Re-authentication Protocol for Vertical Handoff in Heterogeneous Wireless Networks

Ikbel Daly, Faouzi Zarai, and Lotfi Kamoun

LETI Laboratory, University of Sfax, Tunisia
{ikbel.daly,faouzi.zarai,lotfi.kamoun}@isecs.rnu.tn

Abstract. The Heterogeneous Wireless Networks (HWN) is a type of framework which includes different varieties of wireless technologies. To ensure a robust management and a reliable behavior of HWN, it is necessary to well manage the interworking between its technologies and in particular to secure interworking and roaming between the 3rd Generation Partnership Project (3GPP)/Long Term Evolution (LTE) and Wireless Local Mesh Networks. A whole of solutions has been proposed to solve this problem; we quote mainly Extensible Authentication Protocol-Authentication and Key Agreement (EAP-AKA) which still suffers from some vulnerabilities such as, man-in-the-middle attack, Sequence Number (SQN) synchronization, and disclosure of user identity. In this paper, we propose new re-authentication protocol. The suggested solution proves its effectiveness following the studies of simulation which carried out according to different criteria handoff latency, loss and blocking rate.

Keywords: Re-authentication protocol, Heterogeneous Wireless Networks, 3GPP LTE, Mesh networks, Handoff, Security.

1 Introduction

A heterogeneous network is an association between several types of networks which belong to various generations and technologies. These varieties of equipments manage between them to provide a new range of functionalities with a better quality of services and more security. One of the most important kind of this heterogeneity in wireless networks, we find 3G-WLAN interworking which is the future generation of mobile and wireless communication systems. Indeed, this specific environment integrates two various types of networks; the WLANs networks and the cellular networks of the third generation.

Each category of these networks brings a whole of assets with an aim of guaranteeing the best interworking of various procedures and mechanisms between its components and of fulfilling the user's requirements and needs. Consequently, the integration of these different architectures makes it possible to benefit from the diversity of the advantages brought by each category and thereafter this complementarity improves the effectiveness of network as it guarantees the resolution of some problems such as the security, the interference and the quality of services.

J. Del Ser et al. (Eds.): MOBILIGHT 2011, LNICST 81, pp. 219–230, 2012.

In our study, we will extend our research to illuminate the interworking between SAE/LTE (System Architecture Evolution / Long Term Evolution) network [1], [2] (or simply LTE network) and the Wireless Mesh Network (WMN) [3]. On the one hand, the first type of network, developed by the 3rd Generation Partnership Project (3GPP), presents an improved and more secure version of the system UMTS (Universal Mobile Telecommunication System). In addition, WMN presents one of the promising technologies in the world of wireless communications. Indeed, Mesh network makes it possible to provide a free mobility and the self-configuration of the various equipments of network, extensible zone of cover by the addition of routers, as well as a better quality of services.

In spite of the diversity of the benefit brought by each one of these technologies as well as the multiplicity of the research carried out in this field in order to improve the performances of these two types of networks, the security remains an enormous challenge which needs to be studied. Indeed, the open medium of these technologies increases their vulnerabilities and the risks of attacks. Moreover, the integration of the networks, 3G-WLANs worsens the situation and the environment of association becomes increasingly vulnerable and less protected.

The architecture of LTE-Mesh interworking is illustrated by Figure 1. This environment is composed of the set of components belonging to the Mesh and LTE networks. First of all, in Wireless Mesh Network, we distinguish the following equipments; WMR, Mesh AG and AAA server. The nodes WMRs (Wireless Mesh Router) support the services of Mesh network and make it possible to establish connections with the close nodes in order to ensure the property of the transmissions multi-hops.

The communication with the external networks is carried out by the entity Mesh AG (Mesh Access Gateway). And with an aim of controlling the access to Mesh network, a procedure of authentication must arise in this environment. Indeed, WMN has recourse to an authentication server called AAA (Authentication, Authorization and Accounting). This entity is the responsible for mobility management, the registration, the authentication and the re-authentication of the various equipments of Mesh network.

