RE-AUTHENTICATION PROTOCOL FOR FAST HANDOFF WITH MOBILE STATIONS AND ROUTERS IN WIRELESS MESH NETWORKS

Ikbel Daly[1], Faouzi Zarai[2] and Lotfi Kamoun[3]

LETI laboratory, University of Sfax, Tunisia
[1]ikbel.daly@isecs.rnu.tn
[2]faouzi.zarai@isecs.rnu.tn
[3]lotfi.kamoun@isecs.rnu.tn

ABSTRACT

Wireless Mesh Network (WMN) is one of the promising technologies in the world of wireless. Indeed, it makes it possible to provide a free mobility and a self-configuration of the various network equipments, an extensible coverage area by the addition of routers, as well as a better quality of services. Despite all of these assets, Mesh technology still suffers from some problems such as security. Thanks to the importance of this issue, researchers do not stop proposing solutions to solve this problem. In this paper, we deal with the subject of insecurity during the location change of some equipment, known by handoff, by proposing a re-authentication protocol. The suggested model considers the case of clients' mobility as well as the routers movements by taking advantage of some existing techniques like Blom Key pre-distribution scheme and Du Key process generation method. According to the simulation results obtained by the application of the proposed protocol, we notice that this solution presents optimal values which satisfy the need for security as well as the quality of services.

Keywords : Re-authentication, Protocol, Handoff, Mesh Networks.

I. INTRODUCTION

Wireless Mesh Network is a type of wireless network where its various nodes appear as routers which are able to receive and to transmit packets towards their destinations. This characteristic makes it possible to provide a continuous connection and a flexible network reconfiguration through the possibility of building multiple paths between these various nodes [1].

Indeed, this makes it possible to avoid the problem of blocked ways because of the idleness or the disconnection of some Mesh nodes. In this same context, the Mesh network is based on multi-hop transmissions allowing the construction of various paths between such a source and destination [2]. Moreover, the self-configuration permits to widen the network spread by the addition of the new points in an automatic way without recourse to decontaminate the whole or partial network or to modify the installation [3]. The idea of Mesh network and its first application start in the field of military service. At that time, the radios are characterized by a very expensive cost as they require a raised energy for their operations.

Consequently, the first generation of Mesh network is characterized by the equipment with only one radio operator (single-radio router). This interface is shared between the backhaul and the clients. What presents on the one hand an expensive solution side price and energy and on the other hand insufficient side quality of services. Following the reduction of the cost, the size as well as the power consumption, a second generation of Mesh network using two radios appears (two-radio router). In this type of network, the first interface is related to the clients and the second on the backhaul. What makes it possible to separate the two types of traffic and to facilitate the routing of the packets in the network.

The third generation is called three-radio router. As its name indicates it, it is equipped with three radios equipments. The first interface is devoted to the transmissions between the Access Points (APs) and the clients. And the two other radios are reserved for the backhaul with an aim of providing simultaneously one for the reception and the other for the transmission and while using separate channels [4].

Concerning topology, we distinguish two great families: full Mesh topology and partial Mesh topology. For the first topology, each node is connected directly towards all the other nodes. In the second, some nodes are linked between them and not all at the same time. Since WMN is characterized by its capacity to extend its zone of cover, its architecture is able to change dynamically to allow the free mobility of stations. This freedom during the moving of the clients imposes several challenges of which we quote mainly the security problem [5], [6]. Indeed, we must ensure the access only to authorized users by eliminating all risks, attacks and intrusions [7]. This issue becomes increasingly serious and vulnerable especially with the opening of medium network towards the outside and in the case of routers moving [8].

In this work, we have dealt with this problem of security lack in WMN by proposing a re-authentication protocol. The suggested mechanism makes it possible to limit the access to the network only to the authorized users and thereafter to avoid the intrusions and the attacks which can be carried out during the moments of location change. Indeed, the mobility of the different equipments present the most critical moments

because on the one hand we must minimize the re-authentication time to support the transparency of this operation on behalf of the mobile and on the other hand we must ensure more security mechanisms to protect the Mesh network from various risks and threats.

Our study contemplates the case of users' movement and even of the routers inside their domains (clusters) and between various domains of Mesh network by exploiting some existing mechanisms such as Blom Key pre-distribution scheme and Du Key process generation method.

The remaining part of this paper is organized as follows: In Section II, we give some related work concerning the security issue in Wireless Mesh Network. In Section III, we detail our effective and robust authentication protocol. First, we precise the framework and the architecture of this study. Then, we mention the different schemes used in the proposed protocol. And finally, we illustrate the details of the solution. In Section IV, we describe a simulation method of our schemes and analyze the numerical results derived from simulation and highlight the contribution developed in the previous sections. Finally, we conclude the study in Section V.

II. RELATED WORK

WMN is distinguished by its capacity to provide a free mobility for its various equipments. This mechanism is known by the term handoff which specifies the point of attachment change of an entity during its communication. These movements can be classified under two great levels. The first type is called intra-domain handoff (intra-cluster), which is carried out by the cross from a node to another that belong to the same domain. In the inter-domain handoff (inter-cluster) case, the mobile equipment changes its location from a domain to another [9].

By taking account of these concepts and in order to solve the security problem especially during the handoff of various equipments, a set of proposals was been suggested in the literature. These solutions are based mainly on the implementation of a re-authentication protocol to limit the access to network only to the legitimate users and to minimize the risks of attacks and intrusions.

The security presents a challenge and a very vast topic which can be studied from several sides. Firstly, this aspect threatens all type of wireless networks since their medium remains open vis-a-vis the external attacks and even internal ones and during the various phases of communication. Then, security can be explored during the neighbor discovery phase, authentication or re-authentication or others.

In our case, we are interested in the security topic during the execution of the handoff i.e. the application of a re-authentication protocol. In the same way on this level, there is multiple visions to treat this subject. Indeed, we can suppose on the one hand the mobility of the clients and moreover the mobility of some other Mesh equipments such as WMRs and on the other hand the type of the handoff can be either inter-domain or intra-domain. In this context, we find in the literature various solutions which deal with one or more of these aspects that quoted previously.

Dynamic Distributed Authentication (DDA) [10] is one of these solutions which studies only the case of the clients' (STAs) movement and in a centralized architecture guided by an entity called AAA server (Authentication Authorization Accounting). This approach is based on the search of the shared key and then the establishment of a new secrecy between STA and the new AP or WMR (Wireless Mesh Network). Its distributed authentication algorithm, which is intended for dynamic topologies, uses the protocols EAP (Extensible Authentication Protocol), IEEE 802.11i as well as a modified version of the Otway-Reese protocol. This last indicates a security protocol proven for the authentication and the exchange of keys between three parts of the network. The DDA authentication model is composed of 4 phases:

- Initialization of the authentication: it is carried out by the EAP protocol by exchanging the identities between the mobile station and the new WMR.
- Search for T (Trusted WMR): it seeks for a trusting WMR with which the mobile station was associated and generates a secret key between these two WMRs if there does not exist before.
- Key Authentication and distribution: it uses the Otway-Reese protocol allowing the calculation of a shared key between the three parts (mobile Station, Trusted WMR and new WMR) by using parameters provided by these equipments. First of all, a key called master key (K) resulting from the application of TLS-Pseudo Random Function (TLS-PRF) is generated by the part of confidence T. Then, after the exchange of the necessary elements, the station and the new WMR can extract the value from K.
- Key session Distribution: Only the new WMR and STA know the derived session key by achieving the procedure of IEEE 802.11i 4-way handshake.

