Securing Wireless Mesh Networks

Naouel Ben Salem Jean-Pierre Hubaux

Laboratory of Computer Communications and Applications (LCA)
EPFL – Lausanne, Switzerland
naouel.bensalem@epfl.ch jean-pierre.hubaux@epfl.ch

Abstract

Using Wireless Mesh Networks (WMNs) to offer Internet connectivity is becoming a popular choice for Wireless Internet Service Providers as it allows a fast, easy and inexpensive network deployment. However, security in WMNs is still in its infancy as very little attention has been devoted so far to this topic by the research community. In this paper, we describe the specifics of WMNs and we identify three fundamental network operations that need to be secured.

1 Introduction

Wireless Mesh Networks (WMNs) represent a good solution to providing wireless Internet connectivity in a sizable geographic area; this new and promising paradigm allows for network deployment at a much lower cost than with classic WiFi networks. As shown in Figure 1 (a), a large number of Wireless Hot Spots (WHSs) is needed to deploy a WiFi network; extending further the network coverage requires the deployment of additional WHSs, which is costly and delicate. In WMNs, it is possible to cover the same area (or even a larger one) with only one WHS and several wireless Transit Access Points (TAPs) (see Figure 1 (b)). The TAPs are not connected to the wired infrastructure and therefore rely on the WHS to relay their traffic. The cost of a TAP is much lower than that of the WHS, which makes the use of WMNs a compelling economical case; WMNs are thus suitable for areas where it is costly to install a traditional WiFi network (e.g., buildings that do not have existing data cabling for WHSs) or for the deployment of a temporary wireless network.

WMNs, however, are not yet ready for wide-scale deployment due to two main reasons. First of all, the communications being wireless and therefore prone to interference, WMNs present severe capacity and delay constraints [1]. Nevertheless, there are reasons to believe that technology will be able to overcome this problem, e.g., by using multi-radio and multi-channel TAPs [2]. The second reason that slows down the deployment of WMNs is the lack of security guarantees, which is the topic of this paper: we identify the security challenges introduced by WMNs by analyzing the specifics of this new kind of networks. This analysis leads us to the identification of three fundamental operations that have to be secured in WMNs. We discuss the security challenges introduced by the interworking of several networks belonging to different operators and we present a special example of WMNs: Vehicular networks.

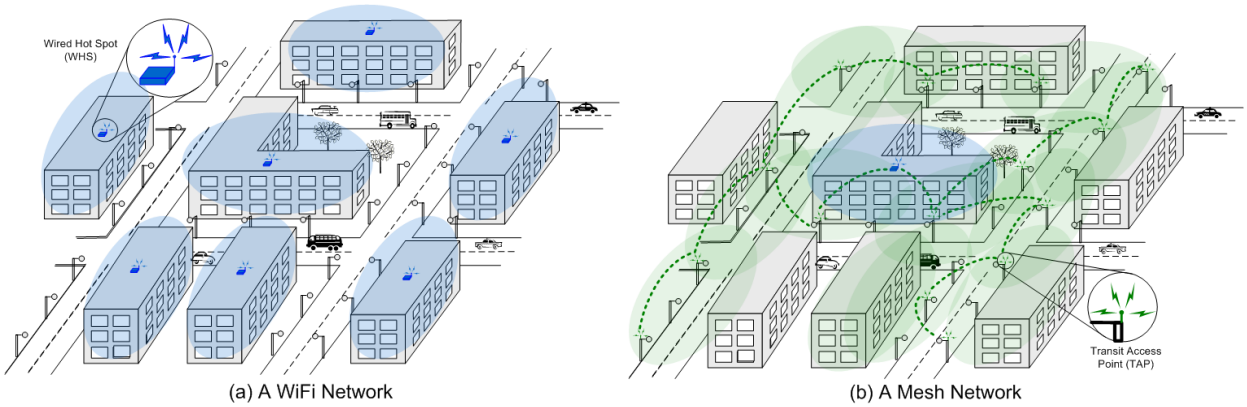

Figure 1: Two approaches to providing Internet connectivity. (a) WiFi Network: several Wireless Hot Spots (WHSs) are needed to offer good coverage of a given area; (b) Wireless Mesh Network (WMN): by using one WHS and several Transit Access Points (TAPs), it is possible to cover the same area as in (a); the TAPs rely on the WHS to transmit their traffic to and from the Internet.

