LITERATURE REVIEW: RF SIGNAL SOURCE MAPPING

Daniel Wells
Supervisors: Barry Irwin and Ingrid Siebörger
22nd June 2007

Department of Computer Science
Rhodes University
Grahamstown, South Africa

Abstract

Wireless networking has brought computer networks into a new, exciting and hostile environment. Factors that need to be considered and understood during implementation include interferences and security protocols. Setting up a WLAN is relatively simple, allowing users to achieve mobility, but in some cases, the default security configuration on the devices leads to inferior security measures implemented. Security leads to a higher implementation complexity. Wireless access points (AP's) can be connected at any open port on a network, allowing unauthorised external users to gain access to the secure internal network, bypassing a vast majority of security measures. Discovering the location of rogue AP's aids the wireless user in protecting their secured network. Using spectrum analysis and trilateration, these rogue AP's can be located.

1 Introduction

Recent years have seen the rise of mobile users with PDA's, laptops and mobile phones, at the same time, network connectivity is becoming increasingly integral into this wireless environment. With the added convenience of wireless networking, new problems have arisen.

The 802.11x range of technologies has been adopted on a global scale, making Wi-Fi near ubiquitous. In this paper we will be dealing specifically with 802.11b/g/n wireless technologies.

Security in the wireless network has had to overcome some hurdles, with default settings on hardware most frequently set to the least secure mode to aid in user friendliness. The first wireless security protocol, WEP, was widely adopted and initially proved effective at preventing unwanted users gaining access. After scrutiny of the protocol by attackers and cryptologists, WEP was discovered to have serious flaws. Security has since been improved with the release of WPA and WPA2, although still not widely adopted in the home or small office environment due to a lack of wireless education of the end-user.

Wireless networking, specifically Wi-Fi (802.11b/g/n) technologies, propagates over a cluttered band, 2.4 GHz, with a variety of other radio devices additionally operating at this frequency. Interference needs to be evaluated, understood and avoided otherwise network throughput will decrease. One particular method of evaluating interferences is by conducting a site survey in the wireless environment to maximise wireless usage, but also keep unnecessary hardware and maintenance costs down.

Hardware and software to track user and AP locations in the wireless environment have been produced, effectively locating users to within a couple of meters. Proprietary hardware in this regard is expensive, although the cost of software running over an already existing wireless network is cheaper in comparison. The *Wi-Spy* 2.4 GHz spectrum analyser has been produced as a low cost site survey tool and has the potential to be used in location tracking.

Using three machines, in three locations, each with a *Wi-Spy* spectrum analyser, and by using their combined data (frequency and amplitude) and trilateration it will be possible to locate Wi-Fi devices within listening range.

2 Terminology

Trilateration is the method used in the Global Positioning System (GPS), allowing the location of a point to be discovered in space by using three known and fixed locations; although this method is similar to triangulation, no angle measurements are required. The measurement of wireless signal strength (*dBm*) is used to approximate the distance that the signal has originated from. Using trilateration and this distance approximation from three points, we can discover an estimated location of the source of the signal.

2.1. Trilateration and Triangulation

Trilateration is the method of determining the relative positions of objects using the geometry of triangles in a similar fashion to triangulation. Triangulation uses angle measurements, with a minimum of one known distance, to find an object's location, where trilateration uses the known locations of two or more reference points and the measured distance between the target subject and each reference point [14].

Figure 1 shows a simple example of triangulation, with two known points, P_1 and P_2, the distance between them (d) and the two angles, a and b, to the third point P_3. Because of the nature of

triangles, we know that the sum of all angles within a triangle is 180 degrees, which gives the angle *c*. Using the *Law of Sines*, the lengths of the missing sides can be calculated [19]:

