As such, cellular networks such as 2G do not perform any authentication during handovers.

Neuro-fuzzy optimization has been applied in fields such as adaptive control systems and system identification. In Fuzzy Logic (FL) mathematical models, human language is employed to express inputs as well as outputs and it offers a straightforward method of achieving a conclusion based on imprecise or ambiguous input information [6]. Low-complexity FL is suitable for wireless sensor networks (WSNs) and as such, [7] investigated FL-based routing path search for a maximum network lifetime and minimum delay. The fuzzy membership function was employed for formulating a multi-objective cost aggregation function that reflected the effects of all the objectives collectively as a scalar value.

To address the authentication and delay constraints during the handover process, this paper developed a Globally Unique Temporary Identifier (GUTI) based handover authentication and optimization protocol based on timing advance where the handover figures of merit are measured and buffered as the user equipment (UE) approaches the handover region. The GUTI has five components which are frequently refreshed and hence overcome the updating issues in the current Authentication and Key Agreement protocol (AKA). The contributions of this paper include the following:

I. We develop a GUTI-based protocol that addresses the root key updating issues in the current LTE AKA.
II. We partition the tracking area into three regions namely the No Handover Region (NHR), Low Probability Handover Region (LPHR) and High Probability Handover Region (HPHR) that facilitated timing advance by buffer handover figures of merit (FOM) whenever an UE was detected at the LPHR.
III. We develop a multi-factor authentication protocol composed of six parameters: the frequently refreshed GUTI, which we hash, salt and pad to further randomize the root key; the next chaining counter (NCC); next hop next chaining counter (NH_{NCC}); key derivation function (KDF); Physical Cell Identity (PCI); and E-UTRAN Absolute Radio Frequency Channel Number on the Download (EARFCN-DL) are utilized to authenticate the handover entities.
IV. We demonstrate that (II) above prevents denial of service (DoS) while (I) and (III) render the handover resistant against de-synchronization, session hijacking, masquerade and network impersonation attacks. In so doing, both (I) and (III) assure both confidentiality and integrity of the communication process.

The rest of this paper is organized as follows: Section (II) illustrates related work in as far as LTE handover and security are concerned while section (III) provides the methodology that was adopted to achieve the results presented and discussed in section (IV). Lastly, part (V) concludes the paper.

II. RELATED WORK

Researchers in [8] proposed a scheme based on pre-loaded shared group key between all eNBs and MME to address de-synchronization attacks. However, this scheme does not completely solve de-synchronization, replay and redirection attacks. Further, [9] proposed an authenticated key management scheme for intra-MME handover where the MME acts as a third party and the source eNB is kept out of the key management process. The scheme partially achieves mutual authentication between handover entities by employing pre-shared key for each eNB to protect the handover parameters exchanged between eNBs and the MME. Unfortunately, this technique increases the communication overheads of handover process.

The hierarchical SDN based handover proposed by [10] exhibit very high communication and signaling overhead that result in increased handover delay and packet losses while the vertical handover framework developed by [11] takes longer durations in making handover decisions. On the other hand, the SDN-UAV proposed by [12] cannot be supported by future network such as 5G due to network architecture complexity, high energy consumption, high costs and short lifespan of UAVs.

The handover management with fuzzy logic designed by [13] concentrates only on increased resource utilization for higher successful connections, fewer calls blocking and dropping. User authentication using wireless smart card has been proposed but this method lacks user friendliness, does not provide user anonymity and unfairness in key agreement. In [14], the authors developed a novel anonymous roaming authentication scheme (ARHAP) for the LTE-A based VANETs, but it employs elliptic curve public key cryptography which is computationally intensive.

In [15], a new Lightweight Intelligent authentication protocol that assigns each eNB a certificate issued by Certificate Authority (CA) is designed. This CA may become a bottleneck when several handovers are executed in LTE networks. Researchers in [16] employed the concept of Mobile Relay network (MRN), but which experiences long delays and does not authenticate the UEs. In [17], an X2-based handover in a SDN-based and partially virtualized LTE networks is designed. This technique excluded other mobility management aspects such as handover decision, network selection, and admission control.

The authors in [18] present a handover authentication scheme based on USIM and ECC for 5G-WLAN heterogeneous networks. However, there are many computational issues over the elliptic curve cryptosystem, hence this technique yields high handover latency. In [19], a 4G double authentication scheme handover in which the target generates its own key for future communications instead of using the one generated by the source node is proposed. However, this technique falls short of protecting the handover process due to lack of mutual authentication between handover entities, coupled with inexistence of backward and forward keys separation.

