Portable 3D System for Visualization and Protection of Wireless Networks

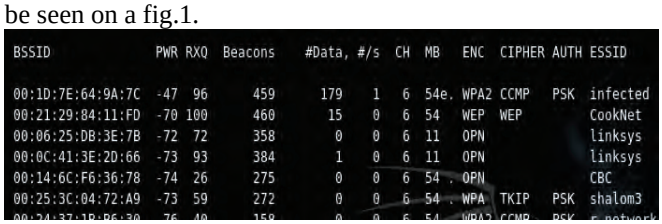
Teodor Kalushkov[1], Plamenka Borovska[2] and Georgi Todorov[3]

Abstract – **This paper describes a wave analyzing system for wireless networks, that can be easy integrated in some working simulators, using the existing or partial made models. The system can visualize real time results, in a 3D form that gives opportunity for enhancing the security and architecture of existing systems, correcting virtual models and researching real networks. The system has an enhanced possibility for detecting external intrusion tries and localization of the external equipment.**

Keywords–**signal, antenna, waves, security, 3D position.**

I. Introduction

Many of the existing systems for modeling and building a wireless networks use different 3D models, based on pure theoretical dependencies, but after real construction of these networks the experimental analysis are made usually only on the base of signal level. Sometimes it is not enough, because there are some other factors that have influence over the desired secure connection. Usually used applications give us information about MAC-addresses of users, of access points, channels of communication, used encryption method and as mentioned before about the signal strength. Such monitor can be seen on a fig.1.



BSSID	PWR	RXQ	Beacons	#Data,	#/s	CH	MB	ENC	CIPHER	AUTH	ESSID
00:1D:7E:64:9A:7C	-47	96	459	179	1	6	54e.	WPA2	CCMP	PSK	infected
00:21:29:84:11:FD	-70	100	460	15	0	6	54	WEP	WEP		CookNet
00:06:25:DB:3E:7B	-72	72	358	0	0	6	11	OPN			linksys
00:0C:41:3E:2D:66	-73	93	384	1	0	6	11	OPN			linksys
00:14:6C:F6:36:78	-74	26	275	0	0	6	54 .	OPN			CBC
00:25:3C:04:72:A9	-73	59	272	0	0	6	54 .	WPA	TKIP	PSK	shalom3

Fig.1. Wireless network monitor

If we have a 3D map of access points and users, it will be easier to detect an intrusion attempts. For building this map theory is not enough and real physical measurements should take their place.

II. Attack Actions And Defence

When hackers realize attacks, they use equipment, which is situated near the desired wireless networks. This equipment usually requires not only a computer but also directional antennas, because they have to jam the signal of the access point or user. The most popular techniques for finding wireless passwords include sending deauthorization signal and capture of four way handshake between user's computer and access point or packet injection. When network password is found, hackers can sophisticate the packets if WEP encryption is used [3]. Otherwise, if WPA/WPA2 is used, online sophistication is not so easy but remains the possibility for capturing packets and decoding them offline [2]. In these situations if access point and user computer can determine their position in a 3D environment, they can easy detect intrusion attempts. So the jamming can be detected not only as a rapid change in a signal level, but also as a position "jump" of the opposite point on the 3D map. This example is shown on fig.2.

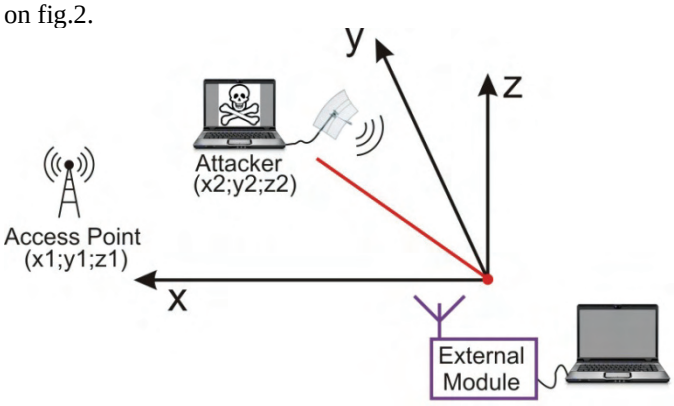


Fig.2. Intrusion detection, using 3D mapping

If we analyze the position, according signal strength and phase of the access point signal, when attacker tries to emulate access point, 3D analyzer will detect immediately change of the coordinates. Often the software protections in this field react against the intrusion with blocking the communication for a short period of time and trying to reestablish the connection afterwards. This approach is not convenient for the user and does not solve the problem permanently.

