

Making HeNB More Secure with Improved Secure Access Protocol and Analyzing It

Fariba Ghasemi Najm^{1(✉)}, Ali Payandeh², and Hashem Habibi³

¹ Informatics Services Corporation (ISC), Network Support Building,
Tehran, Iran

F_Ghasemi@ISC.CO.IR

² Faculty of Information, Communication and Security Technology, Malek
Ashtar University of Technology (MUT), Tehran, Iran

³ Faculty of Computer Engineering, Sharif University of Technology,
Tehran, Iran

Abstract. The 3rd Generation Partnership Project (3GPP) defined a new architecture, called Home eNode B (HeNB). HeNB is able to provide new services with higher data rate in a low cost. Security is a critical aspect of HeNB. In order to have HeNB secure access to core network, 3GPP defines an authentication protocol based on IKEv2. A number of security vulnerabilities such as HeNB masquerading have not been addressed and solved by 3GPP technical specification yet. In this paper an improved HeNB authentication protocol is introduced which does not allow an attacker to connect unauthorized network users using a mask. Finally, we evaluate our protocol performance and verify it by Automated Validation of Internet Security Protocols and Applications (AVISPA). Through our security analysis, we conclude that not only the proposed protocol prevents the various security threats but also it has no significant effect on authentication delay and cost.

Keywords: LTE · HeNB · Protocol · Authentication · Security · IPSec

1 Introduction

LTE (Long Term Evolution) was investigated by 3GPP in 2004. LTE general structure has two parts; access network (E-UTRAN) [21, 22] and core network (CN) [1, 19]. One of elements of E-UTRAN is HeNB that is introduced by 3GPP in release 9.

HeNB is located on the customer premises and connected to the core network via unsafe links such as broadband lines [1]. Some vulnerabilities are emerged by introducing HeNB. 3GPP specifies threats, requirements, and corresponding solution of HeNB security in [4, 16]. 3GPP points that the following authentications are necessary for HeNB authentication:

- Mutual authentication between HeNB device and the operator's network
- Authentication of the Hosting Party (HP) by the operator's network

Among several authentication issues, combined device and HP authentication is an important security mechanism; it guarantees that HeNB device can access Core

Network safely. To achieve this aim, 3GPP has proposed a method that combines certificate and Extensible Authentication Protocol [8] for Authentication and Key Agreement (EAP-AKA [9]) –based authentication running within Internet Key Exchange (IKEv2) protocol [3, 14] between HeNB and security gateway (SeGW) for mutual authentication of HeNB and CN.

To reduce the communication costs of authentication protocol introduced by 3GPP, a low-cost re-authentication protocol [10, 15] is proposed in [5]. HeNB can't access CN via these two protocols (EAP-AKA and the proposed protocol in [5]) safely yet; the threats that make HeNB access unsafe via these two protocols, are explained in [6]. One of these threats is HeNB masquerading attack in which HeNB uses other HeNB's ID during UE connection that that ID differs from the one used during its mutual authentication with SeGW.

In this paper, we propose a method that solves the problems disregarded by available protocols; this aim is done by adding a digital signature of HeNB's identity information that is sent to the CN. Therefore, HeNB masquerading attack and derived attacks such as denial of service, billing issues and user privacy issues [17] are avoided.

The remainder of the paper is organized as follows. A brief explanation of HeNB architecture in LTE is provided in Sect. 2. We specify initial and re-authentication protocol between HeNB and SeGW and their analyzing in Sects. 3 and 4. In Sects. 5 and 6, the proposed improved HeNB secure access protocol and its security analyzing are presented. Finally, conclusions are offered in Sect. 7.

2 LTE Structure with HeNBs

HeNB is introduced to provide mobile communication coverage and allows users to have a local and public access. HeNB architecture in LTE is shown in Fig. 1; some of its elements are described below.

Home eNode B: HeNB is introduced by 3GPP in release 9 and known as a femtocell [2]. HeNB is a base station that makes small cellular communication possible. It is designed for using in small business or residential environments [5].

Security Gateway (SeGW): SeGW is an entrance gateway for all traffics routed to the network and is located on the border of core network. HeNB connects to core network via an IPSec tunnel [12, 13] that is created after mutual authentication of HeNB and SeGW [5, 20].

Backhaul link: The link between HeNB and SeGW that carries S1 and routed management traffic is called backhaul link. Because of extension of backhaul link across the public internet, this link is unsafe; therefore, many of HeNB threats are related to this unsafe link [1].

HeNB Management System (HeMS) or operation, administration and maintenance (OAM): HeMS or OAM is responsible for the management of the HeNB [2]. Depending on the operator's decision, this element may be located within the operator core network or accessible directly on the public Internet [1].