Researchers in [20] and [21] described how network operators can establish an optimal interval for root key updates to protect the LTE network from de-synchronization attacks. Unfortunately, this reduces the efficiency of the entire network by increasing communication overheads. Authors in [22] introduced cell radio network temporary identifier (C-RNTI) to thwart de-synchronization attacks in LTE handovers. However, this led to high communication and computation costs due to increased communications between the entities.

III. METHODOLOGY

In this paper, timing advance was achieved by partition the tracking area into three regions, NHR, LPHR and HPHR, measuring and buffering the handover figures of merit in Home Subscriber Server (HSS) before the actual handover detection. At the center of all these regions is the serving eNB and the UE is free to move to any of these regions at any particular time. At NHR, the signal strength from the source eNB is very strong, and so the UE should not scan the neighbouring cells. When at LPHR, the signal strength from source eNB is relatively strong, and at this point, the UE may start analyzing beacons from the surrounding cells and send this information to the MME.

At the HPHR, the serving eNB signal strength is very weak and the UE should be handed- over to a cell with better figures of merit. The neuro-fuzzy architecture was significant during the handover decision making phase as it helped optimize this process. Its main components were the knowledge base, database, inference engine, and the explanation facility.

The knowledge base consisted of handover conditions expressed in modus ponens statements that evaluated to HIGH or LOW. The database on its part acted as a repository of all measured handover FOMs such as power density, received carrier power, traffic density, call blocking probability and path loss.

The inference engine was instrumental in linking the rules in the knowledge base and FOMs in the database, and hence facilitated the execution of the handover decisions. The explanation facility provided justification for the choice of the target eNB. The neuro-fuzzy rules combines the various criteria using AND or OR logic connectors to arrive at appropriate conclusions, which can be to deny or grant the handover to the mobile user. At any given moment during the time when the UE is in the cell overlapping region, the MME utilized this proposed handover to reduce the handover latency and the attacks.

Regarding the authentication phase, it consisted of 18 steps and it employed Hashed Message Authentication Code- Secure Hashing Algorithm (HMAC-SHA-512) as the key distribution function (KDF). To overcome horizontal key derivation that may compromise forward key secrecy, the frequently refreshed hashed salted padded form of GUTI shown in Figure 1 was employed as the root key, $K_{ASME.}$ The GUTI comprised of the Globally Unique MME Identifier (GUMMEI) and MME Temporary Mobile Subscriber Identity (M-TMSI) which was 32-bits in length. The GUMMEI consisted of the Public Land Mobile Network Identifier (PLMN ID) and the MME Identifier (MMEI).

On its part, the PLMN ID comprised of the Mobile Country Code (MCC) that was 12 -bits in length, and the Mobile Network Code (MNC) which was 12 or 8- bits long.

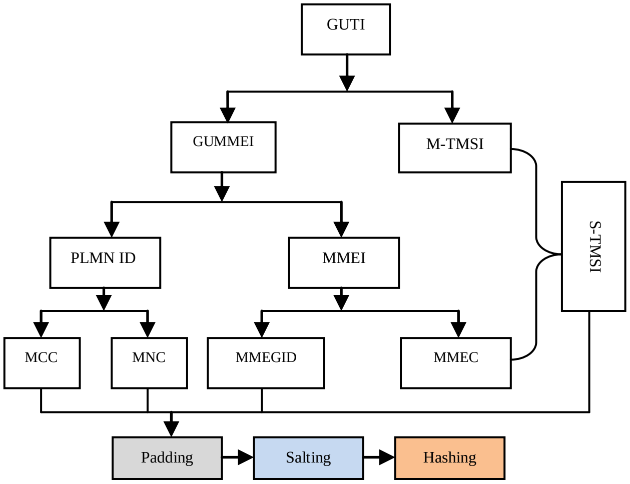


Figure 1: Salted GUTI Architecture

Since the mixing of MCC and MNC bits is not allowed in the 3GPP specification, the MNC bit length depends on the value of MCC and hence 12 bits were employed for MNC instead of 8 bits. The MMEI consisted of the MME Group ID (MMEGID) which was 16- bits in length and the MME Code (MMEC) that was 8-bits long. A combination of the MMEC and M-TMSI formed the System Architecture Evolution Temporary Mobile Subscriber Identity (S-TMSI) that was therefore 40 –bits long.

GUMMEI peculiarly identifies an MME that has allocated a particular GUTI while the M-TMSI uniquely identifies an UE within an MME using the allocated GUTI. The S-TMSI is a temporary UE identifier provided by the EPC to peculiarly identify an UE within a tracking area. The PLMN ID uniquely identifies a particular network and consists of an MCC to denote the UE home country and MNC that identifies the home PLMN of the UE. The MMEI uniquely identifies an MME within a certain network. In LTE-A, an MME pool is controlled by one or more MMEs and represents locations in which an UE can move without changing its serving MME.