On the other hand, the LTE network has its own architecture, which is composed by an access network and a core network. The first block, called EUTRAN (Evolved UMTS Terrestrial Radio Access Network), is made of a whole of nodes, noted eNodeBs, which ensure the transmission of the radio signals [4]. Moreover, the AAA server is used to guarantee the authentication between the networks 3G and Non-3GPP while using the ePDG entity (evolved Packet Data Gateway) and to register the users by allotting a whole of parameters such as IMSI (International Mobile Subscriber Identity). This confidential information will be stored in a data base called HSS (Home Subscriber Server).

In addition, the LTE network is made up of other set of entities such as MME (Mobility Management Entity) for the management of mobility and session, PDN GW (Packet Data Network Gateway) for the establishment of external communications and the allowance of the addresses as well as Serving GW (Serving Gateway) for the packets routing.

The remainder of this paper is organized as follows: In Section 2, we give some related works. In Section 3, we detail a new solution to secure interworking and roaming between 3GPP LTE and Wireless Local Mesh Networks. The proposed authentication protocol uses new equipment, named hybrid unit. In Section 4, we describe a simulation method of our scheme and analyze the numerical results derived from simulation and highlight the contribution developed in the previous sections. Finally, we conclude the paper in Section 5.

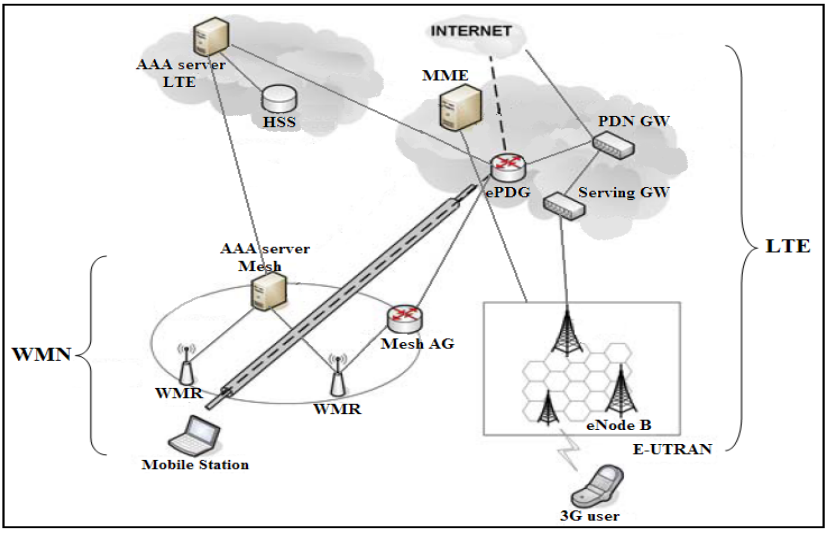

Fig. 1. Architecture of the LTE-Mesh interworking

2 Related Work

Because of the diversity of mechanisms, equipments and technologies within such an LTE network, the constraints and the challenges become increasingly critical and demanding. Indeed, the users, who are by definition mobile, seek to communicate during their moves across different domains without any constraint of connectivity, and having a completely transparent network change.

Moreover, securing the network access is a task whose complexity grows progressively, parallel to the increase in the number of applications and with the degree of opening towards the outside which they imply. Consequently, to provide a robust system of security should solve this problem and maintain the safety of data. Due to the importance of the security aspect in any network and in particular in LTE network, this subject catch sight of the organizations what allows the standardization of some new authentication protocols and the keys management such as UMTS AKA (Authentication and Key Agreement) [5] and EAP-AKA (Extensible Authentication Protocol-AKA) [6]. Besides, the whole of the assets provided by LTE network encouraged the community of researchers to propose new solutions to confront and resolve these problems.

The first study [7] reveals with a whole of mechanisms which make it possible to optimize security following the execution of the vertical handoff in a heterogeneous environment (Heterogeneous Wireless Networks - HWN). First of all, the authors have proposed a new model for optimizing network access authentication procedure. Then, they have detailed a mechanism ensuring the security context transfer.

Our field of research is limited to the first procedure which accentuates the integration of a new intermediate entity between WLAN network and LTE network, called "Interworking Unit". This component ensures a protected communication and safe data exchanges between the various types of networks in the heterogeneous environment.

