Military Technical College
Kobry El-Kobbah,
Cairo, Egypt

11th International Conference on Electrical Engineering
ICEENG 2018

Efficient Modified Intra-MME Handover Authentication and Key Management Protocol for LTE Networks

K. M. Khairy*, A. Diaa Elbayoumy*, A. Abd Abdel-hafez*, E. Abd El-Wanis*

ABSTRACT

Long Term Evolution (LTE) is the standard for high-speed wireless communication for mobile devices and data terminals. Although, the 3rd Generation Partnership Project (3GPP) has specified some security mechanisms to insure the security of intra-MME handover, but there exists a few vulnerabilities compromising the security of the LTE entities. The most harmful vulnerability is the de-synchronization attack. This attack aims to compromise the new session keys using a false base station by de-synchronizing the target eNodeB during the handover process. In this paper, a modification for the standard protocol is presented to overcome this attack. Also the paper investigates the performance of the modified protocol in terms of the handover phase's latencies according to the 3GPP technical specifications. Finally, the open-source framework *LTE-Sim* is used to provide complete performance evaluation for the modified protocol, by measuring the received packets average delays and the Packet Error Loss Ratio (PELR) of the transmitted packets, comparing with the 3GPP requirements.

KEYWORDS

LTE, 3GPP, Handover, De-synchronization Attack, Latency, PELR, LTE-Sim.

1. Introduction

Long Term Evolution (LTE) is the standard for next-generation mobile networks, comes out of the Third Generation Partnership Project (3GPP) [1]. This standard was designed for providing seamless coverage, high data rate, full interworking with heterogeneous

* Egyptian Armed Forces

radio access networks and service providers, and low latency. The LTE standard specifies an IP-only network supporting data rates up to 100 Mbps downlink and 50 Mbps uplink over a wide area. These high data rates will enables new applications and services such as voice over IP, streaming multimedia, videoconferencing or even a high-speed cellular modem.

With the growing need for mobility in the LTE networks, when an UE moves away from the source Evolved Nodes (eNB) to the target eNB, it is indispensable to achieve a fast and stable Handover (HO). On one hand, the UE and the target eNB need to perform a mutual authentication with key agreement to withstand several protocol attacks. On the other hand, HO procedure needs to be efficient with a lower computational complexity and less communication costs for the continuous connectivity.

When performing the HO, the source eNB decides the type of HO. The X2 HO is used when direct connectivity exits via X2 interface between the eNBs serving by the same Mobile Management Entity (MME). And S1 HO is performed when there is no X2 connectivity or when it is not allowed to use X2 interfaces. The X2 HO can be described in three phases; HO preparation, HO execution, and HO completion phase.

During the HO preparation phase; the source eNB derive the new key (K_{eNB}*) value for the target eNB from either the currently active K_{eNB}, shared between the source eNB and User Equipment (UE), or from the New Hop (NH_{NCC}) key received from an MME on the previous HO, respectively, in the horizontal and vertical key derivations. The NH_{NCC} key is derived at the MME side using the Access Security Management Entity key (K_{ASME}), permanently stored in the Universal Subscriber ID Module (USIM) and in the core network Authentication Center (AUC). The source eNB will forward the K_{eNB}* with the Next Counter Chain (NCC) value to the target eNB via X2 interface. The subsequent session key (K_{eNB}**) between the UE and the target eNB is derived directly from the new K_{eNB}* [2].

Before the K_{ASME} is updated, an intruder may apply the de-synchronization attack using a false base station [3]. This attack aims to disrupt the updating of the NCC value: either by manipulating the message between eNBs via X2 interface, or by manipulating the S1 path switches Acknowledgment (ACK), leaving the target eNB desynchronized. In this attack the intruder will derive the new K_{eNB}* directly from the old K_{eNB}. Intruder will also send the UE an extremely high value of NCC enforcing the UE to use the horizontal key derivation. Consequently, the intruder may compromise the new session key K_{eNB}** derived from K_{eNB}*. The effect of the de-synchronization attack lasts until K_{ASME} is revoked using the Evolved Packet System Authentication and Key Agreement (EPS-AKA).

