Detecting and Localizing Wireless Network Attacks Techniques

Iyad Aldasouqi iyad@rss.gov.jo
Princess Sumaya University for Technology
The King Hussein School for Information Technology

Walid Salameh walid@psut.edu.jo
Princess Sumaya University for Technology
The King Hussein School for Information Technology

Abstract:

In order to increase employee productivity within a feasible budget, we have to track new technologies, investigate and choose the best plan and implementation of these technologies.

WLAN is vulnerable to malicious attacks due to their shared medium in unlicensed frequency spectrum, thus requiring security features for a variety of applications.

This paper will discuss some techniques and approaches which can help to detect, localize and identify wireless network attacks, which present a unique set of challenges to IT and security professionals. All efforts were focusing on the ability to identity based attacks in which a malicious device uses forged MAC addresses to masquerade as a specific client or to create multiple illegitimate identities. Also, to be sure that the network is able to robustly identify each transmitter independently of packet contents, allowing detection of a large class of identity-based attacks with high probability.

The attacker can listen to all wireless traffic, compromise encryption and Use attenuators, amplifiers, directional antennas, software radios, but he cannot be at the location of user or at the location of access points. However, we have to choose the best design, implementation, and evaluation techniques in order to secure our network from attackers, where our choice will depend on a technical implementation to mitigate the risk on the enterprise network infrastructure.

Keywords : *Security, Sensors, Access points, wireless, Authentication*

1.Introduction:

Wireless Local Area Network (WLAN) which became increasingly viable for many reasons, the same wireless technology that can erase the physical limitations of wired communications to increase user flexibility, boost employee productivity, and lower cost of wireless network ownership.

Security becomes a key factor and boosts employee demand for access to their enterprise's wireless network beyond the area of their office workstation. In addition, wireless access to a network can represent the entry point for various types of attacks, which can crash an entire network, render services unavailable, and potentially subject the enterprise to legal

liabilities, so we can understand that there are many factors affected on the quality and strength of the security, such as the signal propagation characteristics, limited bandwidth, weak processing capability, and various other reasons.

Wireless Network

Wireless frequencies are designed to be used by anyone with a wireless receiver – anyone can connect to a wireless network in the same way that they can tune into a radio station.

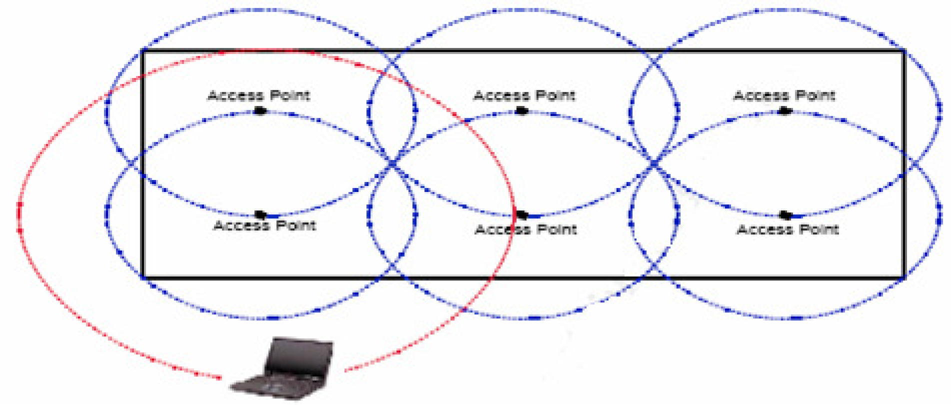


Figure 1: WLAN Coverage can often overrun a building's boundaries.

A wireless local area network (WLAN) is a flexible data communications system that can use either infrared or radio frequency technology to transmit and receive information over the air. In 1997, 802.11 was implemented as the first WLAN standard. It is based on radio technology operating in the 2.4 GHz frequency and has a maximum throughput of 1 to 2 Mbps. The currently most spread and deployed standard, IEEE 802.11b, was introduced late 1999. It still operates in the same frequency range, but with a maximum speed of 11 Mbps.

WLAN has been widely used in many sectors ranging from corporate, education, finance, healthcare, retail, manufacturing, and warehousing. According to a study by the Gartner Group, approximately 50 percent of company laptops around the world will be equipped for WLAN by 2006 [3]. It has increasingly becoming an important technology to satisfy the needs for installation flexibility, mobility, reduced cost-of-ownership, and scalability.

1.1 Intrusion Detection

"For an enterprise to protect itself from abuse of its information, it must monitor the events occurring in its computer system or network and analyze them for signs of intrusion. To do this, the enterprise must install an Intrusion Detection System (IDS)." *Ant Allen, research director at Gartner.*

IDS watch the wired and wireless network from the inside and report or alarm depending on how they evaluate the network traffic they see. They continually monitor for access points to the network and are able, in some cases, to do comparisons of the security controls defined on the access point with pre-defined company security standards and either reset or closedown any non conforming AP's they find. The distinction between placing IDS sensors on both wired and wireless networks is an important one as large corporate networks can be worldwide.

IDS systems can also identify and alert to the presence of unauthorized MAC addresses on the networks. This can be an invaluable aid in tracking down hackers.[1]

However, IDS is a vital component in auditing a network installation.