The implementation of this protocol makes it possible to relieve significantly the burden of the WDS (Wireless Distribution System) management and deployment. As it ensures the reduction of the memory capacity reserved in Mesh nodes and of the saturation of network with the control messages by exploiting the distributed nature of the authentication model. Moreover, DDA offers a high level of scalability.

In spite of the whole of the insured assets, the suggested solution still suffers from some limits. First of all, the security aspect is not ensured between Trusted WMR and the new WMR, thus a confidence relation is supposed between these two pieces of equipments. What contradicts the existing and the reality. Moreover, according to the proposed algorithm in this model, if the search for T does not give any result so the station cannot be authenticated. Concerning the equipments mobility, this solution is being limited only to the study of the stations handoff and not the mobility of WMRs.

With an aim of studying the notion of WMRs mobility, the authors of the work [11], seek to design a pre-authentication model for the fast handoff in Wireless Mesh Network with mobile access points. They improved some existing methods, particularly Mishra' et al. scheme, named pro-active key distribution using neighbor graph for the fast

handoff [12], so that they can be applicable inside the Mesh networks. Moreover, their model creates a group of keys, called PMKs (Pairwise Master Keys).

However, the suggested model avoids the chained relation between the set of PMKs in the neighbors graph with an aim of solving the pre-authentication problem. Indeed, each STA carries out a complete authentication with its Authentication Server (AS). Thereafter, a tree of PMKs is well defined and distributed in the network. Then, the STA can move between APs by knowing beforehand the shared keys. This operation is appropriate for fixed APs. But, if we have the case of mobile AP (MAP) and following the movement of the STA towards its next AP which is MAP, the two pieces of equipments (STA and MAP) cannot execute the mutual authentication since they do not share the same information for this process. This situation requires the re-authentication of the STA with the application of the complete authentication procedure by the intermediary of AS entity and the redistribution of a new keys group of PMKs.

Consequently, the Mishra's model has just considered the fixed APs, which does not change their location. Thus, the application of this last method inside WMNs, characterized by a set of mobiles APs, requires the addition of some supplementary procedures. Indeed, the present solution applied the key generation process of Du [13] for the production of PMKs. This last method is associated to the key pre-distribution scheme, based on Blom's model [14], which handles a whole of matrixes. A succession of calculations and mathematical operations are applied to these parameters in order to derive the secret keys between the various network equipments and thereafter to ensure a fast handoff. In fact, this approach proves its effectiveness in the WMN with mobile APs.

Although the suggested solution presents a secure mechanism for the fast handoff as well as a robust key management, there remains a whole of limits to be studied. First, a signal overhead can be caused by the diffusion procedure of the various matrixes used in this solution towards the different components of the Mesh. Moreover, the phases of key generation and distribution require the execution of an enormous calculation applied to the matrixes. Finally, this method can be applicable only in the case of an intra-domain handoff. And with the extension of Mesh network, by the addition of new access points, the size of these matrixes increase more and more and consequently the rate of calculation grows gradually. As a second result of the Mesh extension, the Authentication Server must modify the used matrixes during the authentication and re-authentication procedures of clients since these data depend on the size of the network (i.e. the number of APs and STAs).

With an aim of solving the network security problem at the time of the clients' mobility as well as WMRs mobility, the authors of the study [15] proposed a new authentication model named WMNSec (Security for Wireless Mesh Networks). This suggested protocol presents an adoption of the security standard IEEE 802.11i, specifically aimed to WMNs by taking account of the CPU limited power, the nodes mobility and the free interruption of connectivity. Moreover, WMNSec is characterized by the deployment of only one coding key, for the whole network. This key is delivered by an entity named MKD (central Mesh Key Distributor) and is propagated towards the other authenticated nodes by employing the 4-Way-Handshake technique of the standard IEEE 802.11i. This solution is made up of three phases:

- Key management: this phase is based on the deployment of the key GK (Global Key) which is regenerated periodically by using a reliable generator of random number. Thanks to the unicity of this key, all the network nodes can decipher and check the messages coming from any other node. Then, the mechanism of regeneration of GK is associated with a relative validity value Vn. This value is produced by the MKD and is simultaneously propagated with the key GK.
- Key authentication and distribution: in order to ensure the authentication, the suggested protocol employs the 4-Way-Handshake technique and for the GK transmission, it uses the Group Key Handshake technique. Contrary to the IEEE 802.11i standard which requires the authentication of each station with each other station in order to ensure more security, for this model each station can carry out only one authentication to become part of the network and to receive the Global Key. Following the key distribution procedure, an iterative authentication phase is carried out forming a gradually extended tree which begins from MKD to the whole network.
- Key regeneration and re-authentication: to prevent the security breaking, each key must be replaced after a period of use. This issue requires the replacement of the keys in the whole network in an instantaneous way. This last procedure can be carried out by the transition phase. Indeed, this mechanism makes it possible a node to emigrate from the old to the new key without losing the connectivity capacity with its neighbors and the strict synchronization model.

Thanks to the used mechanisms, WMNSec succeeds in reducing the authentication time by a factor of 3 compared with the IEEE 802.11i standard. In addition, the proposed protocol makes it possible the mobile stations to move without carrying out other additional authentications. Moreover, the profitability of WMNSec can be confirmed by the signal overhead and the effect of the mobility as well as the security of WMNs.

On the other hand, a whole of problems remains to be solved. Firstly, the GK regeneration results in an additional signal overhead which overloads the network. Furthermore, the application of the transition phase increases the Vn value that may cause the raise of the utilization period of the same key. This extension, the key unicity as well as the centralization of the used model amplify the risks of attacks.

The work [16] presents a deep study of the security subject in Mesh networks. Consequently, it reveals with a whole of recommendations which includes the relations between the various network equipments such as the mutual authentication, the location privacy, the service availability.

The new approach, named ARSA (Attack-Resilient Security Structures) does not require the application of a bilateral roaming agreement or the establishment of a real time interactive communications between the network operators following a location change. On the contrary, ARSA avoids the concept of user membership to a well defined operator by adding a new parameter, called universal pass and generated by a third-party broker. This mechanism aims at ensuring a robust and effective mobility and a seamless roaming between the equipments and the domains in WMN. Indeed, ARSA applies a mutual Authentication and Key Agreement (AKA) between a user and its associated domain.

The principle of this approach is inspired by our everyday life and in particular the use of credit card obtained from a bank with an aim of buying goods from any merchant accepting this type of card. By analogy with the Mesh network, each bank plays the role of a broker which generates a universal pass (credit card) for each user for being recognized on the level of the various domains and network equipments (similar to merchants). This approach presents a whole of advantages. First of all, it is practical and lightweight since it eliminates the bilateral communications phase and the immediate interactions between the different network equipments. Besides, ARSA provides the free mobility of users who discharge from their interdependence to one of the domains thanks to obtaining the universal pass parameter on behalf of the Trusted Third Party (TTP).