This loophole has been presented in some recent works [3-4], proposing some solutions to overcome the de-synchronization attack [5-8], but those could not completely prevent the attack or the proposed solutions were infeasible to implement. Therefore, proposing

other solutions to prevent this attack and to maintain the forward key separation during the HO procedure is still needed.

This paper proposes a modification of the Intra-MME HO standard protocol over X2 Interface, to prevent the false base station from de-synchronizing the target node and compromising the session keys. The rest of this paper is structured as follows: in section 2, the modified protocol is presented. The performance analysis including the total latency of the current protocol is discussed in comparison to the modified protocol, in section 3. Moreover, the modified protocol is simulated under an open-source framework LTE-Sim to verify the feasibility of implementing the modified protocol. Finally, the conclusions are drawn in section 4.

2. The Modified Protocol

The main idea of the modifications is to keep the source eNB out of the key management process during the HO, and involves the MME as a Third Trusted Party (TTP). The modified protocol can be described in three phases, as shown in Fig.1.

Before the HO: UE is attached to the source eNB, the Dedicated Radio Bearers (DRBs) and Signalling Radio Bearers (SRBs) are established, and Uplink/Downlink (UL/DL) traffic is transmitted between the source eNB and the UE. The UE remains in the RRC-connected, with respect to the source eNB, and keep all the resources allocated by Evolved Universal Terrestrial Random Access Network (E-UTRAN) and the Evolved Packet Core (EPC).

The modifications will show up in the HO preparation phase, in which the target cell assigns the necessary radio resources for taking over the connection and sending back a HO command message containing the new radio parameters to the source cell. Also the authentication and key management procedures are processed to ensure the entities identities' and to derive the new session key K_{eNB}*.

In this phase, the source eNB triggers the HO and chooses the best reported target cell by the UE, based on the UE's measurement report. Then, the source eNB will send an X2 HO request to the target eNB, including (UE context information, Radio Access Bearer (RAB) context, target cell ID). The target eNB performs call admission control considering the Quality of Service (QoS) in the RAB context.

If the target eNB is able to provide the requested resources for the new UE, the target eNB will request an Authenticator (AUTH) related to the UE from the MME via S1-C interface for the authentication and key management process.

The MME will response with AUTH includes (the request time stamp t, NCC, NH_{NCC-1}, UE ID, and target eNB ID) all encrypted under $K_{ASME,}$ as a challenge to the UE. Upon receiving the AUTH, the target eNB will forward it to the UE. Also, the MME will response with the new key parameter's to the target eNB encrypted with the pre-shared

IPsec association key (K_{IP}) between the target eNB and the MME to derive K_{eNB}* using Equation (1), where (α) is the target physical cell identity and frequency, and then derives the AS security keys.

$$K_{eNB}^{*} = KDF\ (NH_{NCC}, \alpha) \qquad (1)$$

The UE will verify the target ID, increment the (NCC-1) value and compare it with the received NCC value. If they are the same, UE will update the NH_{NCC-1} key and derive the new key K_{eNB}* using Equation (1). Then, UE will prepare the challenge response includes (the request time stamp t, UE ID, and the target eNB ID) encrypted under the new session key K_{eNB}*, and send it to the target eNB. Upon receiving the challenge response, the target eNB will check its contents, if it was as expected; it sends a HO request ACK to the source eNB via the X2 direct tunnel setup (i.e., authentication and key management processed successfully and the HO is accepted). If the target eNB could not accept the HO request, due to the call admission control or authentication failure, it responds to the source eNB with an X2 failure message. During this phase, the UE states remain unchanged.

