Secure and Efficient Uniform Handover Scheme for LTE-A Networks

Zaher Haddad*†‡, Mohamed Mahmoud‡, Sanaa Taha†, and Imane Aly Saroit †

*Department of Computer Science, Al-Aqsa University, Gaza, Paleestine

‡Department of Electrical & Computer Engineering, Tennessee Tech University, Cookeville, TN, USA

†Department of Information Technology, Cairo University, Cairo, Egypt

***Abstract*—In this paper, we propose a secure and efficient handover scheme for the Long Term Evolution-Advanced (LTE-A) networks. The proposed scheme does not trust the base-stations because they may be accessible to attackers and operated by subscribers, rather than service providers. First, we propose a registration procedure to enable the base-stations to authenticate and register with the Home Subscriber Server (HSS). Then, we propose a procedure to enable the user equipment (UEs) to authenticate and exchange keys with the Mobility Management Entity (MME) and base-stations. Finally, we propose a secure and fast handover procedure. To reduce the handover latency, the HSS is not involved and the computation overhead on the UEs is very low. The proposed scheme is uniform in the sense that one procedure can be used for all handover scenarios. Our security analysis demonstrates that the proposed scheme can thwart well-known attacks such as impersonation, man in the middle, packet replay, etc. The proposed key agreement procedures can achieve backward/forward secrecy, where attackers cannot derive the past or future session keys. Our performance evaluation results demonstrate that the proposed handover scheme is fast because it needs few computations and exchanges few number of packets. This is important to improve the quality of service, avoid call termination, and service disruption. Moreover, the proposed scheme imposes minimal overhead on the mobile nodes, which is very desirable because these nodes usually have low computational power and energy.**

***Index Terms*—LTE-A, authentication and key agreement, security, uniform handover.**

I. Introduction

The Long Term Evolution-Advanced (LTE-A) network is the packet based system specified by the Third Generation Partnership Project (3GPP) as 4G cellular network system [1]. The increasing demand for high data rates to support new applications such as mobile Internet and wireless multimedia services has motivated the development of the LTE-A cellular wireless technology [2].

The LTE networks have base-stations that communicate with user equipments (UEs). There are two types of base-stations, namely, evolved node B (eNB) and Home evolved Node B (HeNB). HeNB is a low-power access point that is typically installed by a subscriber in a residence or a small office to enhance the indoor coverage for high speed data service. Moreover, the Internet can be used to enable communications between a HeNB and another HeNB or eNB. However, the introduction of base-stations that are owned and operated by subscribers rather than service providers and the potential use of the insecure Internet connections raise a number of security threats in the LTE-A networks.

When a UE moves away from its eNB/HeNB, handover procedure should be executed to allow the UE to roam to a new eNB/HeNB during the active session without call termination and quality of service degradation [2]. In the handover procedure, the UE should share a key with the new base-station. In the existing LTE-A networks, the source base-station calculates a new session key by applying a one-way function to the current session key and sends it to the target base-station. One threat to the handover key management is that a malicious base-station (such as HeNB) can use the session key to derive the following session keys.

There are mainly two different types of handover called intra-MME and inter-MME. In intra-MME handover (also called horizontal handover), the source eNB and the target eNB are managed by the same MME; on the other hand in inter-MME handover (also called vertical handover), they are managed by different MME [1]. Handovers can also be performed from an eNB to another eNB, from a HeNB to an open access HeNB, or from an eNB to HeNB. Therefore, different handover procedures for different handover scenarios increase the overall system complexity. It is desirable to use a uniform handover for different scenarios. Moreover, a handover procedure should have low computational and communication overhead, especially at the UE side, to ensure continuous connectivity and avoid performance degradation.

In this paper, we propose a secure and efficient handover scheme for the LTE-A networks. Each node in the network has a certified public/private key pair that are issued by the Home Subscriber Server (HSS). In authentication and key agreement phase, each UE shares keys with the MMEs and the base stations. The proposed scheme does not trust the base-stations because they may be accessible to attackers and operated by subscribers, rather than service providers. The scheme is uniform in the sense that it can be used for all handover scenarios. To reduce the handover latency, the HSS is not involved and the computation overhead on the UEs is very low and the number of exchanged packets is reduced. This is important to avoid degradation of the quality of service and call termination. Our security analysis demonstrates that the proposed scheme can thwart well-known attacks and the proposed key agreement procedures can achieve backward/forward secrecy. Our performance evaluations demonstrate that the proposed handover scheme requires the exchange of few packets and impose minimal overhead on the mobile devices, which is very desirable because these