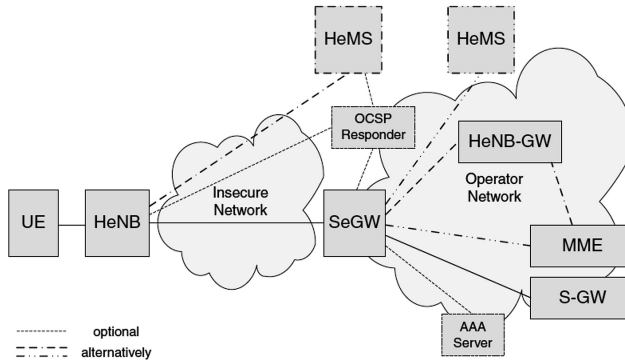


Fig. 1. Structure of HeNB access to the core network [1].

Authentication, Authorization and Accounting (AAA) server and Home Subscriber Server (HSS): HSS stores the compromised, signed, and authenticated data of the HeNBs. When hosting party authentication is required, AAA server authenticates the hosting party based on the authentication information retrieved from HSS [5].

Figure 2 describes the system architecture of HeNB. A HeNB needs to be configured and authorized by the OAM or HeMS. In Fig. 2, UE-A and UE-B belong to the LTE core network-1 and core network-2, respectively. OAM supports both HeNB-A and HeNB-B and allows them to operate. CN has a contractual relationship with limited number of OAMs [18]. In this circumstance, UE must confirm whether the specified HeNB belongs to one of the contracted OAM or not; for example, UE-A cannot connect to its CN via the HeNB-C because its CN does not have any contract with the HeNB-C’s OAM while UE-B can do [7].

TR 33.820 defines the security requirements for the support of HeNB; one of these requirements is mutual authentication between HeNB and SeGW for HeNB secure access.

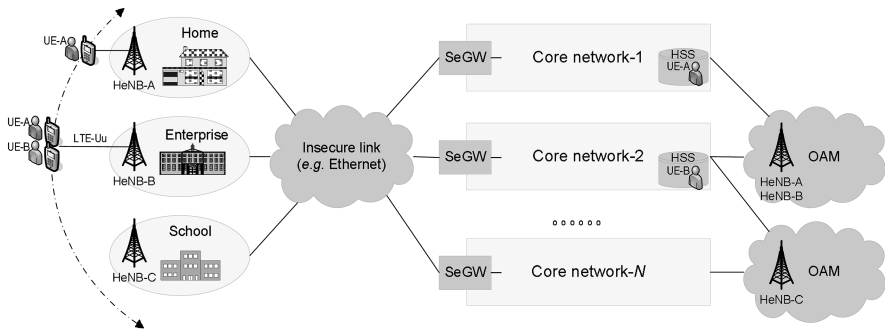


Fig. 2. HeNB system architecture [7].

3 Initial Authentication and Re-Authentication Protocol Between HeNB and SeGW

Combined device and HP authentication including mutual authentication between HeNB and CN based EAP-AKA protocol is shown in Fig. 3.

In order to reduce communication, computation and energy cost, a simple and low-cost re-authentication protocol is proposed in [5], which does not compromise the provided security services. The proposed protocol in [5] uses a Master Session Key (MSK) parameter that had been computed in the initial authentication, and does not require the full initial authentication to be repeated. In fact the proposed protocol in [5] does not modify 3GPP infrastructure and is applied to the HeNB system.

For implementation of re-authentication protocol, it is required to apply minor changes to the initial authentication protocol. In Fig. 3, Step 10, when AAA server received AVs from HSS, it computes an MSK as

$$\text{MSK} = \text{prf}(\text{CK} || \text{IK} || \text{Identity}). \quad (1)$$

Where prf is a pseudo-random function, “||” denotes concatenation, CK is the encryption key, IK is the integrity key, and Identity belongs to HeNB. In initial authentication, MSK is used in AUTH calculation. In addition MSK is an authentication parameter in re-authentication protocol.

Then AAA server stores the calculated MSK and creates a list that binds the identity of HeNB with corresponding MSK. Similarly, HeNB computes an MSK using formula (1) and stores it. The proposed re-authentication protocol is shown in Fig. 4.