2 Characteristics of WMNs

WMNs represent a new network concept and therefore introduce new security specifics. Here, we describe these specifics by giving an overview of the fundamental differences between WMNs and two well-established infrastructure-based technologies: cellular networks and the Internet.

Difference between WMNs and Cellular Networks The major difference between WMNs and cellular networks - besides the use of different frequency bands (WMNs usually make use of unlicensed frequencies) - concerns the network configuration: In cellular networks, a given area is divided into cells and each cell is under the control of a base station. Each base station handles a certain number of mobile clients that are in its immediate vicinity (i.e., communication between the mobile clients and the base station is single-hop) and it plays an important role in the functioning of the cellular network; the entity that plays an equivalent role in WMNs would be the WHS.

However, whereas all the security aspects can be successfully handled by the base station in cellular networks, it is risky to rely only on the WHS to secure a WMN, given that the communications in WMNs are multi-hop. Indeed, centralizing all security operations at the WHS would delay attack detection and treatment and therefore would give the adversary an undeniable advantage. Furthermore, multi-hopping makes routing in WMNs a very important and necessary functionality of the network; and like all critical operations, an adversary may be tempted to attack it. The routing mechanism must thus be secured.

Multi-hopping has also an important effect on the network utilization and performance. Indeed, if the WMN is not well-designed, a TAP that is several hops away from the WHS would receive a much lower bandwidth share than a TAP that is next to it. This leads to severe unfairness problems, and even starvation [1]; it thus can be used by an adversary to disturb the functioning of the WMN.

Note that multi-hopping is also the main difference between WMNs and WiFi networks, which means that the security problems we already identified and that are related to multi-hop communications are the main security challenges introduces by WMNs, in comparison with WiFi networks.

Difference between WMNs and the Internet In WMNs, the wireless TAPs play the role that is played, in the classic (wired) Internet, by the routers. Given that wireless communications are vulnerable to passive attacks such as eavesdropping, as well as to active attacks such as Denial of Service (DoS), WMNs are subject to all these attacks whose effects are amplified by the multi-hop aspect of the communications.

Another fundamental difference between the Internet and WMNs is that, unlike Internet routers, the TAPs are not physically protected. Indeed, they are most often in locations that are accessible to potential adversaries, e.g., deployed on rooftops or attached to streetlights. The absence of physical protection of the devices makes WMNs vulnerable to some serious attacks. Indeed, one very important requirement regarding the TAPs - for the concept of mesh networks to remain economically viable - is their low cost that excludes the possibility of strong hardware protection of the devices (e.g., detection of pressure, voltage, or temperature changes) [3]. Therefore, attacks such as tampering, capture or replication of TAPs are possible and even easy to perform.

This brief analysis of the characteristics of WMNs clearly shows that, compared with other networking technologies, the new security challenges are mainly due to the multi-hop wireless communications and by the fact that the TAPs are not physically protected. Multi-hopping delays the detection and treatment of the attacks, makes routing a critical network service and may lead to severe unfairness between the TAPs, whereas the physical exposure of the TAPs allows an adversary to capture, clone or tamper with these devices.

3 Security Challenges of WMNs

Before discussing the details of the security challenges in WMNs, let us give an example of a simple and typical communication in WMNs: Figure 2 shows a branch of a WMN where a mobile client MC is within the transmission range of TAP_3 and therefore relies on it to get Internet connectivity; the data generated and received by the MC goes through TAP_1, TAP_2 and WHS. Let us consider an upstream message, i.e., a message generated by the MC and sent to the Internet. Before this message reaches the infrastructure, several verifications need to be performed successfully.

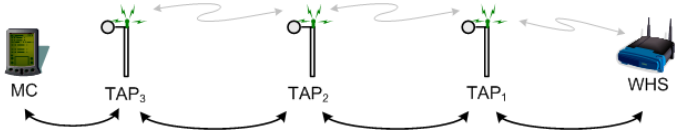

Figure 2: A typical communication in WMNs: The mobile client MC is within the transmission range of TAP_3 and relies on TAP_1 and TAP_2 to relay its traffic to and from WHS.

