Determining an Optimal Number of Access Points Using GPS Data to Secure a Wireless Network Environment

Iyad Aldasouqi iyad@rss.gov.jo
Royal Scientific Society
Information Technology Center
Amman, 11941, Jordan

Walid Salameh walid@psut.edu.jo
Princess Sumaya University for Technology
The King Hussein School for Information Technology
Amman, 11941, Jordan

Abstract

Determination of the position enables location awareness for mobile computers in any place and persistent wireless computing. In addition utilizing location information, location aware computers can render location based services possible for mobile users. In order to design and implement a technique to identify the source network interface card, a feasibility study should be done to keep the project within the budget; also tracking of new technologies will enhance the methodology of choosing these techniques. Wireless Local Area Network (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 a technique that helps in determining the best location for access points using GPS system, in order to choose the optimal number of them; which guide to localize and identify attacks with optimal IDS method and cheapest price. The other thing is to locate the intruder within the monitored area by using a hybrid technique, which came from exist techniques, by focusing on the advantages of these techniques and come with a new one to give more accurate results with less price by using available resources.

Keywords: Security, Sensors, Access points, Wireless, Authentication

1. INTRODUCTION

WLAN is a flexible data communications system that can use either infrared or radio frequency technology to transmit and receive information over the air. Also WLAN has been widely used in many sectors starting from corporate, education, finance, healthcare, retail, manufacturing, warehousing, clinics airports and schools; since it can overcome the physical limitations of wired communications and the simplicity of its installation, so it increases the user flexibility, employee motivations, and reduces the cost. Furthermore, the WLAN infrastructure can be applied to provide indoor location service without deploying additional equipment [19]

The use of different technologies (attenuators, amplifiers, antennas, and software) can be attached by smart attackers, but the attacker cannot masquerade the identity of the user; because in this case he should be located on the same location of the user or at the location of access points. However, to secure the network, we have to cover the area with certain pattern of access points; so we can be sure that each access point has the ability to cover its own area and can identify the login users depending on his/her identity and physical location. By this the network will be secured against any attack and the budget of the project will be under control.

In the last decade, researchers have proposed a number of WLAN positioning techniques for (local area) wireless networks [26,27,28,29]. Despite the cost advantage and productivity offered by WLAN, the used radio waves in wireless networks create a risk, and give a chance for the hackers to attack the network. So the real challenge is to boost employee demand for access to their enterprise's wireless network beyond the area of their office workstation. In addition, the controlling of the quality and strength of the security (Signal propagation, characteristics, limited bandwidth and other) is another challenge which the designer of the network should consider.

The Global Positioning System (GPS) is used for position location, navigation, and precision timing. It accomplishes this using three segments: (1) satellites, (2) ground control centers, and (3) receivers. Anyone can simply go online and get a map of the exact location of an insecure network identified by a war driver [16]. But unfortunately, the GPS system cannot be used effectively inside buildings and in dense urban areas due to its weak signal reception when there are no lines-of-sight from a MS to at least three GPS satellites [18], for this reason the experiment in this paper done outdoor using the same AP which will be used indoor to now the coverage of each AP.

1.1 Wireless Network

The physical architecture of WLAN is simple. Basic components of a WLAN are access points (APs) and Network Interface Cards (NICs)/client adapters. In addition Wireless frequencies are designed to be used by anyone with a wireless receiver (NIC)

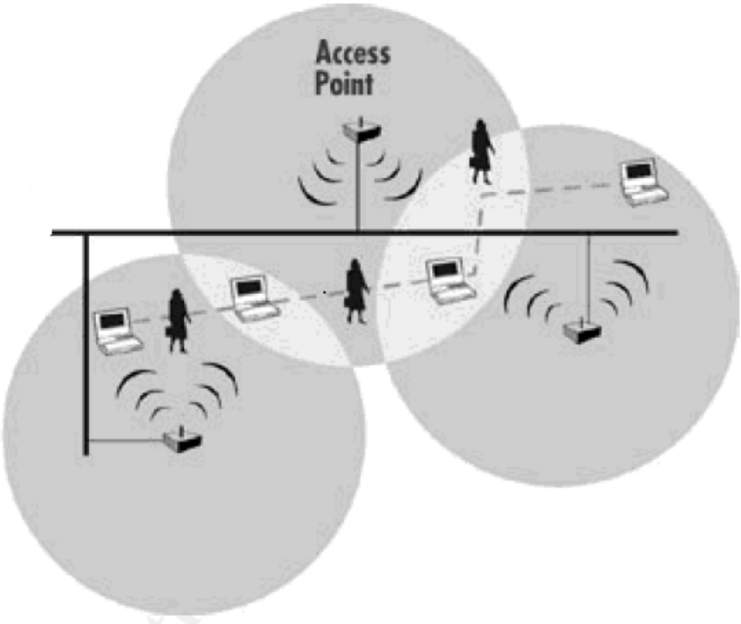

FIGURE 1: WLAN Coverage [1]

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 order to extend WLAN range, and facilitate the user mobility a multiple access points is required, which is one of the main benefits of WLAN. Therefore, it is very important to ensure that users can move seamlessly between access points without having to log in again and restart their applications.