$$\frac{a}{\sin A} = \frac{b}{\sin B} = \frac{c}{\sin C}$$

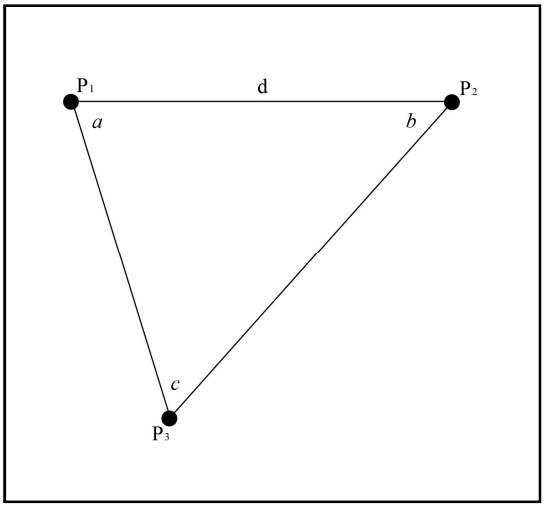

Figure 1: ***Triangulation***

Trilateration on the other hand, demonstrated in *Figure 2*, uses the distance from the three reference points to the object A. These distances will give the radii of three circles and object A will be at the intersection point. Having the radii of the circle and the centre points, we obtain the equations for the circles [14]. The equation for a 2-dimensional circle is

$$(x-a)^2 + (y-b)^2 = r^2$$

assuming that all the points are on the same plane. To find the intersection point (x, y) of the circles, the equations of the three circles need to be solved simultaneously.

To solve for 3-dimensions (a sphere) the equation is extended to deal with the z-axis [14]:

$$(x-a)^2 + (y-b)^2 + (z-c)^2 = r^2$$

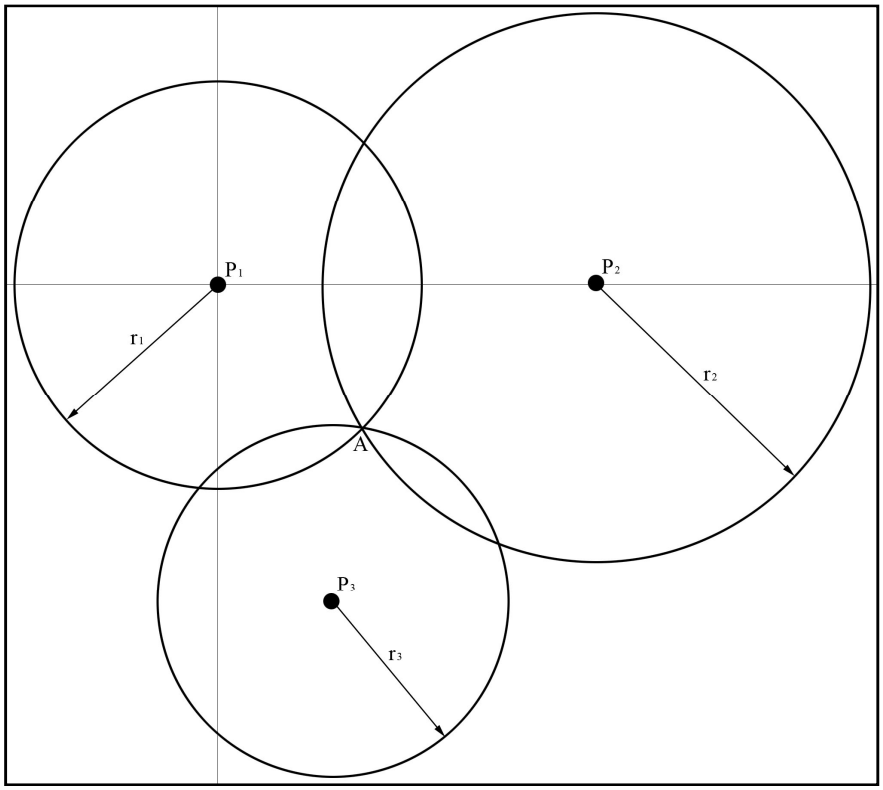

Figure 2: ***Trilateration***

2.2. dBm units of Measurement

Signal strength in a wireless network is measured using *dBm* (decibel milliwatts), which is measured on a logarithmic scale. *dBm* and *mW* (milliwatts) both measure the power level, but *dBm* is most widely used as *mW* can become a very small meaningless number very quickly. Devices will be marked with a receive sensitivity and a transmitter power output in this scale. An important fact about this scale is if you add 3 *dBm*, you double the power output and subtracting 3 *dBm* will halve it [6].