In spite of these various assets brought by ARSA, the proposed mechanism still suffers from some limits. Indeed, it supposes a trust model on the level of brokers which operate for a whole of confidential domains with an aim of granting universal pass to the authorized clients and operators. Moreover, this approach is based on a centralized architecture that includes the TTP equipment, which is responsible for passes generation.

III. PROPOSED SOLUTION

In this section, we detail our authentication protocol at the time of STAs and WMRs mobility and during two types of movements. Firstly, the intra-domain handoff presents the mobility which is carried out within the same domain. On the other hand, if the equipment moves across various domains, we have the inter-domain handoff. In order to clarify the proposed mechanism, we need to specify the architecture of the study environment for the Mesh network.

A. Network Architecture

Before beginning any study, we must specify the framework, in which we will develop our new protocol and thereafter we will evaluate its performances. Since the IEEE 802.11s standard is in the course of standardization, there is not yet a fixed architecture for a Wireless Mesh Network. Thus, those which treat or study this network, industrialists or researchers, have the choice either to create their own architecture while obeying the different recommendations and requirements for the Mesh network or to adopt a version described in the drafts of this future standard by respecting the various concepts and conventions quoted in such a proposal of IEEE 802.11s [17].

In this subsection, we will specify our network architecture as well as the various equipments and the fundamental terminology for the implementation of our suggested protocol. First of all, we begin this study by the selection of the adequate architecture kind. While basing on a work carried out on various WMN architectures, we ended to choose the hierarchical architecture as being the most adapted approach for the study of mobility as well as security. First, the central architecture is composed of multiple access points and only one authentication server, which provides the access decisions for WMN. Second, hierarchical architecture is characterized by the use of a hierarchical function for access decision (Hierarchical Access Decision-HAD). HAD is located in a node equivalent to a temporal server. In the same way a distributed function for access decision (Distributed Access Decision-DAD) is reserved for a distributed architecture. The DAD is localized on the level of each Mesh node.

The comparison between these three types of architectures, fulfilled in [18], showed that the hierarchical architecture provides the fastest handoff behavior. Indeed, in re-authentication case, data and authentication delay will be more reduced as well as the elimination of the data congestion on the level of only one authentication entity or the increase of the signaling overhead. Fig. 1 shows that the structure of WMN is decomposed into three levels:

- IGWs (Internet Gateway): the equipment connecting the Mesh network to external networks and mainly Internet,
- WMRs (Wireless Mesh Routers): routers having Mesh services (self-configuration, self-healing,..) and allowing the transmissions routing,
- STAs (Stations): the nodes of the network which do not have Mesh services.

In order to support the installation of our hierarchical architecture, the network is dissociated in a set of groups called "clusters". Each cluster is composed of a group of WMRs and one IGW selected as a head of group called "Cluster Head-CH". So that it can apply the function of access decision, CH must contain the base of WMRs and STAs pertaining to its grouping. In order to establish this architecture, we must have an algorithm for the selection of clusters and their heads such as [19], [20].

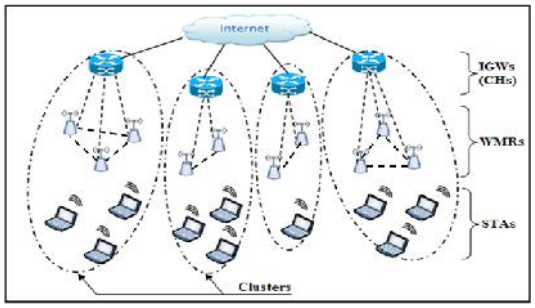

Fig. 1. Mesh environment Architecture

After having fixed the architecture on which we will set up our suggested solution, we detail the authentication

protocol. In the next part, we describe the various used mechanisms which make it possible to ensure a better network security during the mobility of STAs and WMRs.

B. Authentication Protocol

The majority of the works carried out in the field of mobility and security of Mesh network treat the clients' movements since these equipments are by default mobile. But the definition of mobility in WMN exceeds these borders to ensure the WMRs mobility. This procedure becomes possible by the integration of the WDS (Wireless Distribution System) which ensures a wireless connection between different WMRs.

In our study, we are interested in the mobility of STAs and WMRs in intra-cluster and inter-cluster handoff. In the remainder of this subsection, we initially explain the various mechanisms and techniques used in this study. Then, we clear up the various phases of the authentication protocol for these several cases which include the initial authentication, the re-authentication at the time of intra-cluster mobility and inter-cluster mobility.

1) Mechanisms and Techniques: With an aim of ensuring a protected and reliable authentication between the different components of Mesh network, a standard was appeared under the name IEEE 802.11i. This standard starts with a neighbor discovery phase in which we quote the sending and the reception of beacon frames (for a passive analysis). Then, the protocol IEEE 802.1x guarantees an authentication architecture and an access authorization to the network for the various equipments. This protocol can be associated to one of these authentication methods; CHAP (Challenge Handshake Authentication Protocol), EAP-TTLS (EAP- Tunneled Transport Layer Security), EAP-TLS etc. A third phase forms the stage of key generation through the application of 4-Way-Handshake technique.

In our study, we have recourse to a key pre-distribution method in order to facilitate later the execution of the re-authentication protocol inside a Mesh network. Indeed, the Blom scheme for key pre-distribution [14] presents one of the most known mechanisms which treat this aspect. This method is based on the derivation of the Pairwise Secret Key (PSK) between two pairs in the network. Moreover, Blom model is characterized by a threshold value, called "h-secure", which makes it possible to ensure the communications security for numerous connections in the network if the vulnerability does not exceed h compromised connections.

Thanks to its effectiveness in the security field, this method was adopted in sensor networks by Du [13]. The modified version is based on the notion of matrixes by carrying out a whole of mathematical operations and properties in order to extract the key space. In the same way this improvement of key process generation method is exploited in the field of wireless Mesh networks by the scheme Pre-authentication for fast handoff in WMN with mobile APs [11] quoted previously in section II. Consequently, this integration required the modification of 4-Way-Handshake phase of IEEE 802.11i protocol for the generation of the secret keys.

For our solution, we exploited these several mechanisms and models with an aim of setting up a new re-authentication protocol in the case of the intra-cluster and inter-cluster handoff during the mobility of STAs and WMRs.

2) Initial Authentication: To ensure the execution of the continuation of the re-authentication protocol, we specified in a first place the manner used to identify the various equipments of WMN. Then, we determined the chosen infrastructure to guarantee the connections security between the components.

- **Components Identification**

In order to ensure a single identification as well as a secure mean to generate keys, we allot to each node of the network, which can be a STA or a WMR, two parameters (id, ind). This couple is composed of an entity identity and an index indicating the column of the matrix M for STAs and the line of M for WMRs. According to Du model, M presents a matrix of size (h+1, N) with h the threshold value determined by the property h-secure of Blom key pre-distribution method and N is the number of the participants in Mesh network transmissions (STAs and WMRs).