To control the spread of WLAN, a standards was started in order to keep the rangers of wireless waves within ranges and to organize the work, e.x 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.

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]. Therefore, nowadays all laptops are equipped by WLAN from different vendors with almost the specifications with small differences.

1.2 Detecting and preventing network intrusions

Intrusion detection (ID) considered as a type of security management system (device or application) for computers and networks activities for malicious activities or policy violations. An ID system gathers and analyzes information by monitoring the events from various areas within a computer or a network to identify possible security breaches or possible incidents, which include both intrusions (attacks from outside the organization or out side.

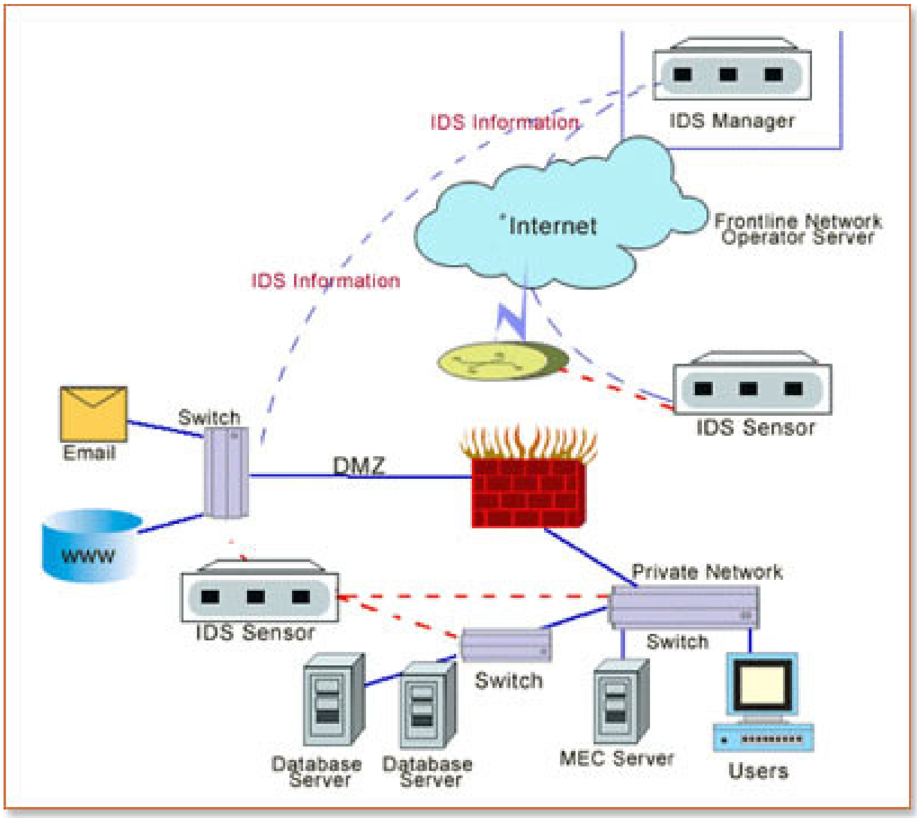

Figure 2: Security Technologies - Intrusion Detection System
(Source: http://indiacyberlab.in/security-awareness/security-technologies.htm)

IDS differ from a firewall, in which a firewall looks out for intrusions in order to stop them from happening. In addition the firewall limits the access between networks in order to prevent intrusion, but can not do the same for an attack from inside the network. Where the IDS evaluates a suspected intrusion once it has taken place and signals

Intrusion detection functions can be summarized as:

- Monitoring and analyzing both user and system activities
- Analyzing system configurations and vulnerabilities
- Assessing system and file integrity
- Ability to recognize patterns typical of attacks
- Analysis of abnormal activity patterns
- Tracking user policy violations

1.3 MAC Spoofing

The phrase “MAC address spoofing” in this context relates to an attacker altering the manufacturer-assigned MAC address to any other value. This is conceptually different than traditional IP address spoofing where an attacker sends data from an arbitrary source address and does not expect to see a response to their actual source IP address. MAC address spoofing might be more accurately described as MAC address “impersonating” or “masquerading” since the attacker is not crafting data with a different source than is their transmitting address. When an attacker changes their MAC address they continue to utilize the wireless card for its intended layer 2 transport purpose, transmitting and receiving from the same source MAC. [4]

Recently some devices can be found on the market, which can easily change the MAC address. By using these tools, the attacker modifies either the MAC or the IP address of the victim in order to adopt another identity in the network.

