Monitoring and Assessment of the Wi-Fi Signal Quality and Detection of Unauthorized APs on High-End Wireless Networks

Eliana Neuza Silva
Instituto Superior Técnico
Lisbon, Portugal
eliananeuza@tecnico.ulisboa.com

ABSTRACT
Operators of large wireless local area networks (WLANs) must pay attention to their Wi-Fi service because its signal quality tends to decrease. This decrease is usually caused by radio planning problems (frequency interferences), a higher number of users than the supported and the introduction of unauthorized access points (APs). No solution existing today integrates both the monitoring of the Wi-Fi signal quality and detection of unauthorized APs or rogue APs (RAPs).

This work proposes the ENDScanning system as a solution that assesses the Wi-Fi signal quality and detects, localizes and counterattacks RAPs. The system also assesses the impacts and interference of RAPs on the Wi-Fi signal in the areas around them. It does this through constant monitoring of the network using a crowdsensing approach and passive nodes. The ENDScanning system is much simpler to use and adaptable than others available today, being easily deployed in any other building and network.

Author Keywords
Wi-Fi, Signal Quality, Rogue APs, Detection, Positioning, Coverage.

INTRODUCTION

Nowadays Internet connection is one of the most common things people expect to have almost anywhere. Therefore, a bad performance of the Wi-Fi service of a large wireless local area networks (WLANs) operator (such as companies, universities, governments, etc.) will not only be a disadvantage to the users, since a poor Wi-Fi connection may delay work and services, but it can also damage the institution's reputation.

WLANs suffer from constant network maintenance and expansion procedures to improve its service. The focus of network analysis and monitorization is to guarantee a good coverage and user experience, but this isn't always easy due to phenomena like high client density or bad AP coverage in certain areas and radio interferences (caused by other devices operating in the same radio frequency (RF)). The biggest cause for radio interferences is the presence of unauthorized APs, mostly known as rogue APs (RAPs). RAPs are access points that don't belong to the facilities' authorized network, deployed without consent or authorization of the network administrators. RAPs not only reduce the Wi-Fi signal quality by interference in the RF, but can also create security holes and be doors for network attacks.

Solutions and systems have been developed mostly by network vendors and network manufacturers to address these problems. Yet, there is still no integrated and cheap solution that can be easily deployed and maintained in large buildings using real-life Wi-Fi information to assess the wireless network. Also, still non-existent is a solution that monitors both the Wi-Fi radio signal (RS) quality and RAP detection that can use the RAPs information into consideration to determine its impact on the Wi-Fi QoS. This work attempted to fill this need. In it, an affordable, efficient and easy to implement innovative system that monitors the Wi-Fi signal and RAP detection in High-End Wireless Networks was studied, planned and developed. The developed system tackles the mentioned problems, by monitoring the Wi-fi signal quality using the real-life information that reaches the network users. It deals with the appearance of RAPs by detecting, locating and attempting to contain them. And it assesses the RAP's impact and interference on the Wi-Fi signal quality in areas surrounding them.

All the developed solution details and implementation are described further in this document.

RELATED WORK

As mentioned, operators of WLANs must guarantee a minimum QoS and network security to all its authorized users, which can be hard due to coverage issues and radio interferences. Specially with today's technology it's becoming even harder to control the RS interferences because almost all mobile devices can be used as an AP, by being on 'portable hotspot' mode. In this chapter, some of the current methods and solutions to address these issues are reviewed.

Wi-Fi QoS Assessment

There are two ways to effectively evaluate the Wi-Fi quality of service (QoS) in the network: through site survey or by assessment of Wi-Fi metrics (raw signal measures).
According to Cisco [1] there are three types of site survey: passive, active and predictive. Passive site surveys are performed in listen-only to collect information about the APs RF. These give an idea of areas poorly covered by Wi-Fi signal, gather received signal strength indicator (RSSI) values, interference, signal to noise ratio (SNR) and can even

identify RAPs. Active surveys can be on-site (performed associated to the APs, extracting data rates, RF performance and changes) or post-deployment (performed in roaming between the APs and analyses the overall network performance such as data rates, jitter, latency, coverage, interference, etc.). Predictive surveys are performed using software with specialized algorithms that execute simulations on the environment coverage area and localization of APs. Good examples of predictive survey software are Wi-Spy [2] and iBwave Wi-Fi [3] that locate interferences, throughput, signal dead spots and saturations with 3D graphical and map representations.

Some of the metrics most commonly used to assess the Wi-Fi QoS [4] are the: RSSI, signal to noise ratio (SNR) Packet-Delivery Ratio (PDR) and Bit-Error Rate (BER).

The RSSI is the signal strength at the receiver. The SNR is how much of the power of the received signal exceeds the noise and interference. The PDR is the number of packets received correctly divided by the number of packets sent. The BER is the ratio of incorrect bits in the total amount of bits sent over a certain period.

