A Survey on Security and Privacy Issues in Wireless Mesh Networks

Aggeliki Sgora[1,3], Dimitrios D. Vergados[1] and P. Chatzimisios[2]

[1]Department of Informatics, University of Piraeus, GR-185 34, Piraeus, Greece, email: {asgora,vergados}@unipi.gr
[2]Department of Informatics, Alexander TEI of Thessaloniki, GR-57400, Thessaloniki, Greece, email: pchatzimisios@ieee.org
[3]VTT Technical Research Centre of Finland, PL 1100, FI-90571, Oulu, Finland, email: ext-angeliki.sgora@vtt.fi

***Abstract*—Wireless Mesh Networks (WMNs) are considered as a promising solution for offering low-cost access to broadband services. However, one of the main challenges in the design of these networks is their vulnerability to security attacks. In this paper, we analyze the fundamental security challenges and constraints of these networks, classify several possible attacks and survey several intrusion prevention, detection and response mechanisms found in the literature.**

***Index Terms*— Wireless Mesh Network (WMN); Security; Attack; Vulnerability; Intrusion Detection System; Authentication; Encryption; Secure Routing**

I. Introduction

Wireless Mesh Networks (WMNs) are characterized by dynamic self-organization, self-configuration and self-healing to enable flexible integration [1], quick deployment, easy maintenance, low cost, and may also be used to improve the performance of multi-hop ad-hoc networks, Wireless Local Areas Networks (WLANs) and Wireless Metropolitan Area Networks (WMANs). WMNs can also provide wireless Internet connectivity at lower cost than the classic Wireless Fidelity (Wi-Fi) networks.

However the multi-hop nature, the lack of physical protection, the dynamic topology and ad hoc connectivity amongst end user nodes are such characteristics of WMN, which not only increase its routing overheads but also expose it to much securities vulnerability [2]. The objective of the paper is to discuss security issues concerning these networks, as well as, their security threats and countermeasures.

The paper is organized as follows: Section II gives an overview of the mesh networking technology. Section III discusses two basic security issues in the WMNs, i.e. their security challenges and their security attacks, while Section IV presents several countermeasures that ought to be taken. Finally, Section V concludes the paper.

II. Wireless Mesh Networks (WMNs) Overview

A WMN, consists of mesh clients and mesh routers [5]. Mesh routers have minimal mobility and form the mesh backbone for mesh clients. Furthermore, in order to further improve the flexibility of mesh networking, a mesh router is usually equipped with multiple wireless interfaces built on either the same or different wireless access technologies. In addition, the bridge/gateway functionalities that exist in mesh routers enable the integration with other networks. Also, WMNs are characterized by infrequent topology changes and rare node failures [50].

WMNs can be classified depending on the architecture in infrastructure /backbone WMNs, client WMNs and Hybrid WMNs. In infrastructure WMNs mesh clients can join the network only through the mesh routers. In client WMNs mesh nodes constitute the actual network while in Hybrid WMNs mesh client may join the mesh network either by connected to the mesh backbone or among each other. Figure 1 depicts a hybrid wireless mesh architecture.

Through the different configurations WMNs can be easily used to build up large scale wireless networks. For that reason, IEEE has established several working groups with aim to develop their mesh standards with coverage ranging from a Personal Area Network (PAN) to a Metropolitan Area Network (MAN) [49], as it can be seen from Table I. Also, several companies are developing their proprietary WMN solutions [3].

A comprehensive survey regarding the mesh technology can be found in [7].

III. Security Challenges and Issues in WMNs

A. Security Challenges and Constraints in WMNs

A WMN is exposed to the same basic threats common for both wired and wireless networks, therefore the messages in such networks can be intercepted, modified, delayed, replayed, or new messages can be inserted [8]. However, WMNs are more difficult to be fully protected for the following reasons [6]:

- Multihop Nature: Multihopping delays the detection and treatment of the attacks [8]. Also, since the majority of the existed security schemes are developed for one-hop networks, render them insufficient to protect a WMN from being attacked [7].
- Multitier System security: In such networks security is needed not only between the client nodes, but also between mesh clients and mesh routers, as well as among mesh routers.
- Multisystem security: Since the WMNs involve the interoperability of different wireless technologies, such as IEEE 802.15, IEEE 802.11, IEEE 802.16, etc. a security mechanism is needed so that inter-network communications can be provided seamlessly without compromising security in all networks.

Siddiqui and Hong [4] and Gao et al. [22] also describe the constraints that should be considered in WMNs or in other system with mobile clients such as PDAs, cell-phones etc. These are:

- Central Processing Unit (CPU): the total computing power on the end nodes is very limited, so large computations on them are slow.
- Battery: the total power capacity is very limited and so it is not desirable to use the device for high range computations and transmissions.
- Mobility: nodes can be mobile, which can produce latency in the convergence of the network and the handover to the networks.
- Bandwidth: bandwidth in amongst the mobile nodes is also limited.
- Scalability: the current wireless networks act poorly, when the networks enlarged in both aspects of members and computation.

In addition, the fact that usually the mesh devices are relatively cheap devices with limited physical security makes them potential targets for node capture and compromise [59].

Zang and Fang [32] highlighted the three different levels, where security requirements of WMNs should be identified: infrastructure, network access and application. Although infrastructure security and application security are goals that can be easily achieved network access security is not an easy task due to the multihop nature of the WMNS and their dynamic network topology. For that reason in this paper we mainly focus our attention on network access security issues and countermeasures.

B. Security Issues in WMNs

The security issues for WMNs are basically identical to security requirements for any other communication system. These issues include:

- Availability: It ensures the survivability of network services despite the following attacks [4].
- Authenticity of network traffic: It ensures the identity of a communicating node. In the absence of authenticity, an adversary could masquerade a node, thus gaining unauthorized access to resources and sensitive information and interfering with the operation of other nodes [2].
- Integrity: It guarantees that data cannot be modified without being detected [8]. Integrity can be compromised either by chance (e.g. a transmission error) or caused by a malicious user (e.g. an attacker that alters an account number in a bank transaction) [2].
- Confidentiality: It ensures that the information is only accessible to those who have been authorized to access it.
- Non-repudiation: Non-repudiation ensures that the sender and the receiver of a message cannot deny that they have ever sent or received such a message.
- Authorization: It is a process in which an entity is issued credentials by the trusted certificate authority. It is generally used to assign different access rights to different level of users [2].
- Anonymity: Anonymity means that all the information that can be used to identify the owner or the current user entity should be kept private and not distributed to other communicating parties.
- Access Control: It ensures that only authorized actions can be performed [8],[10]. Also, access control entails the authentication and authorization of the network entities of the WMNs [34].
- Fairness: Fairness in WMNs deals with the access to the radio channel and access for traffic forwarded through a given station [11]. The fair access to the radio channel is the Medium Access Control (MAC) layer's responsibility, meaning that the MAC layer must ensure that no station suffers from bandwidth starvation, and the fairness on the forwarded traffic are the routing or path-selection protocols responsibility [11].
- Accountability: Aims to detect misbehaving users and, if it is necessary in many cases to deny network access to them via revoking, so that malicious users can be evicted [54], [57].