In spite of the profit illustrated within the execution delay of the re-authentication procedure, the proposed mechanism did not well profit by the addition of Interworking Unit which only plays the role of a protected and safe bridge between the two networks. Moreover, the confidential parameters allotted for each user in a given network should not be circulated towards the other external networks because that makes it possible to increase the risks of attacks.

With an aim of ensuring the security in 3G-WLAN interworking, we have recourse to a protocol called EAP-AKA. But, the latter still suffers from some vulnerability such as Sequence Number synchronization, disclosure of user identity, additional bandwidth consumption and man in the middle. Consequently, a variety of work treated this subject in order to improve this authentication protocol.

Among these studies, we quote [8] which proposes a new protocol of authentication and key agreement based on EAP-AKA, quoted previously. With the intention of overcoming, the vulnerabilities of EAP-AKA, the suggested method exploits the ECDH mechanism (Elliptic Curve Diffie-Hellman) with the encoding technique “symmetric key cryptosystem”.

The proposed protocol is composed of four principal phases namely; Initialization, Registration and generation of TK (Temporary Key), Authentication and key agreement and finally Transmission of MSK (Master Session Key). The authors of [8] underline in their model the need for having secure mutual communications between each pair of equipments of the interworking.

Moreover, the present mechanism makes it possible to ensure a “Perfect Forward Secrecy” (PFS) which provides more security in this environment while making it possible to keep from the replay attack. On the other hand, the suggested protocol handles a great quantity of parameters, which are greedy in memory capacities as well as several functions of encoding and of keys generation that carry out to weigh down the mechanism side time of execution and of calculation, memory capacity for data storage as well as the signaling overhead. Thereafter, this solution does not take into account the mutual authentication between the two types of networks 3G-WLAN and supposes the existence of a confidence relation between these two parts. What contradicts the existing.

In this same context, a second solution [9] which treats the protocol EAP-AKA in order to improve the aspect security in the field of 3G-WLAN. The contribution of this work appears by the proposal of more effective, robust and new authentication procedure as well as a more reliable and protected keys management. To solve the

problems of security in an environment that includes a 3G-WLAN integrated networks, the project 3GPP (3rd Generation Partnership Project) introduced an architecture which is based on the protocol two-pass EAP-AKA authentication [10]. As it is indicated through its name, the mechanism contains two phases of authentication. The first one is used for the user registration in WLAN network. For the second authentication, the EAP-AKA technique is encapsulated in the protocol IKEv2 (Internet Key Exchange version 2) which allows the registration of client in the field of 3G Public Land Mobile Network (3G PLMN).

One-pass EAP-AKA authentication procedure presents the innovation brought by this work. This mechanism eliminates the duplication of the EAP-AKA protocol execution. What causes a reduction of the authentication overhead and the minimization of messages flow exchanged between the various equipments of the heterogeneous network. In addition, the suggested model does not supervise the mutual authentication between the different equipments intervening in the procedure of authentication and it supposes the existence of confidential relations without specifying the means which ensure the security of confidential data transmission.

According to the study of some existing solutions, we could extract an optimal solution by the proposal of a new authentication protocol. During the establishment of this mechanism, we held in consideration the legitimacy of the connections between the various equipments to ensure more security and the minimization of authentication delay in order to preserve a better quality of services.

3 Proposed Solution

This present work deals with the problem of the lack of security at the time of handoff in a heterogeneous framework in particular the interworking between a WLAN network (Mesh) and a 3G network (LTE). The suggested solution is based on a re-authentication protocol by exchanging a whole of parameters between Mesh and LTE. This interworking between these two various types of technologies is ensured by a new entity called “Hybrid Unit” (HU).

On the one hand, HU is connected by a secure channel to the Mesh network while benefitting from the advantages of the VPN (Virtual Private Network) network which allows the data transmission in safety. On the other hand, this entity is binding on the various components of LTE network. Consequently, it profits from a set of parameters and keys such as an identity and the keys CK, IK and K which make it possible to check its legitimacy beside LTE network as well as to ensure the integrity and the data confidentiality exchanged between these components.