To illuminate the spoofing, there are three techniques:

1. Sequence number analysis
2. Transceiver fingerprinting:
3. Signal strength analysis:

1.4 Access Point location

The access point is the first gate that the hacker is thinking to use, and so the best and suitable place for WLAN access points is outside the firewall. Therefore, only legitimate users based on MAC and IP addresses can be able to access the firewall. However, this is considered a perfect solution; since MAC and IP addresses can be spoofed, so by this approach it is difficult for a hacker to attack the network; because we are working with physical layer, which is hard to frog and not easy as the MAC address; since the information in this layer is inherent to radio characteristics and the physical environment, in addition it is used to differentiate devices.

Furthermore, the ability to track and check the location of people or equipment in real time has a large number of application areas such as child safety, prisoner tracking and supply chain to name but a few [23]. Therefore, Over the past two decades a large number of commercial and research location aware systems have been developed [24].

This paper is divided into four sections. Starting by introduction, then by describing available methods to eliminate attacks “IDS”; after that, the approach to increase the security of the network by using minimum number of access points. And the last section is a real test to verify the suggested approach. Finally ending with conclusion and future works.

2. SPOOFING ATTACK AND RELATED WORK

There are many available techniques which can detect different types of intrusion, the differences between these techniques are in performance and in the ability to detect and locate the intruder, and this section summarized some of famous techniques which can do that with an easy implementation and reasonable budget. In addition, these solutions require the cooperation of the APs [29-33].

Location estimation systems based on radio signal strengths can be classified into two main categories [17]: (1) Radio-Propagation Models (2) Empirical-Fit Models. Some of these techniques are used for localization and spoof detection, and others for detection only. Localization considers all measurements gathered received signal strength (RSS) are from a single station; therefore it matches a point in the measurement space with a point in the physical space. Where spoofing detection tries to determine whether the signals are definitely from the same station or not.

2.1 Detecting and Localizing Wireless Spoofing Attacks

It is a method for detecting spoofing and locating the positions of the attacks. This method uses the K-means cluster analysis, and then to localize the position of the attacker it integrates the attack detector into a real-time indoor localization system. In addition it uses two algorithms (once at a time) a) Area-based and b) point-based to localize the intruder; since both algorithms have the same relative errors as in the normal case.

As an implementation and evaluation of this method, the authors used both an 802.11 (WiFi) network as well as an 802.15.4 (ZigBee) network. And they proofed that it is possible to detect wireless spoofing with both a high detection rate and a low false positive rate, thereby providing strong evidence of the effectiveness of the K-means spoofing detector as well as the attack localizer.[5]

2.2 Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength

To monitor any network either a hardware solution (ex. Air monitor AM) or a software solution is needed, sometimes both hardware and software with the same solution (ex. sniffer) can be found. This method beside using the access points uses AM to monitor the traffic, which can be consider as load on the network, but some solution gives the priority for the security. And also developed a RSS profiling algorithm based on the Expectation-Maximization (EM), in which they referenced to Gaussian Mixture Model (GMM) [6]. After RSS receive transmitter's signal, immediately calculate the differences, and if there is any it will consider it as a potential spoofing attack.

In addition this method developed two global detection algorithms which are focusing on:[7]

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

Also it has a role in improving networking intrusion detection via some contributions:[7]

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

2.3 Detecting Identity Based Attacks in Wireless Networks Using Signal-prints

This method proposed a technique to detect spoofing attacks using a signal-print, which depends on RSS for a MAC address measured at multiple AMs. The authors ideas built upon that a transmitting device can be robustly identified by its signal print, where the access point will work as a sensor which sensing the signal strength values. The using of signal strength makes the attackers jammed and also they do not have as much control regarding the signal prints they produce; each signal-print is represented as a vector of signal strength measurements. In addition the authors used 802.11 networks, but the same technique can be applied to other wireless LAN technologies.