First of all, as Internet connectivity is a service that (usually) the MC has to pay for, TAP_3 needs to authenticate the MC in order to perform the billing correctly. This authentication can be done in different ways: For example, using a temporary billing account (e.g., credit card based authentication), a predefined shared secret (if the MC is a client of the operator managing TAP_3), or a roaming system similar to the one used in cellular networks (if it is not a client of that operator); the latter has the advantage of preserving the anonymity of the MC with respect to the foreign operator. Note that we want to avoid, if possible, the use of asymmetric cryptographic operations by the MC. In fact, the MC being battery operated, the authentication has to be energy efficient, which makes the use of public key cryptography primitives unsuitable; these primitives have a high computational overhead and are prone to DoS attacks. Indeed, if the authentication

protocol requires the computation or the verification of a signature, this feature can be misused by an adversary that can continuously ask the MC to compute or verify signatures; this attack can drain MC's battery.

A second verification that has to be made is the mutual authentication of the network nodes (i.e., the TAPs and the WHS). We differentiate between the authentication of the nodes at the initialization (or re-initialization) phase and during the session established by the MC (i.e., during the sending and receiving of the packets of the MC).

The initialization phase takes place when the WMN is first deployed, whereas the re-initialization phase takes place when a reconfiguration of the network is needed (e.g., after the detection of attacks). The TAPs and the WHS are energy-rich and thus can use asymmetric key cryptography to perform authentication. Therefore, for the authentication of the nodes at the initialization (or re-initialization) phase, we can assume that the TAPs and the WHS have each a certified public/private key pair that is assigned to them by the operator that is managing them. These public/private key pairs are used to mutually authenticate the nodes. This assumption is reasonable, given that the size of the WMN is relatively small and that this operation is done only occasionally. Note that the MC can use TAP_3's certified public key to authenticate it during session establishment.

The mutual authentication of the nodes during the session is different: the messages generated or received by the MC are sent using multi-hop communications and the use of public key cryptography to authenticate the sender and/or the receiver of each and every packet is a heavy process that introduces important delays and therefore leads to a suboptimal utilization of the network resources. Public key cryptography is thus not suitable in this case. Instead, the nodes can rely on symmetric key cryptography, using session keys they establish during the initialization (or re-initialization) phase or long-term shared keys that are originally loaded in the devices. If the authentication of the nodes is required at each intermediate TAP, a possible solution consists in establishing or predefining symmetric keys between neighboring TAPs; these keys would be used, typically to compute Message Authentication Codes (MACs) on the exchanged messages[1] and therefore to authenticate the nodes involved in the communication hop by hop. Otherwise, if the authentication is required only at the WHS (at TAP_3 if we are considering a downstream message, i.e., a message sent from the Internet to the MC), the symmetric keys can be established or predefined between each TAP and the WHS and used to compute MACs on the exchanged messages.

Once the mobile client and the nodes are authenticated, it is necessary to verify the integrity of the exchanged messages. This verification can be done end-to-end (i.e., by the WHS for upstream messages and by the MC for the downstream messages) or by each intermediate TAP, or both. A possible way to do this verification is for the nodes to establish a symmetric key with the MC at the establishment of the session; the MC uses this key to protect the message (e.g., using MAC). This key can also be used to encrypt the message if data confidentiality is a requirement.

3.1 Three Fundamental Security Operations

Our study of WMNs' specifics led to three critical security challenges: (i) detection of corrupt TAPs, (ii) securing the routing mechanism, and (iii) definition of a proper fairness metric to ensure a certain level of fairness in the WMN. These challenges are not the only important ones that should

[1]MACs are usually used to verify the integrity of a message, but they can also be used to authenticate the sender of the message. Indeed, assume that two parties A and B share a symmetric key k. A can generate a message m, use k to compute a MAC on it and then send both m and the corresponding MAC to B. Upon receipt of these data, B can use k to compute the MAC on m and compare it to the MAC it received; if the two MACs are identical, and given that A and B are the only two parties that know k, B can conclude that m was indeed generated by A. This authentication technique is weaker than the one that uses asymmetric key cryptography, but it is efficient.

be considered because other network functionalities also need to be secured (e.g., MAC protocols, nodes' location, etc.). We choose to focus however on these three challenges as they are, in our opinion, the most critical for WMNs.

3.1.1 Detection of Corrupt TAPs

As explained previously, mesh networks typically employ low-cost devices that cannot be protected against removal, tampering or replication. An adversary can thus capture a TAP and tamper with it. Note that if the device can be remotely managed, the adversary does not even need to physically capture the TAP: A distant hacking into the device would work perfectly. The WHS plays a special role in the WMN and may handle or store critical cryptographic data (e.g., temporary symmetric keys shared with the mobile clients, long-term symmetric keys shared with the TAPs, etc.); therefore, we assume that the WHS is physically protected.

