Requirements for troubleshooting Wi-Fi network security through location technologies

Nicolás Macia
LINTI-National University of La Plata
Calle 50 y 120
Buenos Aires - Argentina
54 221 422 3528
nmacia@cespi.unlp.edu.ar

Paula Venosa
LINTI-National University of La Plata
Calle 50 y 120
Buenos Aires - Argentina
54 221 422 3528
pvenosa@info.unlp.edu.ar

Luis Marrone
LINTI-National University of La Plata
Calle 50 y 120
Buenos Aires - Argentina
54 221 422 3528
lmarrone@linti.unlp.edu.ar

ABSTRACT
The location of mobile devices in a network can be used to provide services that locate users as well, making positioning and tracking of mobile devices. From the standpoint of security and network administration, the location of mobile devices can be used as a protective mechanism complementary to existing ones, either by detecting unauthorized access to the Wi-Fi network as well as allowing the tracking of stolen mobile computers. The aim of this paper is to study techniques for locating mobile devices in Wi-Fi environments and discuss countermeasures that can be used by users who want to avoid being located. Based on this, will select the most appropriate location technique taking into account the countermeasures discussed. It will analyze the feasibility of implementing location technologies with general purpose hardware, evaluating possible changes to the software needed for access points so as to permit use in the tracking system. From this, we propose a location system architecture taking into account the appropriate security requirements to perform access control to information obtained and to safeguard the privacy and anonymity of the same.

Keywords
Network Security; Signalprint; Monitoring; Location; WiFi.

1. INTRODUCTION
Several location techniques can be used in Wi-Fi networks to determine the position of mobile devices. The techniques known as localization techniques on the client are those that require the user to install a specific application on his mobile device. In these solutions, the localization process is performed on the client using the tools previously installed by him. This will allow him to compare the observations from his laptop against online databases to determine his location.

ICIS 2009, November 24-26, 2009 Seoul, Korea

There are other localization techniques, named localization techniques on the network side, which do not depend on the cooperation of the user. This means that without user consent it is also possible to determine his location

Localization techniques on the network side are more attractive because they have no special requirements on the client. However, the use of these techniques involves the collection of any type of user information which generates controversy in regard to privacy from them, since they may not want to be located. For this reason, applications of this kind must protect the data collected, keeping the same database with well defined access controls.

On the other hand, there are actions that could be used by Wi-Fi network users who do not want to be located. These impede the localization process to a greater or lesser extent depending on the location technique used.

Localization techniques on the network side as well as being used in the same location can also be useful in detecting security issues specific to Wi-Fi networks. For example, if an attacker wants to use the network access of a valid user, the localization system gets a strong indication of the occurrence of an identity theft attack, as it detects that all the user packets are not originated in the same area.

2. LOCALIZATION TECHNIQUES
As mentioned, the localization techniques that are performed on the network side are those who do not require the cooperation of the user. This class of techniques is more scalable and flexible. Cisco offers a Wi-Fi location integrated solution, marketed under the name Cisco Location Appliance [1]. Although there are other initiatives, there are not known open-source projects similar to Cisco's that have this level of development.

To carry out the localization of a mobile device based on the network requires cooperation of the Network Access Points.

The techniques based on networks side that can be used in Wi-Fi environments are [2]:

- Nearest Access Point
- Triangulation between Access Points.
- Signal Pattern Search

The first one, Nearest Access Point, is obviously the least effective because it tells us only that the device is located within the coverage area of a particular Access Point. This technique has low accuracy location, for example, the AP's coverage area. However, in many contexts, this information can be extremely useful. For example, in a large institution, with several buildings scattered around the city or more than one city, the location of the nearest Access Point may be sufficient for many applications.

The second technique, called Triangulation between Access Points is based on information from mobile stations. The Access Points use this information to triangulate the position of mobile stations. There are several variations of this technique depending on the information obtained; it may be time of arrival of packets and the received signal strength. The problem is that Wi-Fi environments lose effectiveness because such techniques do not take into account issues of signal attenuation, multipath or signal reflection. Moreover, obstacles in this type of networks (doors, walls, people, etc.), affect very differently because of the different materials they may have.

The third one, called Signal Pattern Search takes into account aspects of mitigation, multipath and signal reflection mentioned above. The way to consider these issues is to rely on prior information of the signal patterns of a mobile device in different places where it could connect to the network within the building. This will have an organizational vision that takes into account the nature of it. This information is needed to get ahead is what is known as signal map. The signal map is nothing more than a database which records the signal patterns observed by the access points from several devices in various locations within the building of the organization.