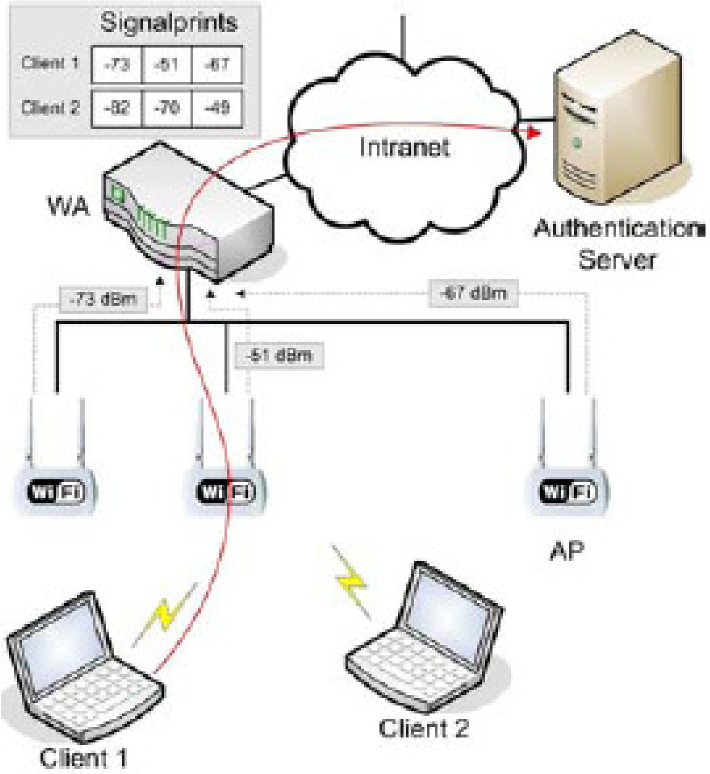

FIGURE 3: Signal-print creation [9]

The Signal-print is used because it is hard to spoof, since its attenuation is a function of the distance between clients and access points.

In addition Signal-prints are strongly correlated with the physical location of clients, with similar signal-prints found mostly in close proximity. [9]

2.4 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. [10]

The puzzle is a question about which other stations are in the client's signal proximity as in figure.4, 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. And depending on the new location of the client (N) there will be different solutions. [7]

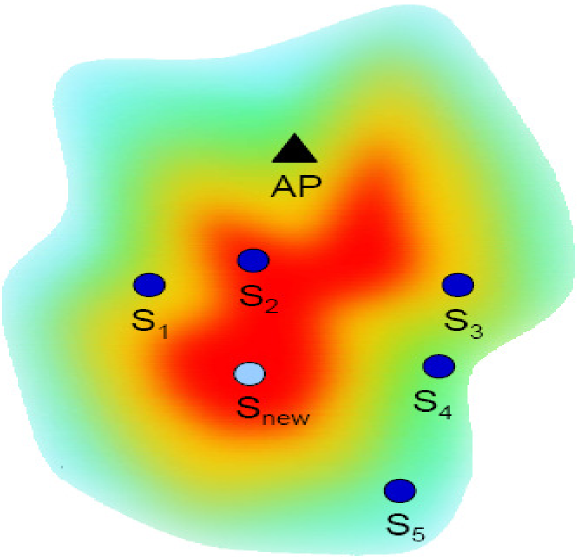

FIGURE 4: Signal Proximity [10]

2.5 Advancing Wireless Link Signatures for Location Distinction (AWLS)

This method is used to locate the transmitters even if the location changed. So it will enforce physical security by identifying illegal transmitter and preventing them from accessing the network.

A sophisticated physical-layer measurement is used to locate distinction. This done by compared two existing location distinction methods: [11]

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.

By combining the benefits of these two methods a new link measurement have been developed, which called the complex temporal signature.

2.6 PARADIS: Physical 802.11 Device Identification with Radiometric Signatures

This method 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. [12]

PARADIS uses a large five distinct features from the modulation domain, namely, frequency error, magnitude error, phase error, I/Q offset, and sync-correlation of the corresponding wireless frame. Also PARADIS is located at the boundary of the analog and digital domains of wireless hardware.

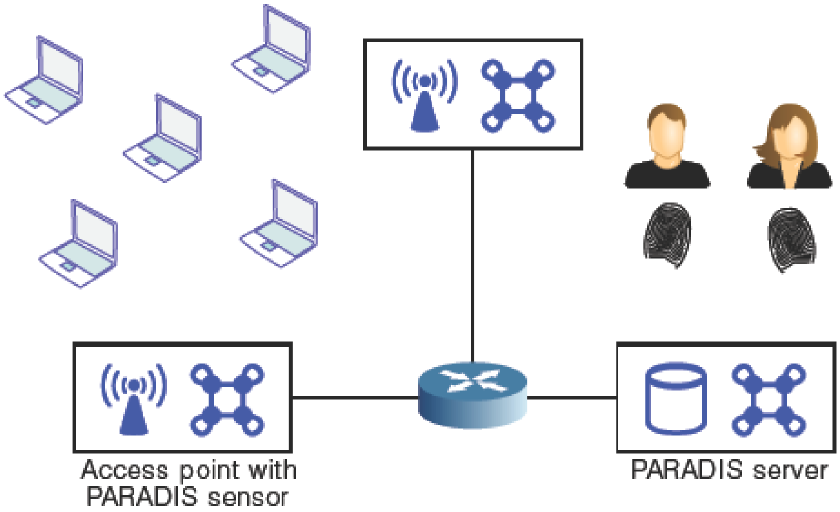

FIGURE 5: PARADIS schematic [11]

3. PROPOSED SOLUTION

A related solution is discussed in [7], but here the issue is not only the security, but also the implementation with taken the budget into the consideration is another issue.