Here, these MME pools are identified using MMEGID and an MMEC uniquely identifies a particular MME within these pools. The algorithm employed to simulate the salted GUTI is shown in Figure 2.

```
INPUT    : MCC, MNC
OUTPUT: Salted GUTI, hashed salted GUTI

BEGIN:
  /* GUTI is 80 bits long*/
        1.    Initialize MCC
        2.    Instantiate MNC
        3.    Generate M-TMSI, MMEC, MMEGID, SALT
        4.    Derive GUTI
              GUTI= binary(MCC)+binary(MNC)+binary(M-TMSI) +binary(MMEC)+ binary(MMEGID)
        5.    Derive Padded GUTI
              Padded_GUTI=binary(MCC)+binary(MNC)+binary(M-TMSI) +binary(MMEI)+binary(PAD_BITS)
        6.    Derive SALTED PADDED GUTI
              SALTED _PADDED_GUTI= Padded_GUTI +binary(SALT)
        7.    Compute hashed SALTED PADDED GUTI
              Hashed_ SALTED _PADDED_GUTI=hash (SALTED _PADDED_GUTI)
        8.    Buffer Hashed_ SALTED_PADDED_GUTI in HSS
END
```

Figure 2: Algorithm for Salted GUTI

Since GUTI consisted of five components which were frequently refreshed, it was considered an ideal root key. To execute handover entities authentication, the hashed salted padded GUTI is employed as the root key to achieve faster root key refreshment and hence thwart de-synchronization attacks. The salting and padding were utilized to further randomize the GUTI while hashing was executed to prevent reverse engineering the GUTI components.

The other parameters utilized for the authentication process included NCC, NH_{NCC}, KDF, PCI, and EARFCN-DL. As such, the authentication was truly multi-factored such that the capture and compromise of any of them would still render it difficult for adversaries to compute valid authentication keys. Here, the serving eNB computes K^*_{eNB} using UE GUTI as K_{ASME} as illustrated in Figure 3.

```
INPUTS     :  MCC, MNC, $PCI, EARFCN - DL$
OUTPUTS :  Salted GUTI, hashed salted GUTI, $K_{eNB}$, $K^*{}_{eNB}$, SH

BEGIN:
  /* $K^*{}_{eNB}$ and SH are 512 bits long* /
        1.    Initialize MCC, MNC
        2.    Instantiate HMAC_SHA_512 /* KDF for this protocol */
        3.    Generate M-TMSI, MMEI, SALT, PAD_BITS
        4.    Derive Hashed_ SALTED _PADDED_GUTI
        5.    Compute initial  $K_{eNB}$, $K_{eNB_0}$
              $K_{eNB}$ = Hashed_ SALTED _PADDED_GUTI$_0$ /* for initial padding and salting */
        6.    Compute $NH0$
              $NH0 = K_{eNB_0}$
        7.    Calculate  $NH1$
              $NH1$ = HMAC_SHA_512 (Hashed_ SALTED _PADDED_GUTI, $NH0$)
        8.    Derive $NH2$
        9.    $NH2$ = HMAC_SHA_512 (Hashed_ SALTED _PADDED_GUTI, $NH1$)
        10.   Compute $NH_{NCC}$
              $NH_{NCC}$ = HMAC_SHA_512 (Hashed_ SALTED _PADDED_GUTI, $NH_{NCC} - 1$)
        11.   Compute $K^*{}_{eNB}$
              $K^*{}_{eNB}$ = HMAC_SHA_512  ($NH_{NCC}, PCI, EARFCN - DL$)
        12.   Derive SH
              $SH = Hash\ (K^*{}_{eNB},\ NCC)$ /* NCC validation parameter */
END
```

