Security in Wireless Mesh Networks

Faouzi Zarai[1], Ikbel Daly[1], Mohammad M. Banat[2] and Lotfi Kamoun[1]

[1]University of Sfax, Tunisia, [2]Jordan University of Science and Technology, Jordan

Abstract

Wireless mesh networks (WMN) have recently captured the interest of academic and industrial researcher communities; because they represent a good solution to providing wireless Internet connectivity in a sizable geographic area. However, the architecture and configuration of this type of network do not ensure protection against unauthorized use of the network. This is because the basic used security measures do not include the notion of mobility, which characterizes these networks. In this article, we first propose a secure re-authentication mechanism named **S**ecure **W**ireless **M**obility **M**anagement (SWMM). This mechanism is carried out while the mobile station (MS) crosses different nodes, to allow users fulfilling an effective and reliable handoff as well as a secure access to services offered by the WMN. Second, we propose a new scheme, called **S**elective and **D**eterministic **P**ipelined packet **M**arking for **M**esh Networks (SDPMM). This scheme is used for IP traffic source identification for tracing denial of service (DoS) attacks. The approach follows the IP traceback approach proposed in wired networks. Our study shows that SWMM outperforms other existing methods in terms of handoff latency, loss and blocking rate. It also shows that the traffic overhead introduced by the traceback scheme does not affect the network performance.

KEYWORDS

Wireless Mesh Network, IEEE 802.11s, Handoff, Security, Authentication, Re-Authentication, IP Traceability, DoS Attacks.

I. INTRODUCTION

Due to its contributions to eliminate the complexity of installation, configuration and maintenance of wireless network, to ensure a better quality of services and to provide compatibility with external and heterogeneous networks, Wireless Mesh network become a universal and topical issue and captured the interest of university research and industry [1], [2]. This new and promising paradigm allows for network deployment at a much lower cost than with classic WiFi networks.

WiFi made it possible to relax the wired constraints by giving wireless access to local area networks. The infatuation of this type of technology opened the way to the appearance of many services making it possible for anybody to connect from anywhere to the Internet or to the local network. This world of wireless saw the birth of new technologies like wireless ad-hoc networks and wireless mesh networks which enable great flexibility of deployment. Indeed, the topologies combining the mesh network and the ad-hoc connections carry in them the promise of a revolution based on the simplicity of implementation and the decentralization of architecture. In such a network, several access points (hot spots) are connected to their closer neighbors, without central hierarchy, thus forming a structure in the form of a mesh network. This structure forms a network known as the backbone, allowing communications between nodes attached to distinct access points.

WMNs are today in a mode of expansion, while the number of deployment projects reveals the promising future of this technology. However, WMNs can reach their full potential only when a standard is associated with them. For this reason, the IEEE has formed the 802.11 Task Group "s" (TGs) in 2004 to prepare an amendment of the 802.11 set of standards for WMNs. The standard, labeled 802.11s, defines a mesh network as two nodes or more which are connected by IEEE 802.11 links that communicate by mesh services and involve in a wireless distribution system [3].

Although there are significant advantages for the deployment of WMNs in the whole world, some technical limitations and problems remain to be solved. More advanced research is required to handle these issues and to enable successful deployment of WMNs. As representative open research areas, we cite the quality of service (QoS) issues [4], security [5], [6], mobility [7] and interference management [8].

In particular, the problem of security is a great concern in all types of wireless networks [6]. While networks continue to be developed, many efforts are concurrently ongoing to make sure that network access is granted to the authorized users only. Moreover, it should be emphasized that a network complexity usually grows with the increase in the number of applications, the nodes mobility and the degree of medium opening towards the outside. Consequently, attack prevention (through the process of authentication) and attack traceback constitute significant measures to confront attacks in mesh networks. For better

Manuscript received November 5, 2012
Manuscript revised November 20, 2012

security, an authentication procedure must be combined with a traceability mechanism, which makes it possible to follow the attacker signal and to know its origin. This can be helpful in making defense decisions.

However, the architecture and configuration of this type of network do not ensure protection against unauthorized use of the network. This is because the basic used security measures do not include the notion of mobility, which characterizes these networks.

In this article, we first propose a secure re-authentication mechanism named **S**ecure **W**ireless **M**obility **M**anagement (SWMM). This scheme is executed during the change of point of attachment for such a station in order to ensure a flexible and secure re-authentication procedure while handoff without degrading the quality of services offered by the WMN. Second, we propose a new scheme, called **S**elective and **D**eterministic **P**ipelined packet **M**arking for **M**esh Networks (SDPMM). This scheme is used for IP traffic source identification for tracing DoS attacks. The approach follows the IP traceback approach proposed in wired networks. These two solutions cooperate inside a Mesh network in order to better secure this environment. Indeed, the re-authentication procedure SWMM makes it possible to limit the access to the network only for the authorized users and thereafter playing a preventive role vis-a-vis the possible attacks. In association to this functionality, the addition of a defensive mechanism allows to ensure a better security with an aim of preventing the network against future attacks by knowing their sources with the SDPMM method. Our study shows that SWMM outperforms other existing methods in terms of handoff latency, loss and blocking rate. It also shows that the traffic overhead introduced by the traceback scheme does not affect the network performance.

The remainder of this article is organized as follows. In Section II, we present an overview of WMNs. In Section III, we focus on the security issue in this type of network. In Section IV, we describe the details of our proposed re-authentication mechanism (SWMM) and we evaluate its performance. The proposed IP traceback scheme (SDPMM) is presented in Section V. Finally, we conclude the article in Section VI.

II. WIRELESS MESH NETWORK

A WMN is an emerging network architecture characterizing the new generation of wireless technologies [2]. WMNs bring about several advantages and offer robust deployment mechanisms.

The WMN technology allows wireless equipment to be connected in a dynamic and instantaneous way, without central hierarchy, forming a net-shaped structure. Consequently, these nodes communicate directly with their neighbors by removing the wired interconnected network between access points. Moreover, Mesh's solutions authorize a fast and simplified deployment and a great extension of network coverage. Thus, they are able to be dynamically organized and configured. Besides, they take the principle of a wireless network based on multi-hop transmission. In fact, this type of network takes account of continuous connections and the reconfiguration around broken or blocked ways by "hopping" from a node to another until reaching the destination.

II.A. Architecture

A WMN is based on a grid arrangement of nodes (radio routers or inter-connected access points). A promising feature of this architecture is the ability to extend the mesh network by adding more nodes. That allows an operator to rapidly extend, at low cost, the geographic coverage of the network in order to offer access to various services available on a wired network or on the Internet.

The architecture of a WMN involves different components which ensure the execution of the network operations. Mainly this kind of architecture is made of a set of wireless mesh routers (WMRs) and mesh nodes (See Figure 1). The mesh routers establish a backbone structure and support connectivity between the various components of the network. In order to benefit from the connection to the Internet inside the mesh, some WMRs, which support mesh services such as control, management, and configuration of the network, play the roles of gateways. The mesh nodes can be clients (or stations) and relay routers at the same time, and so, they can be integrated in the traffic routing. This makes it possible to guarantee the multiplicity of the paths to reach any destination in the mesh network.

II.B. Characteristics

To meet its requirements, WMN technology contains several characteristics such as:

- ***Multi-hop operation***: WMN is a technology of rupture that aims to avoid having sensitive points, which in case of breakdown, cut the connection from part of the network. So, if a host is out of service, its neighbors will pass by another path.
- ***Capability of self-forming, self-healing, and self-organization***: WMN solutions authorize a fast and simplified deployment, a great extension of the coverage and, by their architecture, a strong fault-tolerance for interference and breakdowns. This tends to reduce costs of installation and exploitation of networks.
- ***Station Mobility:*** Clients, in WMN, are by definition mobile. Therefore, they expect to have a continuous connection to their network services. Processes, such as authentication and association, must be done transparently.
- ***Compatibility and interoperability with existing networks:*** Mesh networks offer the possibility to

coexist with existing networks which have other architectures and numerous characteristics that may be different from those of WMN. Indeed, the gateway WMR allows the establishment of connection between WMN and Internet.