Most of the discussed methods were depended on signal-print technique [9] (direct or indirect), which means it is a reference for most of the methods even though some of these methods claim about its results, false alarm and statistics.

As a solution, after understanding the concept of each method we found the strongest methods are the signal-print [9] and the Puzzles [10]; since the ability of identifying and localizing attack are high compared with other method.

Positioning is a process to obtain the spatial position of a target [25], and since the signal-print is an alternative for Puzzle, we suggest to use some of Puzzle's technique (the ability of knowing the neighbor) inside signal-print and come up with a hybrid approach, by which we can reduce the load on the network and be able to distinguish close clients, not only that but come up with testing and evaluation technique, which can minimize the number of access points to the optimum number without affecting on the security level.

The suggested ideas can be summarized as below:

1. Using Signal-print as an authentication technique; since it depends on the signal strength.
2. Using the Puzzles features:
   a. SSL, TCP and as a countermeasure against spam.
   b. If the received signal strengths are equal, use Puzzle's authentication technique in order to locate the neighbors (using AI to determine when to use any of them), Puzzle's authentication illustrated in figure 6. And the frame format as in shown in figure 7.

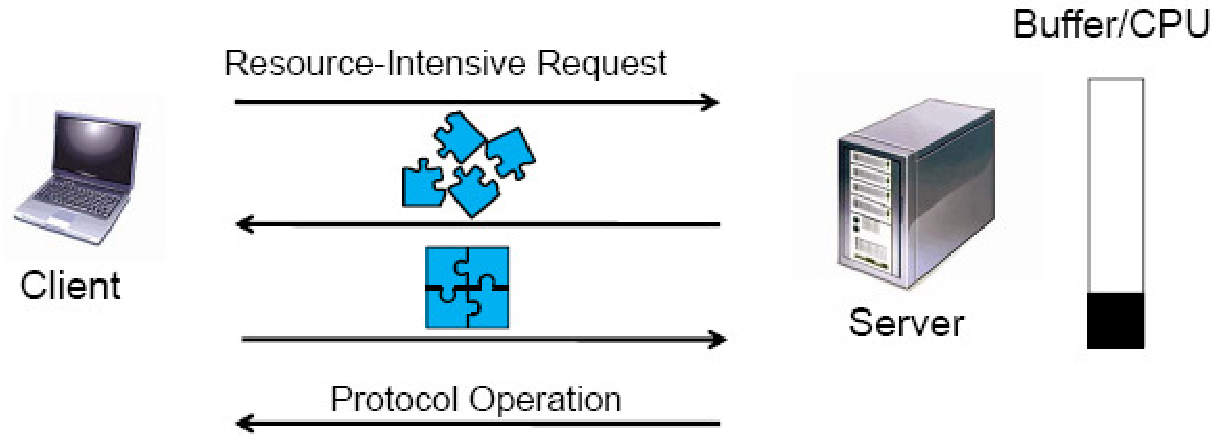

FIGURE 6: Puzzle's authentication concept

$$H(\boxed{\text{Pre-Image X}}\underbrace{\boxed{?}}_{k \text{ bits}}) = Y$$

FIGURE 7: Puzzle's frame format [15]

3. Draw the network diagram to organize the network, by using network drawing software (ex. OMNet++), in order to come with a network diagram similar to figure.8.

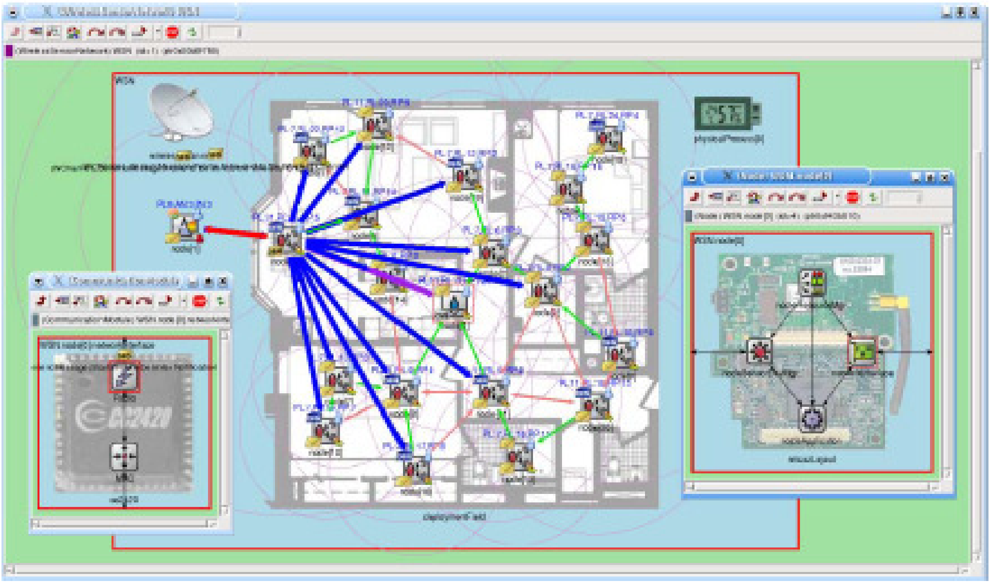

FIGURE 8: Example of Network drawing software (http://www.omnetpp.org)

4. Distribute the access points depending on the coverage of each access point, which can be determined depending on type of the access point and the diversity of its antennas, covered area and antenna types illustrated in figure 9.

