Building Femtocell More Secure with Improved Proxy Signature

Chan-Kyu Han, Hyoung-Kee Choi[1] and In-Hwan Kim
School of Information and Communication Engineering
Sungkyunkwan University, Suwon, South Korea
{hedwig, hkchoi, playkih}@ece.skku.ac.kr

***Abstract*—Demand for the femtocell is largely credited to the surge in a more always best connected communication conscious public. 3GPP define new architecture and security requirement for Release 9 to deal with femtocell, Home eNode B referred as HeNB. In this paper, we analyze the HeNB security with respect to mutual authentication, access control, and secure key agreement. Our analysis pointed out that a number of security vulnerabilities have still not been addressed and solved by 3GPP technical specification. These include eavesdropping, man-in-the-middle attack, compromising subscriber access list, and masquerading as valid HeNB. To the best of our knowledge, any related research studying HeNB security was not published before. Towards this end, this paper proposes an improved authentication and key agreement mechanism for HeNB which adapts proxy-signature and proxy-signed proxy-signature. Through our elaborate analysis, we conclude that the proposed not only prevents the various security threats but also accomplishes minimum distance from user-tolerable authentication delay.**

***Index Terms*— long term evolution (LTE), Home node B (HeNB), femtocell, mobile network security**

I. INTRODUCTION

FEMTOCELL also known as an access point base station enables small cellular communication. It is typically designed for use in residential or small business environments. Femtocell has become even more popular recently in response to increased demand for *always best connected* in fourth-generation networks. 3GPP defines a Home Node B (HeNB) reference architecture to construct femtocell [1][2][3]. As the 3GPP completes the formal standard towards at the end of 2008, network operators (*e.g.* global system for mobile communications, universal mobile telecommunication system, long term evolution) will migrate to support this new architecture for 3GPP femtocell. Note the 3GPP refers to femtocells as HeNB.

A femtocell HeNB can be deployed uncomplicatedly in a variety of indoor scenarios (e.g. home, school and enterprise). Due to its size and weight, these small-sized HeNB can be installed in locations that have stringent site constraints. The valid coverage range of a HeNB is inside a household up to 200m. One of the characteristics in HeNB is to utilize Internet Protocol to connect flat base station architecture. A HeNB is connected to core network via wired broadband connections, which might be insecure. This concept is called *backhaul*.

The 3GPP specifies the threats, the requirements, and the corresponding solution of HeNB security [1]. Most of security vulnerabilities defined in [1] are rooted in (1) a lack of strong mutual authentication between the user equipment (UE) and HeNB, and especially in the UE's lack of capability to authenticate the HeNB with certainty; (2) insecurity of the link between core network and HeNB, backhaul. Wireless link and backhaul are susceptible to many forms of attacks because interception of data in transit and eavesdropping on conversations are highly possible. Furthermore, our analysis indicates that current amendment have still not addressed a number of threats and requirements such that eavesdropping, man-in-the-middle attack, compromising subscriber access list, and masquerading as valid HeNB.

In this paper, we propose the vigorous mutual authentication and access control mechanism by adapting the proxy signature. HeNB operator and core network operator have a contractual agreement on installation, operation and management of HeNB by issuing proxy-signature each other. HeNB operator (core network operator) re-delegates its proxy-signing capability to a HeNB. At the same time, core network operator delegates its signing capability to UE. Hence, the HeNB authenticate UE by verifying signature from HeNB via public key of core network, while the UE authenticate the HeNB by verifying signature from UE via proxy-signed public key of core network operator as well as that of HeNB operator.

The main contribution of this paper are four folds: (1) provide a vigorous mutual authentication and key agreement between UE and HeNB; (2) guarantee secure communication regardless of operation mode in HeNB; (3) prevent a variant of protocol attacks (i.e. masquerading, MitM attack, and DoS attack, etc); (4) present a revocation way of undesirable (a group of) HeNB. To this extent, our analysis and experiment investigates the performance of computation overhead. The result shows that our proposed authentication mechanism performs in only 8.044 microseconds.

The remainder of the paper is organized as follows. We specify HeNB architecture and security requirement in Section 2. Section 3 describes threats on the security of HeNB, and countermeasures. In Section 4, we present the proposed authentication mechanism using proxy-signature. We provide an analysis of security and performance of proposed mechanism in Section 5 and Section 6, respectively. Finally, conclusions are

[1] Corresponding author

978-1-4244-4148-8/09/$25.00 ©2009

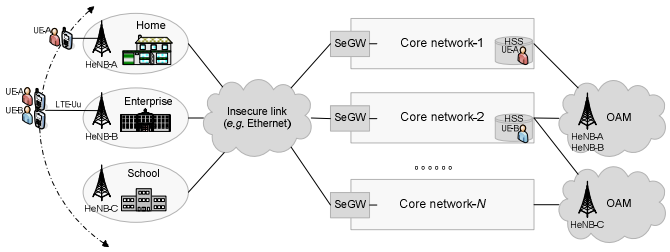


Fig. 1. System architecture of HeNB

offered, along with discussions on future work, in Section 7.

