A Protocol for Re-authentication and Handoff Notification in Wireless Mesh Networks

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

LETI laboratory, University of Sfax
Sfax, Tunisia

Abstract

Mesh technology has captured the interest of university research and industry, because of its capacity to meet at the same time the requirements of Internet service provider and users. But, its architecture and configuration do not ensure a protection against the unauthorized use of the network since the used basic security measures do not include the concept of mobility. Our endeavor in this paper is to introduce a re-authentication scheme for secure handoff based on an efficient mobility management. First, we have treated the mobility aspect. Indeed, we applied the Mobility Notification Message procedure to support an environment which manages handoff in effective way. Then, using this technique, we have defined a new scheme to provide security during handoff. Our study shows that the proposed protocol can provide more protected network and more effective re-authentication scheme in term of minimized handoff latency as well as reduced blocking and loss rates.

Keywords: *Re-authentication, Handoff, Mesh Network, Security, Mobility.*

1. Introduction

The last decades have shown a very significant revolution for wireless networks, which results by the appearance of several models and techniques. These new technologies, which bring new services and improve the used processes, form the next generation of wireless networks. Mainly, we quote two great families for these techniques; Ad hoc networks and Mesh networks.

These technologies are characterized by deployment flexibility, a facility of use and a wider cover. Indeed, Mesh solutions support a diversity of advantages which are essentially the minimization of the network installation cost with a simple maintenance procedure, the robustness of offered networks services as well as the extension of the cover without touching with the reliability of the network.

Moreover, Wireless Mesh Network (WMN) is composed of multiple types of entities which differ according to the adopted architecture. In spite of this diversity, all these nodes are able to be dynamically self-organized and self-configured. In addition, another aspect characterizing the relations between these nodes is the multi-hop transmission.
This procedure makes it possible to build several paths between various components of network in order to reach the target. Thereafter, it may help to solve the problem of corrupted paths, which is caused by the disconnection or the breakdown of an entity inside the network.

This type of network may take all its interest only when a standard is associated to it. Indeed, the IEEE (Institute of Electrical and Electronics Engineers) formed the 802.11 Task Group "s" (TGs) in 2004 to prepare a standard amendment for WMN. This future standard (IEEE 802.11s) defines a whole of terminologies which will be adopted in the remainder of this study.

First of all, any node which supports the Mesh services such as control, management, and configuration of network is a Mesh Point (MP). If the node supports in more the access to stations (STAs) or to the nodes which do not have the Mesh services it is called a Mesh Access Point (MAP). Moreover, a Mesh Portal Point (MPP) is a MP which has a connection with Internet and the external networks.

Although we notice the significant advantages of WMN successful deployment in the whole world, some technical limitations and problems will remain to be solved and will probably require more advanced research for the deployment of such a network [1]. For example, we quote the quality of service, the security, the mobility management and the interference problem.

A principal challenge in WMN is the supply of the mobility, which constitutes a principal need in wireless communications, since network users are increasingly mobile due to the massive deployment of wireless technologies. This new generation of clients, who seek to communicate during their displacements without any constraint of connectivity, and where the network change needs to be completely transparent, pushed the researchers' community to propose a whole of solutions and studies to solve these problems.

To make it possible to users to carry out an effective and reliable handoff (i.e. a change of point of attachment for a client while being in communication) as well as a secure access to the offered services in Mesh network, a study of security aspect should be carried out during the moving of mobile nodes from an MAP to another and through various domains. Indeed, mobility mechanism cannot prove its effectiveness only if it is associated to well defined and studied security mechanism in order to provide access to Mesh network only to authorized nodes. This aspect becomes increasingly critical toward the growth of various attacks which can be carried out in an open medium environment and with a variable topology.

The goal of this study is to design a re-authentication scheme for secure handoff in the wireless Mesh network based an efficient mobility management. First, we begin our study with the treatment of mobility problem. Indeed, we applied the Mobility notification Message (MNM) procedure to support an environment which manages handoff in effective way. Based on this technique, we define a new scheme to provide the security network during the node handoff.

The remainder of this work is organized as follows. In Section 2, we give some related works. In Section 3, we describe the details of our re-authentication protocol. In Section 4, we analyze and evaluate the performance of our proposed scheme. Finally, we conclude the study in Section 5.

2. Related Work

WMN brings several advantages such as the facility and the flexibility of deployment. The prime objective of this type of network is to offer a flexible connectivity to the mobile users. Consequently, the special care must be taken by handling the mobility. In our study, we are interested in stations mobility. Due to the importance of this challenge, various solutions were proposed in the literature in order to solve the problem of lack of security during handoff. Among which we quote the example of SMesh (Seamless Mesh) [2], WMM mechanism [3], Protocol for Macro Mobility and multi-homing notification and also Geo-mobility and location service in spontaneous WMN.

The stations in SMesh are connected automatically to the network by the standard DHCP. SMesh proposes its own solution to solve the handoff problem. This suggested approach can be considered effective since it doesn't include the client in the procedure of handoff neither changes its device nor introduced additional software. On the other hand, the mobile nodes only have localization's precision of 2 seconds. Moreover, a heavy signaling overhead was produced by the diffusion of DHCP requests by the station at each 2 seconds and also created in case where several MAP have good connectivity with certain client, the data packets of this client will be duplicated.