Figure 3: Algorithm for Authentication Tokens Generation

As shown in Figure 3, the inputs to the authentication tokens generation included the MCC, MNC, PCI, EARFCN-DL while the outputs included the salted GUTI, hashed salted GUTI, K_{eNB}, K^*_{eNB} and NCC validation parameter, SH. In Figure 4, the proposed multi-factor authentication algorithm is presented. This figure shows that the input to the authentication process comprised of MCC, MNC, PCI, EARFCN-DL, hashed salted padded GUTI, K_{eNB}, K^*_{eNB} and SH. On the other hand, the outputs were the path switch requests and channel allocation commands.

```
INPUTS:   MCC, MNC, $PCI, EARFCN - DL$, hashed salted padded GUTI, $KeNB$, $KeNB^*$, SH
OUTPUTS:  Path switch requests, channel allocations

BEGIN:
  1.  Execute admission control /*channel reservation for incoming UE at TeNB */
  2.  SeNB computes $K*_{eNB}$
  3.  SeNB sends hashed $K*_{eNB}$ and NCC value via the X2 interface to the TeNB.
  4.  TeNB re-computes the hash in (3) above
  5.  IF hashes in(3) and (4) match THEN
  6.    TeNB sends authentication SUCCESSFUL message to the SeNB
  7.  Else
  8.    Explicitly deny handover request
  9.      SeNB acknowledges receipt of the message in (6) above
  10.       TeNB transmits NCC parameter to connect the UE with it
  11.         SeNB sends handover request command to the UE together with NCC sent from TeNB
  12.           UE confirms the handover message to the TeNB as its new SeNB
  13.             TeNB sends S1 path switch request message to the MME via S1 interface
  14.           MME receives path switch request and computes the fresh NH key and NCC values
  15.         MME sends S1 path switch request ACK message back to the new SeNB
  16.       MME sends  $NH_{NCC+1}$  and NCC+1 for next handover to the new SeNB
  17.   TeNB allocates the incoming UE the reserved channel
  18. MME instructs the previous eNB to release the channel for the just handed over UE
     ENDIF
END
```

Figure 4: Algorithm for the Proposed Multi-factor Authentication

The authenticated entities included the source eNB(SeNB), target eNB(TeNB) and the UE to be handed over. This authentication served to prevent attacks such as session hijacking, masquerading and network impersonation.

IV. RESULTS AND DISCUSSIONS

In this section, the simulation results are employed to demonstrate that the developed protocol was capable of preserving confidentiality, integrity and availability of the communication process.

To address the updating issues in the current AKA and hence thwart de-synchronization attack, GUTI components were refreshed after every handover as evidenced in Table 1 for the first five handovers.

Table 1: Periodic GUTI Refreshing

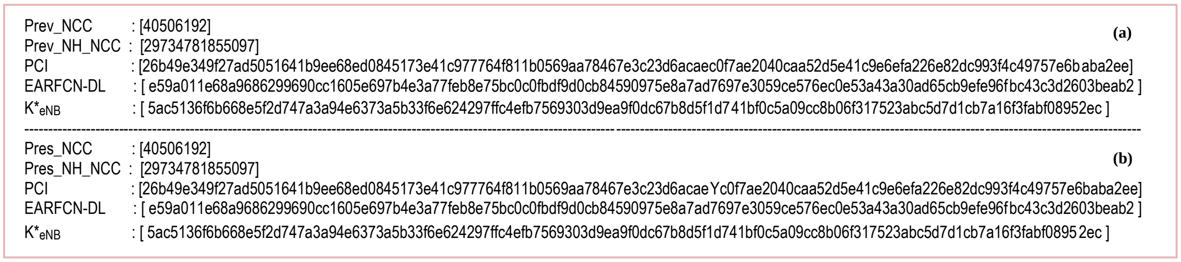
Handover	MCC	MNC	MMEC	MMEGID	M-TMSI
HO_1	001001111111	000000000010	01010111	0001110100011000	00011000011001001000110100100100
	(639)	(2)	(87)	(7448)	(409242916)
HO_2	001001111111	000000000010	01001100	0001101000011011	00101110001011001111001101011101
	(639)	(2)	(76)	(6683)	(774697821)
HO_3	001001111111	000000000010	00011011	0001111100101110	00101001100100000110011001111100
	(639)	(2)	(27)	(7982)	(697329276)
HO_4	001001111111	000000000010	01001101	0001001000111111	00110001101000110001110010010001
	(639)	(2)	(77)	(4671)	(832773265)
HO_5	001001111111	000000000010	00010110	0001100110101000	00001110011110110101110101001011
	(639)	(2)	(22)	(6568)	(242965835)

As shown in Table 1, the values of MCC and MNC remained constant at 639 and 2 respectively since they are globally assigned to a particular country and network respectively. In addition, the values for salting and padding were also refreshed after each and every handover as shown in Table 2 that follows. However, the values of MMEC, MMEGID and M-TMSI varied widely over the five handovers with the greatest variation being observed for the M-TMSI.