The HO execution phase starts when UE receives the RRC connection reconfiguration message and transits to the RRC idle state triggering the detachment from the source eNB. In this phase, UE is not able to send or receive packets and a direct tunnel formed between source and target eNB for downlink data forwarding. The source eNB sends the status transfer message to the target eNB with information About the Sequence Number (SN) and the hyper frame number. The source eNB start forwarding the DL data packet to the target eNB to be buffer locally until the UE is synchronized with the target eNB and the HO confirm message that encloses the RRC connection reconfiguration complete is sent by UE to ACK the successful HO to the target eNB. As a result, the UE transits to the RRC connected state with respect to the target eNB.

In the HO Completion phase: the target eNB starts to forward all the buffered packets received from the X2 interface to the UE before any new ones coming from the Serving Gateway (S-GW). Afterwards, the source eNB UE context is released via receiving UE release context message from the target eNB. Finally, the S1 bearer that was initially established between source eNB and UE is also released. After the HO: UE will be attached to the target eNB. The DRB and SRB are established and UL/DL traffic is transmitted as in the initial phase.

A security verification of the modified protocol was conducted in [9], under three attacking scenarios. As described in the analysis results, the modified protocol has maintained the one-hop forward security and protects the new session key from being compromised. Moreover, the modified protocol has increased the essential root key K_{ASME} update interval.

3. Performance Analysis

In this section, a comparison between the modified protocol and the standard protocol will be introduced per the total latencies of the HO phases. Then, the modified protocol

is modelled and simulated to measure and compare the received packets average delay and PELR with the 3GPP requirements of the Quality of Service Class Identifier (QCI) [10, 11, and 12].

The latency or the packet delay measure the protocol delay (processing time) and the transport delay (transmission time through the physical medium). The LTE U-plane UL/DL delay consists of node processing delays, TTI duration, and the radio frame alignment (T_{FA}) [13]. The LTE U-plane latency can be represented in Equation (2), where; n is the number of HARQ re-transmissions.

$$D_{UP} = (T_{TTI} + T_{FA}) + (T_{eNB} + T_{UE}) + n*5 = 3.5 + n*5. \quad (2)$$

In typical cases there would be 0 or 1 re-transmissions yielding an approximate average U-plane latency of D_{UP}, as in Equation (3), where p is the error probability of the first HARQ transmission on the radio side, assumed of (30%). The packet delay in the U-plan typical cases takes the values of 3.5 ms or 5 ms according to the error probability p of the first HARQ transmission.

$$D_{UP,\ \text{typical}}\ [\text{ms}] = 3.5 + p*5. \quad (3)$$

The PELR measure the packets that are not successfully delivered over the access network and the packets which are not delivered within the packet delay budget according to the standardized QCI characteristics. The objective of this measurement is to measure packets that are dropped due to congestion, traffic management etc. However, a packet should be regarded as invalid if it is received later than 100ms and the PELR should be about 10^{-2} for voice conversation.

3.1 Handover Phases Latencies

The current protocol preparation phase delay is represented in Equation (4), where T_{X2} is the transmission delay between the source and the target eNBs via the X2 interface, and T_{eNB} is the processing delay in the eNB.

$$T_{HOPrep\text{-}current} = 2\,T_{X2} + T_{eNB}. \quad (4)$$

On the other side, the modified protocol needs to add extra messages to the preparation phase for the authentication and the key management process. As a result, the modified protocol will add an extra transport delay ($2\,T_{S1\text{-}C} + 2\,T_{X2}$) and a processing delay of ($T_{MME} + 2\,T_{eNB}$). The modified protocol preparation phase delay is represented in Equation (5). Where, ($T_{S1\text{-}C}$) is the transmission delay between eNB and MME.

$$T_{HOPrep\text{-}modified} = (4\,T_{X2} + 4\,T_{S1\text{-}C}) + (3\,T_{eNB} + T_{MME}). \quad (5)$$

The preparation phase delay of the modified protocol has significantly increased, but it has no effect on the packet delay because during this phase both the UE and the source eNB are RRC-connected and the UL/DL traffic is transmitted between the

source eNB and the UE. So that, The HO preparation period does not contribute to the U-plane interruption time.