We identify four main attacks that may be performed on a compromised device, depending on the goals the adversary wants to achieve: The first attack consists in the simple removal or replacement of the TAP in order to modify the network topology to the benefit of the adversary. This attack can be detected by the WHS or by the neighboring TAPs when a brutal and permanent topology change is observed in the network.

The second attack consists in accessing the internal state of the captured device without changing it. The detection of this passive attack is difficult, given that no state change is operated on the TAP; disconnecting the device from the WMN may not be required for the adversary to successfully perform the attack; and even if a disconnection were required, the "absence" of the device may not be detected, as it can be assimilated to some congestion problem. If this attack is successful, it guarantees to the adversary the control of the corrupt TAP and a perfect analysis of the traffic going through it. This attack is more serious than simple eavesdropping on the radio channel in the sense that the adversary, by capturing the TAP, can retrieve its secret data (e.g., its public/private key pair, the symmetric key shared with the neighboring TAPs or with the WHS, etc.) and can use these data to compromise, at least locally, the security of the WMN, especially data confidentiality and integrity, and clients anonymity. Unfortunately, there is no obvious way to detect this attack. However, a possible solution that mitigates its effect is a periodic erasure and reprogramming of the TAPs; the adversary is then obliged to compromise the device again.

In the third attack, the adversary modifies the internal state of the TAP such as the configuration parameters, the secret data, etc. The purpose of this attack can be, for example, to modify the routing algorithm at the captured node in order to change the network topology. This attack can be detected by the WHS using a verifier such as the one presented in [4].

Finally, the fourth attack consists in cloning the captured device and installing replicas at some strategically chosen locations in the mesh network, which allows the adversary to inject false data or to disconnect parts of the WMN. This attack can seriously disrupt the routing mechanism, but it can be detected using the mechanism introduced in [5].

3.1.2 Secure Multi-hop Routing

By attacking the routing mechanism, an adversary can modify the network topology and therefore affect the good functioning of the network. The reasons behind the attacks can be numerous: The attack can be *rational*, i.e., the adversary misbehaves only if misbehaving is beneficial in terms of price, obtained quality of service or resource saving; otherwise it is *malicious*. For example, a malicious adversary may want to partition the network or to isolate a given TAP or a given geographic region, whereas a rational adversary may want to force the traffic through a specific TAP

in the network (e.g., through a TAP that it has compromised) in order to monitor the traffic of a given mobile client or a region. Another example would be for the adversary to artificially lengthen the routes between the WHS and the TAPs, which would seriously affect the performance of the network. This attack can be rational if it is performed against a competitor for example.

To attack the routing mechanism, the adversary can (i) tamper with the routing messages, (ii) modify the state of one or several TAPs in the network, (iii) use replicated node(s), or (iv) perform DoS attacks:

(i) To prevent attacks against the routing messages, the operator can use one of the proposed secure routing protocols for wireless multi-hop networks [6].

(ii) If the adversary chooses to modify the state of one or several TAPs in the network, the attack can be detected using [4] and the operator can reconfigure the WMN accordingly.

(iii) If the adversary uses replicated node(s), the attack can be detected as the operator will realize that the network topology is not the one it originally deployed; it can therefore disable the rogue devices or install new ones [5].

(iv) Finally, DoS attacks represent a simple and efficient way to attack routing. These attacks are very harmful as they are simple to perpetrate and impossible to prevent. Indeed, the adversary can disturb the communications between the TAPs in a given area and force the reconfiguration of the network. In order to solve this problem, the operator has to identify the source of disturbance [7] and, if possible, disable it.

Note that, except for the first attack, solving all these attacks requires human involvement (i.e., to go to the field and install/remove TAPs or jamming devices), which may be considered a successful attack as such.