- ***Unconstrained power-consumption:*** Mesh routers have a permanent source of power so they do not have strict constraints on power consumption. However, clients in WMN necessitate the installation of power efficient techniques.

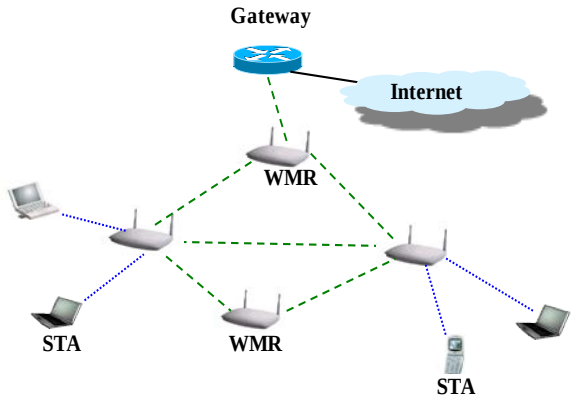

Figure 1: Wireless Mesh Network

III. WMN SECURITY

Inspite of the facilitation of communication and the various advantages brought about by mesh technology, it should be recognized that some new risks are introduced by the techniques of this technology.

Indeed, in a mesh infrastructure, mobile clients are likely to pass from a node to another. Therefore, the problem of the security becomes increasingly critical at times of handoff (i.e. clients may change their point of attachment while roaming in the mesh network). Moreover, this architecture presents a target environment for different kinds of attacks. A main challenge in mesh networks is the supply of security, which constitutes a principal element in wireless communications. This is due to the fact that the users are increasingly mobile; because of the massive deployment of wireless technologies that support user mobility. Newer generations of clients seek to communicate during their displacements without any constraints on connectivity. Throughout the mobile communication process, any change of the network is sought to be completely transparent. Such demands have increased the challenges faced by mesh networks. Additionally, as the medium remains open, the traffic can be easily listened to or even modified by unauthorized parties. In this context, security becomes an essential concern, and proposals for solutions to deal with security issues become a need.

Authentication is a significant measure to anticipate and fight against attacks in WMN. Authentication allows only authorized users to obtain connections to the network, and prevents adversaries from being integrated into the network and from disturbing its operation. This preventive solution can be intensified by the implementation of a defensive mechanism. An example defensive mechanism is the process of traceability in order to follow the attacker's signal and to discover the source of threat so that procedures can be set up to defend the networks against future attacks. In the remainder of this section, we detail some challenges faced by WMN as well as some possible attacks.

III.A. Challenges

In this subsection, we describe some challenges which have motivated researchers to study and ameliorate the mesh technology.

- ***Open and shared medium:*** The radio spectrum presents a common resource in wireless mesh networks, where each node is related via multihop links to other nodes. Thus, this open environment denotes the best target for attackers.
- ***Transparent operations:*** A WMN forms multihop broadcast segments. So, this type of network must transparently manage to use higher layers to provide an efficient support for broad and multicast traffic and even to select the best path.
- ***Security:*** Privacy related issues, integrity of authentication, authorization and accounting (AAA) services can be threatened. Indeed, each station can operate as a relay to send or receive packets for other stations in the WMN.
- ***Fairness:*** The mesh network must guarantee a WMR-fair share of the bandwidth between clients which have the same rights. Also, WMRs have to balance their loads among them to support the best services and grant the stability of connection.
- ***Determining Malicious Behavior:*** Detection of anomalous events presents the first and the fundamental phase to protect the network and to provide the best background of continuous connection and the quality of services.

III.B. Attacks

Attacks in WMNs are very diverse; some are inherited from previous wireless technologies and others appear as part of the new challenges of WMNs. These threats differ on the level of the techniques used, on the exploited faults and on the desired intentions [9]. DoS represents a major type of attacks due to its damaging consequences. DoS is the most harmful and dangerous attack; as it can be

launched from anywhere, on any layer of WMN. Furthermore, DoS is a type of attack aiming at rendering the network services and resources unavailable to authorized users during unspecified times. Generally, attackers try to illegally incorporate faults in the different protocols of the network.

III.B.1. Routing Protocol Attacks

The network layer of WMN can be prone to many types of attacks, especially DoS attacks; because of multi-hop environment, which may cause routing overheads on the level of WMR. Here are some of these threats [10]:

- ***Black-hole:*** impersonating a valid mesh node to attract packets by giving a low-cost path and to subsequently drop packets.
- ***Gray-hole:*** creating forged packets to attack and selectively drop the real ones.
- ***Worm-hole:*** replaying the control messages to disrupt routing.
- ***Route error injection:*** Injecting forged route error messages to break mesh links and disrupt the routing process.

III.B.2. MAC Protocol Attacks:

Due to the manipulation of an open and shared medium in WMN, the MAC channel may suffer from several kinds of attacks such as:

- ***Passive eavesdropping:*** Broadcasting a copy of data to overload the network.
- ***Link layer jamming attack:*** Transmitting regular MAC frame headers on the transmission channel. Consequently, the channel becomes busy and backs off for a random period of time. This leads to a denial of service for legitimate nodes.
- ***MAC spoofing attack:*** Modifying the MAC address in transmitted packets. It can be used to evade intrusion detection systems, masquerade as a legitimate user and even lead to denial of service by injecting a large number of packets which may cause network overload and service unavailability.
- ***Replay Attack:*** Known as man-in-the-middle attack. It can eavesdrop on the broadcast communication between two nodes.

III.B.3. Physical Protocol Attacks:

The physical layer can be affected by using radio jamming devices which may meddle in the physical channels and disturb the network availability:

- ***Radio Jamming Attack:*** Allowing a wireless device to broadcast a strong signal, causing heavy interference and preventing the routing of packets.
- ***Outdoor Deployment:*** WMRs may be installed in external areas where there is lack of control and administration.

III.C. Existing Security Solutions

Authentication represents the first solution for the majority of WMN security problems and particularly for DoS attacks. In [11] a concept and architecture for a location-aware digital rights management system is presented. This system uses signal strengths in a mobile ad-hoc or mesh network to determine the position of each node and to authenticate this location information. It enables devices to control access depending on their position.

In the same context, [11] proposes to analyze a wireless mesh network, which is capable to grow in an ad hoc way by using ad hoc routing capabilities. The technical challenges are related first to the authentication architecture, and second to the data confidentiality. More precisely, the extensible authentication protocol - transport layer security (EAP-TLS) over the protocol for carrying authentication for network access (PANA) is proposed and discussed in a multihop mesh network, and a security analysis is provided. In response to the different threats in WMN, a number of countermeasures have been developed. These include intrusion detection systems that aim to detect anomalous behavior caused by malicious events. Indeed, the study [12] presents a set of socio-technical challenges associated with developing an intrusion detection system for a community WMN. It motivates the need for and describes the challenges of adopting an asset-driven approach to managing the mesh network. In addition, [13] proposes a novel intrusion detection mechanism that identifies man-in-the-middle and worm hole attacks against wireless mesh networks by external adversaries. A simple modification to the wireless MAC protocol is proposed to expose the presence of an adversary conducting a frame-relaying attack.

A novel security architecture for wireless mesh networks, called MobiSEC, is proposed in [14]. MobiSEC represents a complete security architecture that provides both access controls for mesh users and routers, as well as security and data confidentiality of all communications that occur in the WMN. MobiSEC extends the IEEE 802.11i standard, exploiting the routing capabilities of Mesh routers. After connecting to the access network as generic wireless clients, new mesh routers authenticate to a central server and obtain a temporary key. This key is used both to prove their credentials to neighbor nodes, and to encrypt all the traffic transmitted on the wireless backbone links.