This measurement is particularly useful when working out the distance a signal is coming from, if it is known at what strength the signal was transmitted.

3 Wireless Security

Security is often viewed as a complicating factor in wireless networking and can be a difficult task to implement, even for skilled system administrators. Mobile users prefer the connection to be automated as they move between wireless networks, connecting to any AP, obtaining IP addresses, gateway information and DNS server addresses through DHCP. An automated connection process is acceptable in a highly mobile environment, but not when the network needs to be secure [5].

A secure wireless network, in theory, only allows authorised devices to connect and protects those devices from attack. Extensive overhead is carried out to secure the network which becomes increasingly complex as security improves, leading to weak security solutions implemented by the typical end-user. The responsibility placed on the user ranges from specifying the types of security protocol used and specifying passwords for AP's and clients, to managing a Public Key Infrastructure (PKI). A more secure network is more complicated to configure, leading to strong wireless security solutions being out of reach for typical end-users [5].

A trade-off exists between security and usability in any network, a more secure network significantly contributes to the cost of setting up and maintaining the network. In wireless networking environments, where there is a lack of physical barriers to access, a strong security implementation is crucial [5].

Numerous wireless security protocols exist to protect access to the network and prevent packets being interpreted by network packet sniffers. The original and outdated standard wireless security protocol WEP and newer WPA and WPA2, and their strengths and weaknesses will be discussed further.

3.1. Wired Equivalent Privacy Protocol (WEP)

WEP is the original security and encryption standard implemented in 802.11 wireless networks, which requires clients and AP's to share a single secret key which both use to encrypt all datalink layer communication [3]. The goals of WEP are to protect confidentiality, access control and integrity of user data from eavesdropping and tampering. This is the international standard and has been integrated by manufacturers into their 802.11 hardware, this protocol is still in widespread use [7].

WEP has many flaws (*see appendix 8.1*), and is still used in many situations, it is recommended to never use it in sensitive applications. At the time of its release it was considered secure and after cracks were released there was nothing better and marginal security is better than no security at all. Many companies strengthened WEP by deploying it with other solutions like Virtual Private Networks (VPNs), 802.1x authentication servers and other proprietary software [20].

3.2. WPA and WPA2

Due to the vulnerabilities present in WEP, the numerous implemented attacks and concerns that a lack of strong wireless security would hinder the adoption of wireless devices in the market, a more secure protocol was necessary and Wi-Fi Protected Access (WPA) was introduced (*see appendix 8.1*).

WPA addresses all known vulnerabilities in WEP to ensure data authenticity and does so with a minimised impact on network performance. When WPA is properly installed, it ensures user data will remain protected and that only authorised users may access the network, it protects against some of the most targeted hacker attacks. Networks can now offer users the ease and flexibility of working wirelessly and securely without deploying add-on security solutions, like VPNs [20].

WPA2 provides all the benefits of WPA, but uses a newer encryption scheme, The Advanced Encryption Standard (AES). The AES cipher algorithm employs variable key sizes of 128, 192 or 256-bits [20].

3.3. Recommendations on security for wireless networking

For a secure wireless network, under no circumstances must WEP be used, multiple published attacks exist (*see appendix 8.2*) and allow attackers with basic network knowledge to gain access to the network. WPA or WPA2 is recommended in all situations [1, 20].

4 Interference on WLANs

Interferences that can hamper the performance of 802.11b/g/n networks (2.4 GHz frequency) are discussed, with previous findings of performance degradation analysed. 802.11a networks, which operate on a higher frequency of 5 GHz, are not commonly used, even though they operate on a less used band. 802.11a wireless is not discussed, as it does not feature on our campus, or used in our testing. In addition, 802.11b/g/n technologies tend to be near ubiquitous in the market place.