IV. Security Attacks in WMNs

Security attacks may be classified based on several factors, like the nature, the scope, the behavior, or the protocol layer the attacker target. Such a classification is depicted in Table II.

First, depending on whether the operation of the network is disrupted or not, the attacks may be distinguished on active and passive attacks [12]. An active attack is conducted to intentionally disrupt the network operation, while a passive attack intends to steal information and to eavesdrop on the communication within the network [9]. Passive attacks would compromise confidentiality and active attacks would result in violating availability, integrity, authentication, and non-repudiation [4]. Active attacks can be further divided into internal (or insider) and external (or outsider) attacks.

External attacks are conducted by attackers that do not participate in the mesh topology usually by jamming the communication or injecting erroneous information. Internal attacks are conducted by members of the mesh network and for that reason are more severe threats, since they are not as easy to prevent as external ones [8].

An attack also can be rational or malicious. In a rational attack, the adversary misbehaves only if misbehaving may worth something in terms of price, obtained quality of service or resource saving; otherwise it is characterized as malicious [8].

Moreover, the attacks can be classified, based on method the attacker use to accomplish their goal, on impersonation, modification, fabrication, replay and Denial of Service (DoS) attacks [12]. In impersonation attacks, an adversary attempts to assume the identity of a legitimate node of the WMN in order to consume its resources or to disrupt the network operation. Modification attacks target on the illegally modification of the contents of the messages, while fabrication attacks aim on consuming the network resources or the disruption of the network operation by generating false routing messages. Finally, in replay attacks (or man-in-the-middle attacks), the attackers retransmit data in order to produce an unauthorized effect, e.g. to convince mesh nodes to use a malicious path through legitimate means, while DoS attacks target on preventing legitimate mesh nodes to use the network services.

Also, attacks might apply in different protocol layers of a WMN. Glass *et al.* in [11] outline the security threats at all layers of the wireless mesh protocol stack (Table III).

1) *Security Attacks at the physical layer of WMNs*

There are several types of attacks that can affect the physical layer of a WMN. First, since the wireless mesh routers may be installed in external area, an attacker may simply destroy the hardware of such a node. Also, the wireless mesh routers may be tampered and sensitive information may be extracted from them.

In addition the physical layer can be affected by using radio jamming devices, which may meddle in the physical channels and disturb the network‘s availability. Three different types of jamming attacks may be applied as described in [13]:

- The trivial Jamming Attack in which an attacker transmits constantly noise.
- The periodic Jamming (or Scrambling) Attack in which an attacker transmits a short signal periodically.
- The reactive Jamming Attack in which an attacker transmits a signal whenever detects that another node has initiated a transmission.

2) *Security Attacks at the MAC layer of WMNs*

Several different attacks are also possible at the MAC layer of the WMNs. These include:

- Passive eavesdropping: It can be launched by internal, as well as, external nodes. Due to the WMN‘s broadcast nature of transmission, it is possible for external attackers within the transmission range of the communicating nodes to launch passive eavesdropping. WMNs are also prone to internal eavesdropping by the intermediate hops, whereby a malicious intermediate node may keep the copy of all the data that it forwards without the knowledge of any other nodes in the network [16]. Passive eavesdropping leads to the compromise in data confidentiality and data integrity [10].

- Jamming Attack: At MAC layer jamming attacks are also possible. In this case, the attacker instead of transmitting bits, he/she may transmit regular MAC headers on the transmission channel [10]. Seth and Gankotiya [13] consider the following jamming attacks for the 802.11 mesh networks:
    - Unprompted Clear to Send (CTS) Attack: An attacker transmits a CTS message with a long message duration causing all recipients to halt transmission for this duration.
    - Reactive Request to Send (RTS) Jamming Attack: In this type of attack, an attacker whenever detects an RTS message, it disrupts these messages by immediately initiating a transmission.
    - CTS Corrupt Jamming: Upon receipt of a RTS message, an attacker transmits noise during the CTS response.

  A comprehensive description and analysis of selective jamming/dropping attacks can be found in [59].
- Flooding Attack: An attacker sends a lot of MAC control messages to its neighbor nodes. By this attack the fairness of medium access is abused [14].
- MAC Spoofing: An attacker tries to modify the MAC address in transmitted frames [10].

3) *Security Attacks at the Network layer of WMNs*

An attacker could also target the network layer of WMNs. These attacks can be divided into two categories: control plane (or routing [17]) attacks and data plane (or path forwarding [17]) attacks [10]. Attacks on control plane target the routing functionality of the network, while data plane attacks target the path forwarding functionality of the network.

The main control plane attacks are distinguished in:

- Rushing Attack: In on-demand routing protocols, the attacker sends a lot of routing request packets across the network in a short interval of time keeping other nodes busy from processing legal routing request packets [7].
- Routing Table Overflow: In this attack the attacker attempts to create routes to nonexistent nodes with intention to create enough routes in order to prevent new routes from being created or to overwhelm the protocol implementation [18].
- Sybil Attack: In a Sybil attack, a malicious node pretends the identity of several nodes, each appearing as a legitimate node, with intention to disrupt the network‘s normal operation ([10], [18]). This attack degrades the routing performance and also disrupts the routing services.
- Byzantine attack: This type of attack may be launched by a single compromised node or by group of working together compromised intermediates. Their goal is to create routing loops and forwarding packets in a long route instead of optimal one, even may drop packets. This attack degrades the routing performance and also disrupts the routing services.
- Wormhole Attack: A wormhole attack attempts to convince nodes to use a malicious path through legitimate means [8]. During this attack, two or more malicious nodes collude together by establishing a tunnel, i.e a wormhole, using an efficient communication medium [10]. Once the victim node includes the malicious nodes in the routing path, the malicious nodes start dropping packets.

- Sinkhole (or blackhole) Attack: A sinkhole attack is launched when a malicious node convinces neighboring nodes that it is the "most optimal" node for forwarding packets. Then the malicious node drops the packets forwarded by neighboring nodes.
- Greyhole Attack: This type of attack is a variant of the sinkhole attack [8]. More specifically, the malicious nodes in contrast to sinkhole attack do not drop all the packets but they just drop selective packets [13].
- Sleep Deprivation Attack: During this attack, a malicious node attempts to exhaust the batteries of a victim node by requesting routes, or by sending unnecessary packets to it.
- Location Disclosure: A location disclosure attack reveals information about the location of nodes or about the structure of the network [19].
- Route error injection Attack: During this attack, a malicious node injects forged route error messages to break mesh links and disrupt the routing services.

Data control attacks are launched by misbehaving nodes in the network. Bansal et al. [20] classify the misbehaving nodes into two groups: selfish and malicious nodes. A selfish node is only concerned about improving its performance even at the expenses of other nodes, while a greedy node intends to disrupt normal network's operation [20]. The simplest data control attack is eavesdropping: Since routing data can reveal information the network topology in general, an attacker by eavesdropping tries to discover this information by listening to network traffic.

4) Security Attacks at the Transport Layer of WMNs

Possible attacks in this layer are flooding and desynchronization, i.e. the disruption of an existing connection. In the flooding attack, a malicious node may repeatedly make new connection requests until the resources required by each connection are exhausted or reach a maximum limit. In the desychronization attack, a malicious node may repeatedly spoof messages to an end host causing the host to request the retransmission of missed frames. If timed correctly, an attacker may degrade or even prevent the ability of the end hosts to successfully exchange data causing them instead to waste energy attempting to recover from errors which never really exist [23].