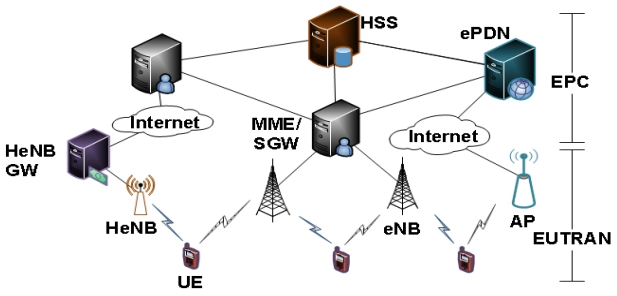

Fig. 1: LTE-A Network Architecture.

devices usually have low computational power and energy.

The remainder of the paper is organized as follows. The related works are discussed in section II. Section III discusses the network and threat models. The proposed scheme is explained in section IV. The security analysis and performance evaluations are provided in sections V and VI, respectively. Finally, section VII concludes the paper.

II. Related Work

Several schemes have been developed to secure different applications such as smart grid [3], [4], [5], [6], [7], vehicular ad hoc networks [8], [9], and ad hoc networks [10], [11], [12], [13], but the problem we address in this paper is different.

Cao et. al. [14] propose a scheme to achieve seamless handovers between HeNBs and eNBs in the LTE networks. The scheme uses Schnorr proxy signature to allow the nodes to authenticate each other without contacting the HSS. The Internet can be used to connect HeNBs to MMEs, but the insecure nature of the Internet connections can introduce new vulnerabilities to the LTE networks. In order to secure this connection, Cao et. al. [15] use a signing delegation technique to authenticate the LTE nodes.

Elbouabidi et. al. [16] propose two authentication schemes to secure the handover between LTE networks and Wireless Local Area Network (WLANs) networks. After the execution of the initial authentication scheme, a key is shared between a UE and the authentication server of the WLAN. The key is used for securing the handover and traffic in WLAN networks. The second scheme, called *Local Re-authentication*, is executed locally in a WLAN network without contacting the authentication server of the home network. Choi et. al. [17] propose a handover authentication scheme using chameleon hashing. However, the scheme requires direct connections between the access points.

III. System Model

A. Network Model

From Fig. 1, the LTE-A network has two main parts; *Evolved Packet Core* (*EPC*) and *Evolved Universal Terrestrial Radio Access Network* (*E-UTRAN*). The EPC has a HSS, MMEs, serving gateways (SGWs), and Evolved Packet Data Network Gateways (ePDN). The HSS stores and manages the subscribers' information. T he MME is in charge of all functions that are relevant to users and session management. Different MMEs can communicate with each other.

The E-UTRAN includes access points (APs) and two types of base-stations, named evolved node B (eNB) and Home evolved Node B (HeNB). In this paper, we use base-station (BS) to refer to APs, eNBs, and HeNB. Each BS is connected to at least one MME. As a low-power access point, HeNBs are typically installed by subscribers in residences or small offices to enhance the indoor coverage. It works on the licensed spectrum and connects to the EPC via the Internet. There are mainly two different handover procedures called intra-MME and inter-MME. In intra-MME handover, the source eNB and the target eNB are connected to the same MME; however, in inter-MME handover, they are connected to different MMEs. Handovers can be performed from an eNB to another eNB, from a HeNB to another HeNB, or from an eNB to a HeNB.

B. Adversary and Trust Models

We assume that the EPC part of the LTE network is secure and trusted. This is because it is owned and run by the network operator who is interested in the secure operation of the network. In addition, the HSS and MMEs are not vulnerable to attacks because they are not accessible to the subscribers. However, the E-UTRAN part is not trusted because HeNBs are owned and operated by the subscribers rather than service provider and the eNBs are deployed in streets and physically accessible to the public. We assume that the base-stations are connected to the EPC via insecure channels, but the links between the HSS and MMEs and between MMEs and HSS are secure. We consider attacks launched by external adversaries and malicious base-stations. Examples of these attacks include:-

1) Impersonation attacks: Adversaries try to impersonate MMEs, HSS, base-stations and UEs and send packets under their names.

2) Unauthorized access: External attackers who are not members in the network try to access the network.