A second vision to solve the problem of mobility management in Mesh network is presented in this work [4]. This study proposes a new model of location service based on a whole of principles. First of all, this approach separates between the allotted addresses, which change according to the geographical location of the node, and their persistent identifiers, which remain unchangeable in spite of these movements. Then, this separation requires the presence of mapping service for these last parameters and to each station to be located whenever its site. This idea is carried out by the installation of "Distributed Location Service" mechanism which is central additional equipment in the network.

This approach requires a long handoff latency since each transmission must have recourse to this service to apply the correspondence identity/address and also each displacement must be announced in this new equipment. Consequently, this procedure requires too much signaling overhead and very considerable handoff latency. Concerning the security aspect, the suggested model supposes the existence of confidence relations between various components inside network, except the clients, which contradicts the reality of wireless networks. In this same context, this mechanism does not take into account the risks and the attacks which can proceed inside Mesh network at the time of handoff.

The mobility management is a very wide issue of research and can be treated from various sides. Indeed, the macro mobility is a type of mobility, which is carried out between various domains inside Mesh network. In this context, the study [5] proposes a notification protocol driven by the access points and independently of the used routing protocol. In this approach, the access points detect the clients' macro mobility by the change of addresses. Following this detection, the MAPs send to source node a notification message containing the new configuration

parameters. This message will be sent at each 60 seconds for each client, which may cause a heavy additional signaling overhead within Mesh network. As the previous study, this approach is studied independently of the security aspect. The innovation brought by WMM is the use of the options field in the header of an IP packet to store the station location information in each MP. But when there is no handoff, these additional bytes aren't necessary. Thus, the proposed method requires a heavy implementation and many procedures. Especially, the query procedure involves flooding signaling messages to the WMN, which results in signaling overhead to the system. WMM as others studies, which treats only mobility, their medium remains open and the traffic can be easily listened or modified.

In this context, security becomes a principal necessity. The issue of insecurity becomes increasingly vulnerable and critical during handoff that requires the application of an effective policy and well defined security. We mention in the remainder of this section some solutions suggested recently solving the security problem. The mechanism [6] is based on the use of a "token" of authentication which is dynamically produced during a handoff by the moving station. In this solution, the structure of the "token" is not defined as well as the manner of the generation of this parameter which will be present at the level of the station and the authentication server at the same time (synchronization between the stations and the server). Furthermore, with each handoff, the server intervenes in the re-authentication phase between a given station and his new MAP what carries out to overload the server then to increase the handoff latency and degrade the quality of network. We notice also the "token" duplication risk or the generation of the same "token" on another station.

In addition, the authors of [7] introduce a Two-Factor localized authentication model for a handoff inter-domain (i.e. the station moves between MAPs which belong to the same Mesh). Although this solution proves its effectiveness in several cases of attack and lack of security, the proposed model use a removable support to store confidential information which amplifies the risk of attack, theft and even the loss of this device. This scheme uses a central entity which carries out several tasks so the architecture becomes centralized, that may multiplies the risks of attack and disturbs the correct functioning of network. This model uses several parameters that require so much memory capacity to store this information in different devices.

Moreover, [8] introduces a secure authentication technique that can be conveniently implemented for the ad-hoc nodes forming clients of an integrated WMN, thus facilitating their inter-operability. The proposed authentication scheme is based on using EAP-TTLS (Extensible Authentication Protocol-Tunneled Transport Layer Security) over PANA (Protocol for carrying Authentication Network Access). The EAP-TTLS extends EAP-TLS to exchange additional information between client and server by using secure tunnel established by TLS negotiation.

In spite of the diversity of the benefit brought by this approach such as a level of security of the stations similar to that proven for EAP-TLS but with very simple implementation and also flexibility by employing any authentication protocol, it remains some anomalies to be rectified. First, the discovery and handshake phase, executed before the establishment of the secure tunnel, is prone to spoofing attacks and the threat of man in the middle by a malicious node as data are sent in clear. Second, this study did not take into account the notion of mobility and handoff in WMN. Finally, this approach presents a long procedure of authentication that may result in a heavy signaling overhead.

With an aim of solving the problem of lack of security following mobility phase, the study [9] seeks to design a pre-authentication model for fast handoff with mobile Access points (APs). This approach improved existing methods, particularly Mishra et Al technique [10], to be applicable inside WMN environment. Besides, the suggested model avoids the chained relation between the whole of PMKs (Pairwise Master Keys) in neighbors graph with an aim of solving the problem of the pre-authentication. Moreover, the authors applied Du et al. method [11] for PMKs generation and for keys pre-distribution procedure. The principle of this last technique is based on Blom model [12] which uses a set of matrices in order to manage the secret keys.

Although the suggested solution presents a secure mechanism for handoff as well as an effective management of keys, it still suffers from a whole of limits. First of all, the procedure of matrices diffusion used in this scheme requires the transmission of a great number of values for all Mesh network components. Consequently, this can cause a heavy signaling overhead.