II. HeNB System Architecture and Security Requirement

Fig. 1 describes the system architecture of HeNB and use case. Air interface between UE and HeNB should be backwards compatible with air interface in evolved universal terrestrial radio access (E-UTRAN) namely LTE-Uu. The backhaul between HeNB and security gateway (SeGW) might be insecure. SeGW represent operator's core network to perform mutual authentication with HeNB. A HeNB needs to be configured and authorized by the operation, administration and maintenance (OAM). In Fig. 1, UE-A and UE-B belongs to long term evolution (LTE) core network-1 and core network-2, respectively. UE-A connects her core network-1 via HeNB-A and HeNB-B at home and enterprise, respectively. UE-B connects his core network-2 via HeNB-B at enterprise. Both HeNB-A and HeNB-B are under OAM whose license a HeNB operates. In this circumstance, three contractual relationships should have been established between (1) a HeNB owner (typically be the lead user) and OAM, (2) UE and core network, (3) UE's core network and OAM.

TS 22.220 define the service requirements for the basic functionalities for the support of HeNB [2]. A closed subscriber group (CSG) identifies subscribers (UEs) of an operator who are permitted to access one or more cells of LTE but which have restricted access (CSG cell). A CSG cell sharing the same CSG identity is accessible by the members of the CSG. UE hold white list in the USIM containing all the CSG identities of the CSGs to which the subscriber belongs. Furthermore, five security features must be satisfied [1].

(1) *HeNB access security* includes mutual authentication and security tunnel establishment between HeNB and SeGW. The authentication and key agreement is established by EAP-AKA based and Certificate-based scheme.

(2) *Network domain security* includes security communication between SeGW and core network guaranteed by IPSec.

(3) *HeNB service domain security* includes security communication between HeNB and OAM located in core network for software and configuration update. HeNB should support OAM procedures which allow the network operator to remotely configure the HeNB, deploy software upgrades and perform general OAM tasks.

(4) *UE access control domain security* only applies to legacy UE. For Rel-8 compliant UEs, the access control of the UE is based on the allowed CSG list. CSG identifies subscribers (UEs) of an operator who are permitted to access one or more cells of the public land mobile network (PLMN) but which have restricted access (CSG cells).

(5) *UE access security* provides UEs with secure access to mobile communication system. These properties are as same as the security features defined in the corresponding mobile communication system specification [4].

III. Security Analysis of HeNB

The possible threats in HeNB and corresponding countermeasures will be discussed. The following list summarizes the potential threats of HeNB security and consequences. A detail of each threat is given in [1] with the impact of each threat on different assets and the risk level they belong to. We exclude threats out of network security scope (e.g. physical attacks, attacks on radio resources and management).

(1) *Compromise of HeNB authentication token*: An attacker reads authentication credentials from the wires of the HeNB and takes a copy. Compromised token can be used to masquerade HeNB to UE and mount further attacks towards UE.

(2) *User cloning the HeNB authentication token*: An attacker clones authentication credential of legitimate HeNB and installs credentials into another HeNB. The impact of the attack is worse than threat (1) because the attacker could eavesdrop or spoof any UE.

(3) *Fraud software update/ configuration changes*: HeNB should obviously accept software updates from the OAM in core network. If the software distribution center (i.e. OAM) is compromised, a huge number of HeNBs may receive and install malicious software.

(4) *Mis-configuration and compromise of ACL*: An attacker modifies CSG list thus allowing UEs that could not have access to the network. Attacker could also eliminate UEs that should have access.

(5) *Man-in-the-Middle attacks on HeNB first network access*: An attacker on the internet can intercept all traffic from HeNB and get access to all private information. Such attack allows for eavesdropping of all the data, passing between the HeNB and the core network, and also for sending any data on behalf of any party.

(6) *Attack on OAM and its traffic*: When an intruder can have access to the communication link between the OAM and HeNB, thus it can perform different attacks like sniffing the traffic, (man-in-the-middle (MitM) attack, mis-configuration of the H(e)NB, and fraud software update.