4.1. Typical interference sources found

Wireless interference can be separated into two broad categories, traffic from other users of the medium and that arising from natural or non-WLAN traffic operating in the same frequency (in this case 2.4GHz) [17]. Non-WLAN traffic is any source which operates in the same frequency band as the wireless network, this includes a range of cordless phones, any Bluetooth device, cordless headsets, wireless bridges, cordless video-game controllers and microwave ovens [10]. A

microwave oven can create interference from up to 50 feet away and incur relatively high packet retransmission [11]. Any source that has the same propagation medium as the wireless network will corrupt the signal reception [21]. Obstructions between antennas also lead to reduced throughput because the radio link depends on the energy diffracted around the object rather than direct radiation [8].

Traffic from other wireless users is of the most concern to those living in densely populated residential areas, or multi-tenant office buildings where wireless networks are prevalent.

4.2. Wireless Denial-of-Service attack (WDoS)

Another source of interference, which is more malicious than those already discussed is produced by a simple device that can be either bought or built, which can be concealed and effectively prevent any wireless transmissions occurring in a given radius. These types of devices output onto a particular band and transmit either Gaussian white noise or a similar relatively high amplitude signal. These devices are illegal, yet plans and kits can be bought on the Internet [10].

4.3. Effects of interference and how to evaluate them

Depending on what sort of traffic the WLAN is being used to transport, the effects appear in different ways. In a scenario of asynchronous traffic (typical data), users will experience decreased or variable throughput resulting in low or non-existent service rates, in this case the signal strength meter on the user's computer will continue to suggest that all is well, even though throughput is down. It could also be the case that the signal strength meter is representing the strength of another wireless networks signal.

Voice over IP over Wi-Fi (VoFi) systems affected by interference will experience dropouts (silent periods), as packets are lost due to collisions and this can occur in both directions of the call. These effects will be familiar to cell phone users, although in this case dropouts are caused by interference and not a fading signal.

Video being streamed over a wireless network is another scenario where high throughput is required to provide the user with real time video. Users will experience dropouts, square boxes in the video and freezing when interference exists. These 'glitches' occur when key frames are lost from the compression of the video and can only correct itself when the next key frame is obtained [10].

A complicating factor when monitoring interference is typical network congestion in either wired or wireless networks that can have similar detrimental results. For interference analysis, two forms exist, protocol analysis (evaluating the response to interference on a given protocol) and energy analysis (using a spectrum analyser to evaluate effects) [10].

When conducting interference testing, a baseline benchmark of the throughput needs to be obtained without any interference and with a repeatable workload. Next, impairment testing is run identically to the benchmark, but with a known interference introduced. These results can be compared to evaluate the effects of the interference [10].

4.4. Recommendations

Interferences sources need to be controlled and managed effectively, allowing full use of the wireless network.

5 Considerations and Asset Tracking

Every building is different in the way they are built, how thick the walls are, what type of paint is used (lead-based paints deter performance), filling cabinets and staircases. All these factors need to be considered when installing a wireless network, to maximise throughput and keep users happy. Wireless site surveys provide network planners with detailed reports about types of antennas to use, number of AP's and interference sources in the environment.

Detecting and locating devices and clients in the network (authenticated or rogue) may provide administrators with advantages in securing their network and controlling interference. In addition, details of typical wireless devices are discussed.

5.1. Wireless Site Surveys

WLAN applications have become increasingly popular over the past decade and become a core part of an enterprise communication infrastructure where it provides real-time access to information either on the Internet or intranet. These applications are expected to reliably support a significant amount of users and mission-critical services. Due to the increase and predicted future increase, it is clear that the completion of an effective radio frequency (RF) site survey is necessary for installing AP's [11].

Unreliable wireless coverage could prevent network connectivity, limit network capacity, cause dropped network connections that may lead to thousands of rands in productivity lost as well as troubleshooting and maintenance costs as the organisation is disrupted.

The primary goal of performing a site survey is to determine the number and location of AP's that provide optimum signal strength for the organisation. A survey should be completed prior to installation, allowing the correct placement of AP's and a sufficient amount of signal overlap. The report from a site survey, together with a detailed map of the area, should supply the exact mounting points with enough detail so that the installation of actual AP's later will produce similar RF signal coverage.