This data is specific to each cluster (i.e. to STAs and WMRs associated with the same IGW). Moreover, this matrix reveals with public information in WMN. Consequently, the values of M, defined by each IGW, will be distributed for their participants authorized as well as a mathematical function "f" guaranteeing the following property: $f(id, ind) = M(ind)$.

Since the connection to the Mesh network, each station must be associated to a cluster. In the same way for the WMRs, they have to be related to a well defined IGW by granting its identity (id_{IGW}) to each STA and WMR pertaining to its cluster. This procedure allows detecting location change of stations and routers between different clusters in WMN.

- **Secured Connections Infrastructure**

In this paragraph, we treat the Mesh network connections infrastructure which makes it possible to ensure secured transmissions between the various components of WMN. First of all, the communications between IGWs and their STAs are enciphered by a shared key called Master Key (MK). The generation of this key is carried out since the STA connection or following to its moving towards a new cluster.

Then, a second level of transmissions is elaborate between IGWs and WMRs associated with their clusters. In order to guarantee the communications security between these entities, we used the certificate concept by allotting to each IGW and each WMR a certificate. In addition, this procedure aims to ensure the confidentiality and the integrity of the transmitted data.

Finally, in inter-cluster handoff we need to support a secure communication between the old IGW and the new IGW. To achieve this, we exploited the notion of VPN (Virtual Private Network) by using a secure tunnel between different IGWs in Mesh network for the protected transfer of the confidential data.

3) Re-authentication Procedure: The re-authentication procedure is carried out following the equipments mobility while being in a state of communication. In the rest of this part, we treat the different handoff cases of the stations (STAs) and the routers (WMRs); inside the same cluster (intra-cluster handoff) or between different clusters (inter-cluster handoff).

- **Intra-cluster Handoff**

In this type of handoff, we study the location change of the client or the WMR within the same cluster controlled by only one IGW. As it was mentioned in the part of initial authentication, each STA and each WMR can extract its own value of M (ind) while referring to its identity (id) and its index (ind) as well as the application of the function f. The sequence of the exchanged messages during the re-authentication procedure in intra-cluster handoff case between the various Mesh equipments is shown in Fig. 2. This procedure starts with a neighbor discovery phase called Scan. Then, WMR sends a request (EAP-Request / identity) towards STA to require its identity (step 1).

The station answers by the emission of a message (EAP-Response/identity) containing its identity and its index enciphered by the key MK which is shared between STA and its corresponding IGW (subsection III-B-2). Moreover, STA must specify the cluster to which it belongs by announcing the identity of its IGW (step 2).

Following the reception of this last message, WMR adds some information to prove its legitimacy. These data state its identity and its index which are enciphered by the public key of its IGW obtaining from its certificate. Furthermore, WMR associates the identity of the IGW, which is the head of its cluster, and sends the complete message towards the current gateway (step 3).

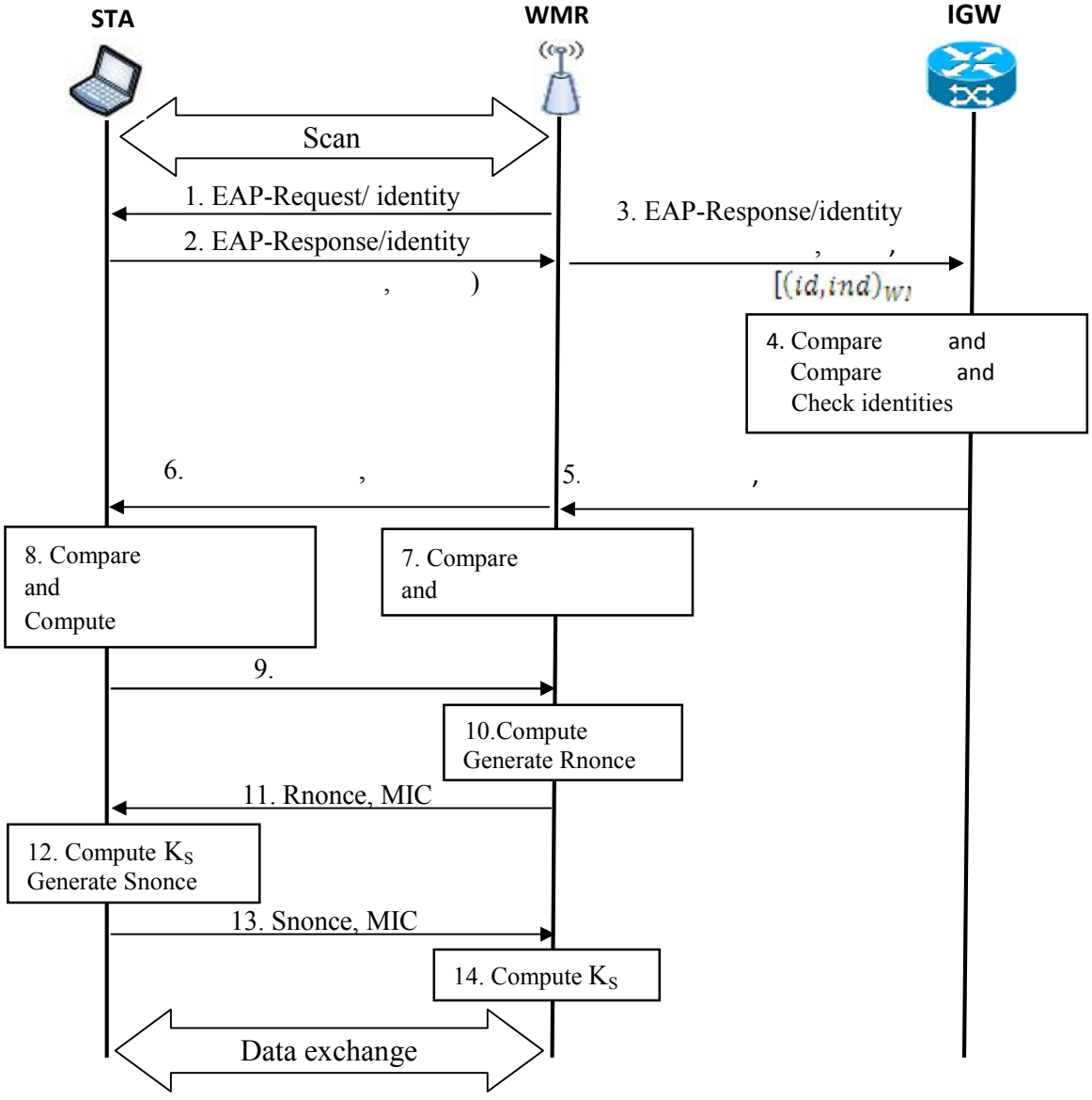

Fig. 2. Re-authentication procedure in intra-cluster handoff

On the level of the cluster head, the IGW entity starts with the location checking of STA and WMR by comparing the received identities (,) with its one. If these identities are not identical, then we have the case of inter-cluster handoff, which will be treated in the remainder of this section. If not (i.e. and are identical to the identity of the current IGW), the re-authentication procedure following an intra-cluster handoff is carried out and the IGW launches a checking mechanism for the conformity of the received information on behalf of the station and WMR. So, IGW deciphers the data of STA and WMR by using the shared key MK and IGW private key respectively (step 4).