Second, this model requires a huge amount of calculation to be carried out and treated in order to extract the matrices. Then, to extend the Mesh cover, we proceed simply by the addition of access points. As a result of this network extension, the authentication server must change the matrices which are used for client authentication and re-authentication procedure because these various matrices depend on network size (i.e. the number of present MAPs).

3. Proposed Scheme

In this section, we describe the principle of our proposed re-authentication protocol, which is applicable in Wireless Mesh Network. First of all, we define the adopted architecture of our study environment to facilitate the implementation of our suggested solution. Our studied issue can be divided into two great phases. The first aspect is the mobility since we will be interested in the nodes mobility management, which is known as handoff. The major problem which is derived from mobility is security. Indeed, this second aspect makes it possible to eliminate risks, attacks and vulnerable actions in Mesh network.

3.1 Network Architecture

In order to be able to apply our re-authentication protocol, we need to specify the architecture of the adapted environment. In our study, we have slightly modified the terminology used in the draft D2.0 of IEEE 802.11s (described in the introduction section) [13]. Moreover, we selected the hierarchical architecture because it presents the most adapted approach for mobility and security treatment as well as it has the most powerful platform, which is compatible with Mesh network requirements and challenges. This choice is based on a comparative study made between three types of architecture; centralized, distributed and hierarchical.

Indeed, the work [14] presents a study on the authentication behavior for mobile nodes in Wireless Mesh Network. This study evaluated the latency and the resources consumption of authentication inside this same type of network and by considering the nodes mobility. Following this comparison, the results showed that hierarchical architecture provided the fastest handoff behavior since in case of re-authentication the data and the authentication latency will be more reduced as well as the elimination of the congestion on the level of a unique authentication entity.

In our hierarchical architecture and as shown in Fig. 1, the network is divided into groups called "Clusters". For each group or cluster, we select a Mesh Access Point as a head of group called "Cluster Head", noted CH. This selected MAP will drive the different operations proceeding inside each domain such as; load balancing between MAPs, access control, decision of handoff authorization, etc.In addition, MAPs nodes in IEEE 802.11s draft are by definition stationary to provide more stable and invariable architecture. But this condition does not meet the needs and requirements wished of Mesh network deployment where mobility is the first aspect to be respected. Then to ensure a closer architecture reality and more adjusted with clients' hopes, it is necessary to hold in account the mobility of MAPs. This architecture is used with an aim of facilitating the implementation of mobility and re-authentication protocol explained in the next subsections.

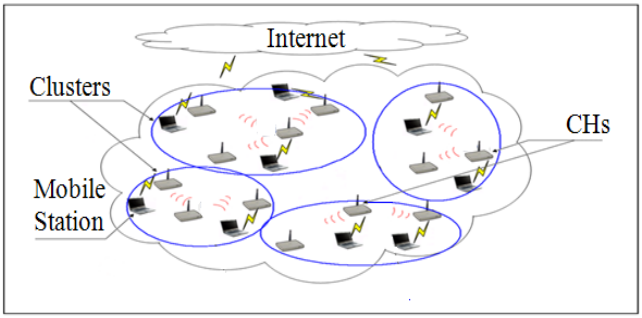


Fig. 1 The adopted Mesh network Architecture for the proposed solution.

3.2 Handoff: Mobility Management

After having fixed the architecture of our study on which we will implement our re-authentication protocol, we will be interested in the first aspect, which is mobility. Moreover, we cannot solve the lack of security problem during handoff without initially ensuring an effective mobility protocol. Indeed, this aspect facilitates the integration of the re-authentication protocol and the preparation of a suitable platform. The purpose of such mobility protocol is to supervise and follow the location information change of the various nodes inside the network.

The prime objective of Wireless Mesh Network is to offer a supple connectivity to mobile users. However, the ease of communication should not make forget the new risks introduced by these techniques. Indeed, in Mesh network the clients (mobile by definition) are likely to move from a cell (Mesh node cover) to another. Moreover, the protocols, intended to manage mobility in wired networks, give bad results on this new technology. So the installation of a mobility mechanism (roaming) will be a crucial issue for services continuity and consequently the special care must be taken by handling these subjects.

In Mesh network, there are various mobility types; users' mobility and network devices mobility. Besides, this aspect has several levels: intra-cluster and inter-cluster mobility. For the first type, the displacements of clients are limited to the cover of only one cluster. On the other hand, the various network components are likely to roam from a cluster to another. In our work, we are interested in these various aspects of mobility. Thus, we refer to the mobility of the users simply by the term handoff.

Components Identification: To be identified in a unique

way inside Mesh network, we allot to each client an identity. This parameter is obtained since the connection establishment and following a success authentication of a new client. This procedure allows to provide a secure and robust network which can be protected against the various attacks and to avoid the anonymity problem. The identities attribution phase does not relate only to clients but rather all the other Mesh network components. Indeed, each MAP and each CH has a preset identity since the connection of the considered node. These additional parameters will be used to prove the device validity using some other information. Concerning the allotted identities to a client, who is already disconnected from the network, they will be added, by the Mesh Access Point (MAP) associated with this client, to the list of revoked identities. Thereafter, this list will be updated in the corresponding Cluster Head in Mesh network so that identities list cannot be re-used by another client.