None of these metrics alone can make a good assessment of the Wi-Fi signal quality. The RSSI can't grasp interference fluctuations; the SINR is accurate, but extremely hard to measure; the PDR is a good metric, but depends on the packet size and transition rate; the BER is a better metric, but to use it, it's necessary to compute it several times along the process. Therefore, these metrics should be used as a set to classify the signal quality.

The solution in [5] attempted to measure the signal interference and had good signal quality assessment results by using the RSSI, packet loss and latency.

Dealing with Unauthorized APs

To deal with the presence of RAPs several systems were developed to prevent and/or detect them, these are widely called Wireless Intrusion Prevention Systems (WIPS). The approaches used by WIPS can be detection and alert, detection and containment or detection and physical localization. Several network vendors [6], [7], [8] also implemented methods in their devices to scan the network and detect RAPs. These methods can operate on the client/user side, on the server/administrator side or can be a combined hybrid approach.

In the client/user side the objective is to prevent the user's mobile device of connecting to a RAP. According to already existing systems, [9], [10], [11], [12], this approach normally uses statistical or comparison based techniques by performing packet comparison, RSSI value measurements and statistical anomaly detection. Timing based techniques like the ones in [9] use the Round-Trip Time (RTT) values between the client and the Domain Name System (DNS) server to determine if that AP is a rogue or not. Packet comparison techniques like the ones in [10] compare the APs Service Set Identifiers (SSIDs), Media Access Control (MAC) address, Internet Protocol (IP) address and traceroutes of the packets with the ones of the legitimate APs to warn the client if it is safe to connect to that AP. Other techniques that use RSSI values are based on the distance between the client and the AP. The ones that measure and compare these values, like [11], are based on profiles broadcasted by the legitimate APs.

The major disadvantages of these approaches are that most of them need to analyze network packets in mobile devices, that takes time and resources (battery) from the user. It takes time on the user to connect to an AP because they must first guarantee that it's not a rogue. It also needs to know the standard RTT values for that network making it necessary to collect samples and gather information of the legitimate network beforehand.

The server or administrator side approaches are the most common ones. They're used on a network administrator's centralized server with the help of the existing network elements (the facilities' APs, switches, …) and/or with the use of an add-on passive network composed by monitoring nodes. Most of the companies selling networking products have APs that can be switched into scanning modes, making it easier to implement the detection of RAPs on the server side.

Juniper Networks [13] APs scan the network for RAPs, and if they discover a device whose MAC address is not in their database, a series of rules are applied to classify that device.

The largest network hardware producer, Cisco, has a Meraki's Air Marshal platform [14] where normal APs can perform scans of the network or even be placed in WIPS sensor dedicated mode. This platform creates scanning reports, detects RAPs and attempts to contain them. The counterattack consists of generating a very large number of 802.11 frames in a technique called spoofing. Those frames are the following:

- the first is to use 802.11 broadcast de-authorization frames with the source MAC address being the rogue Basic Service Set Identifier (BSSID);

- the second is to use 802.11 de-authorization message frames with the source MAC address being the rogue BSSID and the destination MAC address of the client (connected to the rogue);

- and the third is to use 802.11 de-authorization and disassociation messages with the source MAC address of the client and the destination MAC address of the rogue.

Aruba Networks' APs can be configured to detect and interfere with RAPs [8]. The interference goal is to try to disconnect the clients from the RAP. This can be done with two methods: de-authenticate only mechanism, where there is an attempt to dissociate the clients from the RAP, or the "trapit containment" mechanism, where an AP on the same channel as the RAP will try to lure its rogue clients to connect with him instead.

The disadvantages with these systems is that the AP's scanning configuration is hard and time consuming [14]. Worse, if a network is composed of different APs it's even harder to configure and perform a synchronized scanning. Many APs that can perform scanning don't have dedicated radios to do so. They need to be dedicated scanning APs or else the AP must cease serving clients to listen and scan the network [14]. Also, while the APs are scanning the network, for an unauthorized AP to be officially detected and labeled as RAP it must be seen by at least two different APs [15]. There is also the lack of constant scanning of the network, for example, Cisco's Hybrid APs only scan the entire network once a day or when there are no clients associated to them. This means that most of the scans will be performed at hours when there are less clients in the network (for example, at lunch time or late afternoon) so these scans won't be 100% useful. Because of this, Cisco recommends turning an AP into a dedicated WIPS sensor or to switch to the newer APs that have three radio channels. This is an expensive solution that takes resources from the network. It's also extremely difficult to apply these platforms and configurations to heterogeneous networks with different types of APs (different AP brands, and different AP models of the same brand).

Detecting a RAP and locating it in the building allows for a more drastic countermeasure, to physically encounter it and shut it down. This method is mostly applied in institutions that have security policies prohibiting the use of unauthorized AP. This is the method applied by [16] where after RAPs are detected, it is tried to physically locate them in the facilities to remove the threat.

The Hybrid [17], [18] approach combines both the client/user side and server/administrator side approaches when tackling the problem of detecting RAPs. The advantage of this approach is that if one of the methods fails to detect a RAP, the other might still detect it.