We present a brief description of Fig. 4 in the following. At first, HeNB and SeGW shares their security association [11], nonce and Diffie-Hellman value (details are available in [3]). After establishment of first phase of IKEv2 or IKE_SA, HeNB sends its ID, nonce, and $\text{AUTH}_{\text{HeNB}}$ (*i.e.* a MAC value computed over the first IKEv2 message using the stored MSK and its N_{HeNB}) to the SeGW.

$$\text{AUTH}_{\text{HeNB}} = \text{prf}(\text{MSK} || N_{\text{HeNB}}). \quad (2)$$

Then SeGW forwards ID_{HeNB} to AAA server. AAA server according to the identity of HeNB, sends pre-calculated MSK to SeGW via the diameter protocol. Upon receiving the MSK, SeGW calculates $\text{AUTH}_{\text{HeNB}}$ using available parameters and verifies it. In this way, HeNB is authenticated.

To complete re-authentication protocol, HeNB verifies $\text{AUTH}_{\text{SeGW}}$ using MSK and N_{SeGW} for authenticating SeGW. After successful verification, HeNB and SeGW have been authenticated mutually using $\text{AUTH}_{\text{HeNB}}$ and $\text{AUTH}_{\text{SeGW}}$, respectively. Finally, an IPSec tunnel is established between HeNB and SeGW that provides security services to the transmitted data [5].

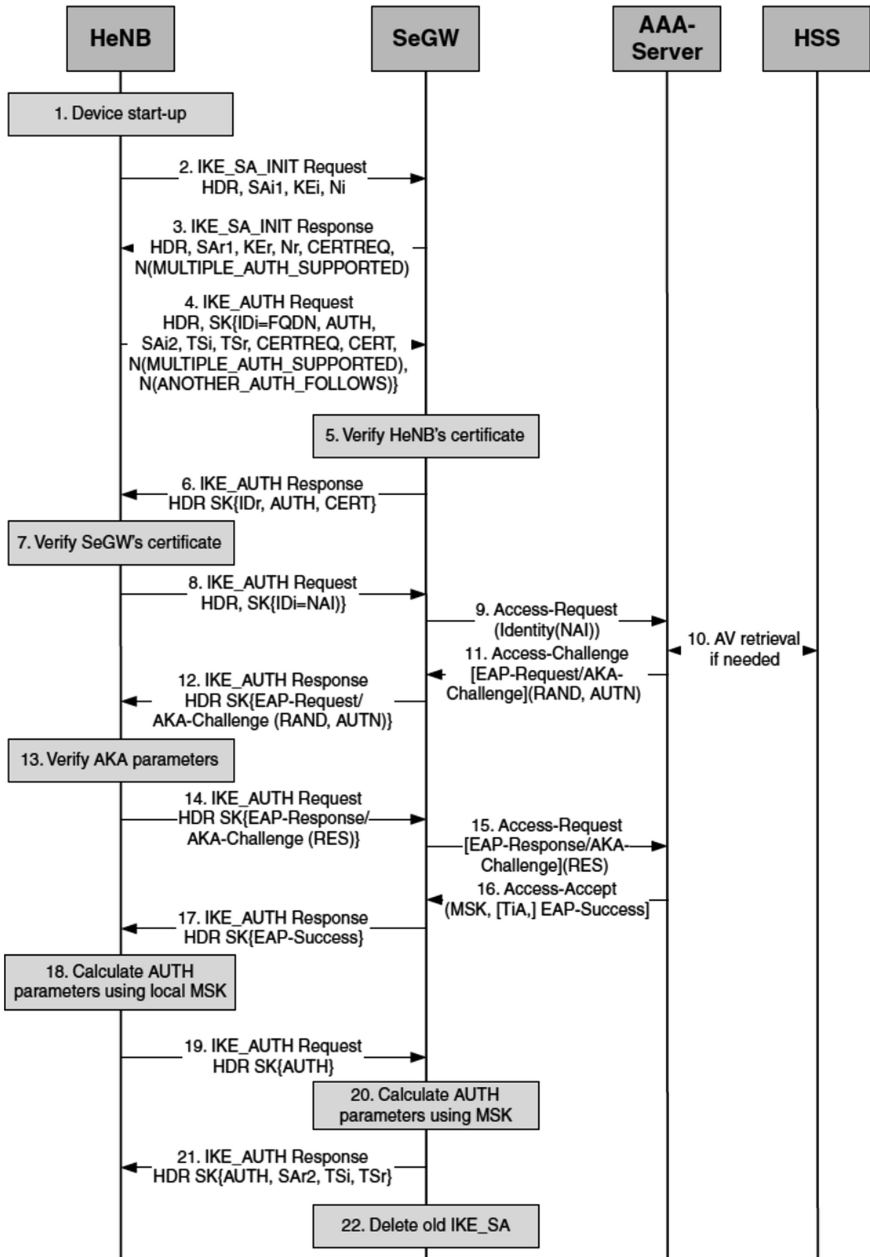


Fig. 3. Initial authentication based EAP-AKA protocol [1].