5) Security Attacks at the Application Layer of WMNs

Application Layer attacks in wireless networks concern viruses, worms, malicious codes, application abuses, etc [21]. Also when data are transmitted unencrypted, they are vulnerable to packet sniffing, as well as, to attacks against applications.

V. Countermeasures for WMNs

In order to alleviate the security problems in WMNs, several defence methods have been put forward that fall into these three categories: intrusion prevention, intrusion detection and intrusion response [35]. The current section discusses several countermeasures for WMNs.

A. Intrusion Prevention Mechanisms

Intrusion prevention mechanisms are considered as the principle line of defense against malicious nodes and include encryption and authentication [35], as well as, secure routing. In particular, several WMNs key management schemes that entail encryption and authentication may be found into the literature.

A key management service is responsible for keeping track of bindings between keys and nodes and for assisting the establishment of mutual trust and secure communication between nodes [4]. Existing key management solutions for wireless and wired networks may be classified into the following three typical categories: centralized, decentralized and distributed key updating protocols [37]:

- Centralized methods rely on a trusted third party called group server that is responsible for the generation and distribution of group keys.
- In the decentralized methods, the group management duty is distributed to multiple subgroup leaders in order to reduce the load at a single point.
- In the distributed key management solutions, the keys are generated collaboratively by one or multiple group members.

Although plethora of key management schemes for wired and wireless networks proposed, the unique characteristics of the WMNs, such as the dynamic, self-organized and multihop nature, as well as the heterogeneity of devices, make them not suitable for WMNs. For this reason lately several key management schemes for WMNs may be found in the literature.

Zhang and Fang [32] propose the Attack Resilient Security Architecture (ARSA) that allows users to access and roam between multi-domain WMNs. To achieve this goal the authors assume that there is a number of trust domains, each managed by a broker or WMN operator that issue universal passes to the members of the WMNs. Also they utilize identity-based public key cryptosystem for authentication and key agreement between mesh clients and routers. The authors also address the problem of user location privacy by providing the user with different alias identities [36].

Yi et al. [15] propose a certificate-less hierarchical key management scheme using threshold secret sharing and certificate-less signcryption. More specifically, they propose a two-layer structure, in which the senior layer network consists of wireless mesh routers to form the cluster heads and the lower layer network is composed by ordinary mobile nodes, i.e. laptops, cell phones, etc. Offline authentication is assumed, i.e. meaning that each node of the network must be registered in a specific offline trusted institution to produce identity. The master key is generated distributed, and each cluster head node has only a shadow of master key. The cluster head nodes use certificate-less technology to generate private key which can be update timely to improve the security of the system. The certificate-less mechanism help to solve the problem of key escrow, while the use of signcryption saves the user‘s computation and improves the system efficiency.

Wang et al. [37] propose a Heterogeneity-Aware Group Key (HAGK) distributed management framework that combines the logical key hierarchical technique together with distributed threshold-based[1] techniques in WMNs that supports both one-to-many and many-to-many group communications. The proposed scheme also adopts the two-layer: the top layer includes all backbone nodes and adapts a threshold-based group key agreement protocol; the bottom layer is composed of a set of hierarchical key trees maintained backbone nodes. The key refreshing for both the top layer and bottom layer happen at the local environment. The authors also use a Bloom Filter based authentication method called semi-anonymity authentication, to allow group members to get authenticated from subgroup leaders without revealing their secure information.

Fu et al. [38], [44] presented a mutual authentication scheme based on a combination of

[1] In threshold-based techniques the group key is either agreed among group members or generated based on shares from group members [37]. Solutions belonging to the second category are also known as contributory key agreement schemes [39] .

techniques, such as zone-based hierarchical topology structure, virtual Certification Authority (CA), off-line CA, identity-based cryptosystem and multi-signature. By applying these techniques, the proposed scheme succeeds in improving key management in security, expandability, validity, fault tolerance and usability.

Kandah et al. [51] propose a Secure Key Management Scheme (SKeMS) that seeks to minimize the malicious eavesdropping ability in WMNs. This is achieved by assigning different as possible S encryption keys among all nodes in a common neighborhood. Simulation results showed that the proposed scheme performs well in terms of smaller malicious eavesdropping ability ratio and less running time.

Boudguiga and Laurent [63] propose an authentication scheme and key encryption schemes for IEEE 802.11s networks. The key idea of the proposed authentication scheme is that each station should authenticate itself to an Authentication Server (AS), which delegates the station key generation to Mesh Key Distributors (MKDs). To achieve this goal the ID-Based cryptography concepts are used for shared secret exchange between the AS and the station and keys' derivation needed to secure the exchanged messages. Also, for the key ID-Based key construction the Sakai-Kasahara method is used. Security analysis showed that the proposed method is suitable to IEEE 802.11s mesh networks and resistant to the key escrow attack.

B. Secure Routing

Due to open medium, the routing protocols are constantly victims of attacks trying to compromise their capabilities. Therefore the routing protocol used inside a mesh should be secured against attacks. To obtain this goal, researchers proposed either mechanisms to enhance existing routing protocols used for ad-hoc networks or new security protocols that are suitable for WMNs.

Oliveiro and Romano [42] propose an extension of the Ad-hoc On-demand Distance Vector (AODV), named AODV-DEX, in order to protect AODV against gray hole or sinkhole attacks. The main idea is to modify the hop count values in order to let them also reflect information about the nodes' reputations along a path. To achieve this goal, two reputation levels are considered the global reputation, a global reputation supplied by other nodes through the dissemination protocol[2], and the local information (i.e. a local reputation, coming from the observations provided by the watchdogs). These two levels are merged to define the reputation that can be exploited to evaluate the real behavior of a node. Simulation results show that the use of reputation metric in AODV can increase both the security level and the performance of the overall network, even in the presence of routing attacks.

Khan et al. [40], [43] propose a secure routing protocol for IEEE 802.11 WMNs, named SRPM. More specifically, the authors modify the AODV's route discovery mechanism, leaving all the routing decisions to access points. Additionally, in order to ensure security, the proposed mechanism keeps the information of two-hop neighbors and to further increase the security level a new routing metric is introduced, which is capable of searching the shortest secure path by computing Unreliability Value (UV) of the neighbors by implementing a two-hop passive acknowledgment scheme. Security analysis showed that SRPM is robust against a variety of security attacks, such as blackhole, greyhole, wormhole, fairness reduction, jellyfish and node isolation.

[2] The reputation is encapsulated in an RREQ (Route REQuest) message of the AODV protocol.

Qazi et al. [45] propose a secure routing protocol that is based on the design AODV protocol, named ticket-based ad hoc on demand distance vector (TAODV). It is a cross layer protocol which works at network layer, but it also provides security for data exchange and avoids the transfer of Address Resolution Protocol (ARP) messages in order to find MAC addresses of source and destination. The protocol also includes encryption and authentication mechanisms to ensure authenticity and integrity of the data. For the authentication, an Authentication Server is assumed, while key management services are assumed to be provided by a trusted Certificate Authority.