The innovation brought by the proposed re-authentication protocol is the preparative phase which precedes the execution of the point of attachment change. In which we arrange a base of identities and keys that facilitates thereafter the generation of the new identity as well as the new key for the mobile station. Indeed, this stage makes it possible on the one hand to minimize the time of the re-authentication and consequently more quality of services and on the other hand to ensure more safety for the exchanged confidential data and the access to the network. This new protocol is composed of three great phases: Initialization, Pre-handoff and EAP procedure, as it

is shown in Figure 2. In the first phase, we prepare a data base formed of the couple identity and key (id, k). This information is shared between AAA server of WLAN network (AAA_{WLAN}) and the hybrid unit (HU) (step 1).

Before carrying out the execution of the point of attachment change mechanism for the mobile station (STA) which migrates from LTE network towards Mesh network, we have recourse to a new procedure, the pre-Handoff phase. This procedure starts by sending a message from the mobile user towards the new point of attachment (WMR). This element contains the temporary identity (TMSI - Temporary Mobile Subscriber Identity) of the station, which identifies in more the identity of its network mother, the first TMSI is transmitted in clear and the second is associated with a Sequence Number (SN) and enciphered by the key CK of STA with an aim of ensuring the confidentiality and the safe and protected data transmission. This association between TMSI and SN makes it possible to minimize the risk of attack especially the Reply Attack (step 2).

After the reception of these data, WMR adds its identity (ID_{WMR}) to the received message and sends it to server AAA_{WLAN} (step 3). Immediately, the Mesh server checks the legitimacy of WMR entity by testing its identity. If step 4 does not cause any doubt on the topic of the wireless Mesh router entity, AAA_{WLAN} transfers, in its turn, the data coming from the station after the addition of its identity (ID_{AAA}) towards the hybrid unit (step 5). In order to ensure more security and in spite of the presence of the secure tunnel, HU checks in addition the identity of AAA server (step 6). Then, it identifies the original LTE network of the mobile STA by referring to its temporary identity TMSI. Afterward, HU sends to MME entity the data which relate to, on the one hand, the station made up of its identity (TMSI) and a Sequence Number (SN) enciphered by the key CK of STA and on the other hand to the Mesh network that contains its identity (ID_{AAA}), which is encrypted with the key CK of HU (step 7).

Following obtaining this information, the MME entity, from LTE network, starts the step 8 that concerns the checking of the station validity and if it is authorized to reach the selected Mesh network while being based on its profile. If the two conditions are valid, MME sends some parameters about STA; its identity IMSI and its key K. The confidentiality of this information exchanged between MME and HU is ensured by the application of encoding with the key CK of the hybrid unit (step 9).

The reception of this last message launches the step 10 for the reservation of an index from the base (identity, key), noted “ind”. HU associates this index to the received parameters of STA from its home network (IMSI, K) then it sends the totality of the data to the server AAA_{WLAN} while using the secure channel to ensure the safety of the transmissions (step 11). At this stage, all the necessary elements for the generation of the new parameters are present on the level of the entities; HU and AAA_{WLAN}. Consequently, on the one hand these two components launch the mechanism of calculation of new identity (ID_{STA}) by taking advantage of a preset function "f" and the old identity of STA (IMSI). On the other hand, they generate the new key (K_{STA}) while referring to old key (k) and a function "g" (step 12).

After the generation of the user new parameters, we send them towards the MME entity encoded by the keys CK and IK of HU in order to ensure the confidentiality and the integrity of the transmitted data (step 13). Then, this information (ID_{STA}, K_{STA}) reached the station STA through its home network at step 14, enciphered by the keys CK and IK of STA. This last message encloses the second phase, the pre-handoff procedure.