MAC Address spoofing

MAC addresses can be easily changed through device drivers, effective attacks can be implemented with some equipment available on the market. IEEE 802.11 facing many security threats, which represented by a class of attacks which can be known as masquerading attacks.[3] With such tools, the attacker modifies either the MAC or the IP address of the victim in order to adopt another identity in the network. By this technique the intruder will be able to operate as a trustworthy node and can advertise incorrect routing information to other participants of the network. Another example is creation of loops in the routing computation which result in unreachable nodes.

To prevent and secure the network from spoofing, the specialist divided the techniques into three categories:

1. Sequence number analysis: by modifying the MAC address header, so each device will have a serial number(SN)
2. Transceiver fingerprinting: where each radio transceiver has its unique shape and pattern.
3. Signal strength analysis: which depends on the strength of the coming signals from the clients.

Physical Layer
Physical layer is hard to frog and not easy as the MAC address; because the information in this layer is inherent to radio characteristics and the physical environment, in addition it is used to differentiate devices. Hall uses the frequency-domain patterns of the transient portion of radiofrequency (RF) signals, as a fingerprint, to uniquely identify a transceiver [5].

This paper is divided into three sections. Starting by describing available methods to eliminate attacks; secondly, comparing between available techniques from different perspectives; and thirdly, are my suggestions which are depending on the first two sections in order to bet better results. The rest of the paper organized as follows: survey 802.11 spoofing-based attacks and related detection methods in Section 2. Then describe the key observation regarding section 2 techniques and compare between them in section 3. The suggested technique, which is a hybrid technique from previous two techniques and finally the conclusion, will be in Section 5.

2.Spoofing Attack and related work

It is very important to distinguish between two terms localization and spoof detection, actually they are different types of problems. Localization is based on the assumption that all measurements gathered received signal strength (RSS) are from a single station and, based on this assumption, the localization algorithm matches a point in the measurement space with a point in the physical space. But Spoofing detection distinguish if all matched measurements are from a single station, and tries to determine whether they are definitely from the same station.

2.1. Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength

This method is using “air monitors” (AMs), which is a device available on the market used to passively sniff wireless traffic, without cooperation with other devices (Access Points (APs), computers).
An AM is an embedded device and may not capture all frames sent by transmitters in its range, due to limited resources. Their own AM sniffing software, basset, passively captures wireless frames and forwards the key frame features to a centralized merger, which removes duplicates and synchronizes timestamps to construct a more complete and coherent frame sequence that is stored for further analysis [6].

They developed a RSS profiling algorithm based on the Expectation-Maximization (EM), in which they referenced to Gaussian Mixture Model (GMM) [7]. Once the RSS is ready to receive from any transmitter in normal conditions, it will distinguish any difference in the RSS signals and it will consider it as a potential spoofing attack. After a set of signals received they did some of hypothesis, algorithms and calculations (Ratio Test) as a detection tool each AM in order to increases detection accuracy.

In addition they developed two global detection algorithms which are focusing on:

1. Combine local statistics from multiple AMs.
2. Works on the frame sequence output by the merger.

This method has a role in improving networking intrusion detection via some contributions:

1. Discovered that antenna diversity is the major cause of multimodal RSS patterns.
2. Presented a new GMM profiling algorithm.

2.2. Detecting Identity Based Attacks in Wireless Networks Using Signal-prints

Faria and Cheriton propose to detect spoofing attacks using a signal-print, which is the vector of median RSS for a MAC address measured at multiple AMs [8]. They believed in that a transmitting device can be robustly identified by its signal print, a stream of signal strength values reported by access points acting as sensors. In addition they proved that, different from MAC addresses or other packet contents, attackers do not have as much control regarding the signal prints they produce. Signal-print can be represented by a signal strength characterization of a packet transmission. Each signal-print is represented as a vector of signal strength measurements, with one entry for each access point acting as sensor.

They restricted themselves to 802.11 networks, but as they said the ideas presented can be equally applied to other wireless LAN technologies. Regarding the network architecture they suggested to use the network as in figure2, which composed of multiple access points (APs) distributed across the environment that feed traffic information to a centralized server, which we call a wireless appliance (WA). In addition they focused on the access points deployed as sensors: by observing the traffic on a channel specified by the WA and collect information such as the received signal strength level for each packet successfully received. This information is then forwarded to the WA, which is able to create a signal-print for each packet of interest. [8]

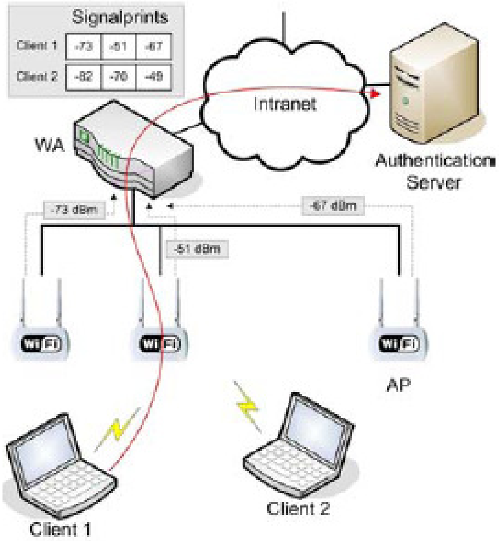


Figure 2: Signal-print creation

Signal-print Properties:

-Signal-prints are hard to spoof. Signal attenuation is a function of the distance between clients and access points, with a strong dependence on environmental factors such as construction materials and obstacles such as furniture items [9, 10].