The HO Execution phase is the most critical phase on the HO performance due to the HO interruption/disconnection that occurs. The HO execution phase delay is represented in Equation (6). Where the T_{HIT} is the Handover interrupt time (detach time), the period the UE is RRC-idle, which obtained by computing the time difference between the reception of the RRC connection reconfiguration and the reception of RRC connection reconfiguration complete ACK.

$$T_{HOExe} = T_{HIT} + T_{UE\text{-}eNB}. \quad (6)$$

The HO completion delay comprises of the transmission delay for exchanging path switch request and path switch request ACK, is represented in Equation (7). Where, ($2T_{MME-P-GW}$) is the transmission delay for delivering modify bearer request and modify bearer response. ($T_{IP.CAN}$) *is* the processing delay of IP–CAN session modification. (T_{S-GW}) is the processing delay in the S-GW. Most of the signaling messages in the HO Completion phase don't pass through the UE, thus not measured by the UE.

$$T_{HO\ Comp} = (2T_{S1\text{-}C} + 2T_{MME-P-GW}) + (T_{IP.CAN} + T_{X2} + T_{S-GW} + T_{MME} + T_{eNB}). \quad (7)$$

The 3GPP has set requirements for the length of the detach time observed by the UE during the HO, by providing a timing analysis of the main component processing delay and the transmission delay [14]. According to the timing analysis, the current protocol HO preparation phase is about (6 ms), while the modified protocol HO preparation phase is about (46 ms). The current protocol HO execution phase is about (61 ms).

3.2 Modelling and Simulation

The system is modeled and simulated in the open-source dynamic downlink system level simulator LTE-Sim [15], implemented in C++. The simulation aims to prove the modified protocol feasibility by measuring the success of the hard HO process [16] with the pre-computed latency in the last section. Also, the simulation aims to;

1- Measuring the PELR of the transmitted VOIP packets.
2- Measuring the received VOIP packets average delay.
3- Comparing the measured results with the 3GPP requirements of the QCI.

3.2.1 Experimentation Setup

As shown in Table (1), there are initially 10, 20, 30, 40, and 50 UEs per cell uniformly distributed over 19 cells. They move at constant speeds of 3, 30, and 120 km/h in random Walk. Each UE holds a 1 VoIP flow for 10000ms during the whole simulation time of 10100ms. The simulations are carried out on a Linux machine with an Intel(R) Core(TM) i7-2640M CPU @ 2.80GHz and 16 GB RAM.

3.2.2 Experimentation Results

The number of successful handover is shown in Fig.2. As shown in figure, as the speed of the UEs increases the number of handover increases. The packets average delay has experimentally measured including the HO buffering delay for the received VOIP packets in each case. As shown in Fig.3, the experimental results show that; the packets average delays for the randomly walking UEs are following the U-plane latencies proposed by the 3GPP technical specifications (typical). The handover has added some delay to the U-plan typical cases of 3.5 ms or 5 ms according to the error probability p of the first HARQ transmission. Also, as the UEs speed increase, the number of HO increased, so that the average delay increased.

The PERL has experimentally measured for the transmitted VOIP packets in each case, as shown in Fig.4. We can notice that; the measured PELR is in the PELR required range for VOIP conversation according to the 3GPP requirements mentioned before (10^{-2}). For a fixed UEs speed, as the number of UEs per cell increase, the measured PELR is increased. Also when the UEs speed increase, the PERL is increased. The minimum measured PELR was 0.0015 with 10 UEs moving randomly at 3 km/h, and the maximum measured PELR was 0.021 with 50 UEs per cell (the boundary of the simulator) moving randomly at 120 km/h.

