Security Issues in an Established Autonomous Wireless Network

Kyriakos Zarifis[+], Dimitris Ztoupis[+], Christos Xenakis[*]
[+]Department of Informatics and Telecommunication, University of Athens, Greece
[*]Department of Technology Education and Digital Systems, University of Piraeus, Greece
E-mail: std02133@di.uoa.gr, std02004@di.uoa.gr, xenakis@unipi.gr

***Abstract* – This work describes the nature, architecture and functionality of one of the largest Wireless Community Networks(WCN), Athens Wireless Metropolitan Network. In addition, it analyses the most common and important attacks that can be carried out on such an autonomous network.**

I. INTRODUCTION

Athens Wireless Metropolitan Network (AWMN) is a wireless community that started forming in 2002. Currently there are 1700 active nodes in the Attica area, while 2500 more have shown interest in connecting to the network and are awaiting its expansion. As a result, AWMN is today one of the largest wireless network communities on Earth. The network is not a product or a service but rather a place of education, research, entertainment and experimentation, providing a wide variety of services such us mail, FTP, web hosting and game servers, VOIP, P2P file sharing, etc. It is described by its strictly non-profit character and relies on private initiative and private means. There is no subscription or any other type of fee and participation is open to anyone, so the network functions more in a best-effort manner rather than 'satisfaction guaranteed'.

Network architecture: The network architecture of AWMN is described in fig. 1.AWMN is composed of the backbone (BB) network and the access network. The BB network consists of BB nodes, which are responsible for routing any transferred data. BB links that connect BB nodes implement the 802.11a standard. Each BB node usually has more than one or two BB links. Thus, local loops or star topologies are created within the core network, resulting in a final *complex topology*. Based on the number of the established connections, AWMN BB nodes are divided in three categories: (i) nodes with more than two active BB links (Cx category), (ii) nodes with two active BB links (Bx category), and (iii) nodes with one BB link (Ax category). Currently there are approximately 650 active BB nodes.

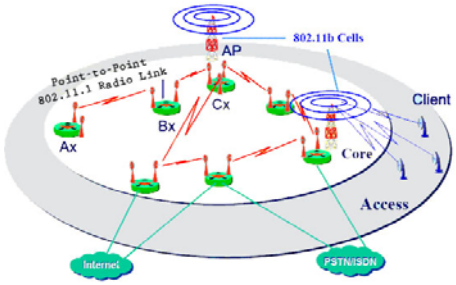

Fig.1: AWMN Topology

Apart from the BB network, the BB nodes also set up the wireless access network by establishing Access Points (AP) for wireless clients. In the access network the connections between the APs and clients implement the 802.11b standard. Based on the analyzed network topology, there is a peer to peer relationship among BB nodes in the BB network, and a hierarchical relationship between the BB nodes that act as APs and the wireless clients in the access network. Currently, there are about 1050 client nodes.

IP Addressing: AWMN uses *Class A private IP addresses* (10.0.0.0-10.255.255.255) as a pool for organizing and distributing IP addresses. IP range 10.0.0.0-10.90.197.255 is reserved for the prefecture of Attica and AWMN. That range is split into even smaller groups that are assigned to municipalities. Every node that has at least 2 BB links (Bx/Cx) is entitled one C-Class subnet. A node can apply further subnetting to its subnet, depending on the requirements of its local network but also the needs of its clients. A DHCP server usually runs on the AP node, using the node's C-Class subnet as a pool for assigning IPs to its clients.

Routing: The routing protocol currently used in AWMN is the Border Gateway Protocol [BGP]. BGP is used to exchange network reachability information between AWMN's *Autonomous Systems* (AS). An AS is a network or group of networks under the control of one entity, that follows a common routing policy. In most of the cases, every BB node sets up a different AS. An AS is identified by a unique AS number which is equal to the BB node's ID number.