Wu and Li [60] propose a private routing algorithm, the called Onion Ring that is based on the Onion routing algorithm [61] that is designed to achieve privacy in wired networks. In the Onion Ring approach whenever a mesh node wants to be connected to the Internet it has to send a request to the Mesh Gateway. Then, the Mesh Gateway selects a route, and uses shared keys between itself and Mesh nodes (symmetric keys) nodes in the route to construct an “Onion", and delivers the “Onion” toward the initiator. Security analysis shows that the “Onion” structure protects the routing information from inside attackers.

Especially, for the WLAN mesh networks several enhancements for the Hybrid-Wireless-Mesh Protocol (HWMP), which is the de-facto routing protocol for 802.11s networks, have been proposed.

Islam et al [53] propose a modification of the HWMP, the Secure HWMP (SHWMP), to provide authenticity and integrity of HWMP routing messages and prevent unauthorized manipulation of mutable fields in the routing information elements. To achieve this, they use the Merkle tree concept to authenticate mutable information and symmetric key encryption to protect the mutable field. Simulation results showed that SHWMP provide higher packet delivery ratio with little increase in end-to-end delay, path acquisition delay and control byte overhead. However, the proposed protocol is vulnerable to the attacks launched by the internal legitimate mesh routers [56].

Ben-Othman and Benitez [47], [48] propose an Identity Based Crytography (IBC) mechanism to increase the security level of the HWMP. The authors propose two modifications trust management for internal nodes and digital signature of routing messages with IBC for external nodes. The use of the IBC eliminates the need to verify the authenticity of public keys and ensures the integrity of the control message in HWMP. Simulation results show that the IBC-HWMP does not induce a long overhead compared to the orignal HWMP protocol.

Bansal and Sofat [46] propose a modified HWMP routing protocol for WMN, which uses cryptographic extensions to protect unprotected routing information elements. More specifically, the authors consider two different kinds of routing fields: mutable and non mutable. They use the existing key distribution specified in the draft 3.0 draft version of the IEEE 802.11s protocol and authenticate the mutable fields in the hop-by-hop fashion using the hash tree based approach. Security analysis show that the proposed security routing protocol protects the networks against of flooding, rooting disruption, routing loops and routing diversion attacks. However, simulation results show that the proposed protocol incurs little overhead in terms of control overhead in bytes and path acquisition delay.

Li et al. [55] propose an enhancement for the on-demand part in HWMP, the SEAODV, a security enhanced version of AODV. More specific, the authors use Blom’s key pre-distribution scheme for the keys establishment and enhanced HELLO message to compute the pairwise transient key (PTK), which subsequently being used to distribute the group transient key (GTK) that secures the broadcast routing messages between the node and its one-hop neighbors. Security analysis and performance evaluation show that SEAODV is more effective in preventing identified routing attacks, such as RREQ flooding, RREP routing loops, route re-direction, formation of routing loops, and outperforms ARAN and SAODV in terms of computation cost and route acquisition latency.

Lin et al. [56] propose an improvement of SHWMP, the Privacy-Aware Secure Hybrid Wireless Mesh Protocol (PA-SHWMP), which combines a dynamic reputation mechanism based on subject logic and uncertainty with the multi-level security technology. Simulation results showed that the PA-SHWMP in comparison with the HWMP and SHWMP protocols has:

1. better performance in packet delivery ratio when the number of malicious nodes and the percentage of lossy links increase.
2. smaller convergence time with any percentage of malicious mesh routers.

Finally, Ben-Othman et al. [62] propose the HWMP-Watchdog mechanism that combines the benefits of HWMP and Watchdog techniques. The main idea is the Watchdog mechanism to detect and exclude malicious nodes during the path-selection process of the HWMP. By applying this internal attacks are reduced. Simulation results showed that HWMP-Watchdog succeeds in detecting both malicious attacks and selfish behaviors without significant overhead.

C. Intrusion Detection Systems (IDSs)

Since, only the usage of protection and encryption software to protect WMNs are not sufficient and effective, intrusion detection systems are also deployed to provide a second line of defence [33]. Intrusion Detection Systems in wired or wireless networks are used to alert the users about possible attacks, ideally in time to stop the attack or mitigate the damage [24]. They consist of three functions [24], [26] :

1. Event monitoring: The IDS must monitor some type of events and maintain the history of data related to these events.
2. Analysis engine: The IDS must be equipped with an analysis engine that processes the collected data to detect unusual or malicious behavior.
3. Response: the IDS must generate a response, which is typically an alert to system administrators.

Several IDSs may be found in the literature. These systems may be classified based on detection action that are used to Anomaly Detection IDSs and Misuse Detection IDSs [25], or Pattern-based Detection IDS [58]. Anomaly detection tries to characterize normal behavior, and everything is assumed to be anomalous, while misuse detection tries to characterize attacks, and everything else is assumed to be normal [26]. The first detection action is a very challenging issue in WMN due to the used unreliable physical medium [39], fluctuating operational environments, unavoidable signal interference, and unpredictable traffic congestion [29].

Also, depending on the monitoring events the IDSs can be also classified [4] into three categories:

- Standalone IDS: in which IDS runs on each node independently to determine intrusions.
- Distributed and Cooperative IDS: An IDS agent that runs on each node is responsible for the detection and collection of local events and data to identify possible intrusions,

as well as, for the initiation of a response independently.

- Hierarchical IDS: Cluster-heads act as control points to provide the functionality for its child nodes.

Although a majority of IDSs for wired infrastructures may be found into the literature, the characteristics of the WMNs, such as the open medium, the dynamic network topology, the multi-hop nature, and the lack of concentration points where traffic can be analyzed, make them inapplicable in WMNs. Also the fact that the Internet uplinks in a WMN can be decentralized makes the selection of a single location to deploy IDS functionality impossible [28]. For that reason the majority of the IDSs for WMNs are either distributed and cooperative or hierarchical [4].

Bansal et al. [31] propose an IDS to detect greedy MAC misbehavior 802.11 WMNs. The proposed IDS implemented on mesh point can detect two MAC misbehaviors: the oversized NAV attack and the reduced backoff attack, as well as, the switching between these two attacks. The fact that the detection method is implemented on each Mesh Point and there is no need to rely on receiving nodes makes the proposed IDS cost effective and also helps in avoiding the problem of colluding partner.

Zhou et al. [27] propose a probability based IDS for 802.16 mesh networks. More specific, the authors propose a distributed reputation-based IDS, where each node collects not only the list of Base Stations (BSs) and neighbors, but also the honesty probability of the node. Then each node enrolled the WMN reports its communication state. Thus, the security of the network is increased, since its time the more secure node will be selected to a path.

Hugelshofer et al. [28] propose the OpenLiDS, a lightweight decentralized intrusion detection system for WMNs. It uses efficient anomaly-detection metrics to identify generic classes of attacks, including scanning, resource starvation attacks and unsolicited email distribution caused by mass-mail Internet worms. Experiment results show that OpenLIDS is superior to over other signature-based approaches both in terms of memory requirements and packet delivery ratio. However, simulation results show that OpenLIDS is unable to distinguish an RTP stream from a UDP DoS flood with fixed source and destination ports [24]. Furthermore, for new connections, this approach is not as efficient as expected as generating and receiving connection tracking events is costly [24].