Issues with radio signals are that they do not propagate in equal distances in all directions as obstacles such as walls, filing cabinets and other interferences discussed previously cause more or less signal attenuation. In the case of a microwave oven, an AP may have to be placed near that area for users to have lessoned effects of the interference. The best channel to utilise should also be included in the report.

A survey should offer valuable information regarding the choice of antennas, whether they be directional or not and correctly placed to ensure boundaries inside and outside the building, and that no coverage holes exist [6].

5.2. Location Tracking

The mass production of portable computing devices (laptops, PDA's, even some mobile phones) has allowed users to remain connected whilst moving about inside buildings. This has generated a lot of interest in applications and services regarding the mobile user's physical location. Location information allows effective use of the mobile environment. Such advantages include printing a document to the closest printer, locating a mobile user within the environment or guiding a user through a building [4].

The granularity of the information needed varies from one application to another. For example, selecting which printer to use would require coarse-grained location information, whilst locating a book in a library would require fine-grained information. In general, the amount of precision required dictates the cost and complexity of the location tracking system [4].

Cisco Systems provides the *Wireless Location Appliance,* a proprietary solution to location tracking. The price for this device varies between $8500 and $10500 USD (www.pcmall.com; www.cdw.com). As a part of the *Cisco Unified Wireless Network*, this is a costly solution but can efficiently track devices to within a couple of meters. The device has a fully integrated API, and many applications can utilise the data received to provide multiple services [9].

RADAR User Location and Tracking System is a software-only system built over an off-the-shelf RF wireless local area network. The location-aware services enabled by *RADAR* compliment an already useful data network, makes the WLAN more valuable and reduces costs of specialized location tracking hardware. This software is able to track a mobile user to within a few meters of their location [4].

5.3. Standard devices available on the wireless network

Two types of communication devices exist, clients and access points. Clients can either connect to each other in a peer-to-peer configuration or by introducing an AP to provide a network infrastructure. Often an AP is a bridge between the wireless and wired portions of the network, allowing clients to use existing network infrastructure, but have the advantage of being mobile.

Peer-to-peer arrangements are typically used as a temporary solution to connect two clients in an ad-hoc fashion for short periods. Whereas an AP provides many network services (including DHCP and DNS) and attempts to prevent difficulties in media access control, typically in the case of the hidden terminal problem (one node trying to talk to a second node, whilst a third unseen node is attempting to do the same).

A site survey is an extensive, labour intensive task to collect signal propagation data around the building being surveyed; a spectrum analyser can speed up this process. One low-cost spectrum analyser and its capabilities are explained in detail in the next section.

6 MetaGeek Wi-Spy 2.4 GHz Spectrum Analyser

A spectrum analyser takes measurements of signal strength across a set radio frequency range. The *Wi-Spy* measures between 2400 MHz and 2483 MHz, which is the full range of 11 channels in Wi-Fi 802.11b/g/n networks. The *Wi-Spy* device has a form-factor of a small USB flash drive. Retailing at $99 USD, it is relatively inexpensive for the data that can be retrieved from it. It simply consists of a 2.4 GHz radio and low-speed USB controller. Another spectrum analyser on

the market is the *Cognio AirMagnet Spectrum Analyser* which provides more advanced features (device recognition and interference signatures) and retails at $4000 USD [12].