III. Main Parts And Operating Principles Of The System

In order to detect the phase and strength of the opposite side, our system should ask the access point to return a test signal which will give us a base for our calculations and orientation in the 3D space. In order to avoid latencies and complications the system will use its own unit, of antennas. In 2D space we need minimum three of them. According to our goals the system should have minimum four antennas,

[1]Teodor Kalushkov is with the Faculty of Mathematics and Informatics, St.Cyril and St. Methodius University of Veliko Tarnovo, Arch. G. Kozarev 3, V.Tarnovo 5000, Bulgaria, E-mail: teodork@abv.bg

[2]Plamenka Borovska is with the Faculty of Computer Systems and Control, Technical University of Sofia, boulevard Kliment Ohridski 8,Sofia 1000, Bulgaria, E-mail:pborovska@tu-sofia.bg

[3]Georgi Todorov is with the Faculty of Mathematics and Informatics, St.Cyril and St.Methodius University of Veliko Tarnovo, Arch.G.Kozarev 3, V.Tarnovo 5000, Bulgaria, E-mail:g.todorov@uni-vt.bg

positioned in the edges of a virtual pyramid. The distances between them should be as longer as they can be, in the range of a room, in order to reach greater accuracy. This is the other reason for choosing external antennas, despite of using existing ones. All antennas will only receive signals. It is good decision because so they can not be detected from intruders and the whole system will require less power consumption. Each antenna should contain three elements, if we want make our system compatible not only with IEEE 802.11b and g standards but also with IEEE 802.11n one.

The antennas should be connected with other external device, using equal length cables. It is required of the attenuation in the cable. If the system uses different distances between antennas and concentration device, we should integrate some kind of signal compensators or provide some extra computations and will complicate the prototype at all.

All cables can be concentrated in external device, that measures the strength and phase of all antennas, converts the signals into a digital form, calculates the coordinates and sends them to the personal computer via proper interface for post processing. External device can contain the elements, shown on fig.3.

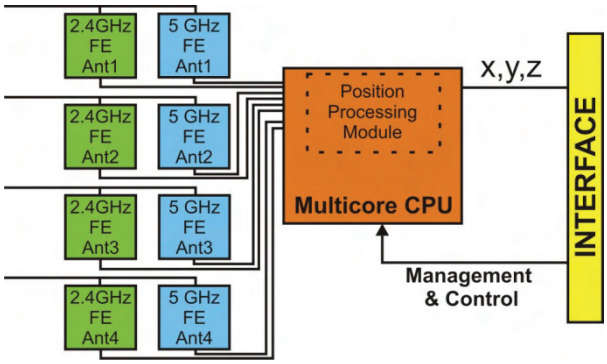


Fig.3. Block diagram of multiple antenna external module

For more secure and accurate computations the system can use a phase differential and amplitude processing from four antenas.When the signals are received from antennas, they are processed in front-end modules in RF part of the external module. These front-end modules convert the analog signal streams into digital format, which is proper for further processing. After front-end modules, data streams are processed into a multi-channel, multi-core CPU that calculates the 3D coordinates. External module outputs low-noise phase/amplitude measurements from 4 antennas. Its interface is used also for feedback control, which is applied direct to the multicore CPU.In this way it is possible to achieve full software configuration management over the real time measurements and processing.

The suggested external module can be assembled on a single small-size board. It is very important according portability of the whole system. External part is consistent also with weight and consumption limitations. Most of the modern multicore processors can scale their power consumption according to their workload. Another advantage is that duplication of hardware modules is minimized and it reduces the price.

In some applications, that use the same principles, one of the antennas is accepted as a main and the others are auxiliary [6]. It is good approach, but only if we need some extra measurements like speed, attitude, deformation of objects.In our case is better to give an account of thephase differences between all the couples of antennas as presented in a table 1.