The signal map is assembled prior to localization process, and it reflects the reality of the specific environment and not just an approximate theoretical model of signal propagation.

The localization process involves determining the signal pattern of a particular mobile device and searches the pattern in the database (signal map) to determine their position.

2.1 Localization on Wi-Fi network

For the above, the most appropriate technique for location on Wi-Fi network, is that one based on patterns of signal, since it takes into account aspects of attenuation and multipath reflection signal which are very common in them.

In our particular case, the pattern of signal to be used is signal print, which is the tuple of signal intensity records that capture different APs for the same packet of a particular mobile station.

Signal patterns or signal prints play a fundamental role in the location of devices in Wi-Fi networks, proving to be a primary information source in this process. Contrasting the signal print a mobile device with data stored in the signal map or map, one can estimate the device position. It can be used different mechanisms to manipulate signal print and determine the position of mobile stations. For example, [3] and [4] use Bayesian methods to determine the most likely location of the mobile device to locate.

2.2 Concealment techniques location

With the aim of providing users with valid network privacy, [4] describes techniques that can be used for that purpose. They can hide the location of a valid user by manipulating the signal strength of the transmitter, the MAC address used, the point in time at which data is sent or the use of different antennas.

In [3] and [4], the use of heterogeneous hardware (wireless network cards or antennas other than those used in the training stage) as well as the use of different power levels on the part of users may affect the normal functioning of the system. Another problem with these ways to get the location is that they do not take into account the existence of security problems, such as a third party cloning the MAC of a valid user to enter the network. For this reason, security problems as described above will confuse the system into thinking that the user is jumping from one place to another.

.

3. LOCATION TECHNIQUE SELECTED

In [5] it is presented a most appropriate technique to address jointly the location of mobile devices and detection of security problems in a Wi-Fi network. The localization process used is not based on a probabilistic approach as was the case mentioned above. In this technique signal prints are interpreted as relative signal prints according to the best signal received therein. In other words, when you assemble the signal print of a mobile station, it is rewritten so that each value represents the difference between it and the best signal obtained therein. For example, if I have 4 PCs that gather signal prints, and they report the following values for a given station (AP1, AP2, AP3, AP4) = (-50, -80, - 73, -60), since in the same, the AP1 is the best package received the signal, when processed this signal print, it will be turned on as signal print resulting in the following: (AP1, AP2, AP3 , AP4) = (0, -30, -23, -10).

The basic idea of this location system is to make comparisons with other signal prints previously collected. By comparing the obtained signal prints gathered in the signal map, one can estimate the location of the mobile device. For example, the observed signal print should not vary by more than a certain amount of decibels (e.g. 5dB)

Conference'04, Month 1–2, 2004, City, State, Country.

in each of the values of the tuple, regarding the signal print observed in the location where the mobile station is.

Safety issues can be checked by comparing the obtained signal print with the previous one from the same station. For example, if in the last signal print collected, there is some value in the tuple that varies over a certain high amount of decibels (e.g. 10db) for an earlier signal print observed for the same season, it is likely that there is an attacker cloning the MAC address of a valid user.

As already mentioned, in [6] there are a number of techniques proposed to avoid detection by location systems. Although that work demonstrates a high degree of success, they will not be effective in a location system like this, if they are used to connect to the network with valid user credentials, as it can manipulate many things in sending the information (signal level, antenna, MAC address), but it is not possible to manipulate the signal level observed by the access points of the organization, since it is very difficult to produce the same signal print of another mobile station
Furthermore, the use of these techniques only to conceal the position of a user will make the system to detect an anomalous situation, since in the proposed location system it could be seen as an identity theft attack, too..

4. DEFINING THE LOCATION SYSTEM ARCHITECTURE AND ITS OPERATIONS

There are several Access Points in an organization, when you configure a Wi-Fi network to provide coverage throughout the building. These access points should be configured to run on the same network name (SSID), but must use different channels to avoid interference. Fig. 1 shows the overlap of 802.11b's channels.

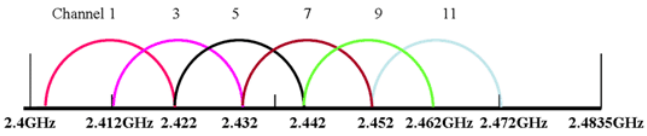

Fig. 1

Because of this overlap, it is necessary to properly plan the channels to be used by the network access points.