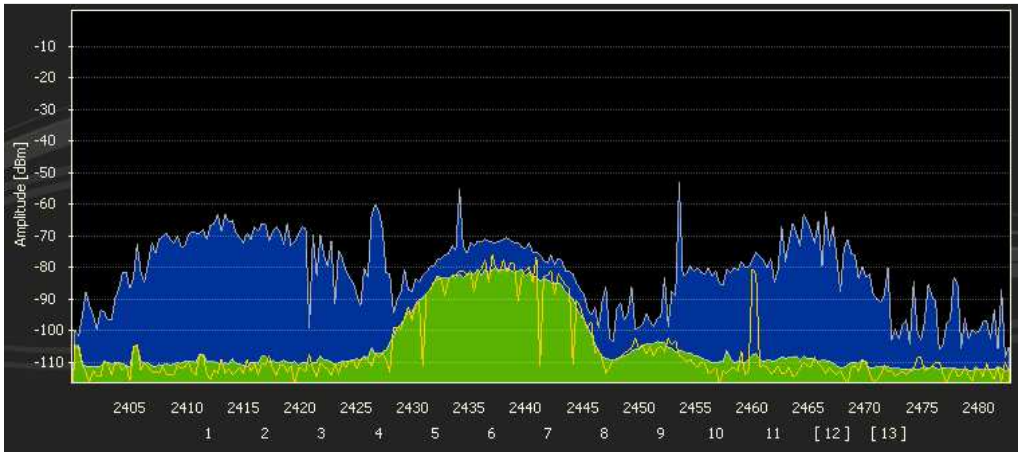

Figure 3: ***Sample Wi-Spy output using Chanalyzer***

In *Figure 3*, the type of output that can be received from the Wi-Spy is displayed using the included software package by *MetaGeek*, *Chanalyzer*; with the frequency running along the x-axis, against amplitude (signal strength) along the y-axis. The above diagram shows the typical usage of channels in a busy area, with heavy usage on channel 6, and light occasional usage of channels 1 and 11. Notice how usage of channel 6 overlaps over multiple frequencies (utilising channels 4, 5 and 7, 8), when doing calculations with data received, this will need to be taken into account.

6.1. Technical Details/Hardware Interface

The *Wi-Spy* radio has a receive sensitivity of *-90 dBm* and has a top data transfer rate of *62.5 kbps*. The device enumerates as a low-speed USB Human Interaction Device (HID), allowing multiple operating systems to use standard drivers. In order to receive data a *Get Feature Report* is sent and the device responds with an 8-byte feature report (*see Table 1*). The first byte is the current frequency position, and the following 7 bytes are the measured Receive Signal Strength Indication (RSSI) at that frequency and the next six frequencies in increments of 1 MHz.

Table 1: ***Message received from Wi-Spy device after Get Feature Report***

Byte 0	Byte 1	Byte 2	Byte 3	Byte 4	Byte 5	Byte 6	Byte 7
Frequency X	RSSI of X	RSSI of X+1	RSSI of X+2	RSSI of X+3	RSSI of X+4	RSSI of X+5	RSSI of X+6

Feature reports are sent sequentially and non-overlapping. The first report received will contain RSSI measurements for 2400-2406 MHz, and the next report will contain 2407-2413 MHz, and so

on. When the report for 2477-2483 MHz is received, the hardware will return to 2400 MHz, and continue to loop as long as *Get Feature Report*'s are received [13].

RSSI needs to be converted to dBm units in software using the following algorithm:

$$dBm = RSSI * 1.5 - 9.7$$

The *dBm* value for the frequency can be converted to give us an approximation of the distance that the signal has travelled.

6.2. Usage of the output

Utilising multiple spectrum analysers to collect frequency data from different geographical locations, a scale grid can be drawn with the fixed points of the known locations of the listening nodes shown. Each node will retrieve signal strength information and calculate the distance the signal has travelled. This is drawn on the grid by circles with the radius of the calculated distance and the origin at the node's location. By combining this distance information and trilateration, the direction toward a device can be discovered. The discovered device's location can then be drawn on the grid.

A minimum of three listening nodes will be required for trilateration yet more accuracy can be obtained with additional nodes. A margin of error will have to be catered for, where no or only some circles intersect, this will decrease the accuracy of the trilateration but provide an area where the device may be. Signal strength can be influenced by interferences discussed in previous sections.

More detail of *Wi-Spy* usage and implementation of trilateration are discussed in further chapters of this project.