Indoors Localization

Indoors localization is important to not only localize RAPs but also to link the Wi-Fi QoS to a certain area.

Indoors localization technologies are infra-red, ultrasound, use of Radio-Frequency Identification (RFID), use of WLAN and use of Bluetooth. Infra-red, although efficient, needs line of sight. Ultrasound is more accurate but not very scalable because it uses dense sensor infrastructures. The use of RFIDs has the disadvantage that each user or object needs to have an RFID and it's also necessary to have a large infrastructure of RFID readers. The use of WLANs is the most popular method, because it has a better range and is easy and cheap to use. The use of Bluetooth is also easy and cheap, but it has a smaller range than the use of WLAN and has more latency.

WLAN technology is the most used for indoors positioning because these networks exist almost anywhere and they can extend through large areas. It gathers the best properties for location purposes maintaining the scalability and flexibility of the system. Localization with WLAN can follow two approaches: Signal Propagation Model (SPM) approach and Location Fingerprinting (LF) approach.

The SPM estimates the positions by measuring the RSS, the Angle of Arrival or Time Difference of Arrival and then using mathematical models [19], [20]. The LF calculates a device's positioning by comparing the RSS with the RSS values previously measured on known positions [21], [22].

A very common SPM positioning method is trilateration [23], [24] using the Friis formula (1) used for telecommunications in transmissions between antennas. This formula allows to determine the distance between two antennas (a fixed antenna with known position and a non-fixed antenna with unknown position) by knowing the power of the emitting and receiving antenna, the antenna gains and the wavelength of the electromagnetic wave.

$$\frac{p_r}{p_e} = g_e \cdot g_r \cdot \left(\frac{\lambda}{4\pi d}\right)^n \quad (1)$$

The problem with this method is the value of the free path exponent, n [25]. This value changes within the buildings, therefore it's necessary to perform site surveys to find an average value for it and that usually causes precision errors.

After calculating the distances (2), d, the trilateration algorithm is performed by creating circumferences around the known antennas' position, with d radius to determine the interception area between all circumferences where the unknown antenna is most likely to be. There are several methods to determine a more exact position within this area like the least squares approach or determine the area's center of mass.

$$d = \sqrt[n]{\frac{\left(\frac{c}{f}\right)^n \times p_T \times g_T \times g_R}{p_R \times 4\pi^n}} \quad (2)$$

Another problem with trilateration is the accuracy in determining the floors location. In fact, if a building has more than one floor, it's hard to know the floor where the devices are. Solutions to this problem are hard to obtain and most base themselves in asking the user to input their own z coordinate localization [10]. There are still always uncertainties with trilateration due to range measurement and precision errors.

ENDSCANNING SYSTEM

Unlike the solutions mentioned or any system existing today, the ENDScanning system fills the need of a solution that monitors the Wi-Fi network for both signal quality and detection of RAPs and that also crossmatches information between both. With the ENDScanning system it's possible to monitor Wi-Fi signal quality and coverage of an area and assess the interference in the same RS by any presence of RAPs detected. The ENDScanning system is also much easier, simpler and more adaptable than others available

nowadays, being quickly and easily deployed in any other building and network.

The system's architecture (Figure 9) can be divided in two major parts: Nodes and Server. The Nodes have two types: the Crowdsensing Nodes and the Monitoring Nodes. Crowdsensing Nodes are the type of nodes responsible for collecting information on the Wi-Fi network signal. They consist in users' smartphones, connected to the Wi-Fi, running a background APP. Monitoring Nodes are responsible for scouting the Wi-Fi network for any RAP. They are devices that act as constant sniffers of the Wi-Fi network. This means that they constantly scan the network to detect RAPs that might appear. These nodes don't interfere in the legitimate network and are independent from it.