IV. PROPOSED AUTHENTICATION PROTOCOL

Due to the importance of security and mobility in wireless mesh networks, research goes on in these subjects with the objective of solving these problems. When the security

and mobility concepts coexist in a mesh network, the re-authentication procedure becomes one of the significant measures to confront attacks. Only authorized users are allowed to obtain connections to the network, while the adversaries are prevented from being integrated into the network and from disturbing its operations.

In this section, we begin by detailing some suggested solutions in the literature related to security and mobility issues. Based on previous research, we develop our proposed SWMM solution for resolving the problem of security during handoff among the mesh nodes.

IV.A. Security and Mobility Studies in the Literature

WMN brings several advantages such as the ease and the litheness of deployment. The prime objective of this type of network is to offer flexible connectivity to mobile users. Consequently, special care must be taken in handling mobility issues. We are mainly interested in user mobility during handoff. Due to the importance of this challenge, various solutions have been proposed in the literature in order to tackle the handoff problem. We quote examples of the seamless mesh (SMesh) in [15] and the mobility management mechanism (WMM) in [16]. In the SMesh approach, stations are connected automatically to the network by the standard dynamic host configuration protocol (DHCP). SMesh [15] proposes its own solution to the problem of handoff. This scheme can be considered to be effective; since it does not include the client in the handoff procedure, neither changes its device nor introduced additional software. On the other hand, the mobile nodes have a location precision of only 2 seconds. Moreover, a heavy signaling overhead produced by the diffusion of DHCP requests by each station at every 2 seconds. It was also created in case several WMRs had good connectivity with the same client, as the client packets of data are duplicated.

For the WMM method [16], the innovation is the use of the options field in the header of an IP packet to store the station location information in each WMR. However, when there is no handoff, these additional bytes are unnecessary. Thus, the proposed scheme requires heavy implementation and many procedures such as registration, location update, routing and querying. In specific, the last procedure involves the flooding of signaling messages into the WMN, which results in a signaling overhead to the system. Like other studies which treat only mobility, in WMM the medium remains open and the traffic can easily be listened to or even modified. In this context, security becomes a principal necessity in this type of network. In addition, the issue of insecurity becomes increasingly critical during handoff, demanding the incorporation of an effective policy and a well-defined security method. In the remainder of this section we discuss some existing solutions that have been suggested recently in this same context.

The work in [17] is based on the use of a token of authentication which is dynamically produced during handoff by the moving station. In this solution, the token structure and its method of generation are not defined. Note that this involves both the station and the authentication server (AS) at the same time (synchronization is required between stations and the server). Furthermore, with every handoff, AS intervenes in the re-authentication phase between a given client and its new WMR, overloading the server, increasing the handoff latency and degrading the quality of the network. For this solution, there is also a risk of token duplication or the regeneration of an existing token by another station.

In [18], the authors introduce a two-factor localized authentication model for an inter-domain handoff (i.e. the client moves between WMRs of the same Mesh). This solution proves its effectiveness in several cases of attacks and lack of security. However, the proposed model uses a removable support to store confidential information which amplifies the risk of attack, theft and even the loss of this detachable device. This scheme uses a central entity which carries out numerous tasks, so the architecture becomes centralized, and that may multiply the threats and disturb the correct functioning of network. This model uses several parameters which require a large memory capacity to store this information in different entities.

The study [19] presents 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 of EAP- tunneled transport layer security (TTLS) over PANA. The EAP-TTLS extends EAP-TLS to exchange additional information between the client and the server by using secure tunnel established by TLS negotiation. PANA is an IP-based protocol which allows dynamic service provider selection, supports various authentication methods, is suitable for roaming users, and is independent of the link layer mechanisms. For these reasons, EAP is used over PANA to carry the EAP payload. The aim of PANA is providing a mechanism of agnostic transport to the link layer in order to carry the authentication information of the network based on EAP. Within the PANA concept, four principal components can be identified:

- ***PANA client (PaC):*** Represents the final system which seeks to reach a certain network.
- ***PANA Authentication Agent (PAA):*** Belongs to the network itself, and is responsible for PaC authentication, like deciding to accept its access to network.
- ***Enforcement Point (EP):*** Controls access to the network by authorizing or not authorizing those packets sent by PaCs toward the network.

In theory, PAA and EP are two different logical entities, although they can actually be integrated in the same physical device.
Benefits brought by the approach in [19] include providing a level of security for stations similar to that proven by EAP-TLS with very simple implementation, and the flexibility of employing any authentication protocol. However, some anomalies remain 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; because data are sent in the clear. Second, this study did not take into account the mobility notion and handoff in WMN. Finally, this approach presents a long procedure of authentication that may result in a heavy signaling overhead.

IV.B. Secure Wireless Mobility Management (SWMM)

In this subsection, we describe the principles of our proposed SWMM solution, applied to WMN. We start by defining the environment of our study which specifies the adopted network architecture. Following this, we integrate the notion of mobility into this architecture in order to be able to extract a solution to provide secure WMN access during handoff.

IV.B.1. Network Architecture

In this work, we will slightly modify the terminology specified in the draft D2.0 of IEEE 802.11s [20] where mesh access points (or WMRs) must be stationary. Following [21], we choose the hierarchical architecture as being the most adapted approach for mobility as well as security. Indeed, the authors present a comparative study based on the authentication behavior for mobile nodes in WMN between centralized, hierarchical and distributed architecture.
Figure 2 illustrates a general SWMM architecture. In our hierarchical architecture, the network is divided into groups called clusters. For each cluster, we select a unique WMR to play the role of a cluster head (CH). Thus, every CH will contain the base of all WMRs which belong to its own cluster, the base of their mobile stations as well as the bases of the other CHs. This network decomposition is used to facilitate the study of network mobility. With the purpose of integrating the notion of security into this architecture, we will add nearby every CH a new entity called server TTLS, which will be detailed later in this subsection. In order to establish this type of hierarchical architecture, we must have an algorithm for the selection of clusters and their heads [22], [23].

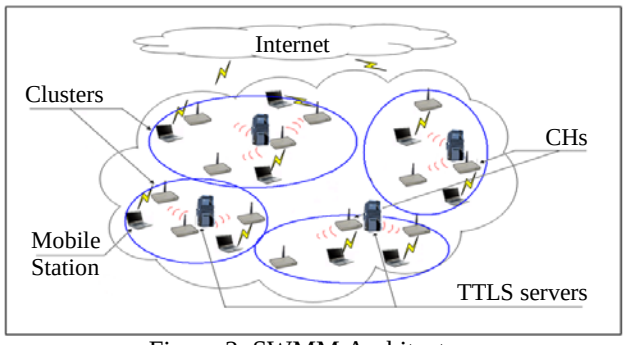

Figure 2: SWMM Architecture

IV.B.2. Improvement of WMM

This study requires the presence of a mobility management protocol. We adopt the WMM mechanism, with some enhancements to optimize various parameters, and with the addition of other variables to prepare this scheme for next phase of re-authentication. WMM is characterized by the adjunction of a set of parameters in the options field of the header of an IP packet. These parameters include the IP addresses of the sender serving mesh access point (SMAP) and the receiver SMAP. To transmit this information, we reserve four bytes for each address. These last entities belong to the same WMN as their clients. The addresses of the sender and the receiver in the IP packet are known. Therefore, the addresses of the two concerned SMAPs have the same prefix as their associated stations. Consequently, we can get rid of these repetitive data and thereafter minimize the number of transmitted bytes. This reduction becomes more important with the high rate of packets circulating at every moment inside a network made up of multiple mesh nodes. Moreover, the proxy table, which is a required element in each mesh node in WMM, maintains the station (STA) location information. This table involves three columns:

- *Im* : STA's IP address,
- *Is* : IP address of STA's SMAP
- *Ts:* The time of STA-SMAP association.