7 Conclusion

In this paper, we discussed triangulation, trilateration and dBm units of measurement and suggested that by using trilateration and signal strength obtained from a spectrum analyser we can discover the location of devices in the Wi-Fi network. Thereby locating rogue AP's and helping secure the network. Security was discussed along with flaws discovered in the WEP protocol, which have led to many attacks and consequently we recommend using stronger protocols such as WPA or WPA2. Interferences that affect Wi-Fi adversely affect performance and need to be kept to a minimum.

Site surveys aid in discovering interferences and efficient placement of AP's. Lastly, using three low cost devices, the Wi-Spy spectrum analyser, and the method of trilateration we can locate Wi-Fi devices. During the trilateration calculation, a margin of error needs to be incorporated due to interferences affecting signal propagation.

8 Appendices

8.1. WEP and WPA Encryption

WEP uses the RC4 cipher [16], which contains several major security flaws, giving rise to a number of attacks that directly violate the goals explained above. The protocol standard specifies use of a 40-bit key however several manufacturers have extended the key length to 104-bits, the latter rendering a brute-force attack on the key impossible. There are shortcuts to brute-force attacks in order to obtain the key, therefore not even 104-bit WEP keys are secure. The typical cipher strength is often advertised as 64-bit, with a 40-bit key and a 24-bit public initialisation vector (IV), or 104-bit key and 24-bit public IV.

For every packet sent, a new IV is generated and appended to the key, RC4 is used to generate a key stream of the length of the plaintext and this key stream is XORed against the plaintext data. The sender appends the IV into the frame header of the packet, and a tag is set indicating that this is a WEP packet [18]. The packet is then sent.

The IV is 24-bits long, appending to the shared key to form a family of 2^{24} keys, each frame transmission selects one of these 2^{24} keys and encrypts under the key. This leads to widespread key abuse as a single AP running at 11 Mbps with a typical throughput can exhaust the key space in about an hour [18].

Numerous attacks exist against WEP. In a TCP/IP network, every data frame contains an IP datagram containing large amounts of known plaintext. In such an environment, an attacker can recover a partial stream for every packet sent. Analysis can be conducted on the traffic to identify the type, and this information can be used to guess the values or other variables in the packet headers, revealing more of the data and the key stream. The known plaintext from a single DHCP exchange can provide enough information to decode almost the entire TCP/IP header of every IP datagram encrypted by the DHCP client. Any fully decrypted packet provides the context and hints that can be used to identify the plaintext of a still not fully decrypted packet. This process can continue until the key streams are revealed for almost every IV [18].

WPA uses the Temporal Key Integrity Protocol (TKIP) for encryption and employs 802.1X authentication with one of the standard Extensible Authentication Protocol (EAP) types available today. AP's and client network interface cards can be upgraded to use WPA by the means of a

firmware upgrade. Enterprises will require an authentication server, and home users can utilise a special feature which allows the use of a shared password [20].

TKIP increases the size of the key from 40 to 128 bits and replaces WEP's single key with dynamically generated keys that are distributed by an authentication server. It uses a key hierarchy and key management methodology that removes the predictability which crackers relied upon to exploit WEP. After the authentication server has accepted a client, 802.1X is used to produce a unique master key or pair-wise key for that particular session. TKIP distributes this key to the client and the AP, which dynamically generates unique encryption keys for that session. On any given data packet in that session, 500×10^{12} possible keys exist.

A protection scheme against alterations to packets is the Message Integrity Check (MIC), which is designed to prevent an attacker from modifying data in individual packets and sending them on. This check involves a strong mathematical function in which the receiver and sender both compute and then compare a MIC, if they do not match, the packet is assumed to be tampered with and dropped.

WPA uses 802.1X authentication with EAP; EAP handles the presentation of users' credentials in the form of digital certificates, unique usernames and passwords, smart cards or any other secure identity. The framework allows clients to mutually authenticate with the authentication server, which prevents clients from accidentally connecting to rogue AP's and ensures that users who access the network are the ones who are supposed to be there.

8.2. Wireless Networking Tools and Cracks

AirSnort is a wireless LAN tool which recovers encryption keys, passively monitoring transmissions and computing the encryption key when enough packets have been gathered, this tool requires approximately 5 to 10 million encrypted packets to be gathered, and can guess the encryption password in under a second [2]. A newer, more advanced WEP encryption cracker is AirCrack-ptw, which can recover the key using as little as 40,000 captured packets which can be captured in less than a minute under good conditions [1].