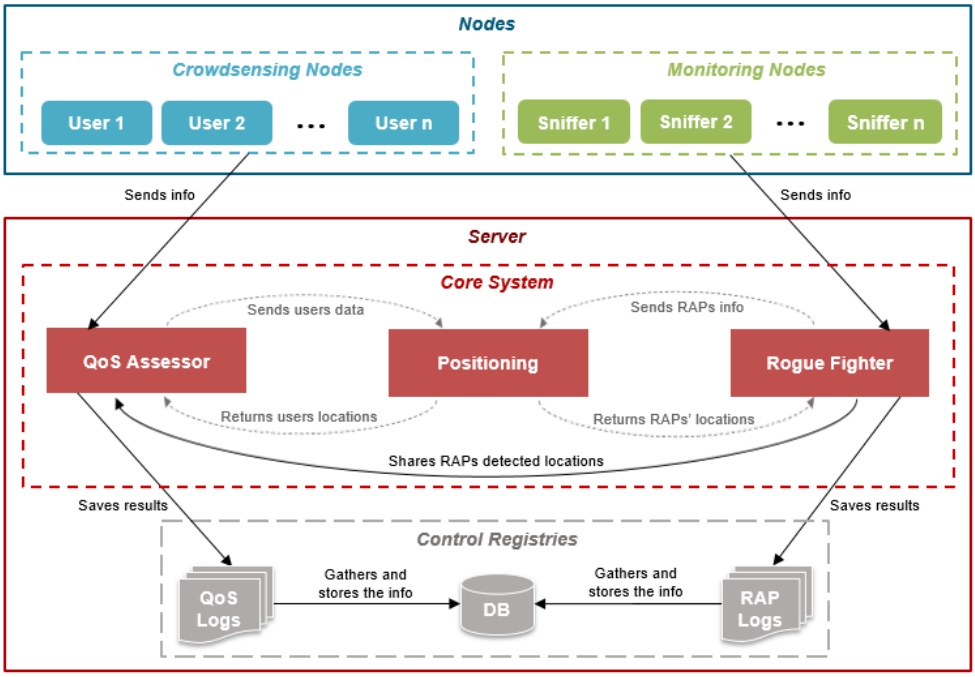

Figure 1. ENDScanning System's Architecture.

The three mentioned services coexist together in the system server, performing its own functionalities and sharing results with each other for a better network monitorization. Even though these three services work together inside the system, there are two of them that can work independent from each other (in case one of them doesn't get implemented by the network manager): the QoS Assessor and the Rogue Fighter. The QoS Assessor service doesn't obligatory need the Rogue Fighter service to work and vice versa. If one of them isn't working the other can still be efficient in developing its purpose, whether it is monitoring the network's signal quality or whether is detecting RAPs. But the Positioning service needs, obligatorily, to be present for either one of the two other services to function. The QoS Assessor needs the Positioning service to localize each data extraction area performed by the Crowdsensing Nodes to associate the signal quality to a certain location. The Rogue Fighter needs the Positioning to be able to localize the RAPs detected by the Monitoring Nodes.

The Control Registries is where all the results are logged and stored for further analysis of a network manager. The system doesn't offer a graphical interface to present the processed results, but this module facilitates the results representation on an external graphical interface (network weather maps, network behavior time maps, …).

The QoS Assessor receives the collected Wi-Fi signal information from the Crowdsensing Nodes and analyzes it to determine the Wi-Fi signal quality in that physical region. Therefore, the Crowdsensing Nodes and the QoS Assessor are the modules of the system's architecture responsible for monitoring the Wi-Fi network signal. The Rogue Fighter receives information from the Monitoring Nodes regarding RAPs that they have detected in the Wi-Fi network. Then it oversees the RAPs location and performs containment techniques. Thus, the Rogue Detector and the Monitoring Nodes are the modules of the system's architecture responsible for detecting RAPs. The Positioning performs calculations to locate the Wi-Fi signal information sent by the Crowdsensing Nodes and assists in locating the detected RAPs.

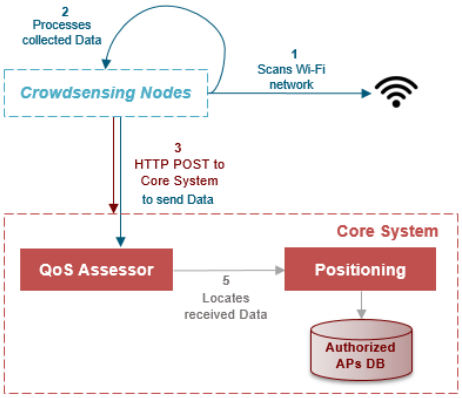

Figure 2. Diagram of the Crowdsensing Nodes interaction with the Core System

As shown in Figure 1, the Crowdsensing Nodes module send, through the ENDScanning smartphone APP, periodic Wi-Fi signal scans to the Core System. This is done only if the nodes are motionless, as to not adulterate results and improve positioning accuracy. In the Core System, the QoS Assessor receives that data and analyses it to perform a quality inspection of the Wi-Fi signal. Then the QoS Assessor, together with the Positioning service, locates the place from where the Wi-Fi signal data was collected. The positioning is performed to associate the Wi-Fi signal strength and coverage to different areas in the building. In the end of this process, the Wi-Fi quality results from the different areas are stored in log on the Control Registries module. To enable this system to function, it's necessary that the system modules perform the interactions represented on the diagram of Figure 2. As the figure illustrates, the Crowdsensing Nodes run a service that allows smartphones to scan the Wi-Fi network RS that they are receiving. After collecting scans and processing it, they connect to the server via HTTP connection sending an HTTP POST with the collected Wi-Fi information. This process is repeated periodically by these nodes while they are connected to the Wi-Fi network.