Fig. 2 shows an adequate channel distribution in which there would be no interference between the access points [7].

When the signal print of a mobile station starts to be gathered, all the APs that perform the readings should be listening to the same channel in which the mobile station operates.

Because the above is not practical from the standpoint of service offered by network access points, a separate monitoring architecture of the existing communications architecture is needed.. Basically, this means that an AP that is serving in the Channel 9 for example cannot simultaneously be trying to collect the signal values of a station that operates on channel 1.

Furthermore, because the number of sensors to collect signal prints is not enough to cover all the operating channels at any time, it is suggested to conduct the location in a reactive manner, i.e. in two stages.

Assuming the best case where we have the same number of APs for monitoring and of APs that give network service, monitoring work like this:

In the initial stage, the APs dedicated to monitoring, will conduct a passive survey from customers who are connected to the network on different channels. Each AP sensor is configured to listen on a particular channel, which will be the channel used by the AP that provides network service.

The information collected passively by the monitoring APs will be sent to the location server which will initially register, for each customer of the network, the channel on which it is operating.

The second stage of monitoring can be triggered by an explicit location request of the system administrator or by detecting an abnormal situation which must be confirmed.

As an example, we analyze the sequence of steps involved when the location system administrator wants to determine the location of a mobile station. Based on information collected by the system at the initial stage, the system knows the channel on which the station is operating. With this information, it triggers the second phase, sending the order to the monitoring APs that report signal levels for the mobile station in question. Based on information received by monitoring the APs, the location server can assemble the corresponding signal prints and compare them

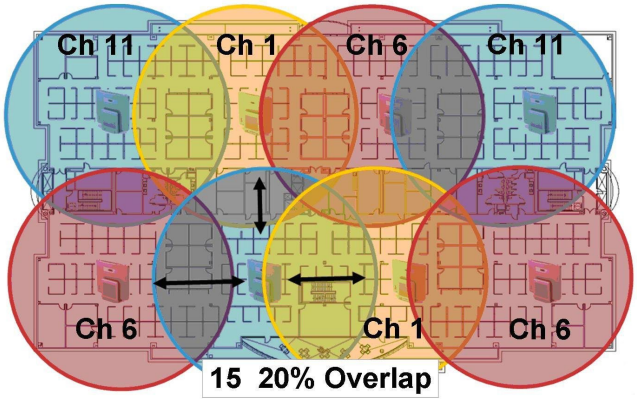

Fig. 2

with those it has in its signal map to determine the likely location place of the station.

4.1 Location server

In order to meet the initial objectives of privacy and safeguard the information collected it should be made the following considerations:

- Communications between the location server and monitoring APs must be made through secure channels. To this end we intend to use a VPN solution such as openvpn.
- Anonymity of data stored on the location server, can be done with the help of hash algorithms. Because the server will store tuples as the following style: (MAC, id, channel, signalAP1, signalAP2, ..., SignalAPn) to preserve the anonymity of the data, instead of storing the MAC address of the station we propose to store the corresponding hash using an algorithm such as SHA512. Thus this would actually be stored: (SHA512 [MAC], id, channel, signalAP1, signalAP2... SignalAPn). With this implementation, the location server is accessing the data directly, as during access it knows the MAC with which it is working

The disadvantage of this data anonymity mechanism is that it is not effective if, for example, an attacker obtains location data from the server. In this circumstance, the attacker can deduce the MACs addresses that correspond to Hashes of the database, by sniffering the wireless network.

One way to mitigate this situation is when you start the location service, to require the administrator a password. This password will be used by the location system to store location records in the following way:
(SHA512 [MAC + password], id, channel, signalAP1, signalAP2… signalAPn)

5. CHANGING THE FIRMWARE OF AN AP TO COLLECT LOCATION DATA

Different Access Points (Linksys, Asus, Dlink, etc) can be flashed with open operating systems such as for OpenWrt [8] or DD-WRT [9]. These systems allow customization of the access point, making it a general purpose device.

To perform the tasks previously described for a monitoring AP it is necessary to be able to collect signal level information from packets that are transmitted in the Wi-Fi environment.

To accomplish this driver of the wireless network card may be changed so you can collect the information as it is received. This has the advantage of having first-hand information requested, with appropriate speed this means. As a disadvantage it might be mentioned that the alternative is somewhat risky because you are manipulating the same wireless card driver that runs in the system kernel, so that any error could produce unexpected situations. Besides to carry on this type of modifications you have to master the kernel internal structure. Finally, the main disadvantage is that this alternative has not a portable solution because changes of the card driver will not serve to implement that solution in a third-party card manufacturer as it will have another driver.