Mobility Notification Message (MNM): In this part, we are interested in the study of inter-cluster and intra-cluster mobility of clients inside the Mesh network. In order to achieve this purpose, we need to supervise the location information of each component and to follow their displacements in the network. The idea is based on the use of the notification message notion. Then, following the displacement of one of the component, a notification message will be sent with an aim of informing the other entities by the movement. This study differs according to the carried out mobility type.

- **Intra-cluster Mobility**

Mobility is carried out within the same cluster. In this case, we are interested primarily in the displacement of clients between different MAPs. Indeed, Cluster Head (CH) has to communicate a notification message to mobile client with an aim of assigning its new credentials and also proving to this node the validity and the legitimacy of its associated CH. This procedure aims at updating the location information of each station inside Mesh network following the displacements of these components.

- **Inter-cluster Mobility**

In In this type of displacement, a component (client or MAP) crosses the cover zone of another neighbor cluster. Consequently, the new CH (CH_{new}) should inform the old CH (CH_{old}) by this location change through sending a notification message. This operation makes it possible to ensure two main functionalities. First one is to notify CH_{old} by the displacement of certain entity and thereafter the cancellation of this later from its base. The second functionality consists on ensuring the legitimacy of these two CHs using a mutual authentication procedure. In this same mobility type, a second notification message, similar to that of intra-cluster mobility, is sent from CH_{new} towards the client.

3.3 Security: Re-authentication Protocol

Although there are many significant advantages and benefits of the Mesh networks successful deployment in the whole world, some technical limitations and problems will remain to be solved and will probably require more advanced research for the exploitation of such a network. We quote some of these weaknesses; the mobility and the security. However, in spite of the study of mobility aspect in previous sub-section, the medium remains open and the traffic can be easily listened or modified. In this context, security becomes a principal concern. Indeed, mobility mechanism cannot prove its effectiveness alone but only when it will be associated to a well defined and studied security mechanism.

Some Possible Attacks: Attacks in WMN are very diverse, some are inherited from previous wireless technologies and others appear with the new WMN challenges. These threats differ on the level of the used techniques, the exploited faults and the desired intentions. Denial of services (DoS) represents the major attack aiming at rendering unavailable during an unspecified times the services and resources of a network for the authorized users. Generally, attackers look for faults in the different protocols of such a network to be incorporate in any system illegally:

- Routing protocol attacks: WMN can be prone to many types of attacks especially DoS because of multi-hop environment which may cause the routing overheads on the level of WMR. Here are some of these threats: Black-hole, Grey-hole, Worm-hole, Route error injection, etc.
- MAC protocol attacks: Due to the manipulation of an open and shared medium in WMN, the MAC channel may suffer from a several kinds of attacks such as: Passive Eavesdropping, Link Layer Jamming Attack, MAC Spoofing Attack, Replay Attack, etc.
- Physical protocol attacks: The physical layer can be affected by using radio jamming devices and the outdoor deployment which may meddle in the physical channels and disturb the network availability.

The diversity of attacks and the high degree of vulnerabilities pushed the community of the researchers to propose a whole of solutions to solve these problems of lack of security. In this context, we have proposed a new re-authentication, which will be described in the next subsection.

Re-authentication Protocol: The authentication is one of

the significant measurements to protect the Wireless Mesh Network from different attacks, allowing only the authorized users to obtain connections and preventing the adversaries from being integrated in the network and disturbing its services and its operations. Moreover, to make it possible to the users to carry out effective and reliable handoff as well as a secure access to Mesh network services, a re-authentication method should be carried out during the crossing of mobile nodes through different MAPs and also various clusters.

In this subsection, we detail our proposed re-authentication protocol in order to guarantee a safe access during the handoff phase. Since the majority of attacks origin remains unknown and unexpected, we should not suppose any confidence relations between all network equipments. Indeed, the source of risk can be a client or a Mesh Access Point or even a malevolent Cluster Head. In our study, we treated the case of clients' mobility in the same cluster (intra-cluster) and between different clusters (inter-cluster).

- **Intra-cluster Mobility**

In case of intra-cluster handoff, the displacement of station is carried out from a MAP to another but while remaining in the same cluster. Fig. 2 shows the exchanged messages flow between the various components during intra-cluster mobility. First of all, the entities intervening in this exchange are:

- Station (STA) : the mobile client which is in communication,
- MAP_{new} : the new Mesh Access Point of the mobile station,
- CH : Cluster Head of the cluster which contains STA and MAP_{new}.

Station STA starts the re-authentication procedure by sending an access message request (1). Then, MAP_{new} answers with an EAP-Request/identity request (2) which requires the client's identity. Following the reception of this last message, the station dispatches the identity of its corresponding CH (ID_{CH}), its own identity (ID_{STA}) ciphered by the session key (K) shared between the station and its associated CH for the preceding session (3).