3.1.3 Fairness

In WMNs, all the TAPs use the same WHS as a relay to and from the infrastructure and therefore the throughput obtained by the TAPs can vary significantly depending on their position in the WMN. Indeed, as shown in [1], the TAPs that are more than two hops away from WHS may starve (i.e., their clients are not able to send or receive traffic), which is highly unfair. The study conducted in [1] identifies the problem and proposes a solution that guarantees a TAP-fair share of the bandwidth. However, a TAP-based fairness is not necessarily the best solution for WMNs. Indeed, consider as an example the one-dimensional WMN presented in Figure 3; a per-TAP fairness policy leads to flows 1, 2 and 3 having each the same share of the bandwidth, without taking into consideration the number of clients that are served by each of these TAPs. We believe that the bandwidth sharing should be fair client-wise, because the purpose of a mesh network is to offer a service (typically Internet connectivity) to the mobile clients that are usually paying the same flat rate. That is why, in the example of Figure 3, flow 2 should have half as much as what flow 1 and flow 3 have, as TAP2 is serving only one client, whereas TAPs 1 and 3 are serving two clients each.

The fairness issue is closely related to the number of hops between the TAPs and the WHS; this means that if the adversary manages to increase the number of hops between a given TAP and the WHS, it can decrease dramatically the bandwidth share of this TAP. A possible solution against this attack can be a periodic reconfiguration of the WMN; given that the WHS and the TAPs are static, the operator can define - based on the traffic in the WMN - the optimal configuration of the WMN and force the routes at the TAPs to the optimal routes. Once the network has an optimal

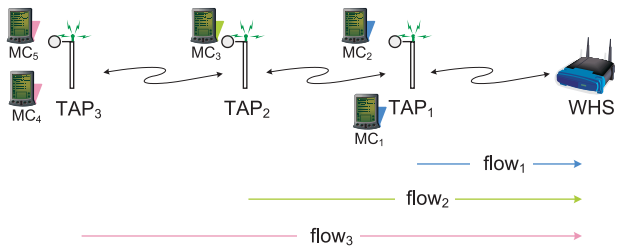

Figure 3: The fairness problem. In order to define the bandwidth sharing, it is important to take into consideration the number of mobile clients served by each of the TAPs. Flow 2 should thus have half as much as what flow 1 and flow 3 have, as TAP2 is serving only one client, whereas TAPs 1 and 3 are serving 2 clients each.

configuration, it is possible to use the scheduling presented in [8] to ensure per-client fairness and to optimize the bandwidth utilization in the WMN.

3.2 Two Attack Examples

In order to illustrate the attacks described so far, we give two attack examples that an adversary may perpetrate against the WMN (see Figure 4 (a)). In the first attack, the adversary corrupts TAP_2 (the TAP marked in red), whereas in the second attack, it performs a DoS attack - based on jamming - on the communication link between TAP_5 and TAP_6. Note that we assume the two attacks to be performed by the same adversary, which represents the worst case (as it gives more power to the adversary).

The motivation behind these attacks can be the following: On the one hand, by corrupting TAP_2, the adversary can retrieve its secret data and therefore can compromise the integrity and confidentiality of the data going through it, as well as the anonymity of the mobile clients attached to TAP_2, TAP_3 and TAP_4. On the other hand, the DOS attack is a very simple and efficient way to partition the WMN and force a network reconfiguration.

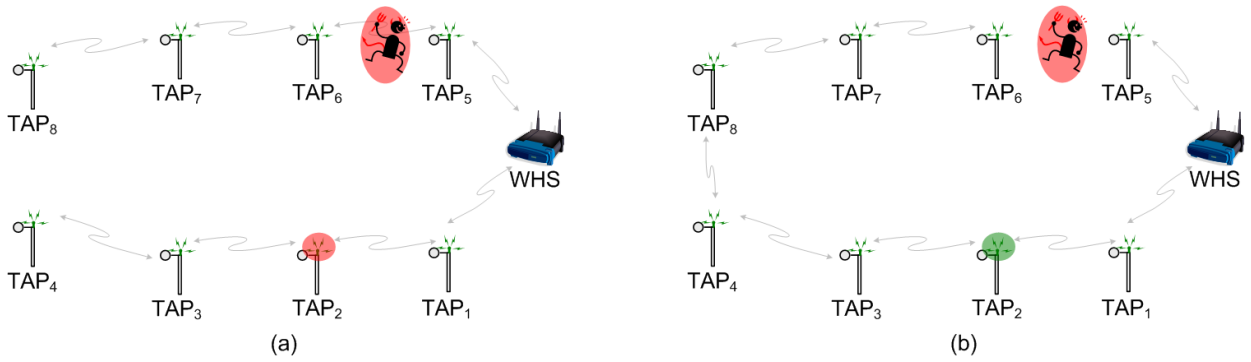

Figure 4: Two attacks and the related countermeasures: In (a), the adversary corrupted TAP_2 and placed a jamming station between TAP_5 and TAP_6. As shown in (b), the detection of these attacks, if it is possible, leads to the reconfiguration of the WMN: the operator replaced the compromised TAP (the TAP circled in red in (a)) by an uncorrupted one (the TAP circled in green in (b)) and updated the routing. In this example, the reconfiguration leads to much longer routes for some TAPs (e.g., TAP_6 was 2-hops away from the WHS and is now 7-hops away).