Zang et al. [29] propose the RADAR system, a reputation-based IDS, whose goal is to identify abnormal mesh nodes in WMNs through a reputation measurement that takes into consideration the spatio-temporal behavior of nodes. The scheme is specified and implemented with DSR routing protocol, aiming on the detection of misbehaving nodes that target on network disruption. Simulation results show that RADAR detects routing loops with higher false alarms, it is resilient to malicious collectives for subverting reputations; but involves a relatively high latency for detection of DoS attacks [24].

Martignon et al. [41] propose a framework to detect selfish behavior of the mesh routers in community mesh networks, based on a trust and reputation management system. The proposed framework consists of three components: a watchdog mechanism to distinguish between selfish and cooperative actions, a protocol to exchange trust ratings among the network nodes and a trust model for quantifying the nodes trustworthiness. Numerical results show that the proposed scheme offers high detection accuracy, even when a high percentage of network nodes provide false trust values.

Yang et al. [25] propose a hierarchical IDS for 802.11 WMNs, which is based on distributed proxy servers. The authors consider two new types of nodes in comparison with traditional wired or wireless IDS: proxy servers, and central consoles. The WMN network structure is depicted in Figure 2. Each IDS proxy runs independently and detects the activities of inner nodes. If the local proxy cannot decide from all the evidence collected, it will report the results to the gateway node in domain. Then the gateway node will execute its own the analysis and detection by itself or by neighbor gateway nodes to complete the cross-domain intrusion detection cooperatively. The efficient multi-level hierarchical grouped topology structure of the proposed IDS provides better security protection for the wireless Mesh network and increases scalability.

Glass et al [52] propose an intrusion detection mechanism for detecting man-in-the-middle and wormhole attacks in 802.11sWMNs. More specific, the authors propose a simple modification to the MAC layer in order to detect inauthentic acknowledgments in encrypted data frames and to suppress the initial acknowledge (ACK) when required. Experimental results showed that the proposed mechanism presents a high detection rate, no false positives and a small computational and communication overhead.

Khan et al. [58] propose a cooperative and hierarchical IDS for WMNs. In this system each mesh node has an IDS agent, which monitors independently its neighbor nodes, and in case of misbehavior detection, broadcast the information to its neighbors, as well as, report is sent to the serving mesh router for action. Also, the IDS agent of the mesh router has capabilities for cross layer monitoring and detection (link, network, transport). By this cooperation the proposed IDS achieves to identify several attacks, such as MAC spoofing, selfishness, flooding and routing misbehaviors.

VI. Conclusions

Wireless Mesh Networks is nowdays a very popular technology for providing IP services due to its fast, easy and inexpensive network deployment. However, due to their characteristics, such as the open medium, the dynamic network topology, the multihop nature, and the lack of concentration points where traffic can be analyzed, WMNs pose new challenges in achieving security.

In this paper, we provided a detailed analysis of the fundamental security challenges and constrains of these networks. Furthermore, we classified the possible attacks based on several factors, like the nature, the scope, the behavior or the protocol layer the attacker target. We have also surveyed several defence methods exclusively for WMNs, including intrusion prevention, detection, and response mechanisms found in the literature.

Although security in WMNs has attracted many researchers and many intrusion prevention, detection and response mechanisms may be found in the literature the question about which is the best solution still remain answered, since each of them focus on specific attacks and requirements.

Acknowledgement

This research has been co-financed by the European Union (European Social Fund – ESF) and Greek national funds through the Operational Program "Education and Lifelong Learning" of the National Strategic Reference Framework (NSRF) - Research Funding Program: “ARCHIMEDES III Investing in knowledge society through the European Social Fund”.

REFERENCES

[1] X. H. Wang, M. Iqbal and X. Zhou, “Design and Implementation of a Dual-Radio Wireless Mesh Network Testbed for Healthcare”, In the Proceedings of the International Conference on Technology and Applications in Biomedicine, (ITAB 2008), Ioannina, Greece, 2008, pp. 300-304.

[2] R. Malik, M. Mittal, I. Batra, and C. Kiran, “Wireless Mesh Networks (WMN)”, International Journal of Computer Applications, vol. 1, no. 23, 2011, pp 68-76.

[3] A. Sgora, D. D. Vergados, and P. Chatzimisios, “IEEE 802.11s wireless mesh networks: Challenges and Perspectives”, In the Proceedings of the 1st International Conference on Mobile Lightweight Wireless Systems (Mobilight ‘09), Athens, Greece, 18-20 May 2009.

[4] M. S. Siddiqui, C. S. Hong, “Security Issues in Wireless Mesh Networks”, In the Proceedings of the International Conference on Multimedia and Ubiquitous Engineering (MUE'07) , Seoul,Korea, 2007, pp. 717 – 722.

[5] N. Nandiraju, D. Nandiraju, L. Santhanam, B. He, J. Wang, and D. P. Agrawal, “Wireless Mesh Networks: Current Challenges and Future Directions of Web-In-The-Sky”, IEEE Wireless Communications,vol. 14, no. 4, 2007, pp. 79-89.

[6] I. Akyildiz and X. Wang, “Wireless Mesh Networks (Advanced Texts in Communications and Networking”, John Wiley & Sons Ltd. ISBN: 978-0-040-03256-5, 2009.

[7] I. F. Akyildiz, X. Wang, and W. Wang, “Wireless Mesh Networks: a survey”, Computer Networks, vol. 47, no. 4. 2005, pp. 445-487.

[8] Y. Zhang, J. Luo and H. Hu, “ Wireless Mesh Networking: Architectures, Protocols and Standards”, Auerbach Publications, ISBN: 978-0-8493-7399-2, 2006.

[9] L. Santhanam, B. Xie, and D. P. Agrawal, “Selfishness in Mesh Networks: Wired Multihop MANETs”, IEEE Wireless Communications, vol. 15, no. 4, August 2008, pp. 16 – 23 .

[10] A. Naveed, S. S. Kanhere, and S. K. Jha, “Attacks and Security Mechanisms Security in Wireless Mesh Networks”, Ed (Y. Zhang), Auerbach Publications, ISBN: 978-0-8493-8250-5, 2009.

[11] S. Glass, M. Portmann, and V. Muthukkumarasamy, “Securing Wireless Mesh Networking”, IEEE Internet Computing, vol. 12, no. 4, 2008, pp. 30-36.

[12] M. O. Pervaiz, M. Cardei and J. Wu, “Routing Security in Ad Hoc Networks”, Network Security, Editors S. C.-H. Huang, D. MacCallum, D.- Z. Du, Springer, ISBN: 978-0-387-73820-8, 2010.

[13] S. Seth, and A. Gankotiya, “Denial of Service Attacks and Detection Methods in Wireless Mesh Networks”, In the Proceedings of the 2010 International Conference on Recent Trends in Information, Telecommunication and Computing (ITC 2010), Koshi, Kerala, 2010 , pp. 238 – 240.