This was the way followed by KARMA [10]. KARMA is a tool that implements what is known as Rogue AP. Basically it deceives a valid client making him to use the services of this AP (false) in order to steal sensitive information of the connected user.

The original version of KARMA depended on a modified version of MADWIFI driver, a driver for wireless cards based on Atheros chipsets. Although this worked well, it limited the portability of the tool as it was necessary to use this card type. Moreover, from the standpoint of development, it required an extra effort which was to keep the driver patches with the latest version of MADWIFI source code.

Thanks to the developers of Aircrack-NG project this situation could be resolved. Aircrack-NG enabled KARMA project to dispense from this modified version of the MADWIFI driver, developing a user-mode Access Point, which works with any wireless network card that could be set in monitor mode.
Thus, although not all wireless cards drivers allow setting wireless cards in monitor mode, significantly hardware constraints previously presented could be reduced.

5.1 Proposed solution for monitoring AP implementation

The proposed solution to obtain the values of signal levels in a Wi-Fi environment is based on a tool that works in user space and uses the wireless interface in monitor mode to access signal levels data in the different channels.
It is worth mentioning that only with this requirement; it is possible to implement the functionality of the two stages required for monitoring APs.

5.2 Preparing monitoring AP

For this work, we had an Access Point ASUS WL-500G Premium. The operating system was OpenWRT installed as follows:

- We used the latest version of OpenWrt: kamikaze 8.09.1
- Because the driver version of the wireless card included in the distribution of kamikaze with kernel 2.6 had problems, [11], we used the distribution of kamikaze with kernel 2.4 [12].

The OpenWRT operating system installation was done via TFTP using the steps described in [13].

5.3 Collection of data by monitoring AP

This section shows how to obtain appropriate readings for the implementation of client and server processes of the location system.
Upon connecting to the system and view the status of their interfaces it can be observed as a result of the IFCONFIG command that in addition to the network interface, there is a wireless interface called wl0. Moreover, with the IWCONFIG command we got a detailed information of that interface:

```
root@OpenWrt:~# ifconfig
wl0       Link encap:Ethernet  HWaddr 00:1D:60:46:91:7F
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:207
          TX packets:16 errors:7 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:5137 (5.0 KiB)
          Interrupt:2 Base address:0x2000
root@OpenWrt:~# iwconfig
```

```
wl0       IEEE 802.11-DS  ESSID:"OpenWrt"
                  Mode:Master  Frequency:2.432 GHz
                  Access Point: 00:1D:60:46:91:7F
          Bit Rate=54 Mb/s   Tx-Power:32 dBm
          Retry min limit:7   RTS thr:off   Fragment thr:off
          Link Quality:5  Signal level:0  Noise level:171
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:0   Missed beacon:0
```

To obtain the signal information, you can use the tcpdump tool. For this you must set the interface on monitor mode to view information on signal strength, channel, time of receipt, and so on. The following command can perform this task:

```
root@OpenWrt:~# wlc down ; wlc up ; wlc channel 4 ; wlc monitor 1;
```

The above command besides putting the interface in monitor mode configured the same to listen on channel 4. Looking at the interfaces of the system again we see that we now have an interface called prism0.

```
root@OpenWrt:~# ifconfig
prism0    Link encap:UNSPEC  HWaddr 00-1D-60-46-91-7F-00-00-00-...
          UP BROADCAST MULTICAST  MTU:0  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
wl0       Link encap:Ethernet  HWaddr 00:1D:60:46:91:7F
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:1698
          TX packets:16 errors:7 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:5137 (5.0 KiB)
          Interrupt:2 Base address:0x2000
```

During testing it was observed that re-executing commands on the wireless card such as IWCONFIG, the computer restarted because of the existence of a bug that is not yet solved.