It is imperative to detect these attacks in order to react accordingly. A possible reaction to the corrupt TAP attack can be the replacement, by the network operator, of the compromised TAP_2 (circled in red in Figure 4 (a)) by an uncorrupted one (circled in green in Figure 4 (b)). The detection and disabling of the jamming station can be more delicate. Indeed, finding the exact

location of this station can be difficult and, even if it is found, the network operator may not have the right to disable it (e.g., both the WMN and the jamming station are operating in unlicensed band); in this case, a network reconfiguration is required. This connectivity change affects the routing and can increase the number of hops from a given TAP to the WHS (e.g., in Figure 4, TAP_6 was 2-hops away from the WHS but after the network reconfiguration, it is 7-hops away), which, as shown previously, can dramatically affect the performance of the WMN. Note that the operator can decide to abandon a given TAP location if it is particularly exposed (i.e., the TAP that is in this location is repeatedly corrupted), in which case it may be necessary to deploy additional devices to make up for the coverage gap.

4 Generalized WMNs

In order to make our presentation as easy as possible to follow, we have focused so far on the "classic" definition of WMNs. However, WMNs are in reality a much broader concept. In this section, we present two special cases of WMNs and we briefly describe the security challenges they introduce.

4.1 Vehicular Networks

So far, we have assumed the TAPs to be static. Vehicular networks represent a special case of WMNs that consists of a set of mobile TAPs (represented by the cars) and of roadside WHSs. The spectrum of applications offered by a vehicular network is wide ranging: It goes from safety-related applications such as reporting important events (e.g., an accident, see Figure 5) or traffic optimization through cooperative driving (e.g., deviate the traffic to avoid a traffic jam) to payment services (e.g., electronic toll collection) and location-based services (e.g., targeted marketing).

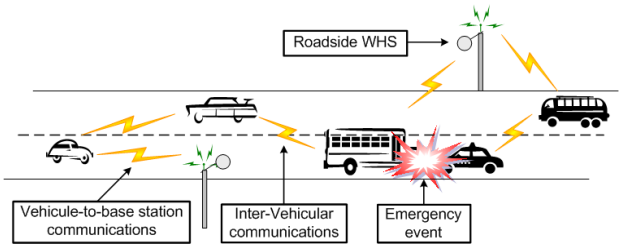

Figure 5: A very special WMN: The Vehicular Network. It consists of a set of cars and roadside WHSs that exchange messages to report some important events or offer services to the drivers.

In addition to the security requirements introduced by WMNs - typically mutual authentication of the different devices (cars and roadside WHSs) and data integrity and confidentiality - vehicular networks introduce some specific requirements, e.g., the need for secure and accurate positioning information or real-time constraints (the report about an important event should not be delayed). In addition, nodes' mobility makes the definition and implementation of some (distributed) network operations more delicate (e.g., a secure routing mechanism or an efficient fairness metric). Moreover, as each car belongs to a different person that can act selfishly and tamper with the embedded devices, the protection of these devices becomes an important issue. Responses to some of these new challenges are presented in [9].

4.2 Multi-operator WMNs

So far, we have assumed the WMN to be managed by a single operator, but a mesh network can also designate a set of wireless devices belonging to different networks and controlled by different operators. These devices can be as various as access points, base stations, laptops, vehicular nodes or mobile phones (see the example given in Figure 6) and their aggregation leads to an unplanned mesh network with interesting properties [10].

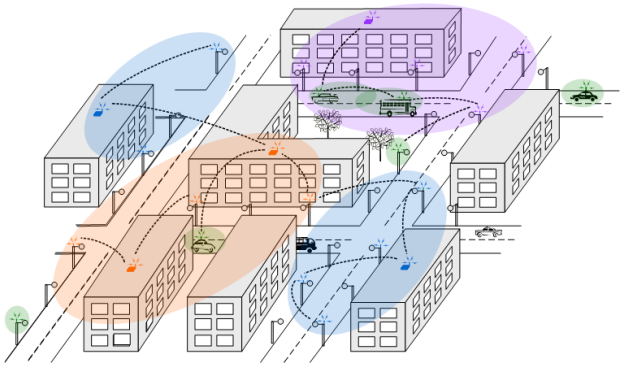

Figure 6: A multi-operator WMN: In this example, three WMN operators (the devices managed by each of them are represented in different colors: blue, purple and orange) and one vehicular network operator (represented in green) coexist in the network.