3) Replay attack: An adversary intercepts valid packets and transmits them in a different time or location, e.g., for resource exhaustion.

4) Packet modification: A malicious base-station alters the packets and EUs can not detect this modification.

5) Man in the middle attack: When a UE establishes a shared key with the MME, a malicious base-station tries to share a key with the UE and another key with the MME so that it can decrypt the exchanged messages and alter them. The malicious base-station makes two separate connections to the MME and the UE, while they believe that they communicate directly.

6) Deriving session keys: In handover procedure, the UE should share a new key with the target base-station. Using this key, a malicious base-station will try to calculate the past keys used by the UE and the keys that will be used in future handovers.

IV. Secure Handover Scheme

A. Initialization

The HSS bootstraps the system as follows. It chooses a large prime number q and creates the finite field Z_q of order

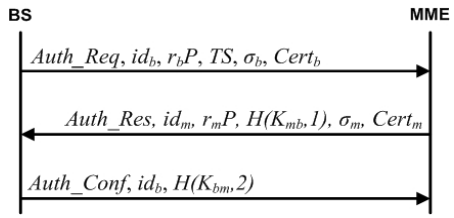

Fig. 2: BS-MME authentication and key agreement.

q. Let G be a cyclic additive group with generator P, whose order is q, and G_T be a cyclic multiplicative group with the same order q. H and H_1 are two hash functions, where H:{0, 1}$^* \rightarrow G$ and H_1: {0, 1}$^* \rightarrow Z_q$. Let $\hat{e}$: $G \times G \rightarrow G_T$ be a bilinear map that is called a bilinear pairing and has the following property: $\hat{e}(aP, bQ) = \hat{e}(P, Q)^{ab}$ for all P, $Q \in G$ and a, $b \in Z_q$. The HSS chooses a random element $sk_h \in Z_q$ and computes $PK_h = \frac{1}{sk_h}P$. sk_h and PK_h are the HSS's private and public keys, respectively. For each MME, the HSS chooses a random element $sk_m \in Z_q$ as a private key and computes the corresponding public key $PK_m = \frac{1}{sk_m}P$. Then, it computes the MME's certificate as follows: $Cert_m = \{id_m, PK_m, T_e, \sigma_h\}$, where T_e is the expiration date of the certificate, id_m is the MME's unique identity, and $\sigma_h = \frac{1}{sk_h}H(id_m, PK_m, T_e)$ is HSS's signature. Similarly, each BS with an identity id_b has a private key $sk_b \in Z_q$, a public key $PK_b = \frac{1}{sk_b}P$, and a certificate $Cert_b$. In addition, each UE with an identity id_u has a private key $sk_u \in Z_q$, a public key $PK_u = \frac{1}{sk_u}P$, and a certificate $Cert_u$.

B. Authentication and Key Agreement

Fig. 2 illustrates the authentication and key agreement protocol run by BSs and MMEs. First, the BS chooses a random element $r_b \in Z_q$, computes r_bP, and sends an *Authentication Request* packet (*Auth_Req*) to the MME. From Fig. 2, the packet has a time stamp (TS), r_bP, the BS's certificate and signature, where $\sigma_b = \frac{1}{sk_b}H(id_b, r_bP, TS)$. Then, the MME checks that TS is within an acceptable range of the current time to ensure that the packet is not replayed. It also verifies the certificate by verifying the HSS's signature as follows: $\hat{e}(\sigma_h, P) \stackrel{?}{=} \hat{e}(H(id_b, PK_b, T_e), PK_h)$. The proof of this verification is as follows:-

$$\begin{aligned}\hat{e}(\sigma_h, P) &= \hat{e}(\frac{1}{sk_h}H(id_b, PK_b, T_e), P)\\ &= \hat{e}(H(id_b, PK_b, T_e), \frac{1}{sk_h}P)\\ &= \hat{e}(H(id_b, PK_b, T_e), PK_h)\end{aligned}$$

The MME should also verify the BS's signature by checking that $\hat{e}(\sigma_b, P) \stackrel{?}{=} \hat{e}(H(id_b, r_bP, TS), PK_b)$. If all verifications succeed, the MME replies with an *Authentication Response* packet (*Auth_Res*). The format of the packet is given in Fig. 2, where $\sigma_m = \frac{1}{sk_m}H(id_m, r_mP, H(K_{mb}, 1))$ is the MME's signature on the packet, $r_m \in Z_q$, and $K_{mb} = H_1(\hat{e}(PK_b, \frac{r_m}{sk_m}r_bP))$ is a symmetric key shared with the BS. The MME sends