-Signal-prints are strongly correlated with the physical location of clients, with similar signal-prints found mostly in close proximity.

-Packet bursts transmitted by a stationary device generate similar signal-prints with high probability.

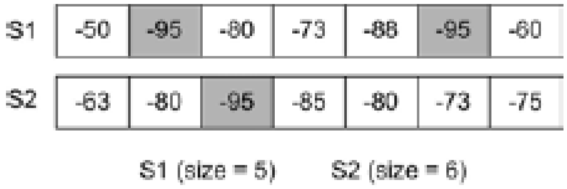
-Signal-prints allow a centrally controlled WLAN to reliably single out clients. Instead of identifying them based on MAC addresses or other data they provide, signal-prints allow the system to recognize them based on what they look like in terms of signal strength levels.

MATCHING SIGNALPRINTS:

In order to distinguish between different based attacks signals matching rules are specified.

These rules can be categorized into:

- Differential Values: which represent the absolute values (In dBm) of the difference between the value at a given position and the maximum value found in that signal-print.

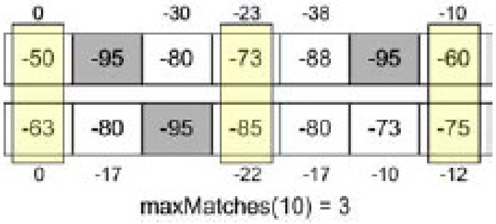


S1	-50	-95	-80	-73	-88	-95	-60
S2	-63	-80	-95	-85	-80	-73	-75

S1 (size = 5)   S2 (size = 6)

Figure 3: Shows two signal-prints and their corresponding sizes.

- Max-Matches: Matches are found by comparing values at the same position in two different signal-prints.

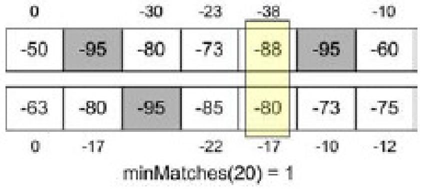


0		-30	-23	-38		-10
-50	-95	-80	-73	-88	-95	-60
-63	-80	-95	-85	-80	-73	-75
0	-17		-22	-17	-10	-12

maxMatches(10) = 3

Figures 4: Demonstrate how max-matches are computed.

- Min-Matches: Analogous to a max-match, which is found whenever values differ by at least a certain value in dB.



0		-30	-23	-38		-10
-50	-95	-80	-73	-88	-95	-60
-63	-80	-95	-85	-80	-73	-75
0	-17		-22	-17	-10	-12

minMatches(20) = 1

Figures 5: Demonstrate how min-matches are computed.

Matching Rules: a pair of signal-prints matches if they satisfy a specified matching rule, a Boolean expression involving numbers of max-matches and min-matches, and possibly signal-print properties such as size. Example: The matching rule max-Matches(S1; S2; 5) ≥ 4 requires two signal-prints to have RSSI values within 5 dB of each other in at least 4 positions.

Finally, attack detection has three properties which are important for the analysis of this method: R denotes the rate in packets per second (pps) required for a given DoS attack to be effective. S denotes the speed of the device. A denotes the number of antennas under the control of the attacker.

2.3. Wireless Client Puzzles in IEEE 802.11 Networks: Security by Wireless

It is a protection method which assists an AP to preserve its resources by discarding fake requests, while allowing legitimate clients to successfully join the network. Rather than conditioning a puzzle's solution on computational resources of highly heterogeneous clients, the puzzles utilize peculiarities of a wireless environment such as broadcast communication and signal propagation which provide more invariant properties. [13]

The puzzle is a question about which other stations are in the client's signal proximity as in figure.6, and can thus be labeled as neighbors. The received signal strength of neighbors is strong, contrary to non-neighbors which are received weakly in relation to a certain signal value. In other words it is security by wireless application, since it is exploit the chaotic and erratic character of radio communications, describing the radio of the neighborhood, do the mutual verification via the broadcasting as in figure 7.and depending on the new location of the client (N) there will be different solutions as in figure 8.

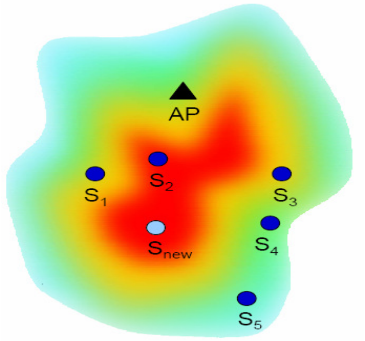
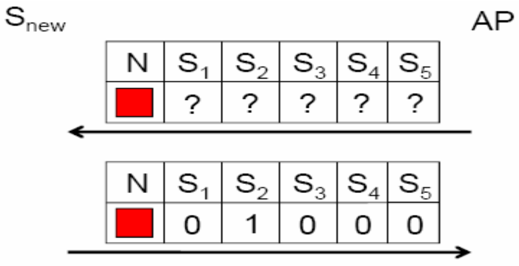


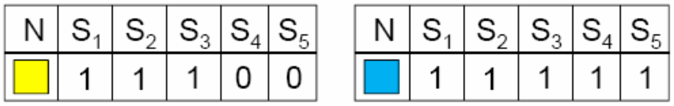
Figure 6: Signal Proximity



N	S_1	S_2	S_3	S_4	S_5
🟥	?	?	?	?	?