[14] H. Moustafa, U. Javaid. T. M. Rasheed, S. M. Senouci and D. Meddour, “A Panorama on Wireless Mesh Networks: Architectures, Applications and Technical Challenges”, In the Proceedings of the First International Workshop on Wireless mesh: moving towards applications (WIMESHNETs ‘06) , Waterloo, Canada, 2006.

[15] D. Yi, G. Xu, and Z. Minqing, “The Research on Certificateless Hierarchical Key Management in Wireless Mesh Network”, In the Proceedings Of the 3rd International Conference Communication Software and Networks (ICCSN 2011), 27-29 May 2011, Xi’an, China, 2011, pp. 504 – 507.

[16] J. Sen, “Secure Routing in Wireless Mesh Networks”, Wireless Mesh Networks, N. Funabiki (Ed.), InTech, ISBN: 978-953-307-519-8, 2011.

[17] D. Divyaand S. Kumar, “Security Challenges in Multihop Wireless Mesh Networks–A Survey”, Information Security and Digital Forensics, D. Weerasinghe (Ed) , Springer Berlin Heidelberg, ISBN: 978-3-642-11530-1, 2010.

[18] H. Redwan and K. Ki-Hyung, “Survey of Security Requirements, Attacks and Network Integration in Wireless Mesh Networks”, In the Proceedings of the 2008 New Technologies, Mobility and Security Conference (NTMS 2008), Tangier, Morocco, 2008, pp. 1-5.

[19] B. Wu, J. Chen, and J.Wu, A Survey of Attacks and Countermeasures in Mobile Ad Hoc Networks Wireless Network Security, Y. Xiao, X. S. Shen, D.-Z. Du (Ed.), Springer, ISBN: 978-0-387-33112-6978-0-387-33112-6, 2007.

[20] D. Bansal, S. Sofat, and A. K. Gankotiya, “Selfish MAC Misbehaviour Detection in Wireless Mesh Networks”, In the Proceedings of 2010 International Conference on Advances in Computer Engineering (ACE 2010), Bangalore, Karnataka, India, 2010, pp. 130-133.

[21] H Yang, H Luo, F Ye, S Lu, and L Zhang, “Security in mobile ad hoc networks: challenges and solutions”, IEEE Wireless Communications, vol. 11, no. 1, February 2004, pp. 38 – 47.

[22] L. Gao, E. Chang, S. Parvin, S. Han, and T. Dillon, “A Secure Key Management Model for Wireless Mesh Networks”, In the Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications (AINA 2010), Perth, WA, USA, 2010, pp. 655-660.

[23] Y. Wang, G. Attebury, and B. Ramamurthy, “A Survey of Security Issues in Wireless Sensor Networks”, IEEE Communications Surveys & Tutorials, vol. 8, no. 2, 2006, pp. 2-23.

[24] N. Deb, M. Chakraborty and N. Chaki, “Title: A State-of-the-Art Survey on IDS for Mobile Ad-Hoc Networks and Wireless Mesh Networks” Book Title: Advances in Parallel Distributed Computing, Springer Berlin Heidelberg, ISBN: 978-3-642-24037-9, 2011, pp. 169-179.

[25] Y. Yang, P. Zeng, X.Yang, and Y. Huang, “Efficient Intrusion Detection System Model in Wireless Mesh Network ; Networks Security Wireless”, In the Proceedings of the 2010 Second International Conference on Communications and Trusted Computing (NSWCTC), Wuhan, China, April 2010, pp. 393-395.

[26] T.Chen G.- S. Kuo, Z.-P. Li, and G. -M. Zhu, Intrusion Detection in Wireless Mesh Networks Security in Wireless Mesh Networks, Ed (Y. Zhang), Auerbach Publications, ISBN: 978-0-8493-8250-5, 2009.

[27] J. Zhou, Z. Chen, and W. Jiang, “Probability Based IDS Towards Secure WMN”, In the Proceedings of the 2010 2nd International Workshop on Intelligent Systems and Applications (ISA), Wuhan, China, 2010, pp. 1-5.

[28] F. Hugelshofer, P. Smith, D. Hutchison, and N. J.P. Race, "OpenLIDS: A Lightweight Intrusion Detection System for Wireless Mesh Networks", In the Proceedings of the 15th annual international conference on Mobile computing and networking (MobiCom'09), Beijing, China, 2009, pp. 309-320.

[29] Z. Zhang, F. Naït-Abdesselam, P.-H. Ho, X. Lin, "RADAR: A ReputAtion-Based Scheme for Detecting Anomalous Nodes in WiReless Mesh Networks", In the Proceedings of the 2008 IEEE Wireless Communications & Networking Conference (WCNC 08) , Las Vegas, NV, USA, 2008 , pp. 2621-2626.

[30] F. Oliviero and S. P. Romano, "A Reputation-based Metric for Secure Routing in Wireless Mesh Networks", In the Proceedings of 2008 IEEE Global Communications Conference (GLOBECOM 2008), New Orleans, LO, USA, 30 November-4 December 2008, pp. 1-5.

[31] D. Bansal, S. Sofat, P. Pathak, S. Bhoot, "Detecting MAC Misbehavior Switching Attacks in Wireless Mesh Networks", International Journal of Computer Applications, vol. 26, no.5, July 2011, pp. 55-62.

[32] Y. Zhang, Y. Fang, "ARSA: An attack resilient security architecture for multihop wireless mesh network," IEEE Journal on Selected Areas in Communications, vol.24. no.10, October, 2006. pp. 1916-1928.

[33] X. Wang, J. S. Wong, F. Stanley and S. Basu," Cross-layer Based Anomaly Detection in Wireless Mesh Networks", In the Proceedings of the 9th Annual International Symposium on Applications and the Internet (SAINT 2009), Bellevue, WA, USA, 2009, pp. 9-15.

[34] A. Egners and U. Meyer, "Wireless Mesh Network Security: State of Affairs", In the Proceedings of the 6th IEEE Workshop on Security in Communication Networks (SICK 2010), Denver, Colorado, USA, 2010, pp. 997-1004.

[35] H.Jiacheng, L. Ning, Y. Ping, Z. Futai, and Z. Qiang, "Securing Wireless Mesh Network with Mobile Firewall", In the Proceedings of the IEEE 2010 International Conference on Wireless Communications and Signal Processing (WSCP 2010), Suzhou, China, 21-23 October 2010, pp. 1-6.

[36] F. A. Zdarsky, S. Robitzsch, A. Banchs, "Security analysis of wireless mesh backhauls for mobile networks", Journal of Network and Computer Applications, vol. 34, 2011, pp. 432–442.

[37] X. Wang, J. Wong, and W. Zhang, "A heterogeneity-aware framework for group key-management in wireless mesh networks", In the Proceedings of the 4th Interntional Conference on Security and Privacy in Communication Networks (SecureComm '08), Instabul, Turkey, 2008.

[38] Y. Fu, J. He, L. Luan, R. Wang, and G. Li, "A Zone-based Distributed Key Management Scheme for Wireless Mesh Networks", In the Proceedings of the 2008 32nd Annual IEEE International Computer Software and Applications Conference (COMPSAC '08), Turku, Finland, 28 July - 1 August 2008, pp. 68 – 71.

[39] J. Dong, K. Ackermann, and C. Nita-Rotaru, "Secure group communication in wireless mesh networks", Ad Hoc Networks, no. 7, vol. 8, 2009, pp. 1563–1576.