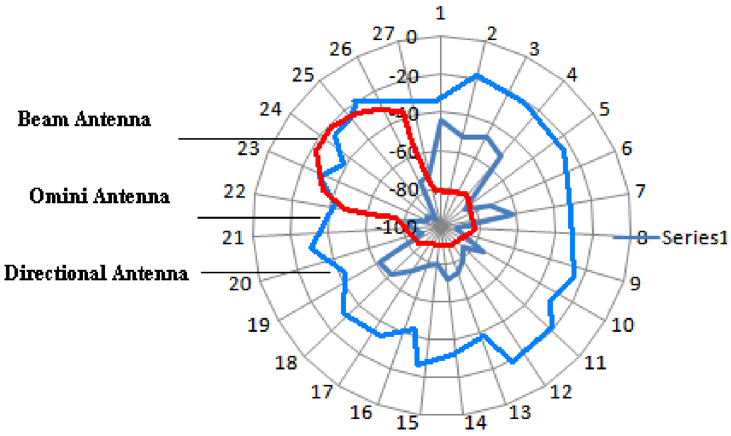

FIGURE 9: covered areas and types of antennas

5. We installed the first access point, then. For demonstration we used the following equipments:

- CISCO Aironet 350
- 13.5db antenna
- Laptop with Network Stumbler software
- TP link External card

We got the results as shown in table 1.

Distance	Bearing	Signal	Noise	mbps
0	230	-41	-100	54
10	273	-48	-100	54
16	255	-45	-100	54
22	283	-50	-95	33
31	71	-81	-100	0
35	355	-68	-95	4
40	33	-60	-95	21

TABLE 1: Test results

6. From signal data we can generate a radar graph which can show access control covered area, Figure 10.

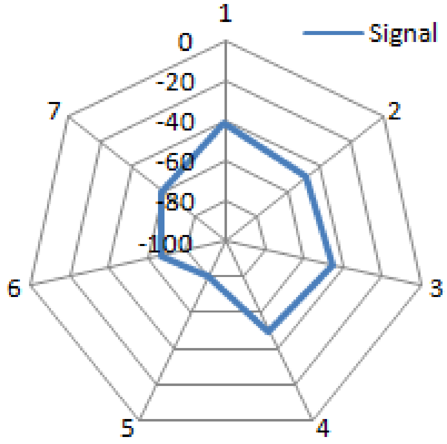

FIGURE 10: Signal data representation

7. From figure 10, we knew the covered area of the first access point, and by repeating the same procedure on the boundaries of first access point we can cover the whole area without overlapping and keeping the level of security without any affect on its level.

8. The above procedure is applied if the area which we are going to cover is open or like figure 11. But if it is a closed rooms or other facilities the type of the walls will judge our decision; since the level of the noise increases, signal will be attenuated as shown in figure.12.

FIGURE 11: offices area covered by wireless network [15]

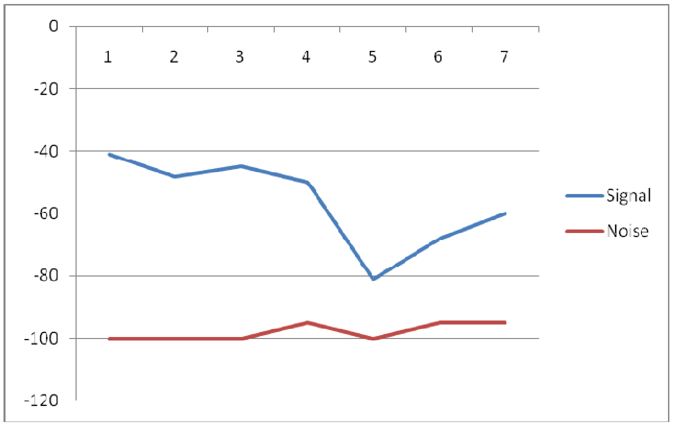

FIGURE 12: Signal / Noise

9. Also, the relation between the distance and the speed has a good role in determining the percent of overlapping between access points as in figure 13.