(7) *Threat of HeNB network access*: If there is no such access control information of the service domain for HeNB in H(e)NB SeGW to check the access right of the H(e)NB, the rouge H(e)NB can gain the network accessibility. The attacker could eavesdrop or spoof any UE that camped on the H(e)NB.

(8) *Changing of the HeNB location without reporting*: HeNB

978-1-4244-4148-8/09/$25.00 ©2009

owner may relocate the HeNB and make the provisioned location information invalid.

(9) *Eavesdropping of the other user's E-UTRAN user data*: An attacker possesses HeNB, installs it, and configures to the open access mode. Data, which is neither available unprotected on air-interface, nor with IP-interface security, could be readable. Victim is using normal air interface, but camps to this HeNB without knowledge.

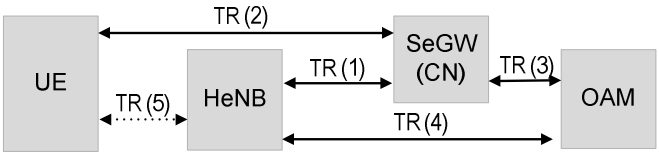
(10) *Masquerade as other users*: The difference with threat 9 is that the attacker in threat 9 only listens such as passive attacker, while in threat 10 attackers also injects spoofed traffic.

(11) *Masquerade as a valid HeNB*: An attacker buys a HeNB and configures it similar to that of the target HeNB's CSG in order to seduce a legitimate UE. Having done that the attacker changes the setting in the HeNB to no encryption and integrity level or has access to the user keys in the HeNB.

Table 1 shows matrix of security threats and countermeasures mapping. To mitigate the previous security threat, security requirements including (1) the mutual authentication and security tunnel establishment between SeGW and HeNB, (2) trusted environment, (3) access control mechanism, (4) location locking mechanism, (5) security mechanism for OAM, (6) user authentication mechanism should be satisfied according to [1].

Fig. 2 depicts the trust relations in HeNB security architecture. The solid arrows represent an explicit mutual trust relationship while the dotted line represents an implicit trust relationship that must be created in order to make security claims about the communications path. Many people believe that the HeNB is sufficiently a trusted party if the core network and OAM authenticates it independently, but this belief is not completely correct.

We have found that the security requirements mentioned in [1] are not sufficient to prevent the security threats completely. Without vigorous mutual authentication between UE and HeNB, it cannot prevent various protocol attack including



TR(1): HeNB access security (Trusted via EAP-AKA, Certificate-based)
TR(2): UE access security (Trusted via 3GPP TS 33.401)
TR(3): Contractual agreement
TR(4): HeNB Ownership
TR(5): Access control for UE (implicit)

Fig. 2. The Trust relations (TR) in HeNB security architecture

MitM attack, masquerade as valid HeNB, attack occurred in the circumstance under OAM disguise both core network and UE. Furthermore, core network and OAM must collaborately authenticate HeNB because honesty between them is not valid in IP based network.

To summarize, UE does not have any clue that a HeNB is guaranteed by both UE's core network and legitimate OAM when it mount on a HeNB. On the other side, CSG which can be compromised and disguised by attacker is not completely sufficient for HeNB to authenticate UE.

IV. Proposed Scheme

In this proposed scheme, we present the vigorous mutual authentication and key agreement protocol between (1) UE and core network (CN), (2) HeNB and OAM, and finally (3) UE and HeNB. As shown in Fig. 1, various CN and OAM are meshed within system architecture. CN have a contractual relationship with limited number of OAM. In this circumstance, UE must confirm whether an associated HeNB belong to one of the contracted OAM with UE's CN operator. Note that UE-A cannot connect to her CN (Core network-1) via HeNB-C because her CN has no agreement with the HeNB-C's OAM while UE-B can do. OAM should convince UE to authenticate HeNB in company with corresponding CN. Proxy-signature scheme provides an outstanding way of delegating and verifying among entities. In this paper, OAM issues the proxy signature on behalf of CN to HeNB. The CN also issues the proxy

TABLE 1. SECURITY THREATS AND ITS COUNTERMEASURE

Threat group	number	Security threats	Countermeasure
Compromise HeNB credentials	1	Compromise HeNB authentication token	Authentication credentials of the H(e)NB shall be stored inside trusted platform module (TPM) or a UICC
	2	User cloning the HeNB authentication token	The users could be required to obviously confirm their acceptance before being joined to HeNB
Configuration attacks on HeNB	3	Fraud software update/ configuration changes	All software and configuration changes shall be cryptographically signed by OAM
	4	Mis-configuration and compromise of CSG	Secure means of creation, maintenance and storage of CSG is required.
Protocol attacks on HeNB	5	MitM attacks on HeNB first network access	HeNB's credentials shall be recognized at the core network operator's side
	6	Attack on OAM and its traffic	The communication between the HeNB and the OAM should be secured
	7	Threat of HeNB network access	SeGW in core network should have the related profile information of HeNB to check whether a HeNB can access the network
	8	Changing of the HeNB location without reporting	Location locking mechanism shall be designed and implemented
User data and identity privacy attack	9	Eavesdropping of the other user's E-UTRAN user data	The user could be notified when the UE camps on a closed or open type HeNB
	10	Masquerade as other users	Same as threat 9
	11	Masquerade as a valid HeNB	CSG setting and other configuration should be hidden