4. Conclusions

This paper has proposed a major modification to the standard Intra-MME handover protocol, this modification aims to overcome the de-synchronization attack and maintains the one-hop forward security during the HO by keeping the source eNB out of the key management process and using the MME as a third trusted party. In the modified protocol, the MME sends the updated materials needed to drive the new session key for both the UE and the target eNB (away from the source eNB) protected by the pre-shared local root key K_{ASME} and the pre-shared IPsec association key K_{IP}, respectively. As a result, the false eNB impersonating the source eNB could not learn the new session key between UE and the target eNB.

A performance analysis was conducted as a comparison between the modified protocol and the standard protocol, per the total latency of the HO procedure phases, according to the 3GPP technical specifications. The analysis results showed that, the modified protocol has increased the HO preparation phase delay. This delay does not affect the U-plane interruption time, because the UE and the source eNB are RRC-connected and the UL/DL traffic is transmitted between the UE and the source eNB.

Moreover, the modified protocol is modeled and simulated in an open-source dynamic downlink system level simulator *LTE-Sim*. The experimental results showed that; the average received packets delay measured has followed the U-plane latencies proposed by the 3GPP technical specifications. Also, the PELR measured is following the 3GPP required range for VOIP conversation. As a result, although the modified protocol could achieve its' security goals but its' performance is still following the 3GPP requirements, and it is applicable to be implemented in the LTE networks.