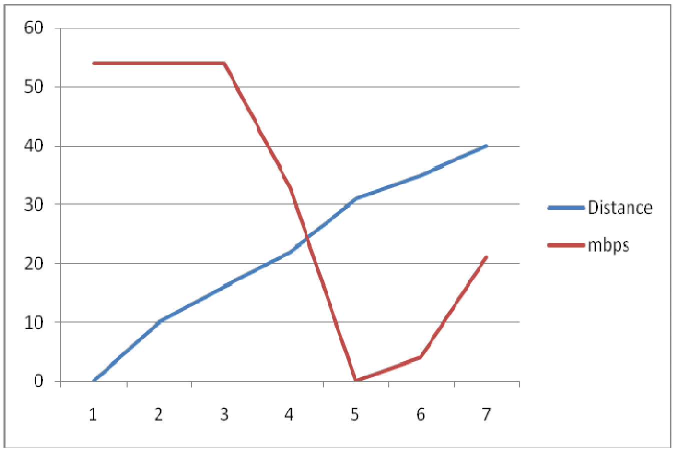

FIGURE 13: Distance / Speed

10. In addition, the rlation between the bearing and the speed, which will give us an idea about uncoverd areas, so we can cover it by other access points, as illustrated in figure 14.

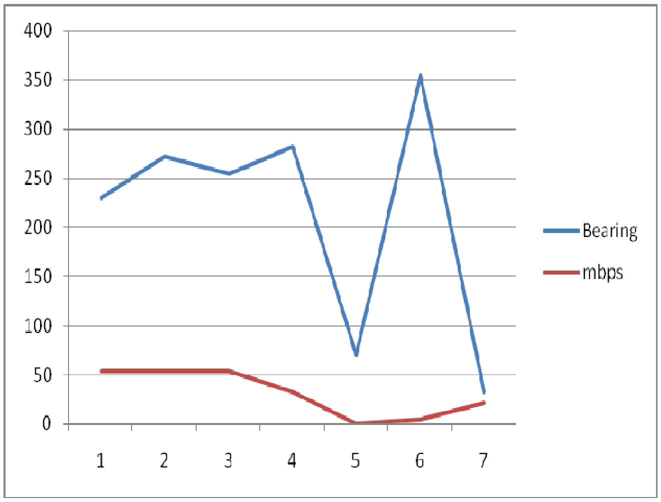

FIGURE 14: Bearing / Speead

11. Finally, the monitored area can be like figure 15.

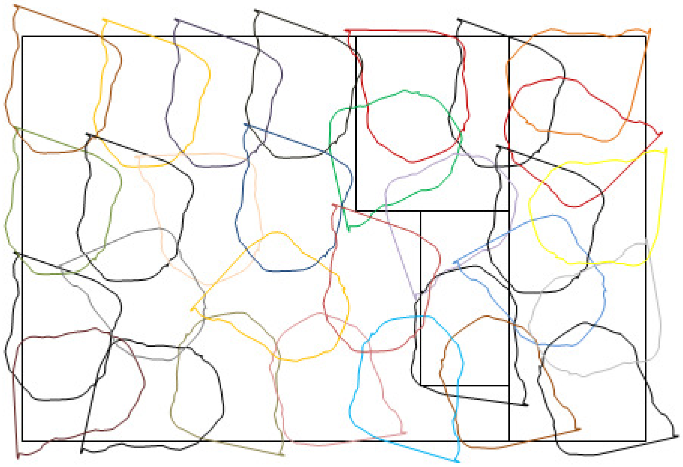

FIGURE 15: monitored area with access points locations and overlaping

4. CONCLUSION AND FUTURE WORK

Securing the network becomes a load on the network administrators; since the wireless network is wildly spread.

Signal Strength which is unique for each device as mentioned in previous works [20,21,22]; because it depends on the type and location of the device is also can be attached by some smart hackers, so the experts try to secure the network using different methods and technique to detect any kind of attack.

Choosing the optimal number of access points is a very important factor in network design; because each AP has its own coverage area, which varies from type to type of APs, therefore to illuminate overlapping problem we have to choose the optimal number, otherwise location of the intruders can't be determined. In this paper the GPS was used for accuracy issues, and as a test bed both indoor and outdoor areas were used, but in the indoor the highest floor of the building were used to overcome the coverage limitation of the GPS.

As a result three things were achieved in this paper, network service is available only for the clients on the test bed (not more); which is a result of good distribution of APs, intruder can't attack any client; because two strong techniques were merged (Puzzle [10] and signal-print [9]) and the last one is a good management for the budget; by reducing the cost into the minimum by choosing the optimal number of APs.

Finally, as a future work, merging between network security and image processing (using remote sensing) to find both the best location of access points and optimal number of them, which can be used for city plans and e-government solutions.