978-1-4244-4148-8/09/$25.00 ©2009

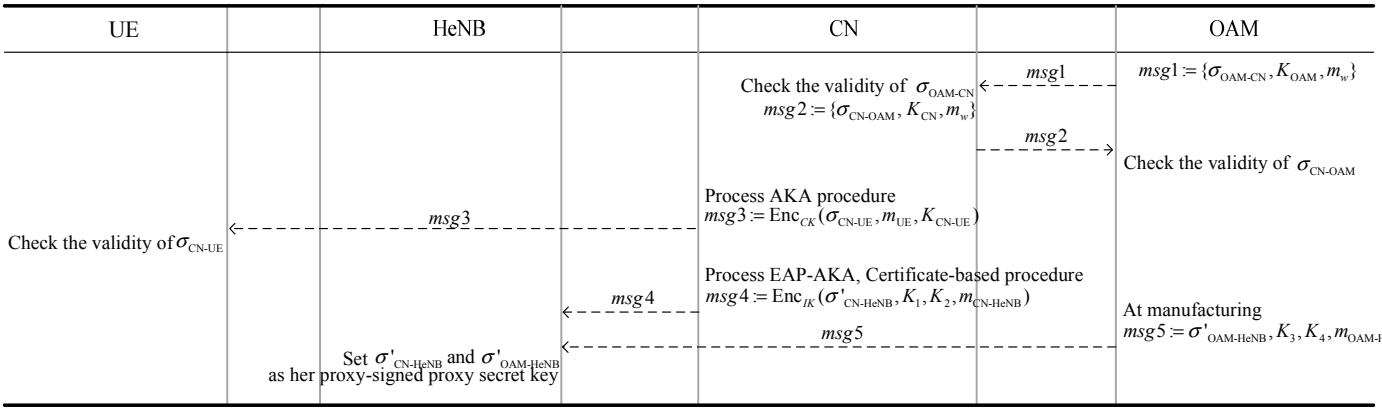


Fig. 3. Registration phase

signature on behalf of OAM to HeNB, and its own signature to UE. And then, UE (HeNB) trust HeNB (UE) with proxy signature on behalf of CN and OAM.

A. Proxy signature

In the proxy signature scheme introduced by Mambo, Usuda and Okamoto [5], an original signer delegates his signing power to another signer called a proxy signer. Then the verifier is able to verify the signature using the original signer's public value. This is similar to a person delegating her seal to another person in the real world. Two large prime number p and q such that $q|(p\text{-}1)$, a generator $g \in Z_p^*$ with order q, and one way hash function $h(\cdot)$ are assumed to be public. The original signer has its private key $s \in Z_q$, and public key v where $v=g^s \bmod p$. Proxy signature scheme consists of three steps:

- (Generation) An original signer select a random number $k \in Z_q$, then compute a commitment $K=g^k \bmod p$. After that, she calculates the proxy signature $\sigma = s + kK \bmod q$.
- (Delivery) The original signer gives (σ, K) pair to a proxy signer in a secure way.
- (Verification) The proxy signer checks a congruence such that $g^\sigma \equiv vK^K \bmod p$. If (σ,K) pair passes it, she accept it as a valid proxy signature confirmed by original signer.

When the proxy signer sign a document *on behalf of* the original signer, she could use σ as an alternative her secret key, and executes the ordinary signing operation based on discrete logarithm problem (DLP). The verification of the proxy signature is carried out by the same checking congruence operation as in the original signature scheme. The computation of new public value v' ($\equiv vK^K \bmod p$) is only the exceptional.

Add to this basic concept of proxy signature, further requirements are satisfied for adapting proxy signature to HeNB security: (1) a warrant stating its valid period, corresponding entities' identity, and their relation should be considered; (2) original signer should not violate the right of proxy signer, and (3) a signer could delegate her signing capability according to the priority order of works. Note that in the real world, a person possess a legal seal and many other seals simultaneously.