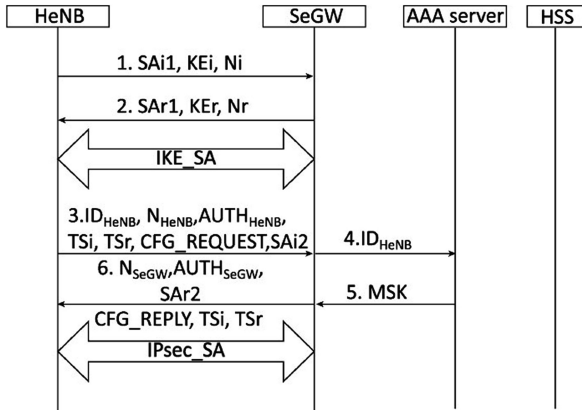


Fig. 4. Re-authentication protocol proposed in [5].

4 Security Analyzing of Authentication Protocol Introduced in 3GPP

After establishment of IPsec tunnel between HeNB and SeGW, HeNB will be reliable from the view point of the SeGW. When UE connects to the core network via HeNB, access control on UE starts to operate. As UE connects to HeNB, if UE belongs to the Closed Subscriber Group (CSG) list, HeNB sends CSG ID supported by itself to CN [2]. CN specifies UE access license according to the subscription data obtained from HSS.

The authentication protocol introduced in 3GPP and [5], does not guarantee that the identity sent to CN by HeNB is the same as the identity during the mutual authentication with SeGW. In fact, in a lot of scenes, HeNB uses the identity in CN, which is different from the one during the mutual authentication with SeGW. According to these protocols SeGW is not responsible for the authentication of the identity used by HeNB in CN.

According to the authentication protocol introduced in 3GPP and [5], HeNB will be able to illegally use other’s user IDs when communicating with CN; for example, first, HeNB1 uses the true identity to establish an IPsec tunnel and mutual authenticate with SeGW; when the UE accesses to HeNB1, HeNB1 sends ID_{HeNB2} and CSG ID supported by HeNB2 to CN. According to CSG ID of HeNB2, the access of UE is allowable; however, the access of UE will not be allowable if it is based on CSG ID supported by HeNB1. So, HeNB1 illegally uses other’s identity, thus enabling the user, who is originally not allowed to access, which results in destroying the security of the network [6].

5 Improved HeNB Secure Access Protocol

According to the current problem of the introduced protocol in 3GPP and [5], SeGW should send valid information of HeNB used in establishment of IPsec tunnel to the CN; so one interface is added between SeGW and CN which carries HeNB

characteristics and forwards it to the CN. Note that in order to design an improved protocol, the selected network element by SeGW (for sending characteristics of HeNB) and the selected network element by HeNB (for connecting to CN) must be the same.

Improved HeNB authentication protocol is shown in Fig. 5 (some of payloads are ignored) and operates as follows.