Also shown in Figure 1, the Monitoring Nodes module is composed of several Sniffers. The Sniffers are devices spread throughout the building scanning the Wi-Fi network for RAPs. When Sniffers detect a RAP, they collect information from it and report it to the Rogue Fighter in the Core System. The Rogue Fighter receives the information of the detected RAP from one or more Sniffers and uses it to locate it in the building with the help of the Positioning. The Rogue Fighter also implements containment measures to attempt to invalidate the RAP. To make this possible it's necessary that the system modules mentioned perform the interactions represented on the diagram of Figure 3. As the figure illustrates, the Monitoring Nodes connect via TCP to the server. Immediately after they connect to it, the Rogue Fighter sends them the DB with the authorized APs. Then each sniffer starts scanning the Wi-Fi network for RAPs. If, during a scan of the network, a RAP is detected, its information is collected and added to the RAPs list that will be sent to the Rogue Fighter. Once the Rogue Fighter starts receiving RAPs lists from various sniffers, it processes the information separately and stores them all organized locally in a Log. It then sends all the combined information of each RAPs to the Positioning to obtain its location. After obtaining the location a warning is generated and the complete RAP's information is stored. Then the Rogue Fighter starts countermeasures trying to incapacitate the RAP. Because the presence of RAPs "pollutes" the radio specter, it causes signal interference to the Wi-Fi network. Thus, the Rogue Fighter shares the RAPs information and location with the QoS Assessor, so it can calculate a better signal quality in that location.

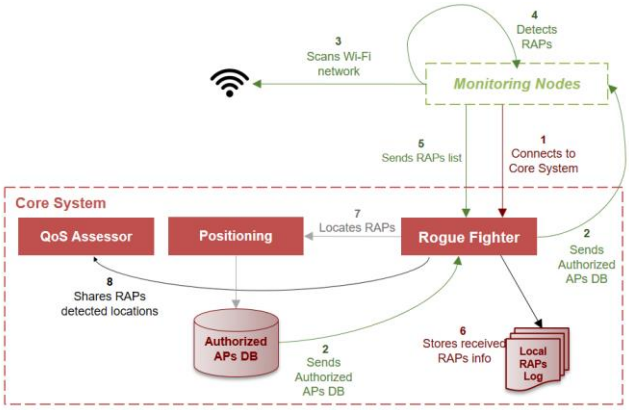

Figure 3. Diagram of the Monitoring Nodes Interaction with the Core System

IMPLEMENTATION

The ENDScanning System was developed and implemented for the IST Taguspark *Campus* facilities, in association with the Direção dos Serviços de Informática (DSI), to monitor the EDUROAM network.

The basis for the system's functioning is the existence of a data base (DB) with all the information about the network's APs (Figure 4) that would be used by all components of the system. Then the architectural modules and components were developed according to the system's functionalities: Positioning method, Wi-Fi QoS assessment, RAPs detection, location and containment.

DB field	Description
SSID	The authorized network AP name
BSSID_E_2.4	AP's MAC address for the "eduroam" in the 2.4GHz
BSSID_TG_2.4	AP's MAC address for the "tecnico-guest" in the 2.4GHz
BSSID_E_5	AP's MAC address for the "eduroam" in the 5GHz
BSSID_TG_5	AP's MAC address for the "tecnico-guest" in the 5GHz
X	AP's X position
Y	AP's Y position
Z	AP's Z position
Floor	Floor of the building where the AP is located
RSSID	AP's emission power
Gain	AP's antenna gain

Table 1. Authorized AP DB fields descriptions

The AP's (x, y) positions were obtained by marking the APs locations on Google Earth and extracting its coordinates. The z coordinate was obtained by measuring the building's floor heights and the distances that the APs were from the floor. Using Google Earth to extract the APs coordinates makes the system adaptable to any other building in the world. This allows the system to be expandable and completely adaptable, because it's quick and easy to add more APs and new buildings, without altering the system's code or functioning.

Positioning

The system's Positioning service uses two different positioning algorithms, one used for the QoS Assessor and another used for the Rogue Fighter. To find the positions of the Crowdsensing Nodes that collect and send information to the Core System the location algorithm is a Weighted Average (WA) of the position [26]. To locate the detected RAPs the location algorithm is Trilateration.

Both positioning algorithms use the Friis formula (1) to calculate distances between anchors (network APs or Monitoring Nodes) and the unknown position (Crowdsensing Nodes or RAPs), as expressed by (2). And to improve the precision for the distances a PLE, n, value was estimated for the building environments. The positioning algorithms also only calculate the positions for the x and y coordinates. Not letting the z coordinate be a variable is an advantage for the system, because this coordinate has a much smaller range. The unknown z coordinate is then determined choosing the z of the anchor with highest received power and use it as the z coordinate of the unknown point. This way both the positioning algorithms determine localization in R^2.

1. Trilateration Algorithm

The Trilateration is used to locate RPAs that where seen by more than three sniffers. This algorithm uses the least mean squares method [23] has the objective of minimizing the distances errors between the measured distance, d, from the sniffers to RAPs and the calculated distance from the sniffers to the estimated position of the RAP, D'.

$$\sum(d_i - D'_i)^2,\ i = 1, \dots, n \tag{3}$$

After calculating the distances (2), through the Pythagoras theorem, we obtain the following:

$$\rho = \sqrt{x^2 + y^2} = \sqrt{d^2 - z^2} \tag{4}$$

That can be solved by the system bellow:

$$2 \times \begin{bmatrix} x_2 - x_1 & y_2 - y_1 \\ \vdots & \vdots \\ x_n - x_1 & y_n - y_1 \end{bmatrix} \begin{bmatrix} x_u \\ y_u \end{bmatrix} = \begin{bmatrix} {\rho_2}^2 - {\rho_1}^2 \\ \vdots \\ {\rho_n}^2 - {\rho_1}^2 \end{bmatrix} \tag{5}$$

2. WA Algorithm

To determine the location of the Crowdsensing Nodes that scan the network the system uses the WA algorithm. This algorithm is also used to locate RAPs that were detected by less than three sniffers (that don't have enough information to perform the Trilateration).