Wireless networks can be discovered and more information can be gathered about them using a tool called NetStumbler [15], this tool is extremely versatile and provides many features. Typical information gathered about any AP is the MAC address, Service Set Identifier (SSID), channel

used, type of wireless (802.11a/b/g/n), form of encryption used, estimated distance of transmission, IP address and subnet.

9 References

[1] Aircrack-ptw Homepage. 2007. http://www.cdc.informatik.tu-darmstadt.de/aircrack-ptw/ (accessed May 28, 2007).

[2] AirSnort Homepage. 2004. http://airsnort.shmoo.com/ (accessed May 5, 2007).

[3] Arbaugh, W. A., Shankar, N. and Wan, J. "Your 802.11 Wireless Network has No Clothes." *Department of Computer Science, University of Maryland*, 2001.

[4] Bahl, P., Padmanabhan, V. N. and Balachandran, A. "Enhancements to the RADAR User Location and Tracking System." *Microsoft Research*, 2000.

[5] Balfanz, D., Durfee, G., Grinter, R. E., Smetters, D. K. and Stewart, P. "Network-in-a-box: How to Set Up a Secure Wireless Network in Under a Minute." *Palo Alto Research Center*, 2004.

[6] Bardwell, J. "I'm Going To Let My Chauffeur Answer That: Math and Physics for the 802.11 Wireless LAN Engineer." 2003.

[7] Borisov, I., Goldberg, I. and Wagner, D. "Intercepting Mobile Communications: The Insecurity of 802.11." 2001.

[8] Button, D. *Tech articles: Effect of Obstructions on RF Signal Propagation.* 1999. http://www.emswireless.com/english/Tech_Articles/tech_art03.asp (accessed March 19, 2007).

[9] Cisco Systems. "Cisco Wireless Location Appliance." *Data Sheet*, 2006.

[10] Farpoint Group. "Evaluating Interference in Wireless LANs: Recommend Practice." *Fairpoint Group Technical Note*, 2006.

[11] Geier, J. "Performing Radio Frequency Site Surveys to Effectively Support VoWLAN Solutions." *Helium Networks*, 2006.

[12] Higgins, T. *MetaGeek Wi-Spy 2.4 GHz Spectrum Analyzer*. 12 February 2006. http://www.smallnetbuilder.com/content/view/24766/96/ (accessed March 4, 2007).

[13] MetaGeek. *Wi-Spy Hardware Interface Specification.* 12 December 2006. http://www.metageek.net/Documents%20and%20Settings/11/Site%20Documents/WiSpyHardwareInterface.pdf (accessed June 5, 2007).

[14] Murphy, W. S. and Hereman, W. "Determination of a Position in Three Dimensions using Trilateration and Approximate Distances." *Colorado School of Mines*, 1999.

[15] NetStumbler Homepage. 2007. http://www.netstumbler.com/ (accessed May 5, 2007).

[16] Rivest, R. L. "The RC4 Encryption Algorithm." *RSA Data Security, Inc.*, 1992.

[17] Rose, C., Ulukus, S. and Yates, R. "Wireless Systems and Interference Avoidance." *WINLAB, Department of Electrical and Computer Engineering, Rutgers University*, 2000.

[18] Walker, J. R. "Unsafe at any key size; An analysis of the WEP encapsulation." *Intel Corporation*, 2000.

[19] Weisstein, E. W. *Law of Sines.* 2003. http://mathworld.woflram.com/LawofSines.html (accessed June 15, 2007).

[20] Wi-Fi Alliance. "Wi-Fi Protected Access: Strong, standards-based, interoperable security for today's Wi-Fi networks." 2003.

[21] Yang, X. and Petropulu, A. P. "Joint Statistics of Interference in a Wireless Communications Link Resulted from a Poisson Field of Interferers." *Electrical and Computer Engineering Department, Drexel University Philadelphia*, 2001.