Kim *et al*. presents a new type of digital proxy signatures called *partial delegation with warrant* [6]. In a *multi-proxy signature* scheme [7], an original signer could delegate signing power to multiple proxy signers. In a contrary concept, a *proxy multi-signature* scheme [8], a designated proxy signer can generate the signature on behalf of a group of original signers. We considered Kim *et al*'s scheme as the solution toward first and second requirement. Multi-proxy signature and proxy-multi signature would be out of candidate, because the entire group member must be engaged in both schemes. Therefore, we propose a new proxy signature scheme that satisfies the above requirement including the third one.

B. Registration

Fig. 3 depicts the message flow of the registration phase in the proposed mechanism. The five messages (from *msg*1 to *msg*5) could be piggybacked in preliminarily authentication scheme (*e.g. msg* 4 is piggybacked in user authentication response message defined in [4]). Throughout this paper, $\sigma_{x\text{-}y}$ means that x delegates her signing power to y. s_x, v_x ($\equiv g^{s_x} \bmod p$), and ID_x are, respectively, x's private key, x's public key, and identity of x. The registration phase is as follows.

*Msg*1: Upon agreement, the OAM issues proxy signature with warrant m_w ($\sigma_{\mathrm{OAM\text{-}CN}}$, m_w, K_{OAM}) to a corresponding CN. Proxy signature generation with warrant is similar to [6] as shown in equation (1). m_w consist of ($\mathrm{ID}_{\mathrm{OAM}} \| \mathrm{ID}_{\mathrm{CN}} \| t_{\mathrm{agreement}}$).

$$\begin{aligned} e &= h(m_w \| K_{\mathrm{OAM}}) \\ \sigma_{\mathrm{OAM\text{-}CN}} &= e \cdot s_{\mathrm{OAM}} + k_{\mathrm{OAM}} \bmod q \end{aligned} \tag{1}$$

Upon receipt of *Msg*1, CN checks its validity by computing equation (2).

$$g^{\sigma_{\mathrm{OAM\text{-}CN}}} \equiv v_{\mathrm{OAM}}{}^{e} K_{\mathrm{OAM}} \bmod p \tag{2}$$

*Msg*2: CN generate proxy signature ($\sigma_{\mathrm{CN\text{-}OAM}}$, m_w, K_{CN}), and then send it to OAM. The OAM check the equality by the same checking congruence operation as in the first step. If the congruence holds, OAM accept $\sigma_{\mathrm{CN\text{-}OAM}}$ as proxy signature.

*Msg*3: We assume that UE performed authentication and key agreement [4] via eNB on behalf of mobility management entity in CN. After AKA, confidentiality key (CK) could be computed by UE and MME. In the last message of AKA, the proxy signature, ($\sigma_{\mathrm{CN\text{-}UE}}$, m_{UE}, $K_{\mathrm{CN\text{-}UE}}$), would be encrypted with CK and sent to UE. m_{UE} consist of ($\mathrm{ID}_{\mathrm{UE}} \| \mathrm{ID}_{\mathrm{CN}} \| \mathrm{AV}_n$) where AV_n is remained number of authentication vector.

*Msg*4: At this phase, CN *again* delegates her *proxy* signing capability ($\sigma_{\mathrm{OAM\text{-}CN}}$) to HeNB. She firstly sets her proxy signing power ($\sigma_{\mathrm{OAM\text{-}CN}}$) as her *proxy-signed* private key (s'_{CN}) and

978-1-4244-4148-8/09/$25.00 ©2009

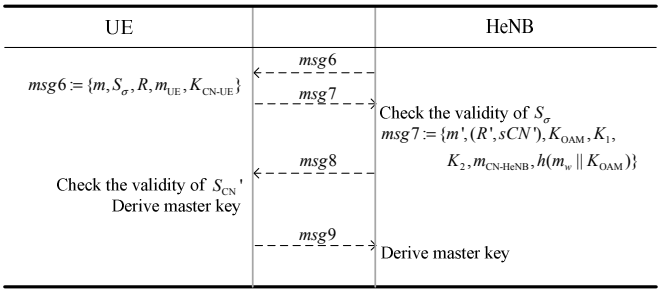


Fig. 4. Authentication and Access control phase

compute corresponding public key (v'_{CN}). CN choose random number k_1, $k_2 \in Z_q$, computes $K_1=g^{k1} \bmod p$ and $K_2=g^{k2} \bmod p$. Then the CN compute her temporary *proxy-signed proxy capability* according to equation (3). σ'_{x-y} means that x re-delegates her *proxy*-signing authority from someone to y, simply *proxy-signed proxy signature*.

$$\sigma'_{CN-HeNB} = k_1 + (\sigma_{\text{OAM-CN}} + k_2) \cdot h(m_{\text{CN-HeNB}}) \bmod q \quad (3)$$

Then, CN publish $\sigma'_{\text{CN-HeNB}}$, K_1, K_2 and $m_{\text{CN-HeNB}}$ in the last message of EAP-AKA, or Certificated-based device authentication securely. $m_{\text{CN-HeNB}}$ specifies corresponding HeNB's identity, belonging CSG cell and ID_{CN}, ($\text{ID}_{\text{HeNB}} \| \text{ID}_{\text{CSGcell}} \| \text{ID}_{\text{CN}}$).