Table 2: Refreshment of Padding and Salting Parameters

HANDOVER	PADDING	SALTING
HO_1	00010010010001101010	00001100011110111011
	(74858)	(51131)
HO_2	00001001000001010110	00000001111011010011
	(36950)	(7891)
HO_3	00000101000000001110	00010100010000110001
	(20494)	(82993)
HO_4	00010010010101100010	00000011011001101111
	(75106)	(13935)
HO_5	00000110001000010101	00001000011100001011
	(25109)	(34571)

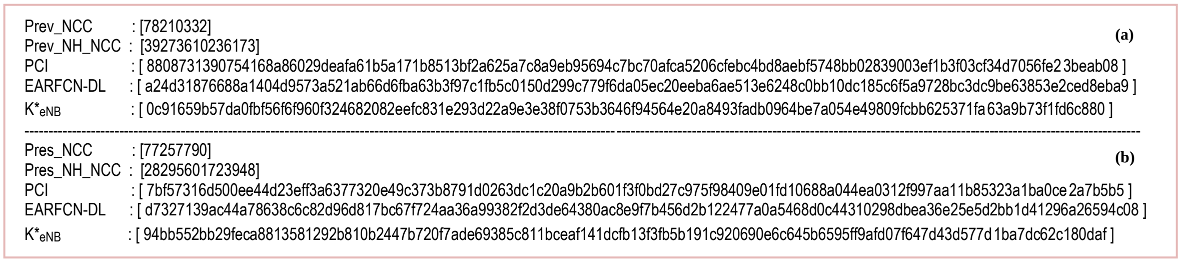
This is because the M-TMSI is provided by the EPC to temporary identify an UE within a tracking area and hence needed to be hard to guess or brute force in order to preserve the privacy and prevent disclosure of user identity. To demonstrate that the developed Protocol was resistant against de-synchronization attack, both horizontal and vertical key derivations were simulated. Figure 5 shows the vertical key derivation process where the previous NCC and the current NCC values match.



```
Prev_NCC      : [40506192]                                                                                   (a)
Prev_NH_NCC  :  [29734781855097]
PCI           : [26b49e349f27ad5051641b9ee68ed0845173e41c977764f811b0569aa78467e3c23d6acaec0f7ae2040caa52d5e41c9e6efa226e82dc993f4c49757e6baba2ee]
EARFCN-DL     : [ e59a011e68a9686299690cc1605e697b4e3a77feb8e75bc0c0fbdf9d0cb84590975e8a7ad7697e3059ce576ec0e53a43a30ad65cb9efe96fbc43c3d2603beab2 ]
K*eNB         : [ 5ac5136f6b668e5f2d747a3a94e6373a5b33f6e624297ffc4efb7569303d9ea9f0dc67b8d5f1d741bf0c5a09cc8b06f317523abc5d7d1cb7a16f3fabf08952ec ]
------------------------------------------------------------------------------------------------------------------------
Pres_NCC      : [40506192]
Pres_NH_NCC  :  [29734781855097]                                                                              (b)
PCI           : [26b49e349f27ad5051641b9ee68ed0845173e41c977764f811b0569aa78467e3c23d6acaeYc0f7ae2040caa52d5e41c9e6efa226e82dc993f4c49757e6baba2ee]
EARFCN-DL     : [ e59a011e68a9686299690cc1605e697b4e3a77feb8e75bc0c0fbdf9d0cb84590975e8a7ad7697e3059ce576ec0e53a43a30ad65cb9efe96fbc43c3d2603beab2 ]
K*eNB         : [ 5ac5136f6b668e5f2d747a3a94e6373a5b33f6e624297ffc4efb7569303d9ea9f0dc67b8d5f1d741bf0c5a09cc8b06f317523abc5d7d1cb7a16f3fabf08952ec ]
```

Figure 5: Vertical Key Derivation

As shown in Figure 5(a), the values of previous NCC (*Prev_NCC*) and present NCC (*Pres_NCC*) shown in Figure 5(b) match and as such, the K^*_{eNB} computed through vertical key derivation process using the parameters shown match. Horizontal key derivation was simulated by attempting to derive K^*_{eNB} using the current value of K_{eNB} whenever received NCC was greater than the current NCC. In Figure 6, the values of *Prev_NCC* and *Pres_NCC* are different and as such, an attempt was made to compute K^*_{eNB} based on the current K_{eNB}.



```
Prev_NCC      : [78210332]                                                                                   (a)
Prev_NH_NCC  :  [39273610236173]
PCI           : [ 8808731390754168a86029deafa61b5a171b8513bf2a625a7c8a9eb95694c7bc70afca5206cfebc4bd8aebf5748bb02839003ef1b3f03cf34d7056fe23beab08 ]
EARFCN-DL     : [ a24d31876688a1404d9573a521ab66d6fba63b3f97c1fb5c0150d299c779f6da05ec20eeba6ae513e6248c0bb10dc185c6f5a9728bc3dc9be63853e2ced8eba9 ]
K*eNB         : [ 0c91659b57da0fbf56f6f960f324682082eefc831e293d22a9e3e38f0753b3646f94564e20a8493fadb0964be7a054e49809fcbb625371fa63a9b73f1fd6c880 ]
------------------------------------------------------------------------------------------------------------------------
Pres_NCC      : [77257790]
Pres_NH_NCC  :  [28295601723948]                                                                              (b)
PCI           : [ 7bf57316d500ee44d23eff3a6377320e49c373b8791d0263dc1c20a9b2b601f3f0bd27c975f98409e01fd10688a044ea0312f997aa11b85323a1ba0ce2a7b5b5 ]
EARFCN-DL     : [ d7327139ac44a78638c6c82d96d817bc67f724aa36a99382f2d3de64380ac8e9f7b456d2b122477a0a5468d0c44310298dbea36e25e5d2bb1d41296a26594c08 ]
K*eNB        : [ 94bb552bb29feca8813581292b810b2447b720f7ade69385c811bceaf141dcfb13f3fb5b191c920690e6c645b6595ff9afd07f647d43d577d1ba7dc62c180daf ]
```