BGP uses four types of control messages:

- The O*pen message*, which is sent after a TCP connection is opened.
- The *Keepalive* message, which is sent to a node's neighbours every 60 seconds in order to keep the connection open
- The *Notification message*, used to notify a peer that an error has occurred, or that the sender is ready to close the BGP connection.
- The BGP *Update message,* which exchanges routing information. The most important fields of this message are: the *Network Layer Reachability Information* field *(NLRI)*, the *AS_Path* attribute in the *Path Attributes* field and the *Withdrawn Routes* field (see fig.2). When a BGP connection is established, a BB node *originates* an update message advertising one or more *IP prefixes* to its peers. These *prefixes* aggregate the addresses assigned to hosts and devices within the originator's AS, including possible wireless clients. In this message, the NRLI lists the IP prefixes that are reachable through the originator. The *AS_Path* field holds the originating router's AS Number. When the peers receive the update message they add their own AS number to the AS_Path and forward the message to their other neighbors. When a node receives an update message, it re-calculates the best route to a specific IP prefix, updates its routing table, and advertises that route only. Usually the route with the least AS numbers is preferred. Thus, BGP routing tables maintain the Autonomous Systems that a packet must traverse in order to reach the destination system. Whenever a node needs to cancel an advertisement of a route that is no longer available, it sends an update message with the specific IP prefix in the *Withdrawn Routes* field to its peers.

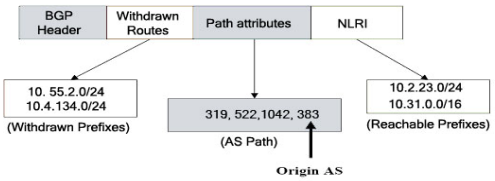

Fig.2: A BPG update message. In this example, the node with ID 383 has sent a message advertising that it can reach the subnets 10.2.23.0/24 and 10.31.0.0/16. This message has been processed and forwarded by nodes 1042, 522 and 319. The message also indicates that node 383 has lost connectivity with subnets 10.55..2.0/24 and 10.4.134.0/24.

This work has been supported in part by the project CASCADAS (IST-027807) funded by the FET Program of the European Commission and the project NoE CONTENT (IST-384239)

II Security Considerations

AWMN is a rapidly expanding network that hosts services and functionalities similar to those on *the Internet*. Furthermore there are gateways linking it to the Internet. Consequently, AWMN has to deal with any kind of security risk that can be found on the internet, be it an application bug or equipment exploits such as router software exploits or misconfigurations. In addition, being a *wireless network, AWMN* is susceptible to any kind of malicious attack wireless technology can undergo. The physical medium is the air which can be accessed by anyone who is between or close to a link. Lastly but maybe most importantly, AWMN is an *experimental network*. That means that so far secure activities rely solely on the members' earnestness. Anyone can become a BB node, and in other words, a router. In the classical wired networks, routing is the responsibility of providers' routers, which are monitored by operators. These companies follow some standards which provide security. Thus, there is a guarantee that a packet will be forwarded, without being eavesdropped, modified etc. This, however, is not the case here. Due to the community based, educational and open source character of the network, the users do not feel the need to address security concerns aggressively. This attitude, although understandable at this stage of development, has the side effect of increasing the network's overall vulnerability even more. Until today no actual security measure has been taken, and data transfer is far from secure, making the network open to all but the most primitive of attacks.

II. Attacks and Risk Analysis

Attacks in AWMN can be carried out from foreign sources (external attack) as well as nodes belonging to the network (internal attack) and can be further divided into *passive* attacks and *active* attacks. A passive attacker is granted access to non-authorized information, without altering it. On the other hand, an active attacker can alter, dump or replay other nodes' (control or data) messages. Finally, attacks can aim at any network layer.

Based on the three basic factors that define risk (Criticality, Vulnerability, Threat), the potential attacks against AWMN are presented and analyzed. Rather than assigning values to these factors, their weight is described through the attacks' presentations:

Passive Eavesdropping: These allow attackers to listen to conversations between network nodes. Packets are not encrypted so any internal or external node between or close to a link can achieve this with a sniffer. Apart from compromising user data confidentiality, the attacker can get valuable network information needed for other attacks such as valid MAC/IP addresses and network topology.