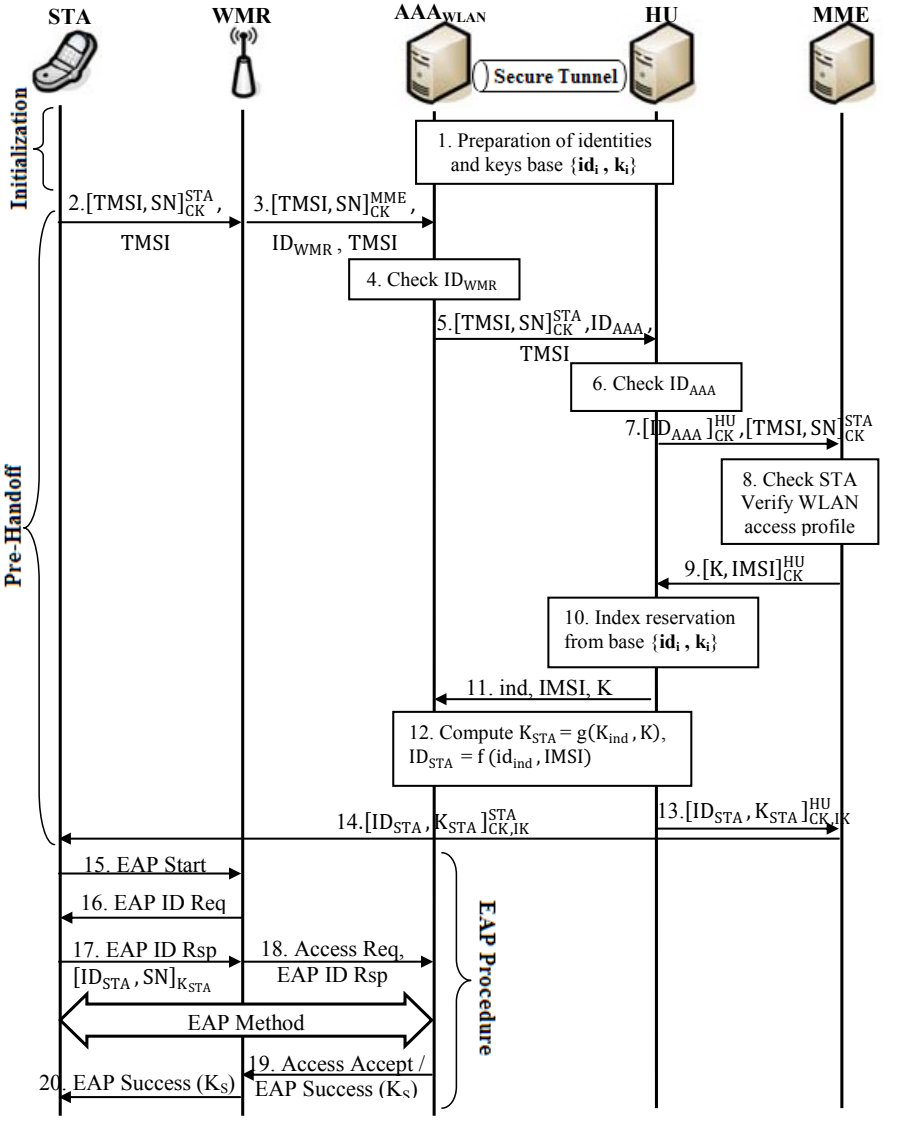

Fig. 2. Re-authentication procedure following the handoff in a heterogeneous network

Following the preparation for the handoff execution, which allows the checking of the legitimacy of various equipments as well as the generation of new identities and keys for the mobile stations, we achieve our proposed re-authentication protocol by the application of EAP procedure. This mechanism is established by sending a message "EAP Start" from STA towards the wireless Mesh router (step 15). The latter answers by a request for identity "EAP ID Req" at step 16. Afterward, STA sends its answer "EAP ID Rsp" containing its identity (ID_{STA}) and a Sequence Number encoded by its new key (K_{STA}) (step 17).

At step 18, WMR transmits this network access request "Access Req" and the received information from message "EAP ID Rsp" to the server AAA_{WLAN}. Thereafter, the application of the EAP method allows the checking of the validity of various equipments and in particular that of STA and the generation of the session key, noted K_S, which is a temporary key shared between the entities STA and WMR. In step 19, the decision of the Mesh server for acceptance or refusal of the access request is mentioned. In case of acceptance, AAA_{WLAN} sends a message "Access Accept / EAP Success" containing the session key (K_S) towards WMR. In its turn, the entity WMR transmits this decision in a message "EAP Success" containing the temporary key (K_S) to station STA (step 20).

