# 802.11 Wireless Network Visualization and Case Study: Lawrence, KS

by

Brett A. Becker

B.S.Co.E., University of Kansas, Lawrence, Kansas, 2005

Submitted to the Department of Electrical Engineering and Computer Science and the Faculty of the Graduate School of the University of Kansas in partial fulfillment of the requirements for the degree of Master of Science.

_____
Dr. Joseph Evans

_____
Dr. Gary Minden

_____
Dr. John Gauch

_____
Date thesis accepted

# Acknowledgements

The Author would like to thank the following people at the Information & Telecommunication Technology Center and the Kansas Applied Remote Sensing group at the University of Kansas.

To my thesis