Before the retransmission of the last received message, MAP_{new} node adds some more information to carry out the mutual authentication with the CH entity. This information is composed by its own identity (ID_{MAP}), a nonce value generated randomly (N_{MAP}) and Res_{MAP} value which represents the result of the application of the nonce value on a whole of the preset algorithms between MAPs and their CHs since their integration in network. Because these data present the evidence of MAP_{new} legitimacy, they should not be transmitted as understandable and legible information but rather enciphered by the public key of CH (4). After the reception of all these parameters, CH starts with the check identity phase of ID_{CH} to know if it corresponds to its one. If it is not the case, we have an inter-cluster handoff. But, if the two identities are identical, CH continues the identities checking procedure in order to make sure of the membership of STA and MAP_{new} with their same cluster. Then, it calculates the result (Res_{CH}) of the nonce value (N_{MAP}) application on the whole of the common algorithms between CH and MAP_{new}.

Then, CH compares the obtained result (Res_{CH}) with that sent by MAP_{new} (Res_{MAP}) to ensure the validity of this access point. Finally, Cluster Head extracts a new key (K') for this new session according to previous session key preceding (K) and an authentication parameter named (Auth) which will be later transmitted to the client. At this stage, CH entity is conscious of STA and MAP_{new} legitimacies and it remains to prove its validity for these two last components. To fulfill this, CH sends an ID Response message (5), enciphered by the MAP_{new} public key and containing a new nonce value (N_{CH}), its response ($Resp_{CH}$) and the new session key (K').

After the reception of these parameters, MAP_{new} applies the received nonce value (NR_{CH}) with the preset algorithms to obtain a result ($Resp_{MAP}$). Then, it compares its obtained result with that sent by CH ($Resp_{CH}$). If they are identical, the re-authentication phase is continued. If not, we stop at this stage and we cancel all the procedure. Thereafter, MAP_{new} records the key (K') to make use of it essentially for the extraction of a temporary key between STA and its associated MAP. With an aim of informing STA by its new connection parameters and of proving its legitimacy, CH sends a message called Mobility Notification Message (MNM) (6). The MNM contains the value (Auth), which is used for the extraction of the new key (K'), a challenge value and a sequence number (SN) to avoid the risk of the replay attack. More additional information will be sent but in enciphered ways, which are the MAP_{new} identity (ID_{MAP}) and the response of the challenge application (Rsp_{CH}).

Following the arrival of this last message, the station calculates the new key (K') by using the parameter (Auth) and it applies a hash function, which is preset between CH and STA, to obtain the resulting value

(Rsp_{STA}). Finally, STA compares its result with that received from CH (Rsp_{CH}) to ensure the legitimacy of the concerned Cluster Head CH.

- **Inter-cluster Mobility**

In case of inter-cluster handoff, the client, which is in communication, changes its point of attachment and also its current cluster. The various intervening components in this type of mobility are:

- STA: the station carrying out the displacement towards MAP_{new},
- MAP_{new} : the new point of attachment,
- CH_{old} : cluster head of the STA home cluster,
- CH_{new} : cluster head of the new cluster containing MAP_{new}.

Our proposed re-authentication protocol is shown in Fig. 3 by the exchanged messages flow between the different components, quoted previously. The first four messages are identical to those indicated in the case of intra-cluster handoff. During this phase, we ensure the identities transmission of both STA and MAP_{new} towards CH_{new}. Then, this last entity checks the cluster membership of STA by testing the (ID_{CH}) parameter. If this identity is identical to the current CH identity, then we treat the case of intra-cluster handoff, detailed in previous subsection. If not (i.e. (ID_{CHold}) and (ID_{CHnew}) are different), CH_{old} seeks the CH having the given identity and then a Mobility Notification Message (5) will be send to the concerned entity. This message contains the (MIC_{CHnew}) (Message Integrity Code) parameter, ensuring the integrity of data coming from the CH_{new} node as well as other enciphered parameters using a key (Kch) divided between different CHs from the same Mesh network. (Kch) is generated periodically to minimize the risks of possible attacks.

The transmitted information are identity (ID_{STA}) enciphered by the session key (K), which is shared between CH_{old} and STA, a (challenge1) value making it possible to check the CH_{old} validity and a response ($Resp_{CHnew}$). Following the reception of these data, CHold checks the integrity of the message then the STA identity (ID_{STA}). If this value exists in its base, CHold continues this re-authentication procedure by calculating the value ($Resp_{CHold}$) which constitutes the result of the application of the challenge1 value with the preset algorithms between the whole of CHs existed in the same Mesh. Then, CHold compares the obtained result and the received one ($Resp_{CHnew}$). And if they are identical, the re-authentication procedure will be continued.

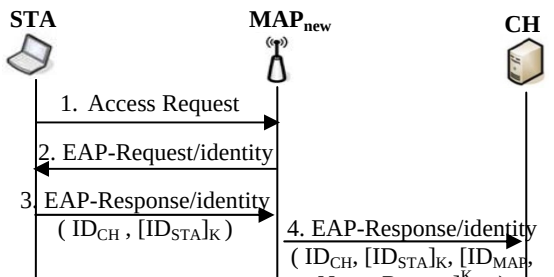
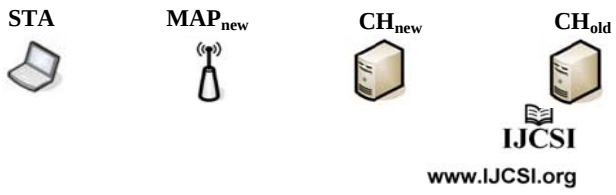


Fig. 2 Re-authentication procedure for intra-cluster handoff.