Figures

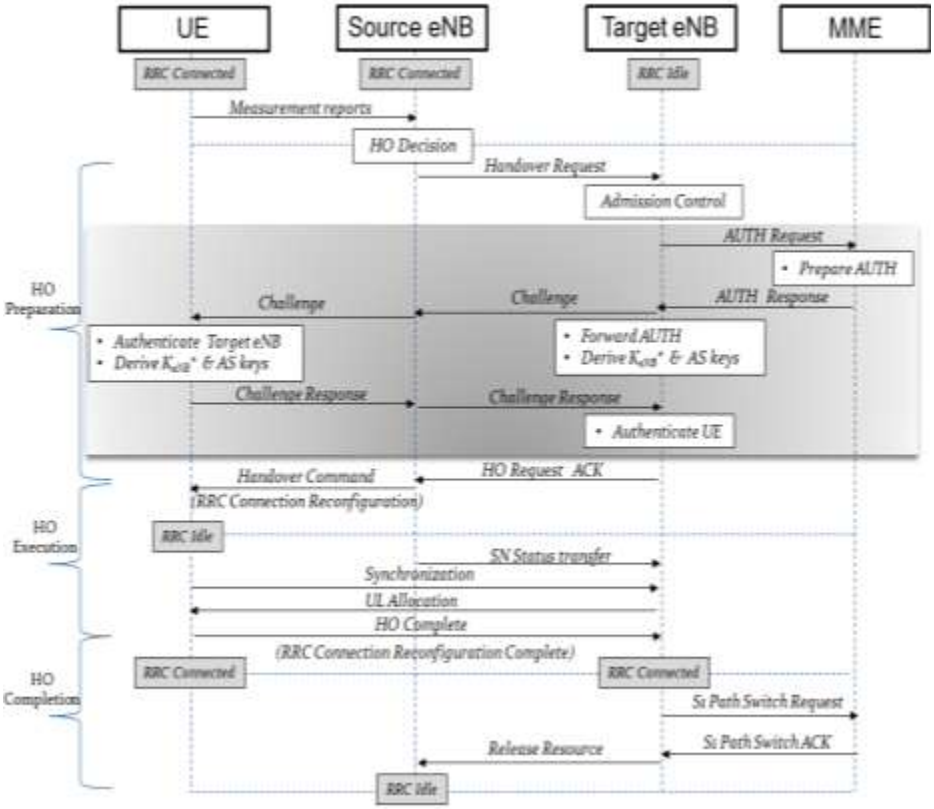

Fig.1: the Modified Protocol

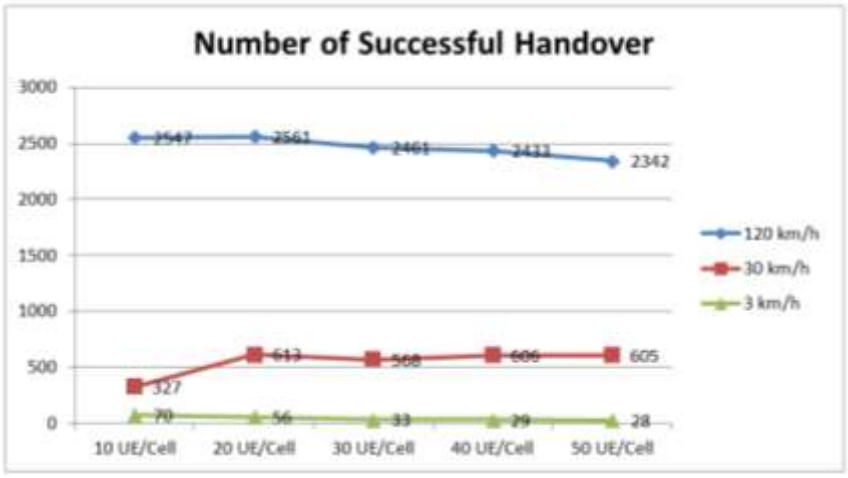

Fig.2: Number of Successful Handover

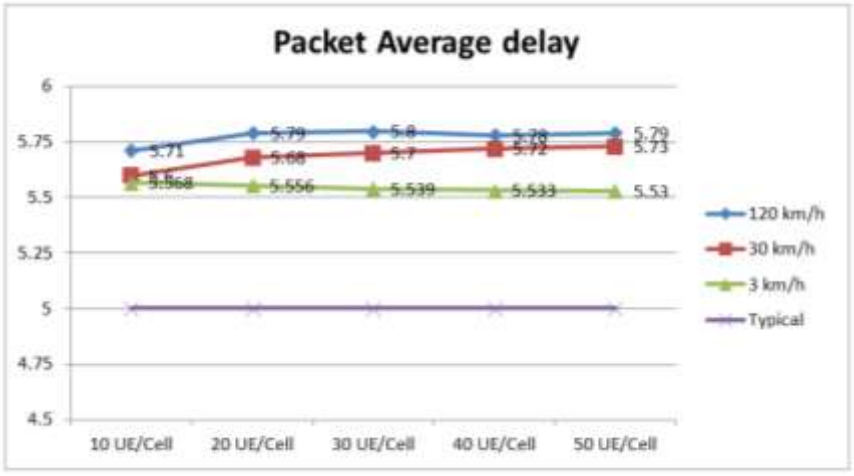

Fig.2: the Packets Average Delay

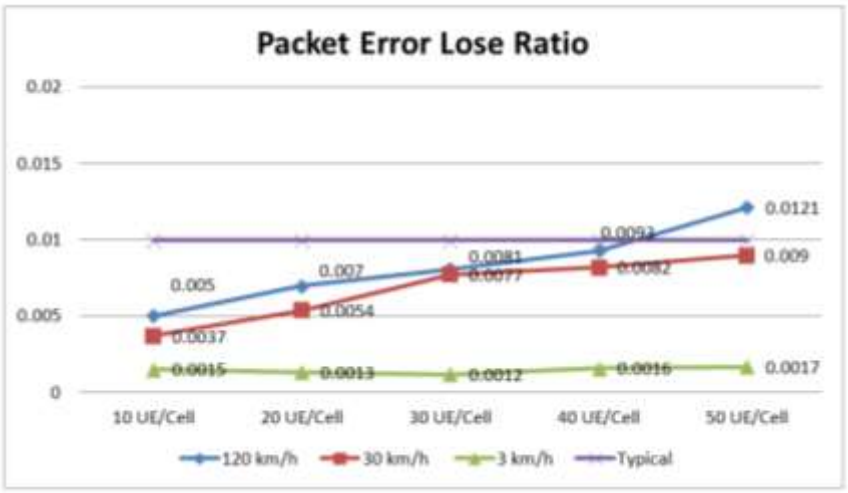

Fig.3: the Packet Error Lose Ratio

Tables

Table (1): Parameters of the Traffic

Parameters	Value	Parameters	Value
Number of Cells	19	Data Traffic per UE	1 VOIP
Radius	1000 m	Maximum Packet Delay	100ms
Number of UE/Cell	10/20/30/40/50	Simulation Time	10,100ms
UE Speed/ Mobility	3/30/120 km/h Random Walk	Duration of VOIP Flow	10,000ms

References

[1] Dahlman, et al, "4G: *LTE/LTE-advanced for mobile broadband*", Academic press (2013).
[2] 3GPP TS 33.401, "*Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution (SAE); Security architecture*", V15.2.0, (2018).
[3] Mavoungou, et al. "*Survey on threats and attacks on mobile networks*", *IEEE Access* 4: 4543-4572, (2016).
[4] Han, et al, "*Security analysis of handover key management in 4G LTE/SAE networks*", IEEE Transactions on Mobile Computing, p.457-468, (2014).
[5] Sridevi, et al, "*Secured Handover Key Management among LTE Entities Using Device Certification*", IEEE Eco-friendly Computing and Communication Systems (ICECCS), (2014).
[6] Xiao, et al. "*An Enhancement for Key Management in LTE/SAE X2 Handover Based on Ciphering Key Parameters*", IEEE P2P, Parallel, Grid, Cloud and Internet Computing (3PGCIC), (2014).
[7] Chandavarkar, B. "*Mitigation of de-synchronization attack during inter-eNodeB handover key management in LTE*", IEEE Contemporary Computing (IC3), (2015).