Msg5: OAM operates as exactly same as the CN did in *Msg*4. OAM embed $\sigma'_{\text{OAM-HeNB}}$, K_3, K_4 and $m_{\text{OAM-HeNB}}$ at manufacturing.

$$\sigma'_{\text{OAM-HeNB}} = k_3 + (\sigma_{\text{CN-OAM}} + k_4) \cdot h(m_{\text{OAM-HeNB}}) \bmod q \quad (4)$$

Note that a group of HeNB with same security policy or CSG identity (white list) might have same $\sigma'_{\text{OAM-HeNB}}$ and $\sigma'_{\text{CN-HeNB}}$. It is not desirable that OAM (CN) delegate her signing capability to HeNB directly, because CN must be notified that OAM configured and operated in accordance with the warranty agreed with the CN, vice versa. In addition, the HeNB becomes a single point of failure, making for easy exposure to potential adversaries.

C. Authentication and Access Control

After registration phase, authentication and access control phase is executed as shown in Fig. 4.

*Msg*6: Upon this phase, mutual authentication phase begins with the request of HeNB toward UE's identity.

*Msg*7: UE prove its authenticity toward HeNB by using its proxy signature received in *Msg*3, ($\sigma_{\text{CN-UE}}$, m_{UE}, $K_{\text{CN-UE}}$). UE sign *Msg*3 where $r \in Z_q$, $R \equiv g^r \bmod p$. Assume that Nyberg Rueppel signature scheme [9] is used. Then, UE send S_σ, R, m_{UE}, and $K_{\text{CN-UE}}$ to HeNB with message $M=(\text{ID}_{\text{UE}} \| \text{ID}_{\text{CN}} \| r_{\text{UE}})$.

$$S_\sigma \equiv r - R\sigma_{\text{CN-UE}} \cdot h(M) \bmod q \quad (5)$$

*Msg*8: Upon receipt of *Msg*7, HeNB would verify the following equation (6) where v_{CN} is the public key of CN. If equation (6) holds, HeNB authenticate UE. ■

$$\begin{aligned} v &\equiv v_{\text{CN}}^{\,h(m_{\text{UE}} \| K_{\text{CN-UE}})} K_{\text{CN-UE}} \bmod p \\ R &\equiv g^{S_\sigma} v^{R \cdot h(\text{ID}_{\text{UE}} \| \text{ID}_{\text{CN}} \| r_{\text{UE}})} \bmod p \bmod q \end{aligned} \quad (6)$$

Note that HeNB would have a temporal proxy-signed proxy signature $\sigma'_{\text{CN-HeNB}}$ (delegated by $\sigma_{\text{OAM-CN}}$). The HeNB chooses r' randomly, and computes for the following equation (7). HeNB send (m', (R', S_{CN}'), K_{OAM}, K_1, K_2, $m_{\text{CN-HeNB}}$, $h(m_w \| K_{\text{OAM}})$) where $R' \equiv g^{r'} \bmod p$ and $m'=(\text{ID}_{\text{HeNB}} \| \text{ID}_{\text{CSG}} \| \text{ID}_{\text{OAM}} \| \text{ID}_{\text{CN}} \| r_{\text{HeNB}})$. ID_{CSG} could include the location information of HeNB.

$$S_{\text{CN}}' = r' + \sigma'_{\text{CN-HeNB}}\, h(m') \bmod q \quad (7)$$

*Msg*9: The verifier UE recovers the proxy-signed public key v_p ($v_p \equiv g^{\sigma' \text{CN-HeNB}} \bmod p$) as shown in equation (8). Note that $v_{\text{CN}}' \equiv v_{\text{OAM}}{}^e K_{\text{OAM}} \bmod p$.

$$v_p = K_1 \cdot (v_{\text{CN}}' \cdot K_2)^{h(m_{\text{CN-HeNB}})} \bmod p \quad (8)$$