N	S_1	S_2	S_3	S_4	S_5
🟥	0	1	0	0	0

Figure 7: Mutual verification



N	S_1	S_2	S_3	S_4	S_5
🟨	1	1	1	0	0

N	S_1	S_2	S_3	S_4	S_5
🟦	1	1	1	1	1

Figure 8: Solutions for different N's

Asymmetries and noise in the wireless channel can cause wrong solutions for honest requests; which caused by small deviations as in figure 9.

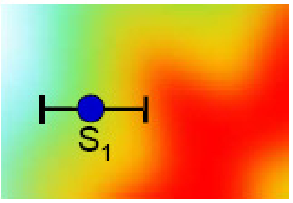


Figure 9: Small deviation gives wrong solutions

Therefore, the attackers can't exploit these tolerance intervals, which make it hard for them to attack the network.

The puzzle experiment started with the AP broadcasting the NST (The Neighborhood Signal Threshold) within a beacon frame. The NST was randomly chosen by the AP from values between -55 dBm and -95 dBm in steps of 5 dBm and changed every 7 seconds. The joining station monitors the channel and computes the sample median (choose a sample size of 20 received frames) that, after receiving a beacon frame and identifying the NST, is used to create a region by selecting those stations as neighbors whose signal strength is greater or equal to the current NST. The region is then sent along with the authentication requests to the AP. If no warnings arrive (the timer was set to 1 second) and no such region has already been used by another associated station, the AP responds with an authentication successful frame and proceeds with the association procedure. On the other hand, if a warning arrives the joining station is declined and it must wait for a different NST to re-attempt the authentication procedure. [13]

An AP has a decision role in selecting a subset of its associated stations to participate in wireless client puzzles in order to avoid increasing the number of false positives in larger networks, which will eliminate the number of warnings and false positives resulting from unsymmetrical channels. So if these subsets changed randomly, it will be too difficult for an attacker to guess which stations are currently monitoring the channel.

2.4. Advancing Wireless Link Signatures for Location Distinction (AWLS)

The authors of this technique want to show that: Detecting whether a transmitter is changing its location or not. In other words, unlike localization or location estimation, location distinction does not attempt to determine where a transmitter is. Therefore it is useful in many applications; especially it can enforce physical security by identifying illegal transmitter.

In this technique they use sophisticated physical-layer measurements in wireless networking systems for location distinction. First they compared two existing location distinction methods

1. Channel gains of multi-tonal probes: where the channel frequency response is sensitive to each multipath. An impulse in the time domain is a constant in the frequency domain, and thus a change to a single path may change the entire multiple tone link signature.
2. Channel Impulse Response (CIR): it uses a time domain signature, which support it with more robust against channel small changes.

Then, they combined the benefits of these two methods to develop a new link measurement that called the complex temporal signature. They used a 2.4 GHz link measurement data set, to evaluate the three location distinction methods. They found that the complex temporal signature method performs significantly better compared to the existing methods. They also perform new measurements to understand and model the temporal behavior of link signatures over time. They integrated their model in location distinction mechanism and significantly reduced the probability of false alarms due to temporal variations of link signatures. [14]

The link signatures in the multiple tones probing method and in the temporal link signature method both make measurements of the multipath channel and use them to quantitatively identify a link.

In addition, AWLS improved the multiple tone probing method by developing a new link signature using the strengths of the two existing methods. The proposed improvements includes:

1. A new metric related to the first method, that improve its robustness to changing received powers.
2. Come with a new method which combines the strength of the two methods, and show that a simple metric is robust to uninformative, random phase shifts, which will give us an accurate measured distance between two link signatures.

2.5. PARADIS: Physical 802.11 Device Identification with Radiometric Signatures

This technique used passive radio-frequency analysis to identify the location. They measure artifacts of individual wireless frames in the modulation domain, identify a suite of differentiating features, and apply efficient 802.11-specific machine-learning based classification techniques to achieve significantly higher degrees of accuracy than prior best known schemes. [17]

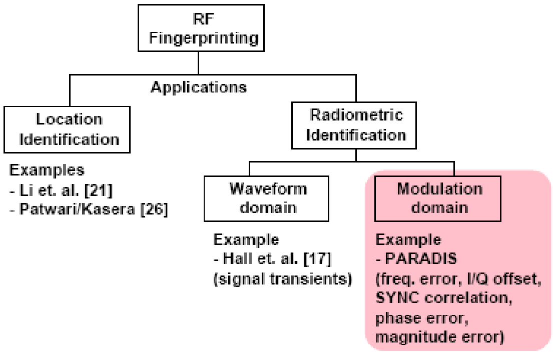


Figure 10: Radiometric identification and PARADIS.

This system built to distinguish between 802.11 nics and to achieve significantly improved identification accuracy when compared to schemes operating over transient signal characteristics. Furthermore Paradis uses distinct features from the modulation domain, frequency error, magnitude error, phase error, I/Q offset, and sync correlation of the corresponding wireless frame.