A second modification in WMM is carried out in the proxy table. The idea is to add a fourth column to contain the STA identity. To be identified within the mesh network, we assign to each station a unique identity different from its MAC address to avoid the anonymity problem which allows following the client traces by attackers. This parameter is obtained at the time of establishment of a successful connection of a new client with the WMN. Then, it is revoked at the time of disconnection of the station, to obtain a new identity with the next connection. This procedure provides a more protected and secure network against various attacks.
The above procedure performs a flexible and quick checking of station legitimacy during the re-authentication process. Thus, the assigned identity gives an anonymous

status to a client along with its location against attackers. Besides, this identity does not require a lot of memory space in order to be registered either in CH bases or in the list of revoked identities.
Concerning cancelled identities, they will be added, by the STA's SMAP, to the revocation list. Thereafter, this list will be updated for other WMRs so that these identities cannot be reused or assigned to another station. Table 1 illustrates the new structure of the proxy table with the additional column called the Id field.

Im	***Is***	***Ts***	***Id***
STA IP address	IP address of STA's SMAP	The time of STA-SMAP association	STA's identity

Table 1: New structure of proxy table

IV.B.3. Integration of EAP-TTLS in WMM

Handoff represents the most suitable moment that can be exploited by attackers to be illegitimately incorporated into the network. In order to secure access to the mesh network at handoff time, the station identity must be verified. To carry out this step, we have integrated a re-authentication procedure into the registration procedure of WMM mechanism, following the reception of the STA's registration request. The objective of this procedure is to register a client with its new SMAP after its migration towards another coverage zone. In our case, we have selected the EAP-TTLS mechanism because it provides flexibility in using any of the authentication protocols, like the password authentication protocol (PAP), challenge handshake authentication protocol (CHAP), or message digest 5 (MD5) etc. The architectural model, shown in Figure 2, points out the choice of CHAP as the selected authentication protocol; because it uses a three-way-authentication technique and offers more security. To ensure more secure and reliable re-authentication in the WMN, EAP-TTLS is used over PANA. This is because the latter protocol suggests embedded mechanisms to counter security threats like passive eavesdropping, message relaying, message distortion, man in the middle, active impersonation, DoS attacks and so on. Afterwards, and to make the EAP-TTLS mechanism functional under our network architecture, we have added, in front of every WMR selected as CH, a server TTLS. This server looks like an intermediate point between the new WMR, with which the mobile station wants to be associated, and the head of the visited cluster. Additionally, it is responsible for the establishment of the secure tunnel.
In addition to the identity allotted to each station since its connection to network, supplementary information will be added on the level of every client, which is the MAC address of the CH with which a given station is associated. This supplement aims to facilitate the study of the station's mobility and its identification during handoff.

IV.B.4. Improvement of EAP-TTLS

The first phase of establishing the secure tunnel used in the EAP-TTLS mechanism is preserved by replacing the authentication server by the cluster head selected with a clustering algorithm. After founding the secure channel, we proceed to accomplish the re-authentication phase. This procedure is applicable with two types of station movement:

- ***Intra-cluster***: the old WMR and the new WMR belong to the same cluster.
- ***Inter-cluster***: the old WMR and the new WMR belong to two different clusters.

Figure 3 illustrates the various stages of the re-authentication phase. This architectural model is comprised of PaC, PAA/EP/AP, TTLS server, CH of new SMAP, noted CH_{new} and the other CHs of the WMN. These entities have been described in subsection IV.A above. PaC adds its identity (ID) and the MAC address of its current CH (CH_{old}) to the PANA authorization answer message, sent towards the TTLS server, and then to the CH of new SMAP (CH_{new}). After the reception of the PaC's credentials, CH_{new} examines the MAC address of CH_{old}. If it is identical to its one, CH_{new} checks the STA identity in its base. If not, it verifies this identity in the base of the specified head (CH_{old}) since CH_{new} has a copy of all bases of other CHs. Then, if STA exists with the same received identity, CH_{new} accepts this access by sending a head-access-accept message which is passed on to the new SMAP as an EAP-success message by the TTLS server. Then, this last message reaches PaC as a PANA-bind-request, which includes EAP-Success, device-Id, protection capability and message authentication code. This code is used to protect the EAP success or failure messages transmitted by PAA to PaC at the end of the authentication process and to prevent attackers from launching DoS attacks.
At the same time, CH_{new} updates its bases, and afterwards a message is sent to other CHs, containing the STA identity, the new SMAP IP address and the MAC address of CH_{new} to refresh their bases.
Furthermore, having received the PANA message, PaC forwards his response called PANA-bind-answer, including device-Id, protection capability and message authentication code to its new SMAP. At this stage, the station is well authenticated and we have guaranteed its access to the network. With an aim to exchange data with its SMAP in full security, we must ensure a secure data tunnel between these two equipments. To realize this purpose, the creation of a session key is carried out in the level of station and its SMAP in order to encipher the transmitted data.
In case we have an inter-cluster movement, the TTLS server informs STA the new MAC address of CH_{new}. If it is not the case (i.e. intra-cluster movement), it is useless to

send this unchangeable data.
Moreover, the update of CH bases is carried out through the options fields of the IP packets by applying the location update procedure of the WMM mechanism. Finally, we mention that we do not need to refer to mesh backhaul node, which serves as the gateway between WMN and Internet, to obtain SMAP IP address, like in WMM mechanism, since each CH has a copy of all other bases so the query procedure is replaced by a simple request of the base to know the location information of such SMAP.