4 Performances Evaluation

In order to test and evaluate the performances of the re-authentication protocol for a mobile station which migrates from LTE network towards a Mesh network, we have recourse to apply the method of simulation which presents a software tool that reveals with a fast, economic and effective solution for the test of networks. Indeed, there is a variety of existing simulators which allow the implementation and the analysis of the new integrated protocols performances in different networks topologies. On the other hand, a whole of new technologies are not yet well adjusted in the majority of the existing simulators in particular that of the Mesh and LTE networks. Following the need to appreciate the performances of the suggested re-authentication protocol, we have developed a simulator which allows the integration of the aspect of interworking LTE-Mesh.

This section is devoted to analyze the results of the protocol implementation in our simulator. First, we have defined some details to put into practice our architecture of Mesh network in which we will integrate the Mobile users (STAs) coming from LTE network. Indeed, this simulator specifies various parameters of this type of network which allows simulating its features to study the performances of the new authentication protocol suggested in 3G-WLAN environment. The selected network covers 300m×300m comprising 9 WMRs and a variable number of Mesh clients and also some visited nodes, which migrated from LTE network. To evaluate the performances of our solution, we will consider two types of traffic: voice and Web communication and many scenarios.

While referring on these types of communications as well as the parameters of simulation, we evaluate the simulation's results according many criteria:

- Handoff latency: the time passed between the change of point of attachment request and the association with the new WMR,
- Blocking rate: represents the number of blocked STA at handoff for the total number of STA which requests handoff,
- Loss rate: represents the number of lost packets for the total number of the emitted packets.

For the remainder of scenarios, we have concentrated on the comparison between Mesh stations behavior on the one hand and the visited stations behavior coming from LTE network on the other hand while basing on three criterion; handoff latency, loss rate and blocking rate. In fact, we have fixed the number of Mesh stations at 200 users and we have progressively increased the number of external users.

4.1 Handoff Latency

Figure 3 shows the results of simulation following the implementation of our new protocol of re-authentication in a heterogeneous wireless environment. First of all, the obtained curves illustrate an increase in the values of handoff latency which accompanies the multiplication in the number of external stations which migrate from the LTE network towards the Mesh network. This rise can be justified by the growth of handoff requests carried out on the level of WMN. Consequently, it may cause the heaviness and the overload of the WMRs nodes.

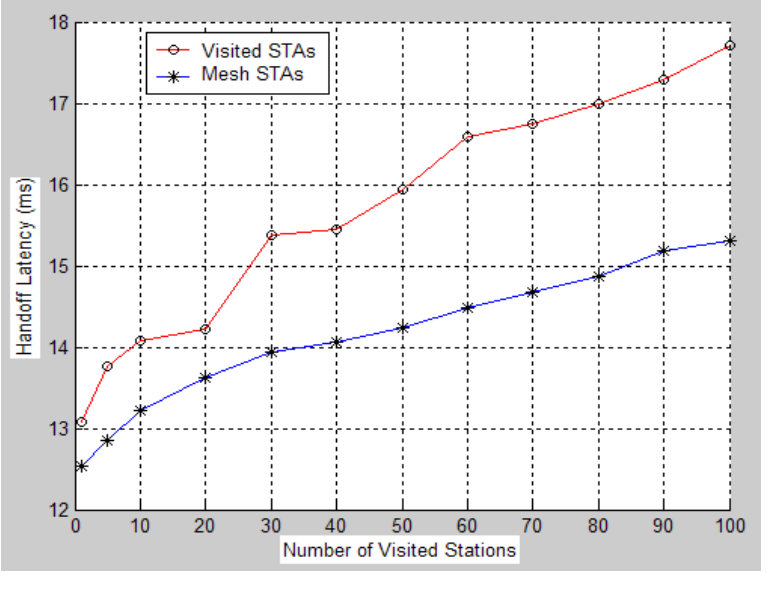

Fig. 3. Handoff latency according to the number of visited Stations for External and Mesh STAs

According to Figure 3, the values of handoff latency for visited STAs visitors are higher than those of Mesh STAs. Indeed, the procedure of legitimacy checking of the external stations which precedes the handoff execution costs more time than the local checking of the Mesh network stations. On the other hand, the obtained values for the visited stations are optimal in the case of LTE-Mesh interworking and with the constraints of quality of service.