At this stage, the IGW entity evaluated the validity of the STA and the WMR. And as our aim is to ensure a mutual authentication between the various components of Mesh network, it remains to prove the validity of IGW. To attain this goal, the current CH sends the value of the matrix columns which correspond to the enciphered indexes and that can be deciphered only by the head of their cluster. According to Du scheme, the whole of the necessary matrixes for the generation of key space are:

- M: matrix of size (h+1, N) with h is the threshold value defined in the h-secure property (subsection III-B-1) and N is the total nodes number (STA and WMR) in the cluster. M is public information and generated by each cluster head. (Since the function f is irreversible then we cannot extract the value from the identity even by knowing the index),
- D: matrix of size (h+1, h+1). It is a symmetrical matrix of random values generated by the entity KDC (Key Distribution Center),
- A: matrix of size (N, h+1). It is secret information, obtained by the calculation of the transpose of the product of two matrixes M and D.

$$A = (D.M)^T \quad (1)$$

The key space is obtained following the multiplication of two matrixes A and M. The result is the matrix K of size (N, N) which is symmetrical.

$$K = A.M \quad (2)$$

Indeed, to calculate the shared key, STA and WMR need to know their value in matrix A. For that, IGW associates the rows of the matrix A which correspond to the indexes of the client and the router (,) to the columns of the matrix M (,). On the one hand, the data which relate to the station will be enciphered by the key MK and on the other hand information with destination WMR will be enciphered by its public key (step 5).

On arrival of this last message, WMR saves the information enciphered by its public key and transmits the remainder as well as the value of to STA (step 6). Then, the two entities (WMR and STA) check the validity of their IGW by comparing the different M (ind) values (steps 7 and 8). Moreover, to generate the shared key between these two nodes and before the application of eq. 2, it is necessary to exchange its columns M (ind) (steps 6 and 9). Thanks to the symmetry property of the matrix K we have M(in = M(in= .

In order to derive the session key (K_S), WMR associates a random value called Rnonce to the message MIC (Message Integrity Code) to ensure the integrity of the transmitted message (step 11). So, STA generates a random value, named Snonce, and sends it to WMR after the addition of MIC message (step 13). Consequently, the two nodes can derive the value of K_S by joining together the following information; , Rnonce and Snonce (steps 12 and 14). Finally, the data can be transmitted in full security by enciphering them with the session key (K_S).

- Inter-cluster Handoff

In this part, we detail the re-authentication procedure following the mobility of STAs and WMRs between different clusters in Mesh network.

Mobility of STAs

For this case of location change, we must grant temporary parameters for STAs so that they can benefit from the Mesh services. Consequently, the sizes of the matrixes M and A of each cluster can be extensible according to the number of the visitors. Moreover, this extension is limited to the overload value specified by each cluster head to avoid the overload problem of WMRs or the IGW and thereafter ensure a balance of loads between WMRs and the clusters.

This procedure begins with a scan phase (Fig. 3). Then, WMR asks for the identity of STA, which answers by sending enciphered by the key MK and the identity of its old IGW. Besides, WMR transmits this message after the addition of its information enciphered by the public key of the current IGW. These stages are similar to those (steps 1 to 3) which are specified in Fig. 2.

After the reception of this information, the current IGW, noted IGW_{New}, compares the received IGW identities with IGW_{New} identity. In inter-cluster handoff and with STAs movement, the id_{IGW} sent by WMR is identical to . On the other hand, the mobile station states the identity of its old cluster head, noted IGW_{Old}. Then, IGW_{New} deciphers the WMR data $((id, ind)_{WMR})$ to verify its validity and sends those of the STA towards IGW_{Old} (step 4). This last message comprises other indications which make it possible to establish a mutual authentication between the two IGWs. The identities association of both IGWs with an authentication parameter called "Auth" allows the generation of a temporary key (K_T). IGW_{New} calculates this key (step 4) then it sends its identity, the Auth parameter, 2 times a random value nonce ; the first is intelligible and the second is enciphered by the key K_T, enciphered by the key MK and a Sequence Number (SN) to avoid the problem of reply attack (step 5).

On the level of the IGW_{Old}, this cluster head generates the temporary key K_T while using the identities of both CHs and "Auth".