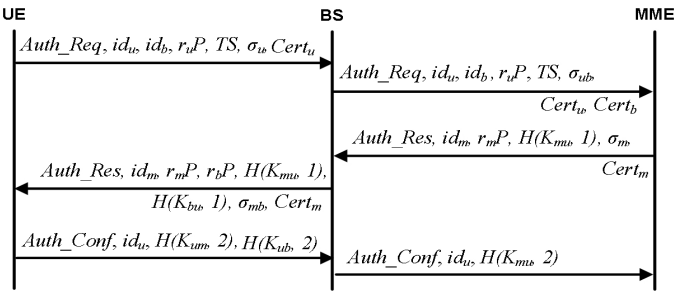

Fig. 3: Authentication and key agreement protocol to authenticate UE to BS and MME.

$H(K_{mb}, 1)$ to enable the BS to ensure that the symmetric key it computes is identical to the key computed by the MME.

Finally, The BS verifies the certificate and signature of the MME. Then, it computes the shared key $K_{bm} = H_1(\hat{e}(PK_m, \frac{r_b}{sk_b}r_mP))$. The proof that K_{mb} equals to K_{bm} is as follows.

$$\begin{aligned}K_{mb} &= H_1(\hat{e}(PK_b, \frac{r_m}{sk_m}r_bP))\\ &= H_1(\hat{e}(\frac{1}{sk_b}P, \frac{r_b}{sk_m}r_mP))\\ &= H_1(\hat{e}(\frac{1}{sk_m}P, \frac{r_b}{sk_b}r_mP))\\ &= H_1(\hat{e}(PK_m, \frac{r_b}{sk_b}r_mP)) = K_{bm}\end{aligned}$$

Then, the BS sends an *Authentication Confirmation* packet (*Auth_Conf*), which has the key confirmation code ($H(K_{bm}$, 2)) to enable the MME to verify the computed key by the BS.

Fig. 3 illustrates an authentication and key agreement protocol to authenticate UE to BS and MME. The UE sends an *Authentication Request* packet (*Auth_Req*) to the BS. The format of the packet is given in Fig. 3, where $\sigma_u = \frac{1}{sk_u}H(id_u$, id_b, r_uP, $TS)$, and $r_u \in Z_q$. The BS verifies the signature of the UE. Then, it sends an *Auth_Req* packet to the MME. From Fig. 3, the packet has an aggregated signature $\sigma_{bu} = \sigma_b + \sigma_u$, where, $\sigma_b = \frac{1}{sk_b}H(id_u, id_b, r_uP, TS)$is the BS's signature. The aggregated signature can prove that the packet is sent from UE via BS. The MME verifies the aggregated signature σ_{bu} by checking that $\hat{e}(\sigma_{bu}, P) \stackrel{?}{=} \hat{e}(H(id_u, id_b, r_uP, TS), PK_u+PK_b)$. The proof is as follows.

$$\begin{aligned}\hat{e}(\sigma_{bu}, P) &= \hat{e}(\sigma_u + \sigma_b, P)\\ &= \hat{e}(\sigma_u, P)\hat{e}(\sigma_b, P)\\ &= \hat{e}(\frac{1}{sk_u}H(id_u, id_b, r_uP, TS), P)\hat{e}(\frac{1}{sk_b}H(id_u,\\ &\quad id_b, r_uP, TS), P)\\ &= \hat{e}(H(id_u, id_b, r_uP, TS), \frac{1}{sk_u}P)\hat{e}(H(id_u, id_b,\\ &\quad r_uP, TS), \frac{1}{sk_b}P)\\ &= \hat{e}(H(id_u, id_b, r_uP, TS), \frac{1}{sk_u}P + \frac{1}{sk_b}P)\\ &= \hat{e}(H(id_u, id_b, r_uP, TS), PK_u + PK_b)\end{aligned}$$

The shared key between the MME and the UE is K_{mu} = $H_1(\hat{e}(PK_b, \frac{r_m}{sk_m} r_uP))$, where $r_m \in Z_q$. As indicated in Fig. 3, the MME sends an *Authentication Response* (*Auth_Res*) packet to the BS, where $H(K_{mu}, 1)$ is key confirmation and the signature $\sigma_m = \frac{1}{sk_m} H(id_m, r_mP, H(K_{mu}, 1))$.