The bug found did not prevent carrying out the solution proposed here. It is possible to capture information on the interface prism0 that allows to report the amount of signal levels from the packets received.

```
root@OpenWrt:~# tcpdump -n -i prism0 -s0
listening on prism0, link-type PRISM_HEADER (802.11 plus Prism header), capture size 65535 bytes
02:51:24.277478 Beacon (k2) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] ESS CH: 6, PRIVACY
02:51:24.379875 Beacon (k2) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] ESS CH: 6, PRIVACY
02:51:24.584681 Beacon (k2) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] ESS CH: 6, PRIVACY
02:51:24.789489 Beacon (k2) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] ESS CH: 6, PRIVACY
02:51:25.506330 Beacon (k2) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] ESS CH: 6, PRIVACY
02:51:25.608727 Beacon (k2) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] ESS CH: 6, PRIVACY
02:51:25.711126 Beacon (k2) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] ESS CH: 6, PRIVACY
02:51:25.813536 Beacon (k2) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] ESS CH: 6, PRIVACY
02:51:25.915938 Beacon (k2) [1.0* 2.0* 5.5* 11.0* 18.0 24.0 36.0 54.0 Mbit] ESS CH: 6, PRIVACY
13 packets captured
13 packets received by filter
0 packets dropped by kernel
```

In this method, each captured packet is encapsulated in a Prism header, which, as we see in Fig. 3, the capture made with Wireshark, it has the desired information in the RSSI field [14].

To make the signal prints, it is necessary to interpret the field value RSSI (Receive Signal Strength Indication) which represents the actual signal value that has the packet when it is captured.

All necessary information for monitoring the two stages described above, is available on this header. It will be part of the application running in the monitoring AP to adequately interpret and report it to the location server.

6. CONCLUSIONS

According to the tests we can say that it is possible to implement a location system with general purpose hardware. To do so it is necessary to have Access Points that can flash with an operating system such as OpenWRT and wireless interface cards that can be set in monitor mode.

The selected location technique through the use of a location system based on the best RSSI signal prints thereof

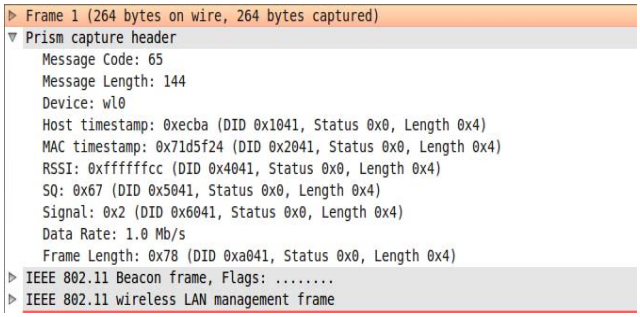

Fig. 3

allows that countermeasures such as the use of antennas with different gain, the change in power levels of wireless cards or using heterogeneous hardware clients do not affect the localization process.

From the point of view of network security, the proposed location system can be used to detect problems such as: (DOS) denial of service by a user as a third party who wants to prosecute him and cloning MAC address.

Furthermore, this system could be integrated with an Access Server to extend the policies of user access to the network. An authentication system that integrates with one location system could require the user access credentials, just after proving that it is in his workplace.

7. ACKNOWLEDGMENTS

To Alexandre Santos, Antonio Costa and the whole team of Computer Science and Technology Center (Centro de Ciências e Tecnologias de Computação, CCTC) University of Minho – Braga – Portugal.

8. REFERENCES

[1] http://www.cisco.com/en/US/docs/wireless/technology/location/deployment/guide/depgd.html

[2] http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/lbswifig_external.pdf

[3] Algis Rudys, Ping Tao, Andrew M. Ladd, Dan S. Wallach. Wireless LAN Location-Sensing for Security Applications

[4] Andreas Haeberlen, Eliot Flannery, Andrew M. Ladd, Algis Rudys, Dan S. Wallach, Lydia E. Kavraki. Practical Robust Localization over Large-Scale 802.11 Wireless Networks

[5] Daniel B. Faria, David R. Cheriton. Detecting Identity-Based Attacks in Wireless Networks Using Signalprints.

[6] Tao Jiang, Helen J. Wang, Yih-Chun Hu. Preserving Location Privacy in Wireless LANs

[7] http://www.cisco.com/en/US/docs/solutions/Enterprise/Mobility/emob41dg/ch3_WLAN.html

[8] http://openwrt.org/

[9] http://www.dd-wrt.com/

[10] http://www.wirelessdefence.org/Contents/KARMAMain.htm

[11] http://oldwiki.openwrt.org/OpenWrtDocs(2f)Hardware(2f)Asus(2f)WL500GP.html

[12] http://downloads.openwrt.org/kamikaze/8.09.1/brcm-2.4/openwrt-brcm-2.4-squashfs.trx

[13] http://oldwiki.openwrt.org/OpenWrtDocs(2f)Hardware(2f)Asus(2f)WL500GP.html

[14] http://www.wireshark.org/docs/dfref/p/prism.html