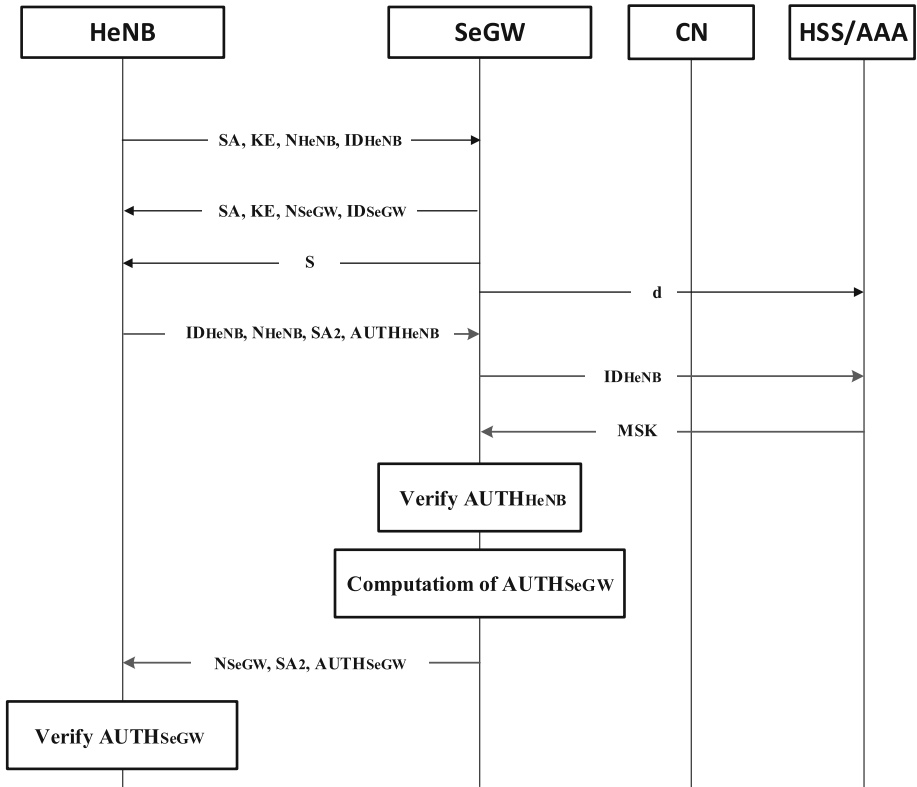


Fig. 5. Improved protocol to authenticate HeNB by SeGW (some of payloads are ignored).

Step 1. At first, IKE phase I exchanges are done as HeNB authentication; this step is explained in Sect. 3.

Step 2. After IKE phase I exchange, SeGW obtains HeNB identity and performs as below.

$$X = \text{hash}(\text{ID}_{\text{HeNB}}|\text{IP}_{\text{HeNB}}). \tag{3}$$

Hash function algorithm is MD5 in this protocol.

Then, SeGW signs X using RSA algorithm. To do this, SeGW selects two large primitive numbers p, q and computes $\gamma(n)$ as

$$\gamma(n) = \text{lcm}(p - 1, q - 1). \tag{4}$$

Then it selects integers e and d that holds following conditions respectively,

$$\begin{aligned} \text{gcd}(e, \gamma(n)) &= 1, \\ e \times d &= 1 \pmod{\gamma(n)}. \end{aligned} \tag{5}$$

d is private key. Digital signature is calculated as

$$S = (X)^d \pmod{n}. \tag{6}$$

SeGW sends S to the HeNB and stores d in HSS and creates a list that binds the identity of HeNB with corresponding d.

Step 3. In this step, for creating IPSec SA, IKE phase II exchanges are done as explained in Sect. 3. In fact, for designing of improved HeNB secure access protocol, the re-authentication protocol is used.

Now, UE wants to connect to the network. Exchanges related to UE connection is shown in Fig. 6 (some of payloads are ignored).

Step 1. UE sends attachment request to HeNB.

Step 2. HeNB forwards UE's request to CN which checks whether HeNB can connect to the network or not; if not, CN sends failure message to HeNB. In this step, CN stores HeNB information such as ID_{HeNB} , IP_{HeNB} and digital signature S.

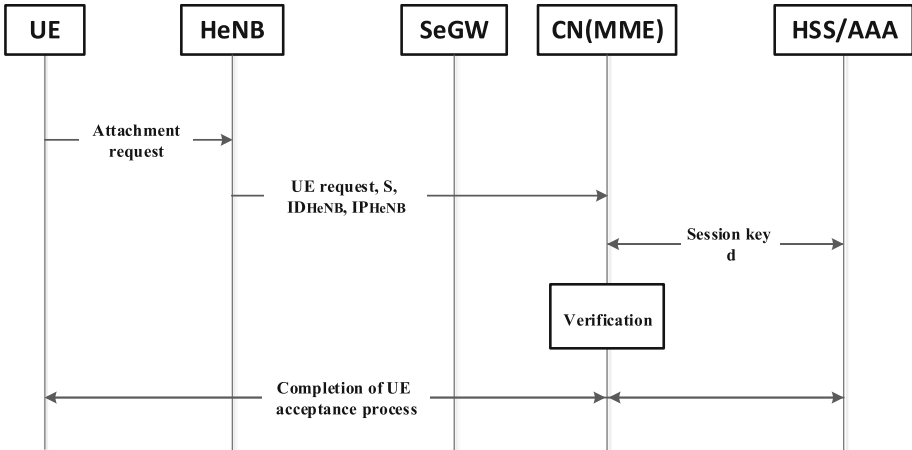


Fig. 6. UE connection to the network in improved HeNB secure access protocol (some of payloads are ignored).

Step 3. CN sends ID_{HeNB} to HSS. Then, HSS sends CSG ID supported by HeNB and digital signature key (d) that had been stored in HSS by SeGW, to CN.

After that, CN verifies the digital signature using d,

$$X' = \text{hash}(ID_{HeNB}|IP_{HeNB}), Y = (X')^d \text{ mod } n. \tag{7}$$

If $Y = S$, then the signature is verified. After verification, remaining procedure for attachment request or routing area is done. This procedure is out of our discussion.