[40] S, Khan, Nabil ,A. Alrajeh, and K.-K. Loo, "Secure route selection in wireless mesh networks", Computer Networks, vol. 56, no. 2, 2012, pp. 491–503.

[41] F. Martignon, S. Paris, and A. Capone, "A Framework for Detecting Selfish Misbehavior in Wireless Mesh Community Networks" Q2SWinet'09, ,Tenerife, Canary Islands, Spain, 2009, pp. 65-72.

[42] F. Oliviero and S. P. Romano, "A Reputation-based Metric for Secure Routing in Wireless Mesh Networks", In the Proceedings of 2008 IEEE Global Communications Conference (GLOBECOM 2008), New Orleans, LO, USA, December 2008, pp. 1-5.

[43] S. Khan, K.-K. Loo, N. Mast, and T. Naeem, "SRPM: Secure Routing Protocol for IEEE 802.11 Infrastructure Based Wireless Mesh Networks", Journal of Network and Systems Management, vol. 18, no. 2, 2010, pp. 190–209.

[44] Y. Fu, J. He, R. Wang and G. Li, "Mutual Authentication in Wireless Mesh Networks", In the Proceedings of the IEEE International Conference on Communications (ICC), Beijing, China, 2008, pp. 1690 – 1694.

[45] S. Qazi, Y. Mu, and W. Susilo, "Securing Wireless Mesh Networks with Ticket-Based Authentication", In the Proceedings of the 2nd International Conference on Signal Processing and Communication Systems (ICSPCS 2008), Gold Coast, Australia, 2008, pp. 1-10.

[46] D. Bansal, and S. Sofat, "Securing IEEE 802.11 based Hybrid Wireless Mesh Networks", In the Proceedings of the 2010 International Conference on E-Health Networking, Digital Ecosystems and Technologies (EDT), vol. 1, 2010, pp. 431 – 435.

[47] J. Ben-Othman,. and Y.I.S. Benitez, "On Securing HWMP using IBC", In the Proceedings of the 2011 IEEE International Conference on Communications (ICC), Kyoto, Japan, 2011, pp. 1 – 5.

[48] J. Ben-Othman,. and Y.I.S. Benitez, "IBC-HWMP: a novel secure identity-based cryptography-based scheme for Hybrid Wireless Mesh Protocol for IEEE 802.11s", Concurrency and Computation Practice and Experience, 2011, DOI: 10.1002/cpe.1813.

[49] M. J. Lee, J. Zheng, Y.-B. Ko, and D. M. Shrestha, "Emerging Standards for Wireless Communications", IEEE Wireless Communications, vol. 13, no.2, 2006, pp. 56-63.

[50] F. Martignon, S. Paris, A. Capone, "DSA-Mesh: a Distributed Security Architecture for Wireless Mesh Networks, Wiley Security and Communication Networks, vol. 4, no. 3, 2011, pp. 242-256.

[51] F. Kandah, W. Zhang, X. Du, Yashaswi Singh, "A Secure Key Management Scheme in Wireless Mesh Networks", In the Proceedings of the 2011 IEEE Conference on Communications (ICC), Kyoto, Japan, 2011, pp. 1-5.

[52] S. M. Glass, V. Muthukkumurasamy and M. Portmann, "Detecting Man-in-the-Middle and Wormhole Attacks in Wireless Mesh Networks," In the Proccedings of the International Conference on Advanced Information Networking and Applications (AINA '09), Bradford, UK, 2009, pp. 530-538.

[53] S. Islam, A, Hamid, and C. S. Hong, "SHWMP: a secure hybrid wireless mesh protocol for IEEE 802.11s wireless mesh networks", Transactions on Computational Science, vol. 5730, Springer-Verlag Berlin Heidelberg. 2009 pp. 95-114.

[54] K. Ren, S. Yu, W. Lou, and Y. Zhang, "PEACE: A Novel Privacy-Enhanced Yet Accountable Security Framework for Metropolitan Wireless Mesh Networks", IEEE Transactions on Parallel and Distributed Systems, vol. 21, no. 2, 2010, pp. 203-215.

[55] C. Li, Z. Wang, and C. Yang, "Secure Routing for Wireless Mesh Networks", International Journal of Network Security, vol.13, no.2, 2011 pp.109–120.

[56] H. Lin, J. Ma, J. Hu and K. Yang, "PA-SHWMP: a privacy-aware secure hybrid wireless mesh protocol for IEEE 802.11s wireless mesh networks", EURASIP Journal on Wireless Communications and Networking, vol. 69, 2012.

[57] A. O. Durahim, E. Savaş, “A-MAKE: An Efficient, Anonymous and Accountable Authentication Framework for WMNs” , In the Proceedings of the 5th International Conference on Internet Monitoring and Protection (ICIMP), Barcelona, Spain, 2010, pp. 54-59.

[58] S. Khan, K.-K. Leo, Z. U. Din, “Framework for Intrusion Detection inIEEE 802.11 Wireless Mesh Networks”, The International Arab Journal of Information Technology, vol. 7, no. 4, 2010, pp. 435-440.

[59] L. Lazos and M. Krunz, “Selective Jamming/Dropping Insider Attacks in Wireless Mesh Networks”, IEEE Network,vol. 25, no.1, 2011, pp. 30-34.

[60] X. Wu and N. Li, “Achieving Privacy in Mesh Networks”, In Proceedings of the 4th ACM Workshop on Security of Ad Hoc and Sensor Networks (SASN '06), Alexandria, VA, USA, pp. 13-22.

[61] M. Reed, P. Syverson, and D. Goldschlag, “Anonymous Connections and Onion Routing”, IEEE Journal on Selected Areas in Communication, vol. 16, no. 4, 1998, pp. 482 – 494.

[62] J. Ben-Othman,. J.-P. Claude and Y.I.S. Benitez, “A Novel Mechanism to Secure Internal Attacks in HWMP Routing Protocol” In the Proceedings of the 2012 IEEE International Conference on Communications (ICC) Techical Symposium on Ad-Hoc And Sensor Networks, Ottawa, Canada, 2012.

[63] A. Boudguiga, M. Laurent, “An Authentication Scheme for IEEE 802.11s Mesh Networks Relying on Sakai-Kasahara ID-Based Cryptographic Algorithms”, Wireless and Mobile Computing, In the Proceedinds of the 2010 IEEE 6th International Conference on Networking and Communications (WiMob),Niagara Falls, 2010, pp. 256 – 263.