After the legitimacy checking of CHnew, CHold sends another value (challenge2) and its answer (Rep_{CHold}) in order to prove its validity. This information as well as the new session key (K') and the authentication parameter (Auth) are sent in an enciphered way using the key Kch. In addition, to ensure the message integrity, CHold transmits a code MIC_{CHold} (6).

The CHnew node checks, first of all, the code of integrity. Then, it calculates its answer (Rep_{CHnew}) and compares the obtained value with that received. If they are not identical, the re-authentication procedure will be cancelled because one of the components seems to be malevolent. If not, we check the validity of the access point by testing its identity and by comparing the obtained results for the nonce value.

The remainder of the re-authentication procedure is similar to that announced in the case intra-cluster (stages 5-6). In which, we carry out mutual authentication between MAPnew - CHnew, STA-CHnew and STA-MAPnew.



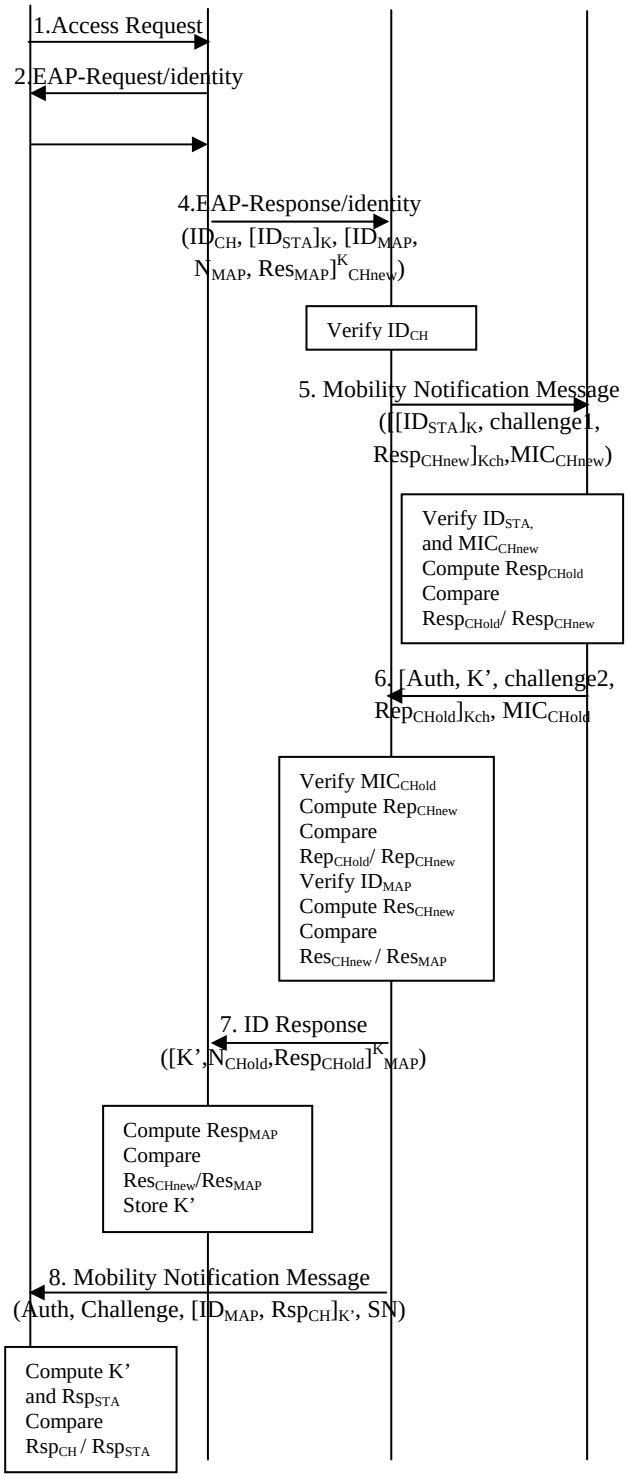


Fig. 3 Re-authentication procedure for inter-cluster handoff.

4. Performances Evaluation

This section is devoted to the evaluation of our protocol performances. First we have developed a network simulator to implement our architecture of Mesh network. 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 MAPs 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 MAP,
- Blocking rate: represents the number of blocked stations at handoff for the total number of stations that require the execution of handoff,
- Loss rate: represents the number of lost packets for the total number of the emitted packets.

4.1 Handoff Latency

In this part, we have tested the influence of the increase of network population on the value of the handoff latency, primary in intra-cluster mobility and then inter-cluster. The speed of the nodes is taken randomly between 0 and 20 m/s. Fig. 4 represents the result of this simulation. Initially, we notice an increase in handoff latency following the increase in mobile stations number throughout the simulation. This augmentation can be justified by the intensification of packets' number and thereafter the treatment time. Besides, we almost observe linearity on these two paces starting from the value 350 mobile stations and with 2,73 10^5µs of handoff latency for intra-cluster mobility and 2,84 10^5µs for inter-cluster.