TABLE I
COMPARISON OF THE PHASES IN ALL POSSIBLE COUPLES OF ANTENNAS – IN CASE OF FOUR ANTENNAS USED

Comparison combinations	Phase I	Phase II
1	φ1	φ2
2	φ1	φ3
3	φ1	φ4
4	φ2	φ3
5	φ2	φ4
6	φ3	φ4

Each of these combinations can be decided as a specific coordinate of the source. On the other side the strength of a signal on every antenna can be visualized as a sphere in the 3D space, and the place where all the spheres cross each other, shows the area of the signal source.

Many sources [4][5], describe wireless network propagation the same way like the light's propagation. The reason is that they both have wave nature. According to this, it is correct to explain that some phenomena present in our situation too. Diffraction, refraction, interference, and attenuation have influence over wireless waves. Practically the result from all these can be observed as a rapid change in the strength of a signal, when moving slowly in a closed area. When building and using described system, we should give account of the fact that the signal on the straight ray between two points has the biggest amplitude if the frequency modulation is used. This rule gives possibility easy to filter the desired signal from source.

When coordinates are already known, two different methods can take place for protecting the connection. First of them can be called "jump detection" and was explained above. It uses detection of rapid change in a phase and amplitude of the received signal. The second method is based on declaring coordinates for the access point area. The administrator can describe the real 3D-area of the opposite communication point and deny access from all other points. It gives high efficiency of the security level.

The coordinates from external module can be integrated into a working simulator or can be used for developing a new one. It is important to note that multicore CPU's are already used in all new computers and the scientists are trying to find new algorithms for parallelization of the processed data in order to improve the performance. Presented system can easily take advantage of multicore technologies not only in external module, because the received signals are highly parallelized by nature. Every antenna is a source of one or more data stream(s). In external module this streams form

different processing threads and are processed using the same instructions. It means that so called SIMD (singe instruction multiple data) computers are proper for the system. At the end of the system all computations present a common result – coordinates and direction of the wave source. If this result should be in a graphic form, this also consumes extra computation power. Then internal multicore CPU can help in visualizing the environment. Other proper technology that is very implemented now and is proper for this system is CUDA (compute unified device architecture). This technology gives possibility to achieve some extra performance, using GPU's resources of the computer.

IV. Practical Issues

The same method as described is used in a military device for finding enemies. It uses multiple microphones placed in different points around soldiers. If enemy shoots, is very hard to find his position if soldiers don't see the gun fire and just hear the bullets. If distance is long enough, bullets come first and then the sound from shooting weapon. The microphones record the sounds, they receive from flying bullets, send them for analysis and results trace the enemy position.

Another system that uses the same principles is used for determination of attitude of the rover based on the L1 signal carrier phase differences from multiple GPS receivers [6].

V. Conclusion

The suggested system is a hardware decision that gives a high rate enhanced security of the connections. It can be used in one side of the communication channel as well as in both sides if higher protection is required. The system is compatible with new hardware technologies and can be easy integrated into software environments. It can be used also in e-learning courses for building and exploring real wireless networks.

Acknowledgement

This paper is financed by project: "Creative Development Support of Doctoral Students, Post-Doctoral and Young Researches in the Field of Computer Science", BG 051PO001-3.3.04/13, EUROPEAN SOCIAL FUND 2007–2013. OPERATIONAL PROGRAMME "HUMAN RESOURCES DEVELOPMENT"

References

[1] Angelov M,"Cells network bases." PAN- VT, Veliko Tarnovo, Bulgaria, 2000

[2] Kalushkov T., Borovska P., "Choosing Of Wireless End-user Passwords. Dual Language Encryption Method." SAI'10 Conference, Sofia, Bulgaria, 2010

[3] Lashkari A., Mansoori M., Danesh A., "Wired Equivalent Privacy (WEP) versus Wi-Fi Protected Access (WPA)." International Conference on Signal Processing Systems, 2009

[4] Schmitz A., Rick T., Karolski T., Kuhlen T., Kobbelt L., "Simulation of RadioWave Propagation by Beam Tracing." Eurographics Symposium on Parallel Graphics and Visualization, 2009

[5] Madej P., "3D Wireless Networks Simulator- visualization of Radio Frequency propagation for WLANs." A dissertation submitted to theUniversity of Dublin, TrinityCollege, in a partial fulfilment of the requirements for the degree of Master of Science in Computer Science, 2006

[6] SimskyA.,Vander Kuylen L., Boon F., "Single-board Attitude Determination System Based on the PolaRx2@ GPS Receiver."ENC GNSS 2005, Munich, Germany, 2005