The BS computes the shared key with the UE K_{bu} = $H_1(\hat{e}(PK_u, \frac{r_b}{sk_b} r_uP)$, where $r_b \in Z_q$. It also aggregates the signatures σ_{bm}= σ_b + σ_m, and sends an *Auth_Res* packet to the UE, where $H(K_{bu}, 1)$ is key confirmation and its signature σ_b = $\frac{1}{sk_b} H(id_b, r_bP, H(K_{bu}, 1))$. The UE verifies the aggregated signature and computes the shared keys with the BS and the MME (K_{ub} and K_{um}) as follows: K_{ub} = $H_1(\hat{e}(PK_b, \frac{r_u}{sk_u} r_bP)$ and K_{um} = $H_1(\hat{e}(PK_m, \frac{r_u}{sk_u} r_mP)$. Finally, it confirms the keys by sending $H(K_{ub}, 2)$ and $H(K_{um}, 2)$ to the BS and the MME, respectively.

C. Handover Procedure

The proposed handover procedure is illustrated in Fig. 4. First, the UE sends *Handover Request* (*HO_Req*) packet to the source BS (BS_S). The packet has r_uP, the UE's identity (id_u), the source base station's identity (id_{bs}), the target base station's identity (id_{bt}), a time stamp (TS), and the UE's signature (σ_u = $\frac{1}{sk_u} H(id_u, id_{bs}, id_{bt}, r_uP, TS)$), where $r_u \in Z_q$ is a random element. The source BS verifies the timestamp to check the freshness of the packet. It also verifies the UE's signature σ_u Then, it signs the packet and aggregates its signature to the UE's signature and sends a (*HO_Req*) packet to the source MME (MME_S).

The source MME verifies the packet's timestamp and the aggregated signature. Then, it computes the new key ($K^{'}_{um}$) that will be shared between the UE and the target MME (MME_T), where $K^{'}_{um}$ = $H(K_{um}, r_uP)$. Finally, the source MME sends a *Reallocation Request* packet (*Reall_Req*) to the MME_T, that sends a *Reall_Req* to the target BS (BS_T).

The target BS chooses a random element $r_{bt} \in Z_q$ and computes $r_{bt}P$. Then, it calculates the shared key with the UE as follows: K_{btu} = H_1 ($\hat{e}(PK_u, \frac{r_{bt}}{sk_{btu}} r_uP)$). Finally, it sends a *Handover Command* packet (*HO_Cmd*) to the UE. As indicated in Fig. 4, the packet has the base station's signature and the key confirmation code $H(K_{btu}, 1)$.

The UE verifies the target base station's signature and computes the shared key as follows: K_{ubt} = $H_1(\hat{e}(PK_{bt}, \frac{r_u}{sk_u} r_{bt}P))$. Then, it sends a *Handover Confirmation* packet (Ho_Conf) to the BS_T. The packet has the key confirmation code $H(K_{ubt}$, 2) and the UE's signature. Finally, the target BS sends Ho_Conf packet to the target MME that sends Ho_Conf packet to the MME_s. The MME_s sends Ho_Conf packet to the BS_s to confirm that handover has been performed to release the reserved channels.

V. Security Analysis

In this section, we investigate the robustness of the proposed scheme against well-known attacks.

Attacks against authentication: Each node in the network, either UE, BS, or MME, has a certificate signed by the HSS. The certificates and signature scheme are used to enable the nodes to mutually authenticate each other. The security of the signatures is based on the well-known discrete logarithm difficulty, i.e., given P and rP, there is no way to compute r. The proposed scheme can secure the authentication process without directly involving the HSS, which is important to improve scalability and efficiency. In addition, impersonating any node in the network is infeasible because all messages are signed and forging signatures is infeasible and computing the private key $\frac{1}{sk_u}$ from the public key $\frac{1}{sk_u}P$ is infeasible because of the discrete logarithm difficulty.

Attacks against key agreement: In our key agreement procedure, the computation of the key is not controlled by only one node, but the two nodes that execute the procedure contribute to the key. This usually produces a more robust key than computing the key by only one node because it may select weak random values. The proposed procedure can also thwart the *Man-in-the-middle* attack by signing the key contributions, such as r_uP, so that attackers cannot know r_u or send r_uP on behalf of the UE. The proposed scheme can provide high level of security because each key is used only for one time and every time a node establishes a key, it calculates a different key. As of *Forward/Backward secrecy*, the base stations cannot use the shared session key to derive neither the past keys nor the future ones. This is because the key shared with the source base station is not used to compute the new key shared with the target base station, but the UE and the target base station use one-time random elements $\in Z_q$ to calculate the key.