Whether the WMN is under the control of a single or more operators, the reasoning behind the choice of such a network remains the same: it allows for an easy, fast and inexpensive network deployment. Ensuring security however is more delicate when several operators coexist in the network. Indeed, to the security challenges already identified in this paper, one has to add challenges such as the mutual authentication of nodes belonging to different "operating domains" or the application of different charging policies for each of these domains (which affects even more fairness).

Another important security challenge results from the utilization of the same spectrum by the different operators. Indeed, if we assume that a mobile client can freely roam across TAPs that are managed by different operators and that it attaches to the neighboring TAP with the strongest signal, each operator can be tempted to configure its TAPs to always transmit at the maximum authorized level (and thus make sure that it is heard by the maximum number of mobile clients); this situation can lead to a bad performance of the WMN [11] but can be solved using Multi-radio/Multi-Channel (MR-MC) TAPs in the WMN. Note that the use of MR-MC TAPs can also mitigate the effect of the DoS attack; instead of jamming a single channel, the adversary has to jam all the channels used by a given node to completely disable it.

5 Conclusion

WMNs represent a simple and inexpensive solution to extend the coverage of a WHS. However, the deployment of such networks is slowed down by the lack of security guarantees. In this paper, we have analyzed the characteristics of WMNs and have deduced three fundamental network operations that need to be secured: (i) the detection of corrupt TAPs, (ii) the definition and use of a secure routing protocol, and (iii) the definition and enforcement of a proper fairness metric in WMNs. We have proposed some solutions to secure these operations. Finally, we have described two future WMNs (vehicular networks and multi-operator WMNs) and briefly analyzed the new security challenges they introduce.

Acknowledgments

The authors would like to thank Virgil Gligor for his valuable comments. Thanks also to Mario Čagalj, Márk Félegyházi, Jacques Panchard and Maxim Raya for their useful feedback.

References

[1] V. Gambiroza, B. Sadeghi, and E. Knightly. "End-to-End Performance and Fairness in Multihop Wireless Backhaul Networks". In *Proceedings of MobiCom*, 2004.

[2] M. Kodialam and T. Nandagopal. "Characterizing the Capacity Region in Multi-Radio Multi-Channel Wireless Mesh Networks". In *Proceedings of MobiCom*, 2005.

[3] R. Anderson and M. Kuhn. "Tamper Resistance - a Cautionary Note". In *The Second USENIX Workshop on Electronic Commerce Proceedings*, 1996.

[4] A. Seshadri, A. Perrig, L. van Doorn, and P. Khosla. "SWATT: SoftWare-based ATTestation for Embedded Devices". In *Proceedings of IEEE Symposium on Security and Privacy*, 2004.

[5] B. Parno, A. Perrig, and V. Gligor. "Distributed Detection of Node Replication Attacks in Sensor Networks". In *Proceedings of IEEE Symposium on Security and Privacy*, 2005.

[6] Y.-Ch. Hu and A. Perrig. "A Survey of Secure Wireless Ad Hoc Routing". *IEEE Security and Privacy, special issue on Making Wireless Work*, vol. 2, no. 3, 2004.

[7] W. Xu, W. Trappe, Y. Zhang, and T. Wood. "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks". In *Proceedings of MobiHoc*, 2005.

[8] N. Ben Salem and J.-P. Hubaux. "A Fair Scheduling for Wireless Mesh Networks". In *Proceedings of WiMesh*, 2005.

[9] M. Raya and J.-P. Hubaux. "The Security of Vehicular Ad Hoc Networks". In *Proceedings of SASN*, 2005.

[10] J. Bicket, D. Aguayo, S. Biswas, and R. Morris. "Architecture and evaluation of an Unplanned 802.11b Mesh Network". In *Proceedings of MobiCom*, 2005.

[11] M. Felegyhazi and J.-P. Hubaux. "Wireless Operators in a Shared Spectrum". In *Proceedings of InfoCom*, 2006.