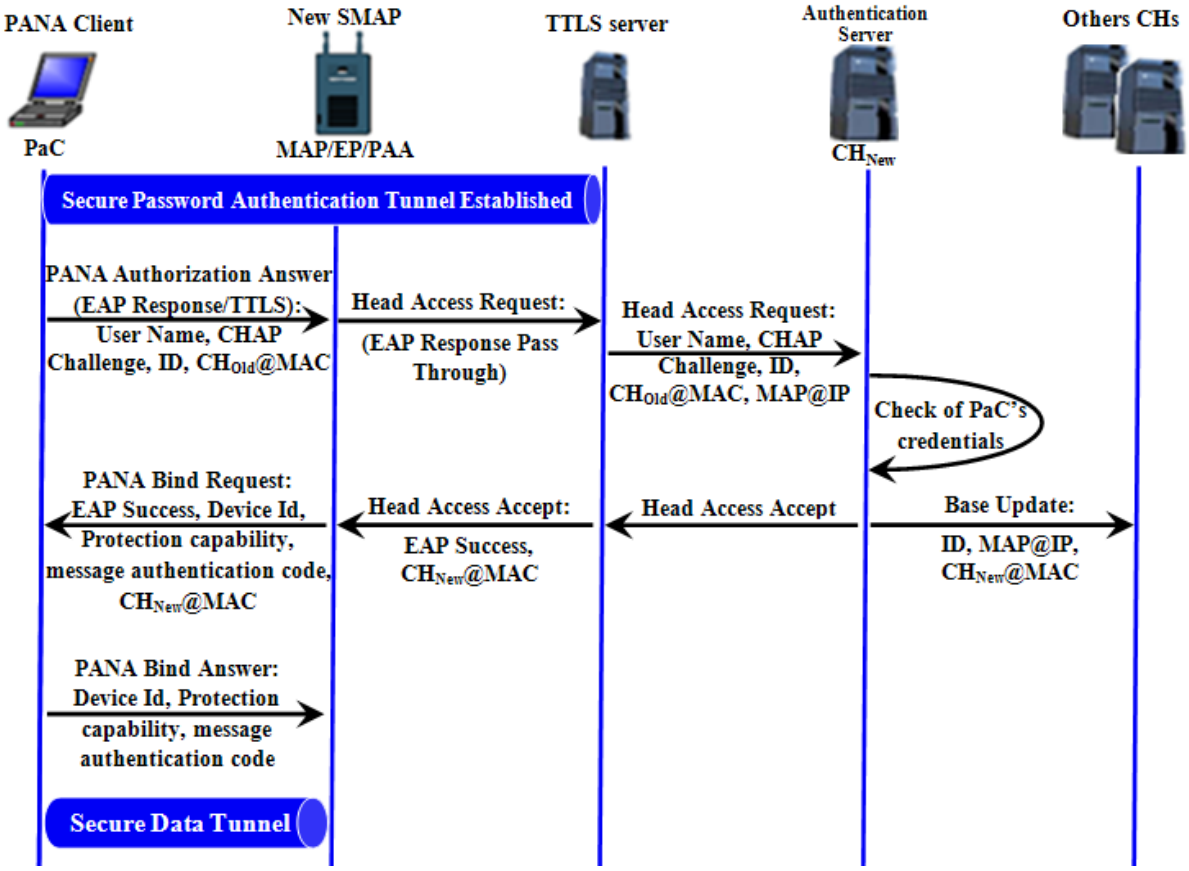

Figure 3: EAP-TTLS over SWMM

V. IP TRACEBACK FOR WIRELESS MESH NETWORKS

Denial of services and Distributed Denial of Services (DDoS) attacks represent potential security threats that face both wired and wireless networks. The success of these attacks is based on the fact that the real identity of the intruders performing the attacks can be hidden. The intruders may spoof IP addresses and use zombies and reflectors to amplify their attacks. To overcome the aforementioned problem, several traceback approaches were proposed to identify the route of the incoming traffic and trace intruders from their source. These techniques can be classified into link testing, deterministic, probabilistic, or selective packet marking [24], logging of packets information or packets digests, and internet control message protocol (ICMP) messaging.

While these approaches have met success in wired networks, their applicability to wireless networks did not show efficiency. This is particularly true for wireless mesh networks, where the problem becomes challenging. For this reason, several issues have to be considered including: the infrastructure variability (every node can act as a host and as a router), topology changing due to node mobility, bandwidth and computational resource limitations, dynamic aspect of routing protocols, and mobility of nodes (intruders, targets, or even intermediate routers).
To the best of our knowledge, very few works have dealt with traceback in wireless mesh networks. Interest in IP traceback in wireless ad-hoc networks started with the work in [25].The authors have focused on studying the applicability of existing traceback techniques using proactive and reactive routing protocols, showing a high dependency on network scale, routing protocols, and used traceback mechanisms. In [26], the authors have proposed

using cumulative IP information to verify the true IP packet origin. The work in [27] introduced an enhancement scheme to ICMP traceback with cumulative path (ITrace-CP) [26] by performing dynamic probability adjustment against hop distance. In other words, [27] has improved the Itrace-CP technique in [26] through probability adjustment and simulated it in both wired and wireless networks. While the technique has brought a remarkable enhancement regarding its feasibility in wireless ad-hoc networks, it is far from being considered suitable and efficient for Wireless Mesh Networks.

The techniques in [28] have used small worlds in mobile ad-hoc networks (MANETs), basing the traceback scheme on traffic patterns and volume matching. Despite its significant results, the proposed scheme is not suitable for a precise tracking of the mobility of intermediate nodes and attack path variation.

We propose in this article a novel traceback technique for wireless mesh networks, called "selective and deterministic pipelined packet marking for mesh networks" (SDPMM). The technique is based on the propagation of the set of IP addresses representing the wireless mesh routers through which attacks are flowing to the target. Moreover, it takes into consideration nodes mobility, IP source handoff, and IP routes updates.

Our contribution is 3-fold. First, the use of computational resources in mesh nodes is reduced through exploitation of the probabilistic pipelined packet marking (PPPM) technique [29]. Second, it makes an efficient source traceback feasible even in the presence of different mobility scenarios because of the determinism of marking. Third, the technique helps considerably network forensic investigation; as it considers tracing the history of the sender access network and the set of routes taken by its traffic.

V.A. Selective and Deterministic Pipelined Packet Marking for Mesh network (SDPMM)

In this subsection, we describe the IP traceback scheme SDPMM. This scheme handles mobility issues such as handoff layer 3 and splitting and merging. It is conceived to identify the WMR from which the attack has originated (path information). As mentioned earlier, having knowledge about entire path of attack packets can be helpful in taking defense decisions. It is also more useful than only locating the attacker because the attacker's network can be cooperative.

In WMNs, the key requirements for IP traceback methods include: the compatibility with existing network protocols, the minimum overhead in terms of time and computational resources, the effectiveness against DDoS attacks, the robustness to handle mobility and the scalability in large mesh networks. The proposed scheme is designed with the following three assumptions:

- The IP header can be modified to have packet marking option with a specified size.
- The wireless mesh routers are trusted.
- The attacker can be aware of the use of the traceback mechanism.

V.A.1. SDPMM properties

Our scheme is inspired by PPPM technique. The aim is to make the wireless mesh routers propagate their IP addresses by marking some packets of the same TCP session. The main properties of the SDPMM scheme are as follows:

- ***SDPMM is selective***: Only selected packets are marked by the marking process (i.e., first or binding update packets).
- ***SDPMM is deterministic***: Each intermediate wireless mesh router decides to mark a packet only if it receives information from one WMR, or if its buffer is not empty. The destination needs only ***n*** packets to identify the attack packets to block all subsequent packets arriving on a path containing ***n*** intermediate WMRs built between source and destination.
- ***SDPMM is efficient***: When an intermediate WMR moves out of transmission range, the WMR preceding immediately the departing WMR (in the actual path) is responsible for triggering the marking process.

V.A.2. SDPMM Marking Scheme

In this subsection, we provide a detailed description of SDPMM, including the marking information (MI), the buffer structure, and the marking scheme.

Marking Information: The following information is inserted in the first packet to launch the marking process:

- ***Flag:*** A one bit field, which is set to 1 when the WMR that accommodates the sender applies the marking process upon establishment of a new route. It is set to 0 when the marking process is established by an intermediate WMR further to the route maintenance.
- ***Packet ID:*** A ***k*** -bit field that is chosen randomly by a WMR each time an attacker initiates a new connection or moves from a LAN to another. The following wireless mesh routers use the same ID when they see subsequent packets going to the same destination from the same source.

- ***WMR@IP***: This designates the IP address of the WMR that marks the packet.

Buffer structure: The marking information found in certain packet is buffered at the receiving WMR before re-marking it. The buffered information contains: the destination IP address Destination@IP, the WMR IP address WMR@IP and the packet identification packet ID.

SDPMM Scheme: SDPMM is based on IP packet marking. When a given source starts a connection with a destination and after the selection of a route path, the wireless mesh router, say WMR1, related to the local access network to which the source belongs, applies the marking process only when it receives the first data packet from the mobile node. It inserts in that packet the MI and sets field flag to 1. Any subsequent WMR that receives a marked packet, checks whether its buffer is empty. If the case is true, it saves the packet's MI in its buffer, and inserts its own MI. If the case is false, it saves the packet's MI and inserts the entry located in the tail of its buffer.

V.B. Handling Mobility Effects

This subsection addresses the mobility issues of the IP traceback mesh. The main problems that are introduced by this network are the IP handoff and the splitting and merging. To take into consideration the mesh characteristics, the source path identification must be done with the constraint that it should minimize the time that WMRs spend on tracking. It should also minimize the storage used to keep the tracking information.

IP Handoff: The wireless mesh network is divided into different local access networks (LANs), each with a unique subnet address. When a mobile node moves from one LAN to another, it changes its IP address to be in the new subnet address [30], and a route discovery procedure will take place. Thus, the marking scheme will be reestablished once again. The receiver can distinguish the IP handoff case upon reception of an IP binding update packet.