Attacks against packet integrity and freshness: Each node can verify the packets' integrity because they are signed and any modification to the packet will result in failure of the signature verification. Timetamps are used in our scheme to thwart packet replay attack. Each node should verify the timetamps to make sure that the packet is fresh. If the nodes are not able to identify the stale packet, attackers can launch attacks to exhaust the network resources. In our scheme, stale packets are dropped by the base stations and they will not be relayed in the network to the MME or the HSS.

VI. Performance Evaluation

The proposed handover scheme is uniform because the same protocol can be used for different handover scenarios, i.e., inter MME, intra MME and between eNBs and HeNBs. In this section, we evaluate the communication and computation overhead of our scheme.

A. Communication Overhead

Table I compares the number of packets exchanged between each pair of nodes in the proposed handover procedures to existing schemes. It can be seen that the proposed procedure requires much fewer packets than Coa_{HeNB} [14] and Coa_{AP} [15]. $Bouabidi$ [16] needs only one packet fewer than our procedure; however, as will be explained in next subsection, it imposes much more computation overhead on UEs than our scheme. This extra packet is sent from BSs to MMEs, where they are connected via a fast wired connection. It can also be seen from the table that all the procedures do not need direct

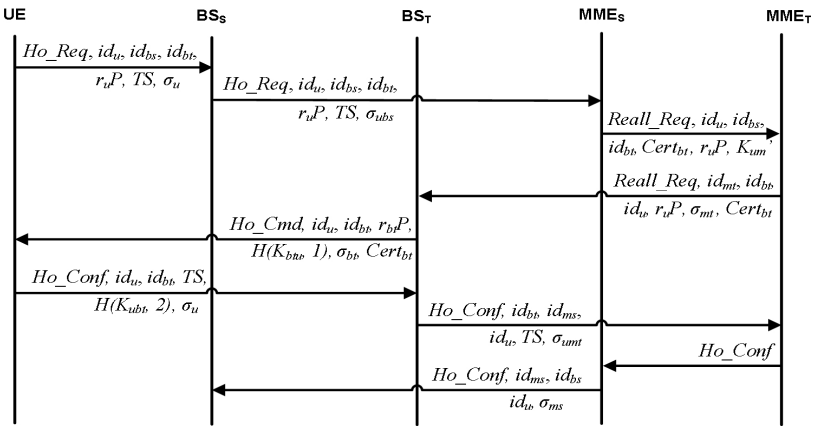

Fig. 4: The proposed Handover Procedure.

TABLE I: Number of packets exchanged between LTE-A nodes.

Schemes	UE-BS	BS-BS	BS-MME	MME-MME	Total
Coa_HeNB [14]	3	0	7	4	14
Coa_AP [15]	8	0	4	4	16
Bouabidi [16]	3	0	3	2	8
Our scheme	3	0	4	2	9

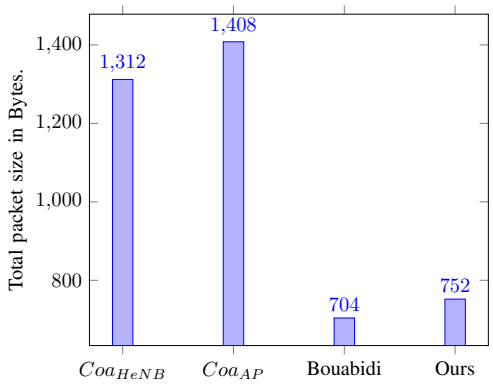

Fig. 5: Communication overhead.

communications between the base stations. Moreover, the UEs should send much more packets in Coa_{AP} [15] which is not desirable because the connection between the UEs and BSs usually has low bandwidth.

We assign two bytes for each identity, 160 bits for q, 20 bytes for each elliptic curve point, 20 bytes for signatures, and 5 bytes for timetamps. A typical certificate should have a public key, an identifier, the issuer's identifier, the issuing data, the expiry date and a signature. Based on that, the certificates' size is 54 bytes. In Fig. 5, we measure the total amount of data (in Bytes) that should be transmitted during handover process. It can be seen that our scheme requires much less communication overhead comparing to Coa_{HeNB} [14] and Coa_{AP} [15]. In addition, our scheme needs only 48 bytes more than $Bouabidi$ [16].