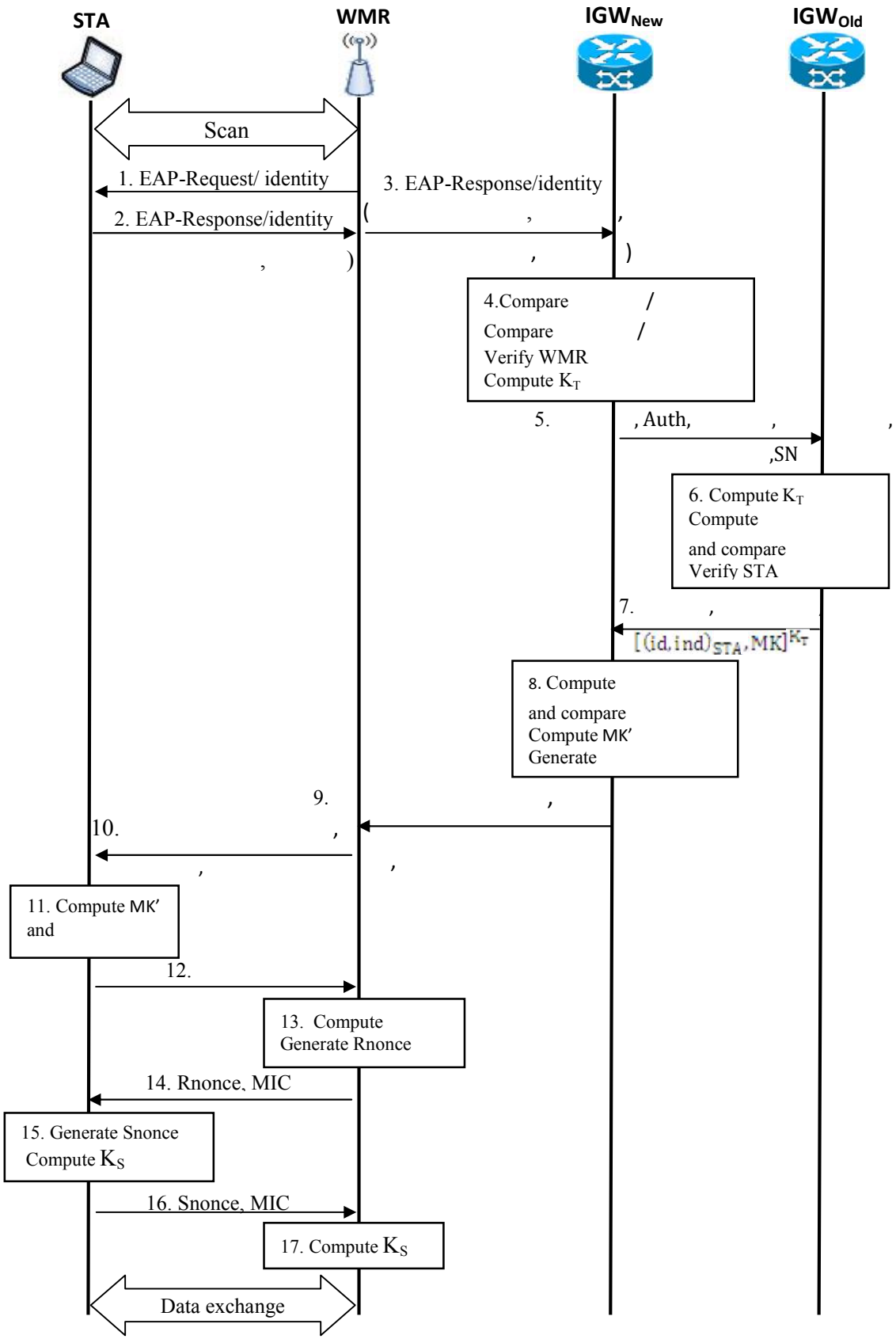

Fig. 3. Re-authentication procedure in STAs inter-cluster handoff

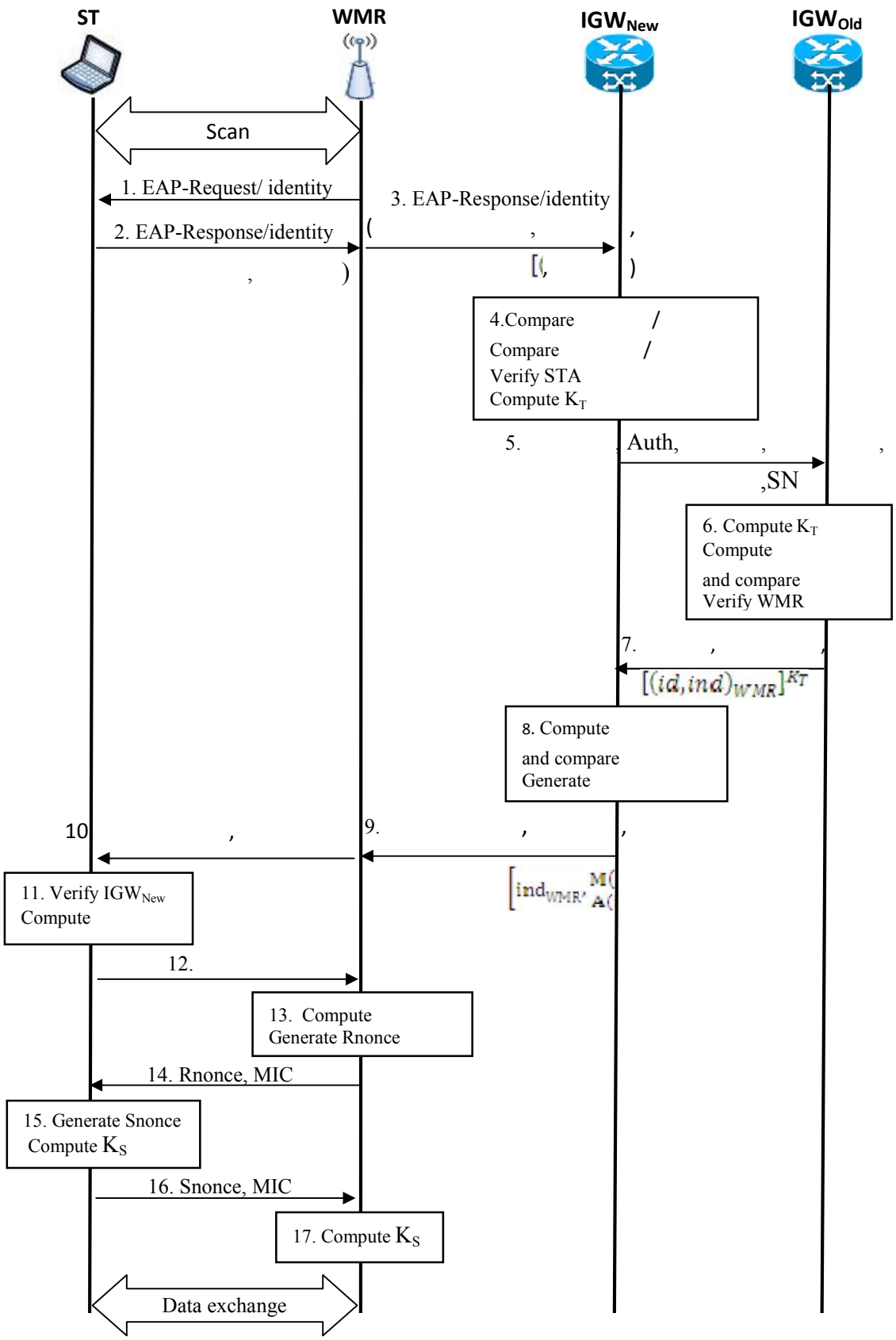

Fig. 4. Re-authentication procedure in WMRs inter-cluster handoff

Then, it calculates the application of the key K_T with the value and compares this result with the value sent by IGW_{New}. This comparison makes it possible to verify the validity of IGW_{New}. Then, the old IGW deciphers the received STA data, checks its legitimacy (step 6) and transmits a message to the new CH, containing 2 times a value noted nonce , the first is intelligible and the second is enciphered by the key K_T and the STA data as well as the key MK enciphered by the temporary key (step 7).

The comparison of values allows the checking of the IGW_{Old} validity. Thereafter, IGW_{New} derives a new key MK' from the old one (step 8) and sends a message to WMR. This message is composed of the new index allotted to the STA (ind_{STA}), the column of the matrix M and the row of the matrix A, all these parameters are enciphered by MK'. Moreover, we note the presence of the identity of IGW_{New} and the column of M and the row of A which correspond to the index of WMR and enciphered by its public key (step 9).

After the reception of this information, WMR deciphers these data and transmits the remainder and to the station STA (step 10). Then, STA stores the values associated with its new index and computes the new key MK' and (step 11). The rest of this procedure, which comprises the generation of in the side of WMR and the session key, is similar to the stages (9-14) in Fig. 2. If IGW_{Old} is unreachable, the mobile station is obliged to carry out the initial authentication with IGW_{New}.

Mobility of WMRs

In this part, we study the location change of WMRs between different clusters in the Mesh network. The re-authentication procedure is illustrated in Fig. 4. This scheme begins with the same messages as (steps 1to 4) from Fig. 3.

After the calculation of the temporary key (K_T) between the two IGWs, the new CH sends its identity, the "Auth" parameter, an intelligible nonce value and another enciphered by the key K_T, a Sequence Number (SN) and the WMR data which are encrypted by the public key of IGW_{Old} (step 5) to the old CH. This last entity calculates the temporary key K_T, checks the legitimacy of IGW_{New} by comparing the result of the encryption of by K_T with the received nonce value from IGW_{New}. Then, IGW_{Old} verify the validity of WMR by consulting its data base (step 6).