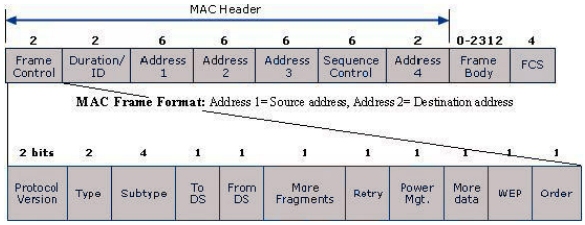

Fig.3: Frame Control Field: Type and Subtype determines the function of the frame. There are three different frame type fields: *Control*, *Data* and *Management.* Authentication frame: Type=0x00, Subtype=0x0B. Deauthentication frame: Type=0x00, Subtype=0x0C

Authentication - Deauthentication attack: This attack can be carried out by external nodes on either client-AP or BB links. AWMN uses *MAC filtering*. This means that when a client wants to connect to an AP, it sends an *authentication frame* (see fig.3) to it. This frame holds the client's MAC address in the *Address 1* field. The AP holds the MAC address of its known clients. When the AP receives the authentication frame, it checks if the *Address 1* value exists on that list. If so, the client is authenticated. Deauthentication works accordingly. Thus, an attacker can sniff the MAC address of a client-target and send a spoofed DEAUTH frame to the AP. The attacker then can send a spoofed authentication frame in order to authenticate himself. Furthermore the attacker can deauthenticate all authenticated clients of the AP by impersonating the AP and regularly broadcasting such a spoofed DEAUTH frame with an omni-directional antenna, forcing the clients to re-authenticate.

Impersonation Attack: The attacker compromises authentication by impersonating a legitimate AWMN node. This attack is very easy to implement in AWMN since there is no strong authentication mechanism: a node confirms the identity of another node based only on the IP address. External or client nodes can easily sniff unencrypted IP addresses. BB nodes also know the other nodes' IP addresses, since they need them in order to route packets. A potential attacker can cause serious damage by impersonating a BGP-router. False routing updates can be sent in order to produce extra traffic, force packets to follow a longer route adding delays, throw them in a loop or overload other routers (DoS). Furthermore the attacker can terminate communication between two BGP peers by sending a false Notification message or an Open message after the connection establishment.

Modification / Fabrication Attack: This kind of attack can be carried out by BB nodes. A BB attacker can modify BGP Update messages that he receives from a BGP peer before forwarding them to their own peers. Attributes that can be modified include:

- the AS Path attribute. If the attacker deletes AS numbers from the path they are basically advertising short paths that pass through the node. This way they will probably force other routers to select paths that go through his node. The attacker can then launch a black hole attack. Furthermore, the modification of the AS numbers can cause the formation of loops.
- the list of IP prefixes in the NLRI field.
- the list of IP prefixes in the Withdrawn routes field

The last two attacks can cause network malfunction since packets may not follow optimum paths, available routes can be considered unavailable and vice versa and routers may overload and be forced to drop packets. A BB attacker can generate and distribute fake BGP Update messages. Fabrication attacks differ from modification attacks in the fact that the attacker creates new messages with false data rather than modifying passing Update messages. A common fabrication attack is prefix hijacking, where a malicious BB advertises a prefix originating from another AS and claims that he is the origin. Again in this case the attacker can advertise a false, non existent route in order to be selected and perform a Black hole attack.

Selfish behavior: All the above attacks act openly against either specific nodes or part or even the whole network. A selfish behavior from a BB node, can decrease network performance. A BB node can refuse to forward incoming packets or advertise routing information, in order to save resources such as bandwidth or computing power. Some more sophisticated ways of acting selfishly other than just discarding packets that should be forwarded include:

- modifying the AS Path attribute by adding AS numbers. This way his BGP peers will probably choose the long paths that the selfish node advertises, leaving the attacker with more resources.
- not advertising all the known optimum paths to one's neighbors. Since fewer routes are advertised, the packet load that needs to be forwarded by him will be small.
- fabricating a BGP Update message which advertises the unavailability of actually available routes, and sending it to one's BGP peers. Nodes that were using these routes will now have to find a way around the selfish node in order to reach their targets.

III Conclusions

Due to the experimental nature of AWMN, guarantying security is usually a secondary objective. This leaves such networks vulnerable to even simple attacks, most of which can be countered by basic security measures.