Splitting and Merging: Intermediate WMRs participating in routing the IP traffic from the intruder to a receiver, may move outside the transmission range of other nodes. Consequently, the network becomes partitioned and two possible cases can be followed in order to update IP route. In the first case, the IP route is discovered once again. It may not only be partially modified (specifically in the portion relating to the node that moved out of the transmission range), but it may also change substantially. This is due to the fact that intermediate WMRs are always on the move leading the old IP route to be no longer the optimal one. The marking procedure is reestablished from the outset by the first WMR, which was informed about the link failure. In the second case, an IP route maintenance is triggered.

The WMR that immediately precedes the intermediate one that went out of transmission range will run the IP route maintenance procedure. After that, it executes the marking procedure and set flag field to 0, while keeping the same packet id field value. The value 0 is useful to let the receiver know that the new marks have to update the old path due to the mobility of intermediate WMRs.

V.C. End-User Traceback

At the end-user side, incoming marks are stored in two different tables; so that they help network forensic investigators trace intruders to their source WMR, and track the mobility of any node that participates in routing IP packets from the intruder to the target. The first table, called up-to-date traceback table maintains for every established connection two fields: the connection id and the current path followed by incoming packets. Note that the current path is built progressively due to pipelining concept by appending the intermediate WMR IP address every time a new MI is received.

Whenever a new MI is received with a flag equal to 0 (an intermediate node has moved), or received immediately after a binding update message (the sender has changed its IP address while keeping its connection), the receiver updates the last attack path of the current connection and moves the old one to the historical mobility table (the second table). If the new marking information is received with a flag equal to 1 without a preceding binding update message, the receiver notices that marking information deals with a new connection. For that reason, it increments the connection id and saves the last attack path in the traceback table.

The second table, called historical mobility table, maintains for every connection up to $\boldsymbol{n}$ previous attack paths that have been followed by the same intruder. Given a connection $\boldsymbol{x}$, every time a new marking process is triggered, the end-user transfers the last traced attack path from the traceback table to the historical mobility table. In order to endow investigators with mobility information, every traced attack path, which is moved to the historical mobility table, is identified by a pair of values $\langle \boldsymbol{t_i}, \boldsymbol{act_i} \rangle$, where $\boldsymbol{t_i}$ is a discrete event time, and $\boldsymbol{act_i}$ is a mobility event (e.g., IP handoff, intermediate node moving).

Illustrative example: We consider the example depicted by Table 2, where a mobile sender S starts communicating with a receiver R. In the beginning, S belongs to LAN 1 and R to LAN 4. Upon the establishment of the routing path, the WMR of LAN 1, WMR_1, sees the first IP packet, say P_1, coming from S. It marks it by inserting MI $\langle \boldsymbol{wmr}_1, 1, \boldsymbol{id}_x \rangle$, where $\boldsymbol{wmr}_1$ represents the IP address of WMR_1, 1 denotes that the marking process was

established by the WMR that accommodate S just after an establishment of a new route and $\boldsymbol{id_x}$ is the randomly chosen identity by WMR_1. Furthermore, when WMR_1 sees new data IP packets coming from the same source, it simply forwards it to the next mobile node. When it receives P1, WMR_2 stores the received MI in its buffer and modifies the MI in P1 by replacing wmr_1 by wmr_2. WMR_3 and WMR_4 proceed the same way as WMR_2 when they receive P1. When WMR_2 receives P2, which was not marked by WMR_1, it retrieves the MI from its buffer, inserts it in P2, and forwards it to WMR_3. When WMR_3 receives P2, it sees that its buffer contains the marking information. Thus, it inserts this marking information in P2 and saves the one that was inserted by WMR_2 in its buffer. The marking process stops after the transmission of the forth packet, because 4 is the number of intermediate WMRs.

The example assumes that, after some period of time, WMR_3 goes out of transmission range and WMR_2 establishes a route maintenance procedure to continue sending IP packets. Immediately after updating the next hop address, WMR_2 triggers the marking procedure by inserting marking information $\langle \boldsymbol{wmr_2}, 0, \boldsymbol{id_x} \rangle$ in the first received packet from source S to receiver R. In this case, the flag field is set to 0 to let the receiver know that an intermediate node has gone out of range.

Event 1: Route is established: S communicates with R using route: $WMR_1 \rightarrow WMR_2 \rightarrow WMR_3 \rightarrow WMR_4$						
S		P_1	P_2	P_3	P_4	…
WMR_1	MI	$\langle \boldsymbol{wmr_1}, 1, \boldsymbol{id_x} \rangle$	-	-	-	-
	Buffer	-	-	-	-	-
WMR_2	MI	$\langle \boldsymbol{wmr_2}, 1, \boldsymbol{id_x} \rangle$	$\langle \boldsymbol{wmr_1}, 1, \boldsymbol{id_x} \rangle$	-	-	-
	Buffer	$\langle \boldsymbol{wmr_1}, 1, \boldsymbol{id_x} \rangle$	-	-	-	-
WMR_3	MI	$\langle \boldsymbol{wmr_3}, 1, \boldsymbol{id_x} \rangle$	$\langle \boldsymbol{wmr_2}, 1, \boldsymbol{id_x} \rangle$	$\langle \boldsymbol{wmr_1}, 1, \boldsymbol{id_x} \rangle$	-	-
	Buffer	$\langle \boldsymbol{wmr_2}, 1, \boldsymbol{id_x} \rangle$	$\langle \boldsymbol{wmr_1}, 1, \boldsymbol{id_x} \rangle$	-	-	-
WMR_4	MI	$\langle \boldsymbol{wmr_4}, 1, \boldsymbol{id_x} \rangle$	$\langle \boldsymbol{wmr_3}, 1, \boldsymbol{id_x} \rangle$	$\langle \boldsymbol{wmr_2}, 1, \boldsymbol{id_x} \rangle$	$\langle \boldsymbol{wmr_1}, 1, \boldsymbol{id_x} \rangle$	-
	Buffer	$\langle \boldsymbol{wmr_3}, 1, \boldsymbol{id_x} \rangle$	$\langle \boldsymbol{wmr_2}, 1, \boldsymbol{id_x} \rangle$	$\langle \boldsymbol{wmr_1}, 1, \boldsymbol{id_x} \rangle$	-	-
R		$\langle \boldsymbol{wmr_4}, 1, \boldsymbol{id_x} \rangle$	$\langle \boldsymbol{wmr_3}, 1, \boldsymbol{id_x} \rangle$	$\langle \boldsymbol{wmr_2}, 1, \boldsymbol{id_x} \rangle$	$\langle \boldsymbol{wmr_1}, 1, \boldsymbol{id_x} \rangle$	-
Event 2: Route maintenance established by WMR_2: S communicates with R using route: $WMR_1 \rightarrow WMR_2 \rightarrow WMR_5 \rightarrow WMR_4$						
S		P_x	P_{x+1}	P_{x+2}	...	
WMR_1	MI	-	-	-	-	
	Buffer	-	-	-	-	
WMR_2	MI	$\langle \boldsymbol{wmr_2}, 0, \boldsymbol{id_x} \rangle$	-	-	-	
	Buffer	-	-	-		
WMR_5	MI	$\langle \boldsymbol{wmr_5}, 0, \boldsymbol{id_x} \rangle$	$\langle \boldsymbol{wmr_2}, 0, \boldsymbol{id_x} \rangle$	-	-	
	Buffer	$\langle \boldsymbol{wmr_2}, 0, \boldsymbol{id_x} \rangle$	-	-	-	
WMR_4	MI	$\langle \boldsymbol{wmr_4}, 0, \boldsymbol{id_x} \rangle$	$\langle \boldsymbol{wmr_5}, 0, \boldsymbol{id_x} \rangle$	$\langle \boldsymbol{wmr_2}, 0, \boldsymbol{id_x} \rangle$	-	
	Buffer	$\langle \boldsymbol{wmr_5}, 0, \boldsymbol{id_x} \rangle$	$\langle \boldsymbol{wmr_2}, 0, \boldsymbol{id_x} \rangle$	-	-	
R		$\langle \boldsymbol{wmr_4}, 0, \boldsymbol{id_x} \rangle$	$\langle \boldsymbol{wmr_5}, 0, \boldsymbol{id_x} \rangle$	$\langle \boldsymbol{wmr_2}, 0, \boldsymbol{id_x} \rangle$	-	

Table 2: Traceback Example

Receiver R can easily:

- Know to which LAN S belongs.
- Reconstruct the path from which the IP packets are arriving.
- Track any mobility event (in this example, the link failure between WMR2 and WMR4).