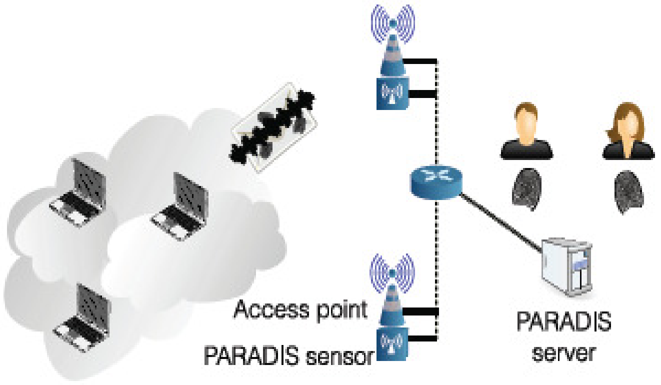


Figure 11: PARADIS schematic

Every radio transceiver can be presented by a unique physical signal, which guided them to build a library of patterns. To distinguish between these pattern they used wavelet and fuzzy neural networks as in figure 12. Therefore, to implement this technique the requirement cost will be high for both measurement and analysis devices, and thus limits the use of this technique.

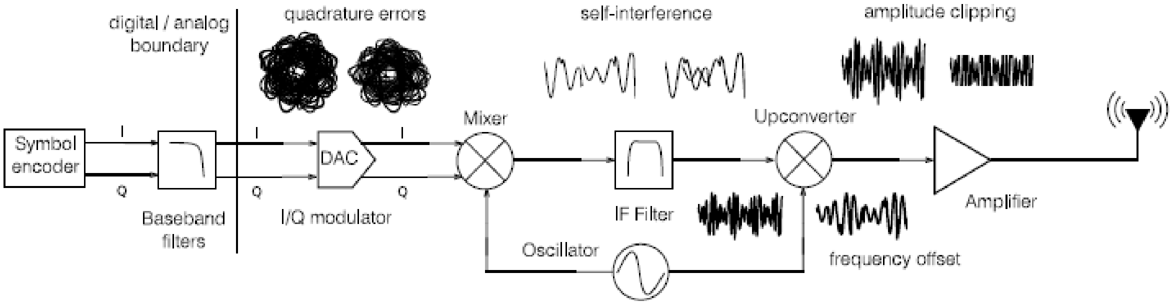


Figure 12: Common transmitter impairments and their sources

3. Analysis and Comparison

3.1 Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength versus other techniques using RSS

Detecting 802.11 techniques believed that these RSS-based detection methods are not effective due to recent advances in wireless hardware. And they proved that via conducting a series of large scale experimental studies of RSS measurements.

There are wireless networks classes that provide automatic reconfiguration of APs, adjusting power levels and channel assignments to optimize coverage while minimizing contention between neighbors. Most such systems reconfigure infrequently. By comparing the detecting 802.11 method with other methods using network management software we can see that this method can re-compute an AP's profile whenever it is reconfigured.

3.2 Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength versus Detecting Identity Based Attacks in Wireless Networks Using Signal-prints

Refers to detecting 802.11, Signal-print demonstrated above 95% detection accuracy in their test bed. False positive rate is not reported. They did observe some missing RSS measurements for AMs, and for signal-print-matching they propose to ignore any AMs with missing RSS values. However, they did not use statistical methods. On the other hand the Detecting 802.11 they did like signal-print's work; they also build a normal profile for a transmitter, and detect spoofing attacks by matching to the profiles. In addition their detector works even if the genuine station is quiet or absent, or there are multiple attackers. Unlike signal-print, their algorithm uses per-frame RSS measurements and multiple AMs. They re-implemented signal-print's algorithms, to the best of understanding.

3.3 Detecting Identity Based Attacks in Wireless Networks Using Signal-prints versus client puzzles

Puzzles technique enforced any incoming request to send back computational puzzles, which require CPU- or memory intensive operations. In addition puzzles demand that both clients and servers be modified, increasing deployment overhead when compared to a signal-print based mechanism, implemented solely at the WA. On another side Signal-print gives a similar efficiency with less cost and equipment. The puzzle weak point is if an attacker finds a physical position, or is able to find a signal strength for transmitting a region such that k stations tolerate it, it can generate as many as 2k different regions that will not result in warnings. But in Signal-print the weak point is when two clients are very close to each other WA can't distinguish them from each other.

Furthermore, puzzle technique has an alternative approach which is to use dedicated devices (ex. Sensors (similar to Signal-print technique)) installed by a network operator to implement wireless client puzzles instead of associated stations. These sensors play the same role and cover more regions with a small number of stations.

3.4 Advancing Wireless Link Signatures for Location Distinction (AWLS) versus other techniques

Importantly, the multiple tone link signatures are a complex measurement, while the temporal link signature is a real-valued measurement. The inclusion of phase information in the multiple tone signature effectively increases the richness of the measurement space. The temporal link signature, with only magnitude information, does not retain some identifiable information about a link captured by the channel phase response, and thus we would expect it to lose some ability to uniquely identify links. [14] Also, unlike localization or location estimation, the objective of location distinction is only to distinguish one link signature from another, and not to map the signature to a particular physical coordinate as in other techniques.

Furthermore, both AWLS and Signalprint are using RSS-based signalprints to prevent impersonation in wireless local area networks, which is readily available in commodity wireless cards. But it fails to capture the rich multipath characteristics of wireless channels. After that Patwari et al [15] solved that problem by proposing the use of temporal channel impulse response, which captures the multipath characteristics of wireless channels, as a link signature for location distinction, and Li et al [16] proposed the use of complex channel gains by multi-tonal probes, that also captures multipath effects, for securing wireless systems.