[8] Sun, et al. "*A secure and effective scheme providing comprehensive forward security to LTE/SAE X2 handover key management*", KSII Transactions on Internet & Information Systems 11.9 (2017).
[9] K. Khairy, and M. Chatterjee, "*Provably Secure Authenticated Key Management Protocol Against De-Synchronization Attacks in the Intra-MME Handover*", International Journal of Research in Engineering and Science (IJRES), ISSN (Online): 2320-9364, ISSN (Print): 2320-9356, Volume 5, Issue 6, PP. 46-55, June (2017).
[10] 3GPP TS 23.203, "*Technical Specification Group Services and System Aspects; Policy and charging control architecture*", Release 15, V15.1.0, (2017-12).
[11] Capozzi, et al. "*Downlink packet scheduling in LTE cellular networks: Key design issues and a survey*", IEEE Communications Surveys & Tutorials: 678-700 15.2 (2013).
[12] 3GPP TS 36.314, "*Technical Specification Group Radio Access Network; Evolved Universal Terrestrial Radio Access (E-UTRA); Layer 2 – Measurements*", V10.2.0, Release 14, (2017).
[13] Han, et al. "*Measurement and stochastic modeling of handover delay and interruption time of smartphone real-time applications on LTE networks*", IEEE Communications Magazine 53.3, (2015).
[14] 3GPP ETSI TR 25.912, "*Feasibility study for evolved Universal Terrestrial Radio Access (UTRA) and Universal Terrestrial Radio Access Network (UTRAN)* ", Release 14, version 14, (2017).
[15] Piro, et al. "*Simulating LTE cellular systems: An open-source framework*", *IEEE transactions on vehicular technology*60.2: 498-513, (2011).
[16] Chen, et al. "*Efficient and prompt handover in LTE-based systems by predicting the target eNodeBs*", *Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 2014 International Conference on* IEEE, (2014).