The WA [26] algorithm is an estimation of the position presented in (6). It's based on the fact that higher SSID values received by users means that those APs are most likely the closest ones to the them, therefore, have the least error when calculating the distance (2). So, the method uses the inverse of the distance value as a weight to calculate the average. Therefore, closer APs have a higher influence in the end value result.

$$P_{u\ estimated} = \frac{P_1 \cdot w_1 + P_2 \cdot w_2 + \cdots + P_n \cdot w_n}{w_1 + w_2 + \cdots + w_n} \tag{6}$$

Where:

$P_{u\ estimated} = (x_u, y_u)$ is the user's position vector (Crowdsensing Node); $P_i = (x_i, y_i)$ is an AP's position vector and $w_i = \frac{1}{d_i}$ where d_i comes from (2).

The problem with this algorithm is that the calculated position will always be confined to the area where the AP's locations are, as exemplified in Figure 4. But this doesn't present a disadvantage to the system, because the Wi-Fi QoS is calculated by area and does not require an exact position. Also, most of the unknow positions of the Crowdsensing Nodes are usually confined to the area between the APs seen with higher RSSID values.

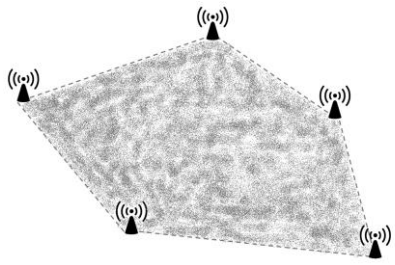

Figure 4. Area where the unknow point position will be located when using WA

Rogue Fighter

The Rogue Fighter service is responsible for dealing with all things concerning RAPs. It performs three main tasks: sending the authorized APs DB to each sniffer; receiving all the detected RAPs data and organize it; and counterattack the RAPs.

When a sniffer connects to the system, the Rogue Fighter sends them the authorized APs DB, and then waits for reports of any detected RAPs. When a sniffer detects one or more RAPs, it sends its information to the server. The Rogue Fighter receives several lists of RAPs from different sniffers and then sends their information to the Positioning service to locate them. After knowing the RAP position, the Rogue Fighter saves all the information and shares it with the QoS Assessor so that he can assess the RAPs interference in the Wi-Fi network. Finally, the Rogue Fighter attempts to contain the RAP by sending it a large amount of 802.11 broadcast de-authorizations frames with the RAP's BSSID. This way the Rogue Fighter performs a sort of a denial of service (DoS) attack leaving the RAP overwhelmed with

802.11 broadcast de-authorization frames making it unable to serve clients.

QoS Assessor

The QoS Assessor is responsible for monitoring the signal quality of the Wi-Fi network. It does this by analyzing the data sent by the Crowdsensing Nodes, and locate it using the Positioning service. The Positioning localizes the position from where the data was collected using the WA algorithm and after doing that it sends the position back to the QoS Assessor.

QoS Assessor calculates the signal quality using raw signal measures: the frequency, latency (Round Trip Time, RTT) and power received by each AP (RSSID), sent from the Crowdsensing nodes. The QoS Assessor first calculates the average power received by the smartphone from the several APs surrounding it. If the average power falls below -69 dBm the quality won't be the best that the network should offer (the system generates a warning of low signal quality) and if the average power falls below -79 dBm it means that the quality of signal in that location is extremely low and this problem needs to be fixed quickly (the system generates a warning of very low signal quality) [27]. With the received frequencies, the QoS Assessor determines if the APs are in interfering frequencies between each other, basing it on the channel in which they are centered. Then, after receiving the location from the Positioning, the QoS Assessor checks if there are any RAPs close to that position. He does it by checking the RAPs list shared by the Rogue Fighter and assessing if the frequency in which the RAP is in causes interference for the Wi-Fi signal of the legitimate APs.

EVALUATION

The ENDScanning system was tested on its three services, the Positioning, Rogue Fighter and QoS Assessor. The main tests performed where on the Positioning service that is used by both other services to determine the calculated positions errors. The Rogue Fighter was tested to assess if RAPs where efficiently detected and counter attacked though DoS attack. The tests on the QoS Assessor focused on determining if the measurements taken were useful in calculating the signal quality. The tests were performed in three different environments described below.

Testing the Rogue Fighter and Positioning of RAPs

Closed, open and multi space environments of the IST Taguspark Campus; Four Raspberry Pi 3 Model B with Wireless LAN as the system sniffers; One portable 3G Wi-Fi router as RAP; The coordinates of the four sniffers where changed to different locations three times. For each different location five measurements of the RAP position were calculated.