4. Improvements and solution

In this section 2 propose improvements to the signal print method described in Section 3.
First, as seen in section one and two, most of Identification techniques are referred to Farias[8] as a reference and tried to compare their results with his result. Therefore I also put my suggestion depending on Farias[8]results. Second, I present how to modify this technique by using two approaches:

First Approach:

Starting from the week point (limitation):

"Due to the use of RSSI levels to characterize wireless clients, one inherent limitation of our mechanism is that it may be unable to distinguish two devices located physically close to each other. Masquerading attempts can be detected if there is a noticeable difference in RSSI with respect to at least one access point. This happens even for some locations in close range, possibly due to obstacles that affect one location more than the other. In some situations - such as multiple clients in a conference room - the system may not have compelling evidence that packets are coming from different devices, making masquerading attacks possible." [8]

As known it is very hard for an attacker in any location to get close enough to the victim in offices or working area and do masquerading attack. But it will be easier for him to do that in meeting rooms or at cafeterias.

In order to prevent this from happing, I suggest doing the following:

1. Depending on the size of (cafeteria or meeting room), I suggest to have at least two AP's (it is an additional cost, but compared with it is benefit it is acceptable), which can help in showing the variances of signal print between closed clients.
2. Some times it is not applicable to have more than two AP in a small location (meeting room or cafeteria), in this case since there is a server (Authentication server), we can get benefit from the response time to calculate the distance from the access point. This addition can be added as a logical statement in the authentication application (program), first by determine which AP gives the highest signal-print, then calculate the distance when received many request from the same location. The distance will help us in determining if the signal is coming from the same client or not, so if there is a difference it means from different clients, in this case matching rules can be applied to a new list which consists of the signal print and the distance. In the existing technique if many requests received from one signal-print, this client will be considered as an attacker, which most of the time is correct, but if there is clients who are very close to each other they will reduce the same signal-print but they are not attackers. From this suggestion, it will be easy to distinguish between closed clients and attackers. (example. channel impulse response)

Second Approach:

In this approach I suggest another solution to overcome Farias[8] limitation by using some ideas from another technique (puzzle technique [13]).

The puzzle technique is using the signal print as an alternative approach, so what I\m suggesting is to use puzzle as an alternative technique for the Signal-print.

In puzzle technique, since it depends on functionality of neighborhood monitoring, so it is centralized /decentralized where each station plus the server can distinguish its neighbors, this will affect not only on the server, but also on the station (authentication on station bases and server), this will secure the network but will exhaust the resources.

In Signal-print the entire load is only on the server and nothing on the stations; so this is the main reason of the limitation.

My suggested solution is get benefit from the authentication technique in the puzzle and uses it in the signal-print. The authentication in the puzzle is not only the username and password, but also part of the packet will represent the puzzle (The frames consist of an IEEE 802.11 frame header and an additional custom puzzle header that contains all required information (Defined within a frame's custom Information Elements)[13]), in addition to get benefit from puzzle zones (without neighbors authentication) to confuse the attacker, so he can't guess to which AP the client related.

By using first approach which can overcome Signal-print limitation with little affect on the server, but by using second approach which can increase the security level by additional affect on the server.

5. Test bid

As an implementation of previous works and explaining the idea in more details, I did the following survey in order to choose the type and direction of the antenna; therefore the zone of the access point can be specified.

This will be a prototype and can be applied to a complex network, so the hacker can't know to which access point the victim is connected. In addition, reference to my second approach (using puzzle authentication technique in signal print), each zone can have its covered area and its range of IP's.
After the survey done, the boundaries of the access point zone can be specified, not only that, but it added strength to the algorithm used to determine the locations of access points (Gaussian Mixture), so this will guide us to choose the optimal number and the most appropriable location of the access points.

To implement this survey I used the area shown in figure.12, I call it Outdoor Test Facility (OTF), which is used for testing and evaluation of wireless video system and ground sensors, the tower is used to hang the camera and wireless system on, where both of them can be powered by electricity of battery charged by solar panel (which is enough for three windy days). To implement this I used the following tools:

- CISCO Aironet 350
- 13.5db antenna
- Laptop with Network Stumbler software
- External either net card
- GPS

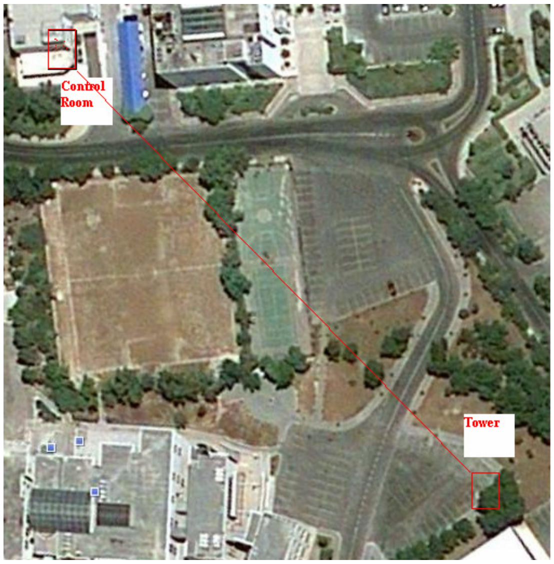


Figure 12: Outdoor Test Facility (OTF)

The distance between source (tower) and destination (control room) is 200m.

As shown in table.1 there are five columns, distance and bearing are readings from GPS, and the rest are from the software. Different types of graphs can be generated which can describe the relation between different readings. As an example, also generate a graph that represents the relation between signal and noise as in figure 13; the signal strength decreases as the noise increases.