The first task is achieved on the reception of the last marked packet from the source. The second task is performed in a backward manner: WMR_4 is first received,

then WMR_3, and so on. The last task is performed upon reception of the marking information whose flag is set to 0. When the receiver collects the subsequent MI, it notices that WMR_3 was replaced by WMR_5 and IP traffic goes now from WMR_2 to WMR_4 via WMR_5.

VI. PERFORMANCES EVALUATION

This section is devoted to the evaluation of SWMM and SDPMM performances. First, we have developed a network simulator to implement our architecture of the mesh network. This simulator specifies various parameters of this type of network and simulates 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 performance of our solutions, we consider two types of traffic: voice and web communication.
While referring to these types of communications, as well as to the parameters of the simulation, we evaluate the simulation results according the following criteria:

- ***Handoff Latency***: Represents the elapsed time between the change of point of attachment request and the association with the new WMR,
- ***Blocking Rate***: Represents the ratio of the number of blocked stations at handoff to the total number of blocked stations,
- ***Loss Rate***: Represents the ratio of the number of lost packets to the total number of the emitted packets,
- ***Overhead***: amount of signaling information transmitted for a given amount of application data.

VI.A. Performances Evaluation of SWMM

VI.A.1. Handoff Latency vs. Number of Mobile Stations

In this part, we have tested the influence of the increase of network population on the value of the handoff latency, primarily on our SWMM solution, and then on another solution suggested in literature. In our study we have selected the EAP Independent Handover Authentication method (EAP-IHA) [31]. This choice enables to highlight the utility of the secure tunnel establishment during the re-authentication procedure. The EAP messages are triggered by the EAP Start, then some additional parameters are included like identification (ID), and the messages of the result (SUCCESS/FAILURE) exchanged between the mobile node and the server. The result message also comprises information about the new derived key and is propagated back to mobile node through the authenticator and the Point of attachment (PoA). A last message is exchanged between the old and the new authenticator in order to transfer the keys that the old authenticator obtained in the preceding authentication. In our study, the new authenticator and EAP server are replaced respectively by TTLS server and Cluster Head. Also, it is not resort to old authenticator because the Cluster Head contains all bases. In addition, we notice the absence of the secure tunnel granted in EAP-TTLS method. Consequently, in EAP-IHA, all confidential information needs to be ciphered from EAP ID Rsp message to Password ACK.
The speed of the nodes is assumed to take random values between 0 and 20 m/s. Figure 4 represents the result of this simulation. Initially, we notice an increase in handoff latency following the increase in the number of mobile stations throughout the simulation. This augmentation can be justified by the intensification of the number of packets, and thereafter the treatment time. Besides, we observe almost linear curves in these both paces starting from the value 2.8×10^5 µs of handoff latency.

Figure 4: Handoff latency vs. number of mobile stations

By comparing the two curves, we note that the increase in handoff latency with SWMM is smaller than that with the EAP-IHA method. This difference is due to the variation between the re-authentication methods used by the two solutions, and thereafter the difference between the realization times of these procedures. Indeed, for EAP-IHA the encryption of messages starts with the beginning of the re-authentication method by sending the confidential information. On the other hand, for SWMM the encryption starts after the establishment of the secure channel. This variance can reach the order of 0.3×10^5 µs , which enables saving a considerable time of treatment and to supporting a better quality of services. In contrast, EAP-IHA requires more handoff processing time, which carries out to weigh down mesh services and decrease the capacities offered by network.

VI.A.2. Blocking Rate vs. Number of Mobile Stations

A station is considered blocked when a threshold handoff latency interval is exceeded. Consequently, the blocking rate depends mainly on the handoff latency value. Figure 5 represents the simulation results showing the blocking rate versus the number of mobile stations. For small numbers

of mobile stations, the blocking rate remains null because we have only some transmitted packets between clients. Therefore, the WMRs operate in a perfect manner so we eliminate the enormous Handoff Latency then no more blocking cases. However with the growth in network population, the blocking values increase. For EAP-IHA, starting from a value of 100 stations, the blocking rate surpasses zero. However for SWMM, a similar effect takes place starting from 150 stations. This result is justified through the relation of the blocking rate to the handoff latency value.

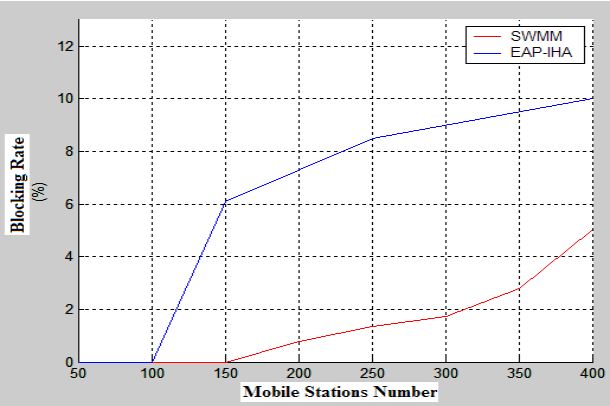

Figure 5: Blocking rate vs. number of mobile stations

Thereafter, this dependency and increase in the blocking rate can degrade the quality of services of the network, in particular at the time of handoff. Moreover, the comparison between the two curves in Figure 5 clarifies a clear difference which can reach 7%.

VI.A.3. Loss rate vs. number of mobile stations

In order to control the features of the network, we can establish multiple communications between stations and, while referring to the number of lost packets, we can determine the nature and the quality of connection. Figure 6 shows the result of the loss rate versus the number of mobile stations. As in the blocking rate case, the two curves start with zero values. That is due to the small number of mobile stations and therefore, the few packets circulating in the network. However, for the EAP-IHA method, starting from the value of 100 stations, packets begin to be lost, and this loss rate gets higher with the increase in network population. In contrast, for SWMM, the packet loss rate starts to increase when the number of mobile stations reaches 200.

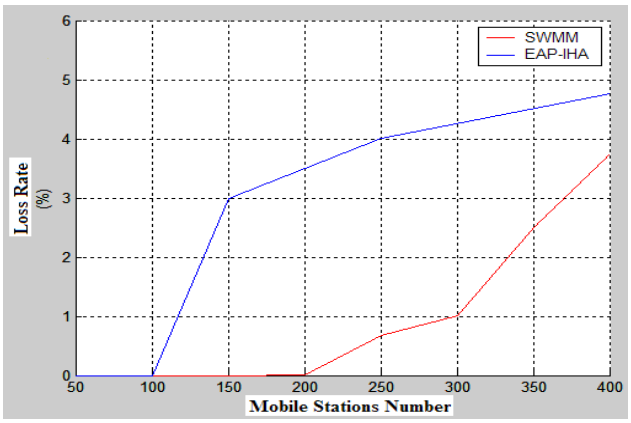

Figure 6: Loss rate vs. number of mobile stations

Packet loss increase in both methods is due to the overloading in packets queues. As long as the loss rate is smaller than 1%, the quality of services can be considered to be acceptable. On the other hand, if the loss rate exceeds 1%, the quality of service in this network is considered to degraded.