Figure 6: Horizontal Key Derivation

It is clear from Figure 6 that the value of the present NCC is less than the received NCC value and as such, the K^*_{eNB} in Figure 6 (b) was computed using the K^*_{eNB} in Figure 6 (a), which in this case was the current K_{eNB}. Since the values of the computed K^*_{eNB} in Figure 6 (a) and Figure 6 (b) are different, the horizontal key derivation failed.

Consequently, de-synchronization attack using horizontal key derivation as a vector failed as well. Another important aspect of the developed protocol was the handover entities authentication. In the current LTE authentication, when de-synchronization attacks occur, the UE and TeNB employ the current K_{eNB} to generate the next session key through horizontal key derivation. Once the subscriber has moved to TeNB, an attacker transmits altered data containing valid NCC until a new AKA procedure is invoked.

As such, an attacker can compute the next K_{eNB} before this new AKA procedure and hence forward security has been compromised and de-synchronization attack is possible. Other attacks that employ de-synchronization as a vector, such as session hijacking, replay, DOS, masquerade, and MitM are hence possible as illustrated in Table 3.

Table 3: Security Comparison of LTE and the Proposed Protocol

Security Feature	Standard LTE Protocol	Proposed Protocol	Security Goal Compromised
Forward Secrecy	No	Yes	Confidentiality
De-synchronization Attack	No	Yes	Confidentiality, integrity
MitM	No	Yes	Confidentiality, integrity
IMSI Interception	Yes	Yes	Confidentiality
Session Hijacking	No	Yes	Confidentiality, integrity, availability
Replay	No	Yes	Integrity
DOS	No	Yes	Availability
Masquerade	No	Yes	Confidentiality, integrity

In the developed protocol, de-synchronization attack is prevented by implementing an NCC validation phase that verifies that NCC value sent from SeNB to TeNB is the same one that is sent from the SeNB to the UE. Here, if these NCC values are not similar, handover request is explicitly denied as demonstrated in step (8) of Figure 4. As such, the developed protocol is robust against attacks that utilize de-synchronization as a vector. Such attacks include session hijacking, replay, DOS, masquerade, eavesdropping, and MitM.

The security of the developed protocol was also compared with other protocols, strategies and schemes that have been proposed to secure LTE and 5G networks. These include double authentication scheme, root key update, certificate authority based, and C-RNTI –based techniques as shown in Table 4. From Table 4, it is clear that only the proposed protocol, double authentication, and C-RNTI based techniques can assure authentication, confidentiality and integrity.

Table 4: Security Comparison of Proposed Protocol with other Techniques

Security Technique	Authentication		Confidentiality		Integrity		Trade-off
	SeNB	TeNB	SeNB	TeNB	SeNB	TeNB	
Double Authentication Scheme	Yes	Yes	Yes	Yes	Yes	Yes	High latencies
Root key update	Yes	Yes	Yes	No	No	No	Insecurity
Certificate authority based	Yes	Yes	Yes	No	Yes	Yes	High latencies
C-RNTI –based	Yes	Yes	Yes	Yes	Yes	Yes	Increased costs
MRN-based	Yes	Yes	No	No	No	No	High latencies
Proposed Protocol	Yes	Yes	Yes	Yes	Yes	Yes	One extra cost

In double authentication scheme, the TeNB generates its own key for future communication instead of utilizing the SeNB generated key. In so doing, forward secrecy is assured. Here, the UE compares the received NCC with its own and provided they are equal, TeNB key is generated via vertical derivation. However, the UE NCC received NCC are not equal, a request is sent to the HSS over the S1 interface for verification of the TeNB. The S1 interface carries heavy loads from the MME to various eNBs under its control and as such, this scheme can lead to long handover delays.