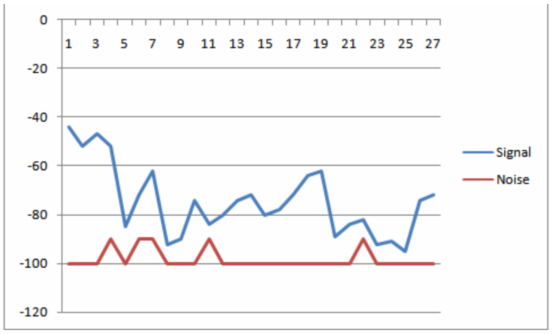


Figure 13: Signal / noise relationship

Another relation can be built between the signal and the data rate. The relation between them is a direct correlation as shown in figure 14

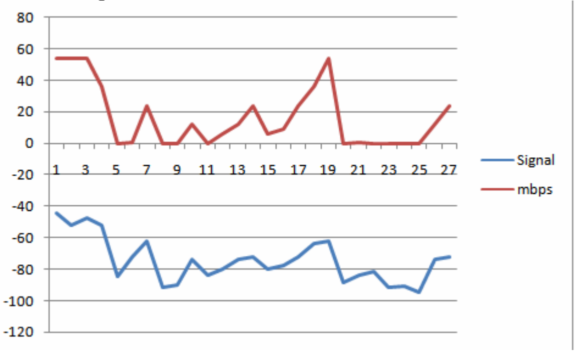


Figure 14: Signal / Data rate relationship

A third relationship can be built between the signal and distance; the signal strength becomes weaker as go further from the source as in figure 15.

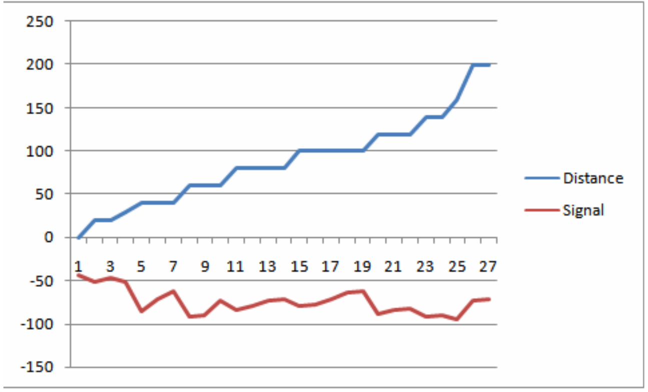


Figure 15: Signal / distance relationship

In order to choose the appropriate type of antenna, not all readings are taken into consideration. However readings are needed to verify our assumption. Only distance and signal will be used to draw the output, fist order the readings depending on distance then on signal. After that draw a radar chart of the signal readings, finally the output will be as shown in figure.16

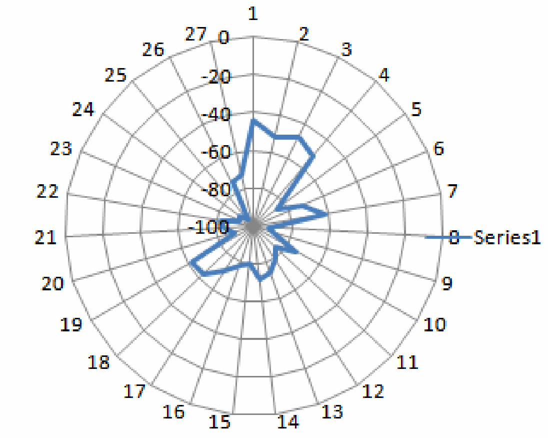


Figure 16: Signal out put

Then by comparing figure 16 with figure 17 recognize that used antenna is a directional antenna.

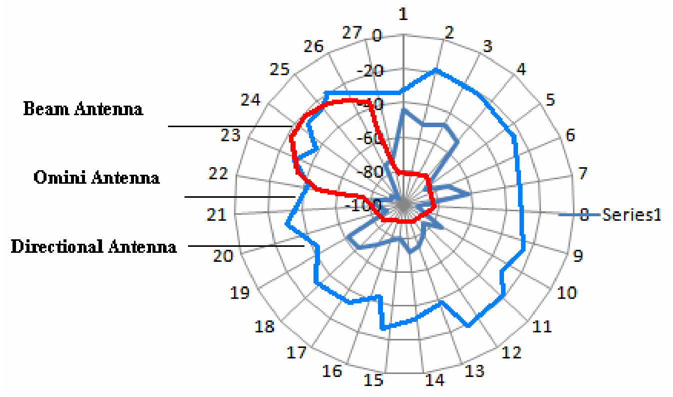


Figure 17: Antennas types

Distance	Bearing	Signal	Noise	mbps
0	240	-44	-100	54
20	270	-52	-100	54
20	250	-47	-100	54
30	290	-52	-90	36
40	80	-85	-100	0
40	340	-72	-90	1
40	20	-62	-90	24
60	100	-92	-100	0
60	120	-90	-100	0
60	140	-74	-100	12
80	160	-84	-90	0
80	180	-80	-100	6
80	200	-74	-100	12
80	220	-72	-100	24
100	330	-80	-100	6
100	300	-78	-100	9
100	280	-72	-100	24
100	240	-64	-100	36
100	260	-62	-100	54
120	20	-89	-100	0
120	0	-84	-100	1
120	340	-82	-90	0
140	60	-92	-100	0
140	40	-91	-100	0
160	60	-95	-100	0
200	230	-74	-100	12
200	240	-72	-100	24

Table1: Survey readings

As a result of this survey, the knowing of the boundaries of the access point can help us to monitor and secure our network. In addition, it will help us in our planning and future expansion, since this survey achieved our goal/assumption, it can be applied to a complex network and which can be considered as an additive security layer.