TABLE III: Computation time of each node.

Schemes	UE	BS	MME
Coa_HeNB [14]	6.73	10.19	6.64
Coa_AP [15]	6.73	10.19	6.64
Bouabidi [16]	9.9	9.9	8.7
Our scheme	0.586	8.87	14.173

B. Computation Overhead

Let the computation time of a bilinear pairing operation, ECC point multiplication operation, ECC point addition operation, and hashing operation are e, m, a, and h, respectively. Table II gives the computation overhead on UEs, BSs and MMEs of our scheme compared to the existing schemes. For instance, our scheme needs in total five bilinear pairing operations, ten ECC point multiplication operations, eight ECC point addition operations and six hashing operations. Following [18], using a 3-GHz pentium IV computer and Java library for pairing based cryptography, the computation times of a bilinear pairing operation, an ECC point multiplication, an ECC point addition, and a hashing operation are $4.14\ ms$, $0.86\ ms$, $0.58\ ms$, and $0.0065\ ms/Byte$, respectively.

Using these measurements, Table III gives the computation times of each node and Fig. 6 gives the total handover delay. It can be seen that the handover delay of our scheme is close to those of the Coa_{HeNB} [14] and Coa_{AP} [15], yet the communication overhead of our scheme is much less, as shown in Fig. 5. It can be concluded from Table III that *the computation overhead on the UE in the proposed scheme is much less than those of the other schemes*. This is a major improvement because the UEs are usually resource limited devices.

C. Practical Consideration

According to [18], one bilinear pairing operation requires $4.14\ ms$. Hence, our scheme requires around $20\ ms$ for all the bilinear pairing operations. According to [19], the handover delay in LTE networks could reach to $50\ ms$ without service

TABLE II: Comparison of Computation overhead.

Schemes	UE	BS	MME	Total
Coa_HeNB [14]	$e + 3m + 4a + 3h$	$e + 5m + 3a + 2h$	$e + 2m + a + h$	$3e + 10m + 8a + 6h$
Coa_AP [15]	$e + 3m + 4a + 3h$	$e + 5m + 3a + 2h$	$e + 2m + a + h$	$3e + 10m + 8a + 6h$
Bouabidi [16]	$e + 4m + 4a + h$	$e + 4m + 4a + h$	$2e + 4m + 2a + 4h$	$4e + 12m + 10a + 6h$
Our scheme	$a + h$	$2e + 4m + 2h$	$3e + 3a + 2h$	$5e + 4m\ 4a + 5h$

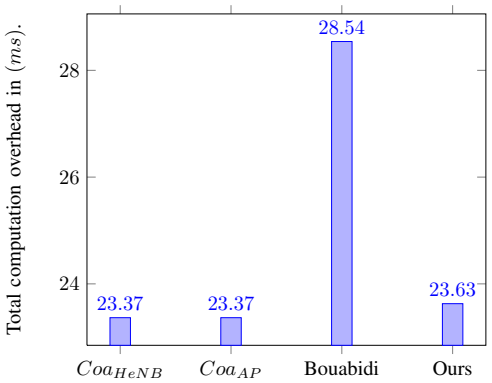

Fig. 6: Computation overhead.

disruption. Therefore, our handover procedure can be used practically. Moreover, unlike traditional hash functions such as SHA-1, our scheme uses hash functions that map to points on an elliptic curve and finite field [20]. They usually use super singular curves with equation $Y^2 = X^3 + b$ and a collision resistance hash function, as explained in [20].

VII. Conclusion

In this paper, we have proposed a secure and efficient handover scheme for the LTE-A networks. The proposed scheme does not trust the base stations because they may be operated by subscribers rather than service providers, accessible to attackers, and use insecure channels like the Internet. Fast handover is important for improving the quality of service and avoiding call termination. The proposed handover procedure needs a small number of packets and little computation delay. The scheme is uniform in the sense that one procedure can be used for all handover scenarios. Our security analysis have demonstrated that our scheme can thwart well-known attacks and achieve backward/forward secrecy. Our performance analysis has demonstrated that our scheme requires a small number of packets and imposes minimal overhead on the mobile nodes which is very desirable because these nodes usually have low computational power and onboard energy supply.