4.2 Loss Rate

A second parameter, which allows the evaluation of the new protocols performances and the test of their network behavior, is the loss rate of the packets in communications. Following the increase in the values of handoff latency, mentioned in the preceding paragraph and in Figure 3, the risk the packets loss grows simultaneously. Indeed, if the values of handoff delay exceed a well defined threshold, which depends on the specific application (example voice or Web application), the data in the course of transmission will be announced as lost.

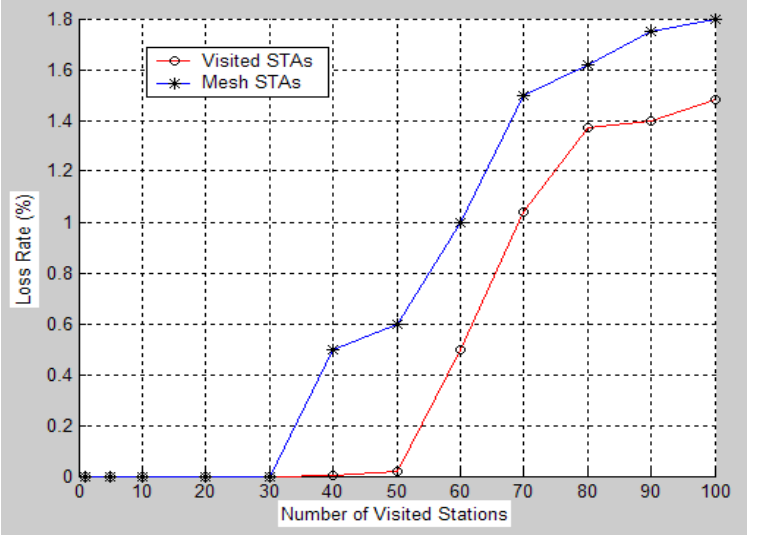

Fig. 4. Loss Rate according to the number of visited Stations for External and Mesh STAs

Figure 4 illustrates the obtained loss rates for the studied protocol with the progressive increase in the number of visited stations to Mesh network. The comparison between these two curves shows a light difference between the loss rates of the two categories of stations. For Mesh STAs, the obtained values by simulation are higher than those of visited STAs. This difference can be justified by the priority granted to the calls for handoff with those of the internal transmissions since these requests present more vulnerabilities and risks of attacks.

The obtained results demonstrate that for the first values of external stations (between 30 and 50), the loss rates are almost negligible. What reflects the effectiveness and the robustness of the implemented re-authentication protocol.

4.3 Blocking Rate

The loss of two successive packets of the same communication results in the blocking of station. This condition becomes increasingly demanding with real time applications. Consequently, the values of blocking rate are related to the results of the obtained loss rates. Figure 5 illustrates the rates of blocking gained with the application of the proposed re-authentication protocol in the environment of simulation for the heterogeneous network.

As in the case of loss rate, the curves begin with negligible values. Then, these rates increase gradually with the increase in the population of STAs, which come from the LTE network. Moreover, a comparison between the curves in Figure 5 shows that the blocking rates for the visited stations are less than those of the local stations that belong to the Mesh network. This result can be explained by the notion of the priority for the handoff service.