In this protocol, HeNB cannot access to the network by another’s ID except provided ID in IPSec protocol (authentication between HeNB and SeGW). The only drawback of this protocol is that obtaining HeNB identity can only be triggered by IPSec message to send to SeGW.

6 Evaluation of the Improved HeNB Secure Access Protocol

6.1 Security Evaluation

This improved protocol satisfies the following basic features of IKEv2.

Confidentiality

Integrity

Anonymity protection

Perfect forward secrecy

Protection against traffic analysis

Authentication of HeNB

MSK security: The ways that an attacker can discover MSK are:

1. retrieving the MSK from $AUTH_{HeNB}$ or $AUTH_{SeGW}$;
2. compromising the security of the entities stored MSK (i.e., the HeNB device and the AAA server);

For first case, the adversary may get physical access to the channel and obtain $AUTH_{HeNB}$ or $AUTH_{SeGW}$. Then, it tries to retrieve MSK using $AUTH_{HeNB}$ or $AUTH_{SeGW}$. However, the intruder is not able to do this, since he should invert one-way hash functions used for generation of $AUTH_{HeNB}$ or $AUTH_{SeGW}$ that it is inapplicable.

Second attack targets are HeNB device and AAA server. The adversary may attempt to retrieve the stored MSK either from HeNB device or AAA server. To defeat such attacks, MSK must be stored in an encrypted form. Moreover, AAA server must be secured using firewalls [5].

Replay attack: Due to the parameter N_{HeNB} and N_{SeGW} included in $AUTH_{HeNB}$ and $AUTH_{SeGW}$ respectively, in each authentication protocol, N_{HeNB} and N_{SeGW} are different. Even if an attacker gains N_{HeNB} and N_{SeGW} , he cannot be able to retrieve $AUTH_{HeNB}$ and $AUTH_{SeGW}$ by reusing the nonce in the new authentication protocol.

Now, security of proposed protocol against related attacks on HeNB specified in 3GPP, is presented.

Compromise of HeNB authentication token by a brute force attack via a weak authentication algorithm: The authentication parameter in this protocol is MSK. According to the aforementioned description of MSK security, this attack is not applicable.

Moreover, some threats included *compromise of HeNB authentication token by local physical intrusion*, *inserting valid authentication token into a manipulated HeNB* and *user cloning HeNB authentication token* are inapplicable due to the same reason mentioned above.

Man-in-the-Middle (MitM) attacks on HeNB first network access: Due to the establishment of IKEv2 protocol between HeNB and SeGW, and diameter protocol between SeGW and AAA server, the tunnel between HeNB and AAA server is completely safe; hence implementation of MitM attack in the improved protocol is impossible.

Denial of service attacks (DOS): In DOS attacks, adversary tries to flood SeGW. In order to make SeGW more secure against DOS attack, unauthorized traffic should be filtered out on the links between the SeGW and HeNB by introducing appropriate policies in IPSec that are out of the scope of proposed protocol security. In addition, IKEv2 protocol used in authentication procedures can also resist DOS attacks.

HeNB Masquerading: Probably after establishing IPSec tunnel and authenticating HeNB, HeNB uses other's ID for connecting an unauthorized user to the core network, such that this ID differs from used HeNB ID in authentication process. Due to the proposed protocol, since SeGW signs HeNB identity and also HeNB forwards it to CN during UE connection, even if HeNB wants to connect to the network using another ID, it will not be authenticated by CN.

6.2 Cost Analysis

Due to the added exchanges in a new modified HeNB secure access protocol with the purpose of preventing from HeNB attacks, we decided to show that these added exchanges have no significant effect on authentication delay and cost.

Communication Cost Analysis. According to [23], we assume that the transmission cost of a message between HeNB and AAA server is one unit, between HeNB and SeGW is $a(<1)$ unit and between SeGW and AAA server is $b(<1)$ unit. In the improved HeNB secure access protocol that is shown in Fig. 5, it involves the exchange of four messages between HeNB and SeGW, and three messages between SeGW and AAA server. Thus, C_{improved} is computed as formula (8), where C_{improved} is transmission cost for the improved HeNB secure access protocol. According to the computed C_{re} in Ref. [5], degradation (d) of the communication cost of proposed protocol over the re-authentication protocol in [5], is:

$$C_{improved} = 4a + 3b, d = \frac{C_{improved} - C_{re}}{C_{re}} = \frac{b}{4a + 2b}. \quad (8)$$

In order to facilitate analysis, we suppose that a and b are equal and set $a = 0.5$, $b = 0.5$. Therefore, the degradation parameter becomes mostly 16 %; it means that the added exchanges in our protocol do not mostly affect communication cost of re-authentication protocol.