References

[1] 3GPP, "Technical specification group services and system aspects; general packet radio service (GPRS) enhancements for evolved universal terrestrial radio access network (E-UTRAN) access (Rel-10)," no. 23.401, v10.5.0, September 2011.

[2] P. Bhat, S. Nagata, L. Campoy, I. Berberana, T. Derham, et. al., "LTE-advanced: an operator perspective," *IEEE Communications Magazine*, vol. 50, no. 2, pp. 104–114, February 2012.

[3] Z. Haddad , M. Mahmoud, S. Taha, and I. Saroit, "Secure and privacy-preserving AMI-utility communications via LTE-A networks," *Proc. of IEEE 11th International Conference on Wireless and Mobile Computing, Networking and Communications, IEEE WiMob'15, Abu Dhabi, UAE*, 2015.

[4] P. Akula, M. Mahmoud, K. Akkaya, and M. Song, "Privacy-preserving and secure communication scheme for power injection in smart grid," *Proc. of IEEE International Conference on Smart Grid Communications, Miami, USA*, 2015.

[5] S. Tonyali, O. Cakmak, K. Akkaya, M. Mahmoud, and I. Guvenc, "Secure data obfuscation scheme for user privacy and state estimation in smart grid AMI networks," *IEEE Journal on Internet of Things (IoT)*, published online December 2015.

[6] K. Rabieh, M. Mahmoud, K. akkaya, and S. Tonyali, "Scalable certificate revocation schemes for smart grid ami networks using bloom filters," *IEEE Transactions on Dependable and Secure Computing*, to appear.

[7] K. Akkaya, K. Rabieh, M. Mahmoud, and S. Tonyali, "Customized certificate revocation lists for IEEE 802.11s-based smart grid AMI networks," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2366–2374, September 2015.

[8] K. Rabieh, M. Mahmoud, M. Azer, and M. Allam, "A secure and privacy-preserving event reporting scheme for vehicular ad hoc networks," *Wiley Security and Communication Networks*, vol. 8, no. 17, pp. 3271–3281, 2015.

[9] K. Rabieh, M. Mahmoud, T. Guo, and M. Younis, "Cross-layer scheme for detecting large-scale colluding sybil attack in VANETs," *Proc. of IEEE International Conference on Communications (ICC), London, UK*, 8-12 June, 2015.

[10] M. Mahmoud and X. Shen, "An integrated stimulation and punishment mechanism for thwarting packet dropping attack in multihop wireless networks," *IEEE Transactions on Vehicular Technology*, vol. 60, no. 8, pp. 3947–3962, 2011.

[11] M. Mahmoud, X. Lin, and X. Shen, "Secure and reliable routing protocols for heterogeneous multihop wireless networks," pp. 1–1, 2013.

[12] M. Mahmoud, S. Taha, J. Misic, and X. Shen, "Lightweight privacy-preserving and secure communication protocol for hybrid ad hoc wireless networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 8, pp. 2077–2090, August 2014.

[13] M. Mahmoud and X. Shen, "A secure payment scheme with low communication and processing overhead for multihop wireless networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 24, no. 2, pp. 209–224, Feb 2013.

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

[15] J. Cao, M. Ma, and H. Li, "A uniform handover authentication between E-UTRAN and Non-3GPP access networks," *IEEE Transactions on Wireless Communications*, vol. 11, no. 10, pp. 3644–3650, October 2012.

[16] I. Elbouabidi, F. Zarai, M. S. Obaidat, and L. Kamoun, "An efficient design and validation technique for secure handover between 3GPP LTE and WLANs systems," *Journal of Systems and Software* , vol. 91, no. 0, pp. 163 – 173, 2014.

[17] J. Choi and S. Jung, "A handover authentication using credentials based on chameleon hashing," *IEEE Communications Letters*, vol. 14, no. 1, pp. 54–56, January 2010.

[18] M. Scott, "Implementing cryptographic pairings," *Lecture Notes in Computer Science, Springer*, vol. 4575, p. 177, 2007.

[19] H. Kwon, K.-Y. Cheon, and A. Park, "Analysis of WLAN to UMTS Handover," in *IEEE Vehicular Technology Conference (VTC-2007 Fall)*, Sept 2007, pp. 184–188.

[20] T. Icart, "How to Hash into Elliptic Curve," in *university of Laxemborg*, online: https://eprint.iacr.org/2009/226.pdf.