Although C-RNTI based techniques achieves authentication, its communication and computation costs are high due to the high number of communication between the handover entities. In the developed protocol, the extra one communication cost is incurred during NCC validation phase that verifies that NCC value sent from SeNB to TeNB is the same one that is sent from the SeNB to the UE. However, since this message flows through the less busy Uu interface, it does not lead to long handover delays.

In MRN-based technique, the emphasis is on MRN and the eNBs authentication, but authentication between the UEs and MRN is not carried out and hence is susceptible to MitM, and de-synchronization attacks. The root key update strategy does not assure TeNB confidentiality nor does it protect SeNB and TeNB integrity, hence is insecure. Regarding certificate based techniques, the security challenge is possibility of DOS due to long delays when multiple requests are made to the certificate authority.

To demonstrate that the developed protocol was resistant against DoS and hence upheld availability of the network resources, the handover durations in the LTE network without the partitioning of the coverage network were measured and compared with the handover durations when the tracking area partitioning was implemented. Table 5 gives the handover latencies for the twelve sampled handover instances. As shown in Table 5, different handovers experienced varied handover latencies.

It is also clear that the average handover latency was 2.498 seconds. In Table 6, the handover latencies after tracking area partitioning are presented.

Table 5: Handover Latencies without Timing Advance

Handover		**Latency (Secs)**
SeNB	**TeNB**	
eNB-3	eNB-1	2.808
eNB-5	eNB-1	2.917
eNB-7	eNB-6	2.957
eNB-5	eNB-4	2.651
eNB-2	eNB-3	2.296
eNB-3	eNB-1	2.371
eNB-7	eNB-6	2.493
eNB-7	eNB-1	2.739
eNB-5	eNB-4	2.502
eNB-3	eNB-1	2.407
eNB-7	eNB-6	2.649
eNB-5	eNB-1	2.384
Average Latency		**2.598**

It is evident from Table 6 that the handovers here experienced shorter latencies compared to the ones in Table 5. As such, partitioning the coverage area into NHR, LPHR and HPHR and starting probing neighbouring beacons at LPHR and buffering these values

Table 6: Handover Latencies with Timing Advance

Handover		**Latency (Secs)**
SeNB	**TeNB**	
eNB-7	eNB-6	0.042
eNB-5	eNB-4	0.033
eNB-3	eNB-1	0.036
eNB-2	eNB-3	0.033
eNB-7	eNB-6	0.074
eNB-5	eNB-4	0.039
eNB-3	eNB-1	0.025
eNB-7	eNB-1	0.057
eNB-2	eNB-3	0.025
eNB-3	eNB-1	0.076
eNB-7	eNB-6	0.040
eNB-5	eNB-4	0.078
Average Latency		**0.048**

in the HSS neuro-fuzzy database, and employing the neuro-fuzzy inferencing mechanism in selecting the most ideal target eNB greatly reduced the handover latencies. For instance, the average latencies in Table 5 were 2.598 seconds against an average latency of 0.048 seconds in Table 6. Consequently, this protocol was resistant against DOS that may lead to packet losses during the handover process.

V. CONCLUSION

In this paper, a GUTI-based handover authentication and optimization protocol has been developed and simulated. The simulation results demonstrated that the developed protocol was resistant against horizontal key derivation and hence de-synchronization attack and other attacks that utilize it as a vector were effectively thwarted. The protocol also facilitated faster handovers when the UE was detected at the HPHR. It is evident that handovers where timing advance was implemented exhibited lower latency compared with handovers without timing advance. This enabled the incorporation of authentication during the handover process to preserve subscriber privacy and ensure security of the communication process. Future work lies in the investigation of how the developed protocol performs in other cellular networks such as MANETs and WSNs. There is also need to validate the performance of the developed authentication protocol in terms of transmission load and space complexity.

REFERENCES

[1] Altaf, S., Ravishankar, B., Asokanz, N., Valtteri, N. and Jean-Pierre, S.: Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems. arXiv, pp. 1-16, (2017).

[2] Cao, J., Li, H., Ma, M., Y. Zhang, Y., and Lai, C.: A simple and robust handover authentication between HeNB and eNB in LTE networks, Comput. Networks, Vol. 56, No. 8, pp. 2119–2131, (2012).

[3] Tayade, P., and Vijaykumar, P.: A Comprehensive Contemplate on Security Aspects of LTE and LTE Advanced in Wireless Communication Network. International Journal of Control Theory and Applications. Vol. 10, No 31, pp.197-217, (2017).