By comparing the two curves, we note that the increase of handoff latency value in intra-cluster case is lighter than that with inter-cluster mobility. This difference is due to the additional time taken by any station which moves from a cluster to another. Thereafter the difference between the realization times of these procedures. Indeed, according to Fig. 2 and Fig. 3, we notice that inter-cluster mobility has more exchanged messages with more components. So, we need more time to execute the handoff and to ensure the mutual authentication between different entities (STA, MAP_{new}, CH_{new} and CH_{old}). This variance can reach the order of 0,13 10^5µs which enables to save a considerable treatment time and to support a better quality of service.

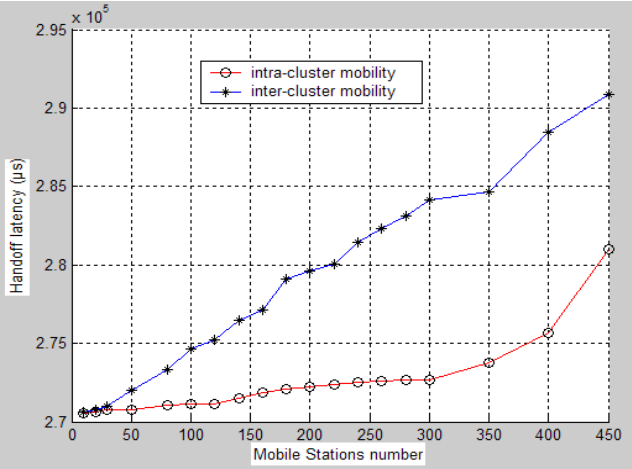


Fig. 4 Handoff latency vs. number of mobile stations.

4.2 Blocking Rate

A station is considered blocked when exceeding a handoff latency interval of threshold. Consequently, this rate depends mainly on handoff latency value. Fig. 5 represents the simulation's result of blocking rate according to the mobile stations number. For the first values of clients' number, the blocking rate remains null but with the increase in network population, the blocking values increases more and more. For inter-cluster mobility, starting from the value of 50 stations, the blocking rate surpasses zero. However in intra-cluster mobility, that is happen starting from 80 stations. This result is justified by the dependency between blocking rate and handoff latency value. Thereafter, this dependency and increase in rate value can degrade the network quality of services, in particular at the time of handoff. Moreover, the comparison between the two paces clarifies a little difference which can reach the value of 2%.

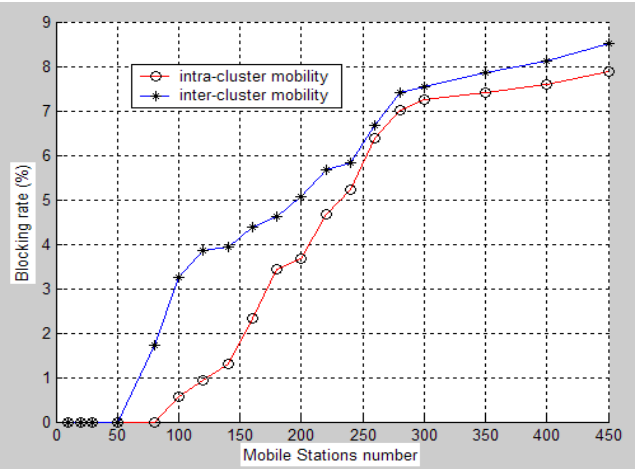


Fig. 5 Blocking rate vs. number of mobile stations.

4.3 Loss Rate

In order to control the feature of such network, we can establish multiple communications between stations and while referring to the quantity of lost packets, we can determine the nature and the quality of connection. Thus, a packet is supposed lost if it goes beyond a delay. Fig. 6 shows the result of the loss rate according to the mobile stations number. As in blocking rate case, the two curves start with zero values. That is due to the small quantity of mobile stations and thereafter the few packets number circulating in network. However, for inter-cluster handoff and starting from the value of 40 stations the packets begin to be lost and this loss becomes more and more bulky with population increase. On the other hand, for intra-cluster handoff, this growth starts from the value of 80 stations. This increase in both curves is due to the overloading in packets queues.

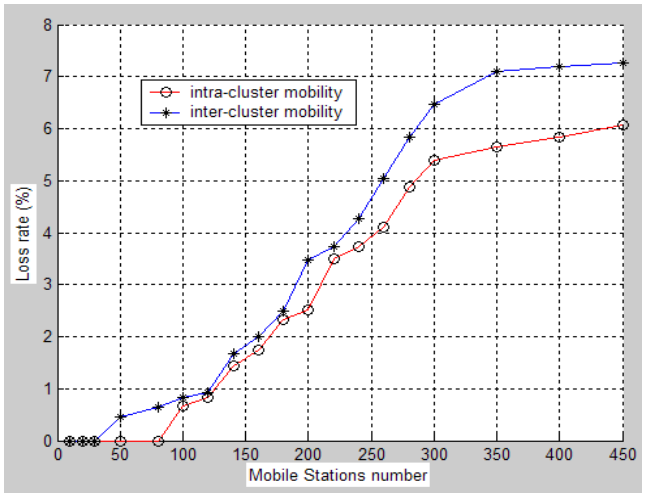


Fig. 6 Loss rate vs. number of mobile stations.