Computational Cost Analysis. We further compare the computational cost of re-authentication and our improved protocol. First, the elapsed time of primitive cryptography operations has been measured using C/C++ OPENSSSL library [24] tested on a Celeron 1.1GHZ processor as an HeNB and Dual-Core 2.6GHZ as an SeGW [5] in Table 1. Table 2 shows the duration of authentication time.

The experimental results show that added exchanges in new improved protocol does not affect computational cost of HeNB; also its effect on computational cost of SeGW is negligible.

Table 1. Time costs of the primitive cryptography operations (1024 bits) [5].

	T_E^1	T_H^2	T_{RV}^3	T_{PM}^4
HeNB	1.698 ms	0.0356 ms	0.957 ms	1.537 ms
SeGW	0.525 ms	0.0121 ms	0.301 ms	0.475 ms

¹ T_E : modular exponentiation
² T_H : hash
³ T_{RV} : RSA verification
⁴ T_{PM} : point multiplication

Table 2. Comparison of computational cost.

	Re-authentication protocol	Improved protocol
T_{HeNB}^1	$T_E + 2T_H + T_{PM} = 3.947$ ms	$T_E + 2T_H + T_{PM} = 3.947$ ms
T_{SeGW}^2	$T_E + 2T_H + T_{PM} = 1.0242$ ms	$T_E + 2T_H + T_{PM} + T_{RV} = 1.3252$ ms

¹ T_{HeNB} : the total operation time of HeNB.

² T_{SeGW} : the total operation time of SeGW.

Note: It is assumed that time cost of RSA signing and RSA verification are same.

6.3 Formal Analysis

As mentioned before, we tried to prevent HeNB masquerading attack in this new protocol. The goal of this protocol is first, mutual authentication between HeNB and SeGW using EAP-AKA protocol based on IKEv2. This goal is achieved in previous protocols. The second goal of our improved protocol and in fact, the only aim that makes this new protocol special among other protocols is re-authentication of HeNB by

CN during UE connection in order to prevent HeNB of false claim. The next goal is secrecy of dynamic key d generated by SeGW. To insure that our protocol provides these goals, we test it using formal security verification tool known as AVISPA [25]. AVISPA provides both automatic security analysis and verification back-end servers like “On-the-Fly Model-Checker” (OFMC), “Constraint-Logic based Attack Searcher” (Cl-AtSe), and SAT-based Model-Checker (SATMC). Protocols must be written in “High Level Protocol Specifications Language” (HLPSSL) before verification in AVISPA. We use OFMC and Cl-AtSe to test our improved protocol.

Table 3 shows the specified goals in our test. Figures 7 and 8 show the output of OFMC and Cl-AtSe back-end, respectively. We can see that OFMC and Cl-AtSe found no attacks. In other words, the stated security goals were satisfied for a bounded number of sessions as specified in environment role. According to these figures, we conclude that this new protocol meets all of these goals and it can resist those malicious attacks such as replay attacks, MitM attacks, HeNB masquerading attack, and secrecy attacks under the test of AVISPA.

Table 3. Specified goals in the test.

goals	description
secrecy_of d	Survey of d security
authentication_on sk1	SeGW authentication by HeNB
authentication_on sk2	HeNB authentication by SeGW
authentication_on si	HeNB authentication by CN during UE connection

```

linux-thnv:/tmp # avispa IKEv2-MAC-newtested1.hlppl --ofmc
% OFMC
% Version of 2006/02/13
SUMMARY
SAFE
DETAILS
  BOUNDED_NUMBER_OF_SESSIONS
PROTOCOL
  /opt/avispa-1.1/testsuite/results/IKEv2-MAC-newtested1.if
GOAL
  as_specified
BACKEND
  OFMC
COMMENTS
STATISTICS
  parseTime: 0.00s
  searchTime: 40.29s
  visitedNodes: 0 nodes
  depth: 1000000 plies

```

Fig. 7. Results reported by OFMC.

```
Linux-thnv:/tmp # avispa IKEv2-MAC-newtested1.hlpsl --cl-atse

SUMMARY
SAFE

DETAILS
BOUNDED_NUMBER_OF_SESSIONS
TYPED_MODEL

PROTOCOL
/opt/avispa-1.1/testsuite/results/IKEv2-MAC-newtested1.if

GOAL
As Specified

BACKEND
CL-AtSe

STATISTICS

Analysed   : 4476 states
Reachable  : 1840 states
Translation: 0.01 seconds
Computation: 0.62 seconds
```

Fig. 8. Results reported by CL-AtSe.