Results

These tests showed that the RAPs were always detected, even if by only one sniffer. The trilateration algorithm had very good results in calculating the RAPs positions, having error values of 2.6866 m for closed spaces, 2.673 m for open spaces and 2.2453m for multi/open spaces. When the RAP was far away from the sniffers, and only one or two detected it, the system still calculated an average position for its most likely position. The calculated position error was higher when the sniffers where further apart from each other, due to their lack of range. The containment of RAPs by sending 802.11 broadcast de-authorizations frames would only work by using wireless interfaces that support monitor/promiscuous mode.

Testing the QoS Assessor and Positioning of Crowdsensing Nodes

Closed, open and multi space environments of the IST Taguspark Campus; Four mobile devices connected to the Wi-Fi (one Samsung Tablet; one Alcatel Android Smartphone; one Sony Android Smartphone; one Motorola Android Smartphone). For each different location five measurements of the RAP position were made, and its position calculated. Each test had 10 measurements sent from the mobile devices in the same location, to four different locations in the building on the same environment, making it a total of 40 position measurements for each environment.

Results

Tests showed that the system behaved as desired by having the mobile devices only send information about the Wi-Fi signal if they were motionless. The WA algorithm also had very good results in calculating positions, with error values of 3.61 m. The quality was assessed through the latency, RSSID values and frequency interferences between APs. The quality results were overall good inside the campus building, and as expected, worse outside of it. RAPs interference was also assessed to which the quality decreased slightly when the rogue was in an interfering frequency.

Discussion

The test results showed that the z coordinate was correct for every measurement. Although the values for x and y coordinates had (for both positioning methods) very good results with small errors, these were higher in closed spaces with many obstacles and architectural barriers. For example, some rooms have the ceilings made of plie wood, but others have aluminum sheets to contain the air conditioning conducts; some rooms have glass on the doors lateral and others don't. This caused a difference in the RSSI values obtained from anchor points (APs and sniffers). The more obstacles, the less RSSID values are received and therefore the positioning precision will be worse. This problem can be dealt with by calculating even more precise PLE values, for example a value for each room, and then the system would determine which n is better to use. The positioning of RAPs suffered errors when the distances between sniffers were very large due to the small number of sniffers (only four) and the Raspberry Pi's small range. This problem is easily overcome by simply adding more sniffers to the system.

For sniffers to perform containment of RAPs in the future they will need to have an additional wireless interface that supports monitor/promiscuous to contain the RAP (maybe by simply adding a dongle with this interface).

CONCLUSION

The ENDScanning system showed to be easy and simple to deploy, adaptable and expandable, because it was implemented in the IST Taguspark Campus, but later the student's residence building was quickly included without having to alter any module of the system.

The system obtained very good results for the tests performed in detecting RAPs and assessing the Wi-Fi RS quality. The positioning of both types of nodes had low error values and the z coordinate always had the correct position. The only big issue encountered was the fact that, even though the RAP's containment through DoS was implemented in the system, the raspberry pi used as sniffers couldn't perform it because they needed to have wireless interface that supported monitor/promiscuous mode to contain the RAP.

To improve the system in the future it would be necessary to use sniffer devices that have monitor/promiscuous interface, to contain the RAPs. For better access, visualization and assessment of the system results the system should work with a graphic interface exposing the building plants, the Wi-Fi signal quality by areas and the detected RAPs.

ACKNOWLEDGMENTS

I would like to thank all my colleagues that brought ideas and helped in the development and testing of this work: Pedro Madeira, Vasco Rato, Professor José Sanguino and all the DSI Taguspark team members.

I would also like to thank all the advices, ideas and guiding given to me by my supervisors, Professor Fernando Mira da Silva and Professor Rui Rocha.

Finally, I thank my mom and best friend, for all her love and support, and my brother Natanael.