Moreover, as long as the loss rate value < 1%, we benefit from an acceptable quality of service. On the other hand, if this rate exceeds this value, the quality of service in this network is degraded more and more. By comparing the two paces, we note that the carrying out of intra-cluster handoff gives a light increase in loss rate compared to the second handoff type.

According to tests carried out on the two handoff types; intra-cluster and inter-cluster, while basing on the criteria of handoff latency, blocking and loss rate as well as the interpretation of the fulfilled curves in several scenarios, we can conclude that our protocol represents satisfactory and optimal value of handoff latency with minimum of

blocked station number during handoff and also few lost packets quantity in Mesh network.

Thereafter, we could highlight and justify the difference between intra-cluster and inter-cluster handoff results by the time held for each station in order to cross the coverage of a cluster towards another cluster. Indeed, the necessary time to carry out the re-authentication procedure becomes increasingly high because we must ensure the mutual authentication between the various intervening components during this phase. Thus, the proposed re-authentication and handoff notification protocol provides numerous advantages over the existing techniques. Major advantages are:

- this protocol treats two aspects in the same time ; mobility and security and also during different handoff cases; intra-cluster and inter-cluster which may ensure a protected, reliable and resistant network against the attacks as well as a more optimal and adequate quality of service to clients' requirements.
- The suggested solution can be adapted in various types of wireless networks and not only in the case of Mesh network.
- Hierarchical architecture based on a clustering algorithm, reduced the rate of exchanged messages during the handoff. That makes it possible to reduce the load of the authentication server if it exists.

5. Conclusion

To allow users to carry out an effective and reliable handoff as well as a secure access to WMN a method of re-authentication, with a reduced delay, should be executed during the cross of the mobile nodes by different MAPs and through various clusters. Indeed, a mobility mechanism cannot prove its effectiveness only if it is associated to a well defined and studied security mechanism. In this paper, we have proposed a new solution to solve this problem of insecurity during handoff by defining a new protocol for handoff identification and re-authentication. This solution has been studied for both types of mobility; inter-cluster and intra-cluster. Then, we could extract various results following the development of a network simulator on which we have tested our proposed protocol. According to the comparison between the results of several scenarios, we noted that both handoff types can provide a protected mechanism and an effective re-authentication scheme in term of the minimized value of handoff latency as well as the reduced blocking and loss rates. But, according to simulation results, we have noticed that intra-cluster handoff protocol give more satisfactory values than the inter-cluster because it required more signal transmission. In the future, we plan to expand our study by fulfilling some testbed with a real environment of Wireless Mesh Network. This will allow exploring the performance of our proposed re-authentication protocol for multiple scenarios. Finally, we hope to ameliorate the proposed solution to solve the problem of security while handoff, which is carried out inside a changeable architecture (i.e. with mobile MPs).

References

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

[2] Y. Amir, C. Danilov, M. Hilsdale, R. Mus_aloiu-Elefteri, and N. Rivera,“Fast Handoff for Seamless Wireless MeshNetworks” ,MobiSys'06, ACM 2006.

[3] D. Huang, Ph. Lin, Ch. Gan, and J. Jeng, “A Mobility Management Mechanism using Location Cache for Wireless Mesh Network”, QShine, ACM 2006.

[4] F. Rousseau, F. Theoleyre, A. Duda, A. Krendzel, M. Requena-Esteo and J. Mangues-Bafalluy, “Geo-mobility and Location Service in Spontaneous Wireless Mesh Networks”, Pro-MobileSummit 2008.

[5] R. Baumann, O. Bondareva, S. Heimlicher and M. May, “A Protocol for Macro Mobility and Multihoming Notification in Wireless Mesh Networks”, Advanced Information Networking and Applications Workshops (AINAW '07), 2007.

[6] R. Fantacci, L. Maccari, T. Pecorella, and F. Frosali, “A secure and performant token-based authentication for infrastructure and mesh 802.1X networks”, 4th ACM symposium on QoS and security for wireless and mobile networks (Q2SWinet '08), 2008.

[7] X. Lin, X. Ling, H. Zhu, P.Ho, and X. Shen, “A novel localised authentication scheme in IEEE 802.11 based Wireless Mesh Networks”, Int. J. Security and Networks, Vol. 3, No. 2, 2008.

[8] K. Khan and M. Akbar, “Authentication in Multi-Hop Wireless Mesh Networks”, Proceedings of world academy of science, engineering and technology volume 16 November 2006 ISSN 1307-6884.

[9] 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.

[10] 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.

[11] 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.

[12] R. Blom, “An optimal class of symmetric key generation systems”, EUROCRYPT, 1984.

[13] Draft IEEE802.11s 2.0 (March 2008).

[14] Andreas Roos, Sabine Wieland, Andreas Th. Schwarzbacher, Bangnan Xu, “Time behaviour and

network encumbrance due to authentication in wireless mesh access Networks", Vehicular Technology Conference (VTC), 2007.