5. REFERENCES

1. Wireless Intrusion Detection Systems, SANS, Ken Hutchison, 2004

2. http://netsecurity.about.com/cs/hackertools/a/aa030504_2.htm

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

4. Joshua Wright, Detecting Wireless LAN MAC Address Spoofing, 2003

5. Yingying Chen, Wade Trappe, Richard P. Martin, Detecting and Localizing Wireless Spoofing Attacks

6. R. A. Redner and H. F. Walker, *“Mixture densities, maximum likelihood and the EM algorithm”*. SIAM Review, 26(2):195–239, 1984

7. Iyad Aldasouqi, Walid Salameh, Detecting and Localizing Wireless Network Attacks Techniques, CSC, 2010

8. M. Ladd, K. E. Bekris, A. Rudys, L. E. Kavraki, D. S. Wallach, and G. Marceau*, “Robotics-based location sensing using wireless ethernet”.* In MobiCom ’02: Proceedings of the 8th Annual International Conference on Mobile Computing and Networking, Sept. 2002, pp. 227–238

9. 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, 2006

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

11. Advancing Wireless Link Signatures for Location Distinction, by J.Z. Mohammad H. Firoozz Neal Patwariz Sneha K. Kaseray

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

13. P. Bahl and V. N. Padmanabhan, “*Radar: An in-building rf based user location and tracking system,”* in Proceedings of the IEEE International Conference on Computer Communications (INFOCOM), March 2000

14. E. Elnahrawy, X. Li, and R. P. Martin, “*The limits of localization using signal strength: A comparative study”.* In Proceedings of the First IEEE International Conference on Sensor and Ad hoc Communcations and Networks (SECON 2004), 2004.

15. Neal Patwari and Sneha Kasera, Robust Location Distinction Using Temporal Link Signatures

16. Aaron E. Earle, Wireless Security Handbook

17. P. Bahl and V. Padmanabhan.” *RADAR: An in-building RF based user location and tracking system”.* In Proceedings of the Conference on Computer Communications, volume 2, pages 775–784, Tel Aviv, Israel, March 2000.

18. G. M. Djuknic and R. E. Richton, \Geolocation and assisted GPS," IEEE Computer, 34(2): 123-125, 2001

19. P. Bahl and V. N. Padmanabhan, *“RADAR: an in-building RF-based user location and tracking system".* In Proc. IEEE Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'00), Tel Aviv, Israel, Mar. 2000,

20. P. Bahl and V. N. Padmanabhan, “*RADAR: an in-building RF-based user location and tracking system,"* in Proc. IEEE Nineteenth Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM'00), Tel Aviv, Israel, Mar. 2000

21. S. Saha, K. Chaudhuri, D. Sanghi, and P. Bhagwat, "*Location determination of a mobile device using ieee 802.11b access point signals,"* in Proc. IEEE Wireless Communications and Networking Conference (WCNC'03), New Orleans, LA, Mar. 2003

22. J. Small, A. Smailagic, and D. P. Siewiorek, "*Determining user location for context aware computing through the use of a wireless lan infrastructure,"* Online, Dec. 2000. [Online]. Available At: http://www.2.cs.cmu.edu/»aura/docdir/small00.pdf

23. Krzysztof, K., Hjelm, J. (2006) LBS Applications and Services, CRC Press, ISBN: 0849333490.

24. Hazas, M., Scott, J., Krumm, J. (2004) Location-Aware Computing Comes of Age. Computer, 37 (2004) 95-97.

25. Küpper, A. (2005) Location-based services. John Wiley & Sons, Chichester.

26. P. Bahl and V. N. Padmanabhan. "*RADAR: An In-Building RF-Based User Location and Tracking System".* In Proceedings of the IEEE Conference on Computer Communications (InfoCom), volume 2, 2000.

27. P. Castro, P. Chiu, T. Kremenek, and R. Muntz. "*A Probabilistic Room Location Service for Wireless Networked Environments."* In Proceedings of the International Conference on Ubiquitous Computing (Ubicomp), volume 2201, 2001.

28. J. Hightower, G. Boriello, and R. Want. "*SpotON: An indoor 3D location sensing technology based on RF signal strength".* Technical Report 2000-02-02, University of Washington, 2000.

29. R. Want, A. Hopper, V. Falcao, and J. Gibbons. "*The Active Badge Location system."* ACM Transactions on Information Systems, 10(1), 1992.

30. S. Pandey, F. Anjum, and P. Agrawal. "*TRaVarSeL–Transmission Range Variation based Secure Localization"*, pages 215–236. 2007.

31. S. Pandey, F. Anjum, B. Kim, and P. Agrawal. "*A low-cost robust localization scheme for WLAN".* In Proceedings of the International Workshop on Wireless Internet, New York, NY, USA, 2006. ACM.

32. S. Pandey, B. Kim, F. Anjum, and P. Agrawal. "*Client assisted location data acquisition scheme for secure enterprise wireless networks"*. IEEE Wireless Communications and Networking Conference (WCNC), 2, March 2005

33. P. Tao, A. Rudys, A. M. Ladd, and D. S. Wallach. "*Wireless LAN location-sensing for security applications.*' In Proceedings of the ACM Workshop on Wireless Security (WiSe), 2003.