By comparing the two curves in Figure 6, we note that the carrying out of SWMM gives a light increase in the loss rate compared to the second solution which increases abruptly and with very large values. The difference between the two curves reaches 3.5%.

Compared to EAP-IHA, SWMM has been found to have considerably lower values of handoff latency, blocking rate and packet loss rate. This demonstrates the importance of establishing the secure tunnel at the time of handoff and during the re-authentication phase to promote a protected, reliable and resistant network against the attacks, as well as a more optimal and adequate quality of services to clients.

VI.B. Performances Evaluation of SDPMM

In the first case, we started simulating one attacker (simple attack) and increasing mobility speed of the attacker from 0 to 30m/s. We repeated the same scenario for the case of two attacks.

To provide DoS and DDoS attacks, we used “SYN Flood” attacks and assumed that the packets are generated by attacker(s) and sent to the victim at a rate of 100 packets per second.

Figure 7 shows the variation of traffic overhead (percentage in comparison to throughput) with respect to mobility speed increasing of attacker(s) for two cases: DoS and DDoS. We can notice that in these cases the traffic overhead does not exceed 0,05% when the mobility speed of attacker(s) is lower than 20m/s. Therefore, it appears that the major factor that has a serious effect on the generated traffic overhead is the mobility. Increasing the number of attack sources makes significant variation in the generated overhead, since nodes move randomly and

traffic sources can move from one cluster to another to become close to (or distant from) the victim.

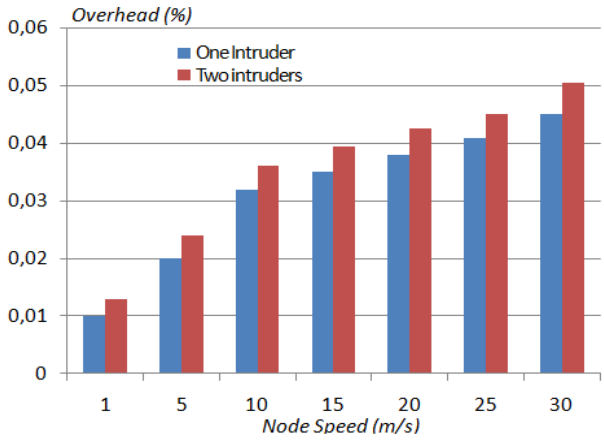

Figure 7: Traffic overhead generated by SDPMM

VII. CONCLUSION

To allow users an effective and reliable handoff, as well as a secure access to the mesh network, a method of re-authentication, with reduced delay, should be executed during the mobility of mobile nodes over different SMAPs 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 addition, a WMN can be prone to many types of attacks, especially DoS and DDoS attacks. The success of these attacks is based on the fact that the real identity of the intruders performing the attacks can be hidden. That is why having knowledge about the entire path of attack packets can be helpful in making defense decisions. Moreover, IP traceability is more useful than only locating the attacker because; the attacker network may happen to be cooperative. In this paper, we have proposed a new solution for the problem of insecurity during handoff. Using the network simulator we have developed for this work, we have tested the proposed SWMM solution against EAP-IHA method. The simulation results have shown that SWMM supports a more protected mechanism and a more effective re-authentication scheme in term of handoff latency, blocking rate and packet loss rate. We have also proposed a novel traceback technique for WMNs, called "selective and deterministic pipelined packet marking for mesh networks" (SDPMM).

REFERENCES

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

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

[3] G. R. Hiertz, S. Max, R. Zhao, D. Denteneer and L. Berlemann, "Principles of IEEE 802.11s," *International Conference on Computer Communications and Networks (ICCCN)*, 2007

[4] P. S. Mogre, M. Hollick and R. Steinmetz, "QoS in Wireless Mesh Networks: Challenges, Pitfalls, and Roadmap to its Realization," *International workshop on Network and Operating Systems Support for Digital Audio & Video (NOSSDAV)*, 2007

[5] Y. Zhang, J. Luo and H. Hu (Editors), *Wireless Mesh Networking: Architectures, Protocols and Standards*, Auerbach Publications, 2006

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

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

[8] J. Lee, S. J. Lee, W. Kim, D. Jo, T. Kwon and Y. Choi, "Understanding interference and carrier sensing in wireless mesh networks," *IEEE Communications Magazine*, Vol. 47, No. 7, pp. 102-109, July 2009

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

[10] 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.

[11] T. Mundt, "Location dependent digital rights management," *IEEE Symposium on Computers and Communications (ISCC)*, 2005

[12] D. Makaroff, P. Smith, N. J. P. Race and D. Hutchison, "Intrusion detection systems for community wireless mesh networks," *IEEE International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, 2008

[13] S. M. Glass, V. Muthukkumurasamy and M. Portmann, "Detecting man-in-the-middle and wormhole attacks in wireless mesh networks," *International Conference on Advanced Information Networking and Applications (AINA)*, 2009

[14] F. Martignon, S. Paris and A. Capone, "MobiSEC: a novel security architecture for wireless mesh networks," *ACM Symposium on QoS and Security for Wireless and Mobile Networks*, 2008

[15] Y. Amir, C. Danilov, M. Hilsdale, R. Musăloiu-Elefteri and N. Rivera, "Fast handoff for seamless wireless mesh networks," *International Conference On Mobile Systems, Applications And Services (MobiSys)*, 2006

[16] D. W. Huang, P. Lin and C. H. Gan, "Design and performance study for a mobility management mechanism (WMM) using location cache for wireless mesh networks," *IEEE Transactions on Mobile Computing*, Vol. 7, No. 5, pp. 546 - 556, May 2008

[17] R. Fantacci, L. Maccari, T. Pecorella and F. Frosali, "A secure and performant token-based authentication for infrastructure and mesh 802.1X networks," *IEEE Conference on Computer Communications (INFOCOM)*, 2006

[18] X. Lin, X. Ling, H. Zhu, P. H. Ho and X. S. Shen, "A novel localised authentication scheme in IEEE 802.11 based wireless mesh networks," *International Journal of*

Security and Networks, Vol. 3, No. 2, pp. 122-132, 2008

[19] K. Khan, M. Akbar, "Authentication in multi-hop wireless mesh networks," *Transactions on Engineering, Computing and Technology*, Vol. 16, pp.178-183, November 2006

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

[21] 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

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

[23] 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

[24] Y. Djemaiel, S. Rekhis, and N. Boudriga, "Adaptive and selective packet marking in communication networks," *WSEAS International Conference on Communications*, 2005

[25] V. L. L. Thing and H. C. J. Lee, "IP traceback for wireless ad-hoc networks," *IEEE Vehicular Technology Conference (VTC)*, 2004

[26] C. J. H. Lee, L. L. V. Thing, Y. Xu and M. Ma, "ICMP traceback with cumulative path, an efficient solution for IP traceback," International Conference on Information and Communications Security, 2003

[27] V. L. L. Thing, H. C. J. Lee, M. Sloman and J. Zhou, "Enhanced ICMP traceback with cumulative path," *IEEE Vehicular Technology Conference (VTC)*, 2005

[28] Y. Kim and A. Helmy, "SWAT: Small World-based Attacker Traceback in Ad-hoc Networks," *International Conference on Mobile and Ubiquitous Systems: Networking and Services (MobiQuitous)*, 2005

[29] B. Al-Duwairi, G. Manimaran, "A novel packet marking scheme for IP Traceback," *International Conference on Parallel and Distributed Systems (ICPADS)*, 2004

[30] H. Zhou, M. W. Mutka and L. M. Ni, "IP Address Handoff in the MANET," *IEEE Conference on Computer Communications (INFOCOM)*, 2004

[31] A. Izquierdo, N. Golmie, K. Hoeper and L. Chen, "Using the EAP Framework for Fast Media Independent Handover Authentication", *National Institute of Standards and Technology*, USA, 2008.