Then, UE check the validity of the next equation (9). If the equality holds the verifier UE accepts (r', S_{CN}') as the valid proxy-signed (proxy) signature, and authenticates HeNB. ■

$$g^{S_{\text{CN}}'} \equiv r' v_p^{\,h(m')} \bmod p \quad (9)$$

In case of $\sigma'_{\text{OAM-CN}}$, it is self-explanatory. We cannot help excluding the correctness of our protocol because of the space limitation. After successful authentication, the two keys, CK and IK, are available to encrypt and to authenticate messages of user data. The CK and IK are derived by diffie-hellmen key agreement as shown in equation (10).

$$CK \| IK \equiv g^{r_{UE} r_{HeNB}} \bmod p \quad (10)$$

V. Security Analysis

Our proposed mechanism satisfies the following proxy-signature properties:

- *Unforgeability*: Only the delegated UE can generate the proxy signature using $\sigma_{\text{CN-UE}}$ on behalf of the CN. HeNB can generated the proxy-signed proxy signature using $\sigma'_{\text{CN-HeNB}}$ on behalf of the CN with the permission of OAM ($\sigma_{\text{OAM-CN}}$), and vice versa. DLP make it computationally difficult to compute $\sigma'_{\text{CN-HeNB}}$ and $\sigma_{\text{CN-UE}}$ although an attacker have its public values, ((R', s_{CN}'), v_p, K_{OAM}, K_1, K_2, $m_{\text{CN-HeNB}}$) and $m_{\text{CN-UE}}$.
- *Undeniability*: When the proxy-signed signature (m', (R', s_{CN}'), K_{OAM}, K_1, K_2, $m_{\text{CN-HeNB}}$) is verified, the warrant $m_{\text{CN-HeNB}}$ is checked, and the signer's proxy public-key v_{CN}', and the original signer's public-key v_{OAM} is used. The signer, CN, cannot deny its signature to be sent to HeNB. Therefore, the proposed scheme satisfies the undeniability property. In case of OAM, it is self-explanatory. UE also cannot deny its signature, for mercy of original proxy-signature property.
- *Identifiability*: The original signer, OAM, can identify the CN corresponding to a proxy signature from that signature S_{CN}' (signed by $\sigma'_{\text{CN-HeNB}}$), and vice versa. Moreover the original signer CN can identify the UE by taking a look into S_σ (signed by $\sigma_{\text{CN-UE}}$).
- *Distinguishablity*: In case of UE authentication, when the proxy signature ($\sigma_{\text{CN-UE}}$, m_{UE}, $K_{\text{CN-UE}}$) is used, anyone can distinguish the proxy signature from normal signatures. And in case of HeNB authentication, proxy-signed public key v_p is used to verify the proxy-signed proxy signature, while v_{CN}' would be used to verify the proxy signature of v_{OAM}. Thus anyone can distinguish it from normal signature.

978-1-4244-4148-8/09/$25.00 ©2009

The following list summarizes the security strength of our enhancement.

- *Mutual authentication between UE and HeNB*: This improvement originates from the fact that CN and OAM collaborately ensures mutual authentication between UE and HeNB. The HeNB check the message from UE whether CN sign or not. The UE also check the message from HeNB exactly proxy-signed by CN and OAM.
- *Key agreement*: The strength of the key derivation scheme is that the authentication entities can contribute to the key generation. The proposed scheme is a good example of the key derivation scheme. Each entity contributes its random value (r_{UE}, r_{HeNB}).
- *Withstanding protocol attacks*: Basically our key agreement is same as in Diffie-hellman key exchange. However, MitM attacker is prevented because OAM and CN confirm this contribution with the proxy-signatures. A malicious OAM with a legitimate HeNB could not deceive CN, because $\sigma_{CN\text{-}OAM}$ will be definitely needed when HeNB communicate with UE. Precisely, neither CN nor OAM operates by itself. An attacker without possessing proxy-signature from CN could not masquerade as a valid HeNB.
- *Revocable proxy-signature*: If OAM (CN) want a specific (group of) HeNB retired, simply it revoke a pair of $\sigma'_{OAM\text{-}HeNB}$ ($\sigma'_{CN\text{-}HeNB}$) and public value. Although it revoke proxy-signed proxy signature, agreement with CN and OAM still valid in terms of proxy signature $\sigma_{CN\text{-}OAM}$ and $\sigma_{OAM\text{-}CN}$. Thus, single-point of failure effect will be minimized.
- *Temporary user authentication:* For temporary members, it shall be possible to limit the period of time during which the subscriber is considered a member of a CSG. In our proposed scheme, UE could re-delegate its proxy signed power, $\sigma_{CN\text{-}UE}$, to temporary member. The generation and verification of proxy-signed proxy signature is equivalent with Msg 4(5).
- *Secure software/configuration update*: All software updates and configuration changes shall be cryptographically signed via v_{OAM}, and encrypted with $\sigma'_{OAM\text{-}HeNB}$ in symmetrical way.