Figures

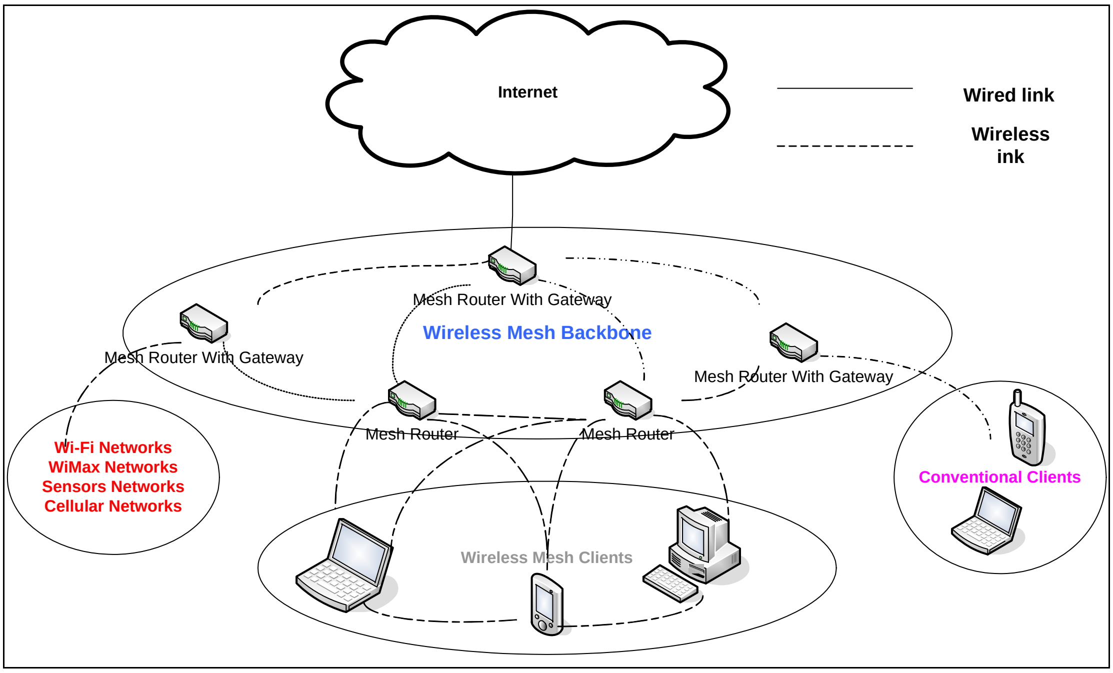

Figure 1 A Hybrid Wireless Mesh Architecture

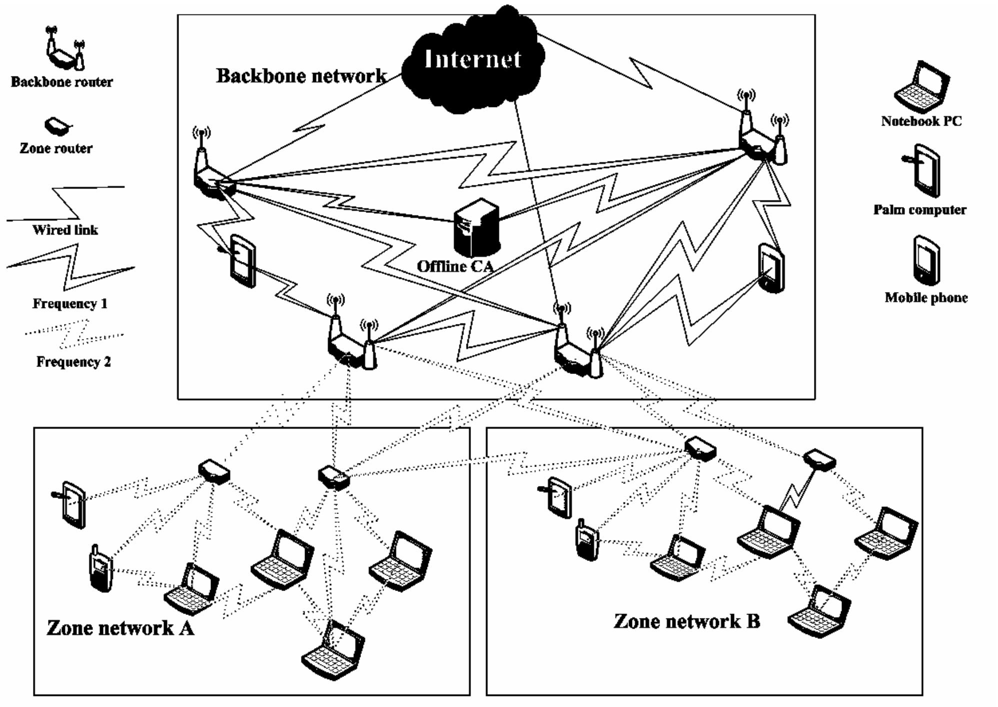

Figure 2 The Network Model

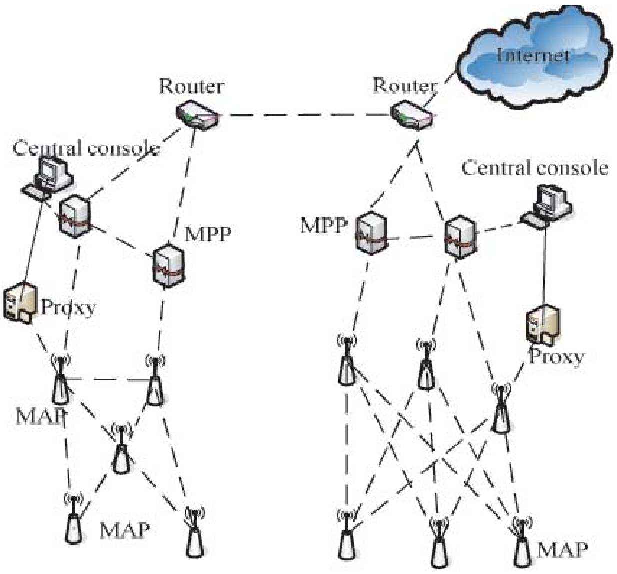

Figure 3 The WMN network structure [25]

Tables

Table I Wireless Mesh Standards

Types of Mesh Technology	IEEE Specification
WPAN mesh	802.15.5
WLAN mesh	802.11s
WMAN mesh	802.16a, 802.16e, 802.20

Table II Security Attacks Classification

Criteria	Classification				
Participation in the communication process	Passive		Active		
Position of the attacker within the network	External		Internal		
Benefit of the attacker	Rational		Malicious		
Method used	Impersonation	Modification	Fabrication	Replay	DoS
Protocol layer	Physical	MAC	Network	Transport	Application

Table III Wireless Security Risks ([11])

Protocol Layer	Threats
Application	Logic errors, buffer overflows, privilege escalation
Transport	DNS spoofing, session hijacking, traffic

	injection
Network	Black/gray/worm holes, misrouting, rushing attacks
Data-link	Traffic flooding, virtual jamming, man- in-the-middle
Physical	Collision jamming, device tampering

Table IV IDSs systems overview

IDS	Architecture	Attacks Detected
Bansal et al. [31]	Distributed	The oversized NAV attack, the reduced backoff attack, the switching between these two attacks
Zhou et al. [27]	Distributed	Sinkhole attack, wormhole attack
Hugelshofer et al. [28]	Distributed	Resource starvation attacks, mass mailing of internet worms, IP spoofing
Zang et al. [29]	Distributed	Malicious behavior of a node, DOS Attack, Routing Loop Attack
Martignon et al. [41]	Distributed	Selfish behavior of a node, bad-mouthing attack
Yang et al. [25]	Hierarchical	Routing attacks
Khan et al. [58]	Cooperative and Hierarchical	MAC spoofing, selfishness, flooding and routing misbehaviours