REFERENCES

1. P. Croak and Y. Kim, "Site Survey Guidelines for WLAN Deployment," 10 April 2013. [Online]. Available: http://www.cisco.com/c/en/us/support/docs/wireless/5500-series-wireless-controllers/116057-site-survey-guidelines-wlan-00.html. [Accessed September 20, 2016]
2. Metageek, "Wi-Spy + Chanalyzer," Metageek, [Online]. Available: http://www.metageek.com/products/wi-spy/. [Accessed September 28, 2016]
3. iBwave Solutions, "iBwave," iBwave Solutions, [Online]. Available: http://www.ibwave.com/. [Accessed September 28, 2016]
4. A. Vlavianos, L. K. Law, I. Broustis, S. V. Krishnamurthy and M. Faloutsos, "Assessing Link Quality in IEEE 802.11 Wireless Networks: Which is the Right Metric?," in IEEE PMRC, 2008.
5. D. Bhardwaj, K. Kataoka, V. A. Vikram and V. Hirani, "Hybrid approach to distributed Wi-Fi performance assessment for multi-floor structures," in 9th International Conference on Software, Knowledge, Information Management and Applications (SKIMA), Kathmandu, 2015.
6. Cisco Systems, "Rogue Detection under Unified Wireless Networks," [Online]. Available: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/70987-rogue-detect.html. [Accessed September 25, 2016]
7. Juniper Networks, [Online]. Available: http://www.juniper.net/us/en/. [Accessed September 29, 2016]
8. Aruba, "Aruba - Enterprise Wireless LAN Solutions," [Online]. Available: http://www.arubanetworks.com/. [Accessed September 29, 2016]
9. H. Han, B. Sheng, C. C. Tan, Q. Li and S. Lu, "A Measurement Based Rogue AP Detection Scheme," in IEEE INFOCOM 2009, Rio de Janeiro, 2009.
10. S. Nikbakhsh, A. B. A. Manaf, M. Zamani and M. Janbeglou, "A Novel Approach for Rogue Access Point Detection on the Client-Side," in 2012 26th International Conference on Advanced Information Networking and Applications Workshops, Fukuoka, 2012.
11. N. M. Ahmad and H. M. Amin, "A RSSI-based Rogue Access Point Detection Framework for Wi-Fi Hotspots," in 2014 IEEE 2nd International Symposium on Telecommunication Technologies (ISTT), Langkawi, 2014.
12. C. Yang, Y. Song and G. Gu, "Active User-Side Evil Twin Access Point Detection Using Statistical Techniques," in IEEE Transactions on Information Forensics and Security, 2012.
13. Juniper Networks, "Understanding Rogue Access Points," [Online]. Available: https://www.juniper.net/techpubs/en_US/junos-space-apps/network-director2.0/topics/concept/wireless-rogue-ap.html. [Accessed December 4, 2016]
14. Cisco Systems, "Cisco Meraki," [Online]. Available: https://documentation.meraki.com/MR/Monitoring_and_Reporting/Air_Marshal#Threat_classifications. [Accessed December 4, 2016]
15. Cisco Systems, "Rogue Detection under Unified Wireless Networks," [Online]. Available: https://www.cisco.com/c/en/us/support/docs/wireless-mobility/wireless-lan-wlan/70987-rogue-detect.html. [Accessed September 25, 2016]
16. T. M. Le, R. P. Liu and M. Hedley, "Rogue Access Point Detection and Localization," in 2012 IEEE 23rd

International Symposium on Personal, Indoor and Mobile Radio Communications - (PIMRC), Sydney, NSW, 2012.

17. S. Anmulwar, S. Srivastava, S. P. Mahajan, A. K. Gupta and V. Kumar, “Rogue Access Point Detection Methods: A Review,” in International Conference on Information Communication and Embedded Systems (ICICES2014), Chennai, 2014.
18. V. S. S. Sriram, G. Sahoo and K. K. Agrawal, “Detecting and Eliminating Rogue Access Points in IEEE-802.11 WLAN - A Multi-Agent Sourcing Methodology,” in 2010 IEEE 2nd International Advance Computing Conference (IACC), Patiala, 2010.
19. C. Gao and R. Harle, “Easing the Survey Burden: Quantitative Assessment of Low-Cost Signal Surveys for Indoor Positioning,” in 2016 International Conference on Indoor Positioning and Indoor Navigation (IPIN), Alcala de Henares, 2016.
20. P. Biswas, T.-C. Lian, T.-C. Wang and Y. Ye, “Semidefinite Programming Based Algorithms for Sensor Network Localization,” in ACM Transactions on Sensor Networks, 2006.
21. E. C. L. Chan, G. Baciu and S. C. Mak, “Orientation-based Wi-Fi Positioning on the Google Nexus One,” in 2010 IEEE 6th International Conference on Wireless and Mobile Computing, Networking and Communications, Niagara Falls, ON, 2010.
22. Bahl, Paramvir, and Venkata N. Padmanabhan. "RADAR: An in-building RF-based user location and tracking system." INFOCOM 2000. Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE. Vol. 2. Ieee, 2000.
23. L. Leite, “Context and Location-Awareness for an Indoor Mobile Guide”, IUI Workshop on Location Awareness for Mixed and Dual Reality, LAMDa’11, 13. February 2011, Palo Alto, California, USA.
24. M. Shchekotov, “Indoor Localization Method Based on Wi-Fi Trilateration Technique,” in Proc. of the 16th Conference of Fruct Associoation, 2014.
25. Theodore Rappaport. 2001. Wireless Communications: Principles and Practice (2nd ed.). Prentice Hall PTR, Upper Saddle River, NJ, USA.
26. Li, Zan, Torsten Braun, and Desislava C. Dimitrova. "A passive Wi-Fi source localization system based on fine-grained power-based trilateration." World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2015 IEEE 16th International Symposium on a. IEEE, 2015.
27. Cisco Meraki, “Channel Planning Best Practices”. [Online] Available: https://documentation.meraki.com/MR/WiFi_Basics_and_Best_Practices/Channel_Planning_Best_Practices [Accessed April 5, 2017]