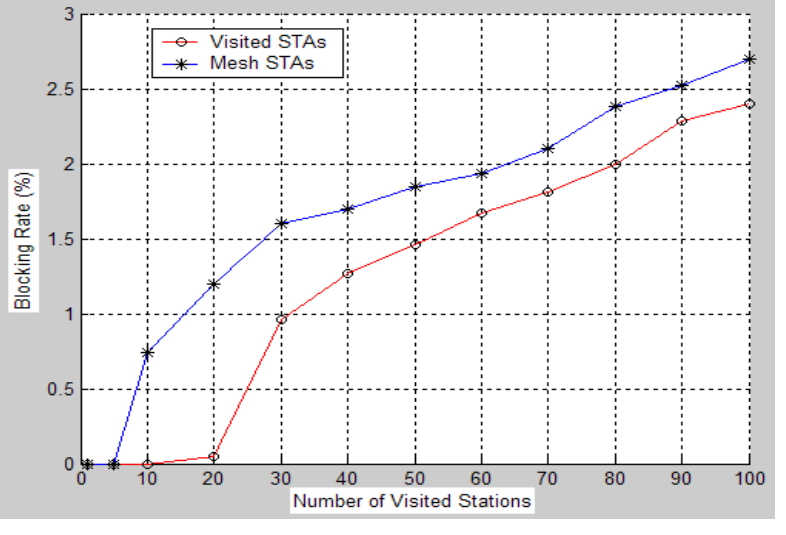

Fig. 5. Blocking Rate according to the number of visited Stations for External and Mesh STAs

5 Conclusion

A heterogeneous wireless network cannot prove its effectiveness and robustness only if it suitably treats its first challenge, which is the interworking between its various technologies. Indeed, this aspect makes it possible to better handle the management of mobility and security. In this paper, we were interested in the study of the LTE-Mesh

interworking and in particular ensuring the security during handoff of the stations, which migrate from LTE network towards Mesh network. Therefore, we have proposed a re-authentication protocol for securing interworking and roaming 3GPP LTE and wireless local Mesh network. Moreover, the suggested solution is based on the use of a hybrid unit. This entity makes it possible to establish a preparative phase which precedes the execution of the handoff mechanism. Consequently, that makes it possible to ensure a better security and a mutual authentication between the various components of the heterogeneous network. These findings can be appreciated by the optimal simulation results and the resistance against replay attack. Compared with the existing protocols, our re-authentication protocol can reduce computational overhead, loss rate of transmitted packets and handoff blocking probability. As a future work, we can extend our study to resolve the problem of lack of security in various types of clients' handoff process between others different technologies in heterogeneous wireless network.

References

[1] 3GPP TS 23.402 v1.2.0, 3GPP System Architecture and Evolution (SAE): Architecture Enhancements for non-3GPP accesses, Release 8

[2] Holma, H., Toskala, A.: WCDMA for UMTS: Radio access for third generation mobile communication, pp. 2927–2932. John Wiley and Sons (2004), 978-1-4244-1997-5

[3] Zhang, Y., Luo, J., Hu, H.: Wireless Mesh Networking: Architectures, Protocols and Standards. CRC Press, Taylor & Francis LLC, USA (2006) ISBN: 0849373999

[4] 3GPP Technical Report 25.814, version 7.1.0, Physical Layer Aspect for Evolved Universal Terrestrial Radio Access (UTRA) (September 2006)

[5] Technical Specification 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Security of Home Node B (HNB) / Home evolved Node B (HeNB) (3G TS 33.320 version 9.0.0 Release (2010), http://www.3gpp.org/

[6] Arkko, J., Haverinen, H.: EAP-AKA authentication. RFC 4187 (January 2006)

[7] Rajavelsamy, R., Jeedigunta, V., Osok, S.: A Novel Method for Authentication Optimization during Handover in Heterogeneous Wireless Networks. In: Communication Systems Software and Middleware (COMSWARE 2007), pp. 1–5. IEEE (2007), 9719237, 1-4244-0613-7/09/

[8] Mun, H., Han, K., Kim, K.: 3G-WLAN Interworking: Security Analysis and New Authentication and Key Agreement based on EAP-AKA. IEEE (2009), 978-1-4244-2588-4/09/

[9] Ntantogian, C., Xenakis, C.: One-Pass EAP-AKA Authentication in 3G-WLAN Integrated Networks 48(4), 569–584 (2008)

[10] 3GPP TS 33.234 (v7.2.0) (2006) 3G security; WLAN interworking security; system description. Release 7 (September 2006)