7 Conclusion

In this paper, description and security analyzing of HeNB authentication protocol introduced in 3GPP and re-authentication protocol proposed in [5] is provided. These protocols are yet unsafe against some applicable attacks on HeNB; such as HeNB masquerading. Vulnerability of these protocols allows HeNB to connect to the network using other user's ID that differs from the ID used during IPsec tunnel establishment. Therefore, the new improved HeNB secure access protocol is introduced, in which, SeGW signs HeNB identity provided by HeNB during initial authentication, and sends it to CN via HeNB during UE connection. In this way, even if HeNB wants to connect to CN with another ID, it will not be verified by CN, and unauthorized users connection becomes impossible. Security analyzing and verification of our protocol in AVISPA shows that it is robust against applicable threats on HeNB and solves the present security problems of previous protocols. Moreover, according to the experimental results, it has no significant effect on communication and computational cost.

References

1. Forsberg, D., Horn, G., Moeller, W., Niemi, V.: LTE Security. Wiley Publishing, New York (2010)
2. Ali-Yahiya, T.: Understanding LTE and its Performance. Springer, Berlin (2011)
3. Doraswamy, N., Harkins, D.: IPsec: The New Security Standard for the Internet, Intranets, and Virtual Private Networks, 2nd edn. Prentice Hall PTR, Upper Saddle River (2003)
4. 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 (January 2009)

5. Chengzhe, L., Hui, L., Yueyu, Z., Jin, C.: Simple and Low-cost re-authentication protocol for HeNB. *IEEE J. Mag. Chin. Commun.* **10**, 105–115 (2013)
6. Zong, Z., Zhou, X., Zhu, L.: HNB or HeNB security access method and system and core network element. U.S. Patent No. 355, 299, Shenzhen City (2014)
7. Han, C.K., Choi, H.K., Kim, I.H.: Building femtocell more secure with improved proxy signature. In: *Global Telecommunications Conference*, pp. 1–6 (2009)
8. Aboba, B., Blunk, L., Vollbrecht, J., Carlson, J., Levkowetz, H.: Extensible authentication protocol (EAP). RFC3748 (2004)
9. Arkko, J., Haverinen, H.: Authentication and key agreement (EAP-AKA). RFC4187 (2006)
10. Narayanan, V., Dondeti, L.: EAP extensions for EAP re-authentication protocol (ERP). RFC5296 (2008)
11. Kent, S., Atkinson, R.: Security architecture for the internet protocol. RFC2401 (1998)
12. Kent, S., Atkinson, R.: IP authentication header. RFC2402 (1998)
13. Kent, S., Atkinson, R.: IP encapsulating security payload (ESP). RFC2406 (1998)
14. Piper, D.: The internet IP security domain of interpretation for ISAKMP. RFC2407 (1998)
15. Clancy, T., Nakhjiri, M., Narayanan, V., Dondeti, L.: Handover key management and re-authentication problem statement. RFC5169 (2008)
16. 3rd generation partnership project: technical specification group services and system aspects; 3GPP system architecture evolution (SAE); security architecture (Release 10). 3GPP TS 33.401 V10.2.0 (September 2011)
17. 3rd generation partnership project: technical specification group services and system aspects; rationale and track of security decisions in long term evolved (LTE) RAN/3GPP System Architecture Evolution (SAE) (Release 8). 3GPP TR 33.821 V8.0.0 (March 2009)
18. Han, C.K.: Security analysis and enhancements in LTE-advanced networks. Ph.D. Thesis, Sungkyunkwan University (2011)
19. Cao, J., Ma, M., Li, H., Zhang, Y., Luo, Z.: A survey on security aspects for LTE and LTE-A networks. *IEEE J. Mag. Commun. Surv. Tutorials* **16**, 283–302 (2014)
20. Smaoui, S., Zarai, F., Kamoun, L.: IPsec tunnel establishment for 3GPP-WLAN interworking. In: *8th International Conference on Informatics and Systems (INFOS)*, pp 74–80 (2012)
21. Raza, H.: A brief survey of radio access network backhaul evolution, Part I. *IEEE J. Mag. Commun. Mag.* **49**, 164–171 (2011)
22. Raza, H.: A brief survey of radio access network backhaul evolution, Part II. *IEEE J. Mag. Commun. Mag.* **51**, 170–177 (2013)
23. Ntantogian, C., Xenakis, C.: One-pass EAP-AKA authentication in 3G-WLAN integrated networks. *Wireless Pers. Commu.* **48**, 569–584 (2009)
24. OPENSSL[EB/OL] (2012). <http://www.openssl.org/>
25. AVISPA—Automated Validation of Internet Security Protocols [EB/OL] (2012). <http://www.avispa-project.org>