6. CONCLUSION:

MAC addresses of wireless frames can be easily forged, imposing a serious security challenge. After many experiments and researches published regarding this problem, the Received Signal Strength (RSS) which is related to the Physical-layer is most appropriate tool and it is hard to forge, in another words it can be used to detect such spoofing.

In this paper compared many existing location distinction methods. I also suggest some improvement for signal-print [8] method by using different approaches, response time approach and used the strengths of the two existing methods [8] and [13]to develop a new approach.

Nevertheless, there are still various interesting issues left open for further investigation; because until now and after all of these researches the number of false positives warning in large networks. If it is possible to control this issue the attacker will be confused and can't predict which stations are currently monitoring the channel.

Signal-prints give a good indication for the relation between mobile devices in wireless network and their physical location. The challenges are for both, the network administrator and for the attacker. For the attacker, it is how to masquerade the victim, and for the network administrator is how to protect the network without extra load and overhead on the network infrastructure.

Finally, Security methods and techniques are like antibiotics', it kills the germs. Meanwhile it has side effects on the body. In other words security slows down the network speed, but without it, we can't run our networks.

7. References:

1. **FOR CONFERENCES:** Wireless Intrusion Detection Systems, SANS, Ken Hutchison, 2004

2. **FOR JOURNALS:**Mobile and Wireless Network Security and Privacy, Edited by S. Kami Makki, Peter Reiher, Kia Makki, Niki Pissinou, Shamila Makki. 2007 Springer

3. **FOR CONFERENCES:** Swisscom.com. "Swisscom Mobile to launch Public Wireless LAN on 2, December 2002." 2 Jan. 2003. URL: http://www.swisscom.com/mr/content/media/20020924_EN.html (9 Dec. 2002).

4. **FOR CONFERENCES:** LAN MAN Standards Committee of the IEEE Computer Society. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Speci_cations - Amendment 6: Medium Access Control (MAC) Security Enhancements. Technical Report 2004 Edition, IEEE Std 802.11i, July 2004.

5. **FOR CONFERENCES:** J. Hall, M. Bareau, and E. Kranakis, "Using transceiverprints for anomaly based intrusion detection," in Proceedings of 3rd IASTED, CIIT, Nov. 2004, pp. 22–24.

6. **FOR CONFERENCES:** Y. Sheng, G. Chen, K. Tan, U. Deshpande, B. Vance, C. McDonald, H. Yin, T. Henderson, D. Kotz, A. Campbell, and J. Wright, "Securing 802.11 wireless networks through fine-grained measurements," Submitted to IEEE Wireless Communications Magazine.

7. **FOR JOURNALS:** R. A. Redner and H. F. Walker, "Mixture densities, maximum likelihood and the EM algorithm," SIAM Review, vol. 26, no. 2, pp. 195–239, 1984.

8. **FOR JOURNALS:** D. B. Faria and D. R. Cheriton, "Detecting identity-based attacks in wireless networks using singalprints," in Proceedings of WiSe'06: ACM Workshop on Wireless Security, Sept. 2006, pp. 43–52.

9. **FOR JOURNALS:** H. Hashemi. The Indoor Radio Propagation Channel. Proceedings of IEE, 81(7):943-968, July 1993.

10. **FOR BOOKS:** T. S. Rappaport. Wireless Communications – Principles and Practice. Prentice Hall PTR, 2nd edition, Jan. 2002.

11. **FOR JOURNALS:** K. J. Ellis and N. Serinken. Characteristics of Radio Transmitter Fingerprints. Radio Science, 36:585-598, 2001.

12. **FOR JOURNALS:** M. Gruteser and D. Grunwald. Enhancing Location Privacy in Wireless LAN Through Disposable Interface Identifiers: A Quantitative Analysis. Mobile Networks and Applications, 10(3):315-325, June 2005.

13. **FOR JOURNALS:** Wireless Client Puzzles in IEEE 802.11 Networks: Security by Wireless, Ivan Martinovic, Frank A. Zdarsky, Matthias Wilhelm, Christian Wegmann, and Jens B. Schmitt

14. **FOR JOURNALS:** Advancing Wireless Link Signatures for Location Distinction, by Junxing Zhangy Mohammad H. Firoozz Neal Patwariz Sneha K. Kaseray

15. **FOR CONFERENCES:** N. Patwari and S. K. Kasera. Robust location distinction using temporal link signatures. In ACM Intl. Conf. on Mobile Computing Networking (Mobicom'07), Sept. 2007.

16. **FOR CONFERENCES:** Z. Li, W. Xu, R. Miller, and W. Trappe. Securing wireless systems via lower layer enforcements. In Proc. 5th ACM Workshop on Wireless Security (WiSe'06), pages 33-42, Sept. 2006.

17. **FOR CONFERENCES:** PARADIS: Physical 802.11 Device Identification with Radiometric Signatures by Vladimir Brik, Suman Banerjee, Marco Gruteser, Sangho Oh