VI. Performance Evaluation

TABLE 2. AUTHENTICATION DELAY IN TERMS OF OPERATIONAL COST

Message	UE	HeNB
Msg6	-	-
Msg7	$2T_M+T_H+1T_A$	$3T_E+3T_M+2T_H$
Msg8	$3T_E+3T_M+2T_H+1T_A$	$1T_M+1T_H+1T_A$
Msg9	$1T_E$	$1T_E$

Table 2 shows the operational cost in proposed scheme. T_E, T_M, T_H, and T_A, respectively, are the operational costs of the modular exponentiation, multiplication, hash, and arithmetic operation. We intently do not include operational cost from Msg1 to Msg4. The reason is as follows. Msg1 and Msg2 could be exchanged when a contractual agreement is associated between the OAM and the CN. Msg5 also would be embedded in HeNB when it is manufactured. Msg3 and 4 could be pre-computed during the ordinary authentication procedure. Thus, the total operational cost will take $8T_E+9T_M+6T_H+2T_A$ to complete four-way handshake (from Msg6 to Msg9).

We measured the computational speeds of the T_M, T_E, T_H and T_A using Xyssl [10]. XySSL is an open-source cryptographic library written in C. It currently features several symmetrical ciphers, hash functions, RSA, X.509 reading support, and so on. We have tested on the Pentium III 500GHz process to simulate mobile computing environment. The results showed that while modular exponentiation took 0.98, multiplication, hash, and arithmetic operation took 0.00758, 0.0202 and 0.00743 in microseconds for 1024bits. Based on these result, the total authentication delay approximately took 8.044 microseconds which could not nearly be recognized in UE side. Note that RSA 1024 encryption took 8.921 microseconds.

VII. Conclusion

In this paper, we have analyzed HeNB architecture and investigated the security that it provides. Although the 3GPP HeNB introduces access control for the UE and HeNB, it is still vulnerable to a variant of malicious attack (e.g. masquerading). This vulnerability allows an adversary to redirect user traffic, induce user to attach malicious HeNB. In order to eliminate these security problems, we have presented a novel authentication and key agreement mechanism. This proposed mechanism improves authentication performance in three ways: (1) enhanced mutual authentication between UE and HeNB, (2) prevention of the rogue HeNB attack and its variants, and (3) reduction of signaling load and computation delay. Finally, several further aspects remain to be investigated to make our system more suitable for real scenario. As many core network operators rely on Internet connectivity for authentication of UE, an interesting *chicken* and *egg* problem must be overcome to adapt proxy-signature.

References

[1] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security of H(e)NB (Rel. 8), 3GPP TR 33.820 v1.3.0, Jan. 2009.

[2] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Service requirements for Home NodeBs and Home eNodeBs (Rel. 9), 3GPP TS 22.220 v1.0.1, Dec. 2008.

[3] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Architecture aspects of Home NodeB and Home eNodeB (Rel. 9), 3GPP TS 23.830 v0.3.0, Feb. 2009.

[4] 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; 3GPP System Architecture Evolution; Security Architecture (Rel. 8), 3GPP TS 33.401 v8.2.1, Dec. 2008.

[5] M. Mambo, K. Usuda, and E. Okamoto, "Proxy signatures: Delegation of the power to sign messages," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, pp.1338-1354, Vol.E79-A, No.9, 1996.

[6] S. Kim, S. Park and D. Won, "Proxy signatures, Revisited," *Proceedings of the First International Conference on Information and Communication Security*, LNCS, Vol. 1334, pp.223-232, 1997.

[7] S.-J. Hwang and C.-H. Shi, "A Simple Multi- Proxy Signature Scheme," *Proceedings of the 10th National Conference on Information Security*, pp. 134-138, 2000.

[8] L. Yi, G. Bai and G. Xiao, "Proxy multi-signature scheme: A new type of proxy signature scheme," *IEEE Electronics Letters*, pp.527-528, Vol.36, No.6, 2000.

[9] K. Nyberg, R. A. Rueppel, "A new signature scheme based on the DSA giving message recovery," *Proceedings of the first ACM Conference on Computer and Communications Security*, pp. 58-61, 1993.

[10] xyssl (PolarSSL), *available at* http://polarssl.org/

978-1-4244-4148-8/09/$25.00 ©2009