In addition, this entity generates an intelligible nonce value , computes the enciphered value of and by the temporary key K_T and collects all these parameters in a message towards IGW_{New} (step 7). To ensure the mutual authentication between the two CHs, IGW_{New} applies the key K_T with the received nonce value , compares the obtained result with that received and generates a new index for WMR ind_{WMR} (step 8). Then, it sends a message containing the column of M and the row of A which corresponds to the index of the STA enciphered by the key MK, the identity of CH_{New} and the new index allotted to WMR, its column from matrix M and its row in matrix A enciphered by WMR public key (step 9).

Following the reception of this information, WMR stores these new parameters, after the deciphering using the private key, and transmits the remainder of the message as well as the value of towards the station (step 10). Thereafter, STA deciphers the data by its key MK and saves them locally after the checking of the cluster head legitimacy by knowing the value of the key MK and the corresponding M column (step 11). The remainder of the re-authentication procedure is in conformity with the steps (9 to 14) of the handoff intra-cluster in Fig. 2. In the case of location change of the associated WMR and its STAs, we combine the two last procedures. Indeed, we allot to these entities new visitor indexes.

IV. PERFORMANCE EVALUATION

Because of the novelty of this technology, Mesh network is not yet installed in the majority of existing simulators. On the other hand, the new simulator, which is called NS3, implements a test version for this type of network. But this implementation is limited to the backbone level and does not yet include the station level which is necessary for the evaluation of our proposed solution that aims at securing the network access. For this reason as well as the multiplicity of the errors that need to be recovered in this test version, we have resort to develop a simulator in order to be able to evaluate the performances of our suggested authentication protocol.

This simulator specifies various parameters of this type of network and to simulate its features to study the effect of security during the handoff of the mobile stations. The selected network covers 300m×300m comprising 9 WMRs and a variable number of clients. To evaluate the performances of our solution, we will consider two types of traffic: voice and Web communication. While referring on these types of communications as well as the parameters of simulation, we evaluate the simulation's results according three 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 stations at handoff for the total number of stations which requests handoff,

- Loss rate: represents the number of lost packets for the total number of the emitted packets.

The remainder of this section relates to simulation results of the various cases studied in the preceding section.

A. Handoff Latency

In this subsection, we will focus on the first parameter which is handoff Latency. This parameter indicates time necessary to carry out the re-authentication procedure from the sending of association request until the moment of attachment with the new desired equipment. Fig. 5 shows the simulation results for the suggested protocol in three handoff cases; intra-cluster handoff (a), inter-cluster handoff with WMRs movement (b) and inter-cluster handoff with STAs movement (c).

By analyzing these various curves, we notice an increase in the values of essential time to carry out the re-authentication phase, relating to the growth of the population (i.e. the number of mobile stations). This observation can be justified by the increase in requests number which demand handoff and thereafter the heaviness of WMRs by additional packets that need a fast treatment.

By comparing the three curves of the various mobility cases of STAs or WMRs, we notice that the handoff latency values for intra-cluster mobility present the least values obtained in the various movement scenarios. That is caused by the minimized number exchanged messages between the equipment of the same cluster without recourse to include thirds, which are outside their routing area in different communications.

The comparison between the curves (b) and (c), for inter-cluster handoff with movement of WMRs and STAs respectively, proves that the values in (c) are higher than those in (b). Indeed, the number of exchanged messages between the equipment, the traversed ways and the intervening equipment in the communications (i.e. in the case of STAs movement the authentication packets circulate mainly between IGW, WMR, as intermediate node and STA and in the case of WMRs movement the authentication messages related to IGW and WMR).

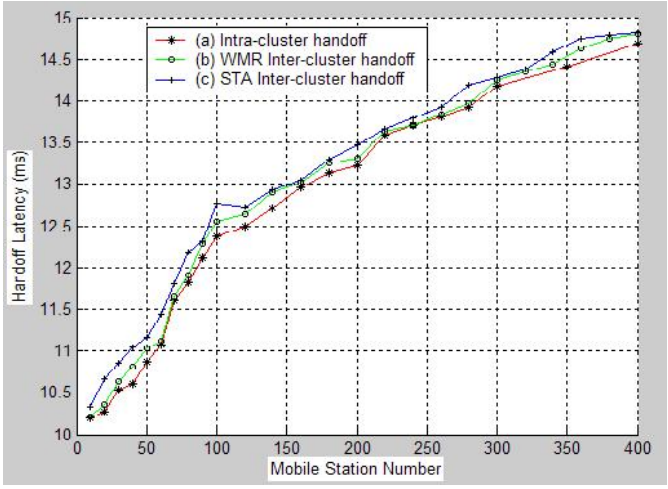

Fig. 5. Handoff latency vs. number of mobile stations in different handoff cases

B. Loss Rate

A second very significant parameter for the performance evaluation of such a studied network is loss rate. It makes it possible to calculate the percentage of lost packets according the totality of the emitted packets by the stations of network. Fig. 6 shows the simulation results concerning the loss rates in the case of intra-cluster mobility (a), WMRs inter-cluster mobility (b) and STAs inter-cluster mobility (c).

These curves illustrate that for minimal values of stations (120 for (a) and 100 for (b) and (c)) the loss rates remain null. However with the increase in the number of the mobile stations, these values amplify more and more. This growth reveals with the rise in the number of packets transmitted to WMRs level and thereafter the increase in the processing time of these messages which drive to beyond the delay and finally the loss of packets.

As the study of handoff latency, the comparison of the loss rate curves indicates a variation of the obtained results. Moreover, in the case of the intra-cluster mobility the rates of loss are lower than these values in the other curves. That is due to the local treatment of data inside the same cluster. For the two other curves (b) and (c), the values of loss rate are almost close but with a light difference which are caused by the variation of hops number (i.e. the number of traversed nodes to reach the destination).

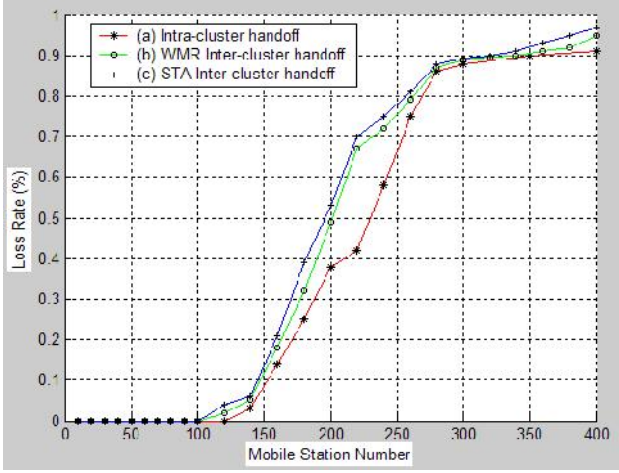

Fig. 6. Loss rate vs. number of mobile stations in different handoff cases

C. Blocking Rate

The loss of two successive packets drives to the blocking of the station. The curves of Fig. 7 show the blocking rate values of stations in three handoff cases; intra-cluster handoff (a), WMRs inter-cluster handoff (b) and STAs inter-cluster handoff (c). This parameter presents the percentage of blocked stations according to the totality of stations which ask for points of attachment change.

The analysis of these curves reveals with an increase in the blocking values which accompanies the growth of the mobile stations number in Mesh network. Indeed, this increase is caused by the rise in the list of the packets with need to be treated, the processing time and the packets loss. Moreover, for the number of stations mobile lower than 120 in intra-cluster handoff and inter-cluster handoff of WMRs and lower than 100 in inter-cluster handoff of STAs, we notice the absence of blocking station.

As it is shown for the comparison of the curves in the evaluation of the preceding parameters; handoff latency and loss rate, the curve of intra-cluster mobility presents better results than the values obtained in the other curves. Moreover, the blocking rates in the case of inter-cluster handoff of WMRs are lower than those resulting in the case of inter-cluster handoff of STAs. That is justified by the same reasons quoted previously in the two former subsections.

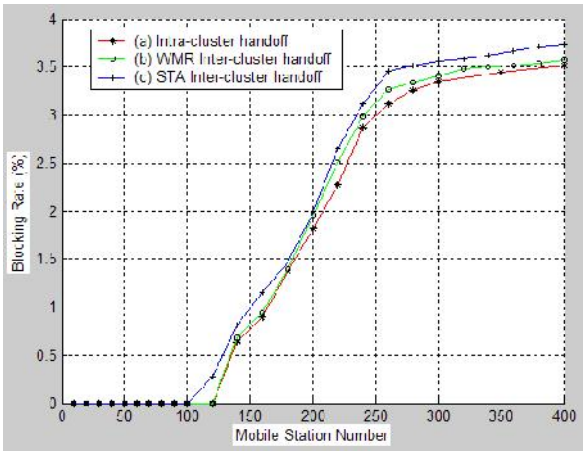

Fig. 7. Blocking rate vs. number of mobile stations in different handoff cases

V. CONCLUSION

Thanks to the various studies carried out in the field of wireless local area networks, the world of wireless saw the birth of new solutions like the Ad hoc networks and the Wireless Mesh Networks (WMNs). These technologies propose a facility and a flexibility of deployment, a highly skilled quality of services as well as additional services.

A great concern with all the wireless networks is security. While WMNs continue to develop, several works are provided in order to grant the network access only to the authorized users and in particular during the handoff phase which forms the most critical moments of security. Our contribution in solving this problem consists in proposing a re-authentication protocol which makes it possible to identify the legitimate clients and routers from the intruders.

The proposed mechanism starts with the identities checking phase of the various equipments. Then, it exchanges the matrixes values in order to calculate the key space. Finally, it generates the session key to secure the exchanged data between the communication members. These tasks are carried out thanks to some existing techniques; Blom Key pre-distribution scheme and Du Key process generation method.

With an aim of evaluating the performances of the suggested model, we simulated the behavior of the network in which we have implemented the re-authentication protocol that makes it possible to protect the network access during the various handoff scenarios of STAs and WMRs. Consequently, the simulation results, which are based mainly in the criteria of handoff latency, loss rate and blocking rate, show that the proposed protocol presents optimal values of handoff latency which do not exceed 15ms, satisfactory loss rates which meet the need for the quality of

services (< 1%) and thereafter the blocking rates those are proportional to the increase in re-authentication time and in loss rate.

REFERENCES

[1] G. Held, *Wireless Mesh Networks,* Auerbach Publications, 2005.

[2] Y. Zhang, J. Luo and H. Hu, Ed. , *Wireless Mesh Networking: Architectures, Protocols and Standards*, Auerbach Publications, 2006.

[3] I. F. Akyildiz, X. Wang and W. Wang, "Wireless mesh networks: a survey," *Computer Networks*, vol. 47, pp. 445–487, 2005.

[4] J. Crichigno, M. Wub and W. Shu, "Protocols and architectures for channel assignment in wireless mesh networks", *ScienceDirect*, 2007.

[5] L. Qiu, P. Bahl, A. Rao, and L. Zhou,"Troubleshooting Wireless Mesh Networks," *SIGCOMM Computer Communication Review (CCR)*, Oct. 2006.

[6] A. Naveed, S. S. Kanhere and S. K. Jha, *Attacks and Security Mechanisms*, Chapter1 of *Security in Wireless Mesh Networks*, Oct. 27, 2006.

[7] A. Gerkis and J. Purcell, "A Survey of Wireless Mesh Networking Security Technology and Threats: Technologies and challenges related to wireless mesh networks," *SANS Institute*, September 2006.

[8] N. Ben Salem and J. P. Hubaux, "Securing wireless mesh networks," *IEEE Communications Magazine*, vol. 13, No. 2, pp. 50-55, April 2006.

[9] J. Xie and X. Wang, "A Survey of Mobility Management in Hybrid Wireless Mesh Networks," *IEEE Network*, Vol. 22, No. 6, pp. 34-40, Nov-Dec. 2006.

[10] I. Lee, J. Lee, W. Arbaugh, and D. Kim, "Dynamic Distributed Authentication Scheme for Wireless LAN-Based Mesh Networks," *Information Networking*, 2008.

[11] Ch. Park, J. Hur, Ch. Kim, Y. Shin, and H. Yoon, "Pre-authentication for Fast handoff in Wireless mesh networks with mobile APs," *WISA'06, Information security applications*, 2007.

[12] A. Mishra, M. Shin, N.Petroni , T. Clancy and W. Arbaugh, "Pro-active Key istribution using Neighbor Graphs," *IEEE Wireless Communication*, vol. 11, February, 2004.

[13] W. Du, J. Deng, Y. Han, P. Varshney, J. Kate and A. khalili, "A Pairwise Key Pre-Distribution Scheme for Wireless Sensor Networks," *ACM Conference on Computer and Communications Security (CCS 03)*, pp.42-51, 2003.

[14] R. Blom, *An optimal class of symmetric key generation systems*, EUROCRYPT, 1984.

[15] G. Lukas, Ch. Fackroth, "WMNSec – Security for Wireless Mesh Networks," *IWCMC'09, International Conference on Wireless Communications and Mobile Computing: Connecting the World Wirelessly*, 2009.

[16] Y. Zhang and Y. Fang, "ARSA: An Attack-Resilient Security Architecture for Multihop Wireless Mesh Networks," *IEEE Journal on Selected Areas in Communications*, 2006.

[17] *IEEE P802.11s/D2.0-Draft Standard for Local and Metropolitan Area Networks - Amendment to Part 11: Mesh Networking*, March 2008.

[18] A. Roos, S. Wieland, A. Th. Schwarzbacher and B. Xu, "Time Behaviour and Network Encumbrance Due to Authentication in Wireless Mesh Access Networks," *Vehicular Technology Conference (VTC)*, 2007.

[19] K. Theriault, D. Vukelich, W. Farrell, D. Kong and J. Lowry, "Network traffic analysis using behavior-based clustering," 2002.

[20] R. Langar, N. Bouabdallah and R. Boutaba, "Mobility-aware clustering algorithms with interference constraints in wireless mesh networks," *Computer Networks*, Vol. 53, No. 1, pp. 25-44, January 2009.