[4] Agarwal, P., Thomas, D., and Kumar, A.: Security Analysis of LTE/SAE Networks under De-synchronization Attack for Hyper-Erlang Distributed Residence Time, IEEE Communications Letters. Vol. 21, No 5, pp.1055-1058, (2017).

[5] Kastell K., Meyer U.,& R. Jakoby R.: Secure Handover Procedures. Department of Computer Science, Darmstadt University of Technology, pp. 1-5, (2013).

[6] AlShawi I., L. Yan L., Pan W., and Luo B.: Lifetime enhancement in wireless sensor networks using fuzzy approach and A-star algorithm, *IEEE Sensors Journal*, vol. 12, no. 10, pp. 3010–3018, (2012).

[7] Gao T., Song J., Zou Y., Ding H., Wang D., and Jin R.: An overview of performance trade-off mechanisms in routing protocol for green wireless sensor networks, Wireless Networks, vol. 22, no. 1, pp. 135–157, (2016).

[8] Lin, Y., Longjhuang, W., & Chen, Y.C.: Enhanced 4G LTE Authentication and Handover Mechanism. International Journal of Electrical, Electronics and Data Communication. Vol. 3, Issue 9, pp. 45-47, (2015).

[9] Khairy, K., Diaa Eldien, A., Abdel-hafez, A., and Abd El-Wanis, E.: Authenticated Key Management Scheme for Intra-Mme Handover over LTE Networks. International Journal of Research in Engineering and Science. Vol, No 10, pp. 19-28, (2016).

[10] Correia, S., Boukerche, A., Meneguette, R.: An Architecture for hierarchical software-defined vehicular networks. IEEE Commun Mag. Vol. 55(7):80-86, (2017).

[11] Li, X., Liu, F., Feng, Z., Xu, G., Fu, F.: A novel optimized vertical handover framework for seamless networking integration in cyber-enabled systems. Future Generation Computer Systems. Vol. 79(1): 417-430, (2018).

[12] Sharma, V., Song, F., You, I., Chao, H.: Efficient management and fast handovers in software

defined wireless networks using UAVs. IEEE Netw. Vol. 31(6):78-85, (2018).

[13] Shanmugam, K.: A novel candidate network selection based handover management with fuzzy logic in heterogeneous wireless networks. In 4th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, pp. 1-6, (2017).

[14] Cheng X., Xiaohong H., Maode M., and Hong B.: An Anonymous Handover Authentication Scheme Based on LTE-A for Vehicular Networks. Wireless Communications and Mobile Computing. Volume 2018, pp. 1-16, (2018).

[15] Mahmoud E.O., Mohamed H.M., and Hassan A.: Design and Simulation of a New Intelligent Authentication for Handover over 4G (LTE) Mobile Communication Network. In Proceedings of the 11th ICEENG Conference, pp.1-12, (2018).

[16] Jin, C., Maode, M., and Hui, L.: G2RHA: Group-to-Route Handover Authentication Scheme for 4G LTE-A High Speed Rail Networks. IEEE Transaction on Vehicular Technology, (2017).

[17] Prados, G.J., Adamuz, H.O., Ameigeiras, P., Ramos, J. J., Andres, P., & Lopez, J. M.: Handover implementation in a 5G SDN-based mobile network architecture. In IEEE 27th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC) pp. 1-6, (2016).

[18] Amit, K., & Hari O.: Design of a USIM and ECC based handover authentication scheme for 5G-WLAN heterogeneous networks. Digital Communications and Networks. Pp. 1-13, (2019).

[19] Mathi, S., and L. Dharuman, L.: Prevention of Desynchronization Attack in 4G LTE Networks Using Double Authentication Scheme. Open Access Procedia Computer Science. Vol. 89, pp.170- 179, (2016).

[20] Han, C., and Choi, H.: Security analysis of handover key management in 4G LTE/SAE networks. *IEEE Trans. Mobile Comput*., Vol. 13, No. 2, pp. 457- 468, (2014).

[21] Eman, F., Hussein, E., & Hesham, M.: Evaluation of Intrusion Prevention Technique in LTE Based Network. *International Journal of Scientific & Engineering Research*. Volume 5, Issue 12, pp. 1395-1400, (2014).

[22] Xiao, Q., Baojiang, C., and Lingrong, L.: An Enhancement for Key Management in LTE/SAE X2 Handover Based on Ciphering Key Parameters. *2014 Ninth International Conference on IEEE P2P, Parallel, Grid, Cloud and Internet Computing* (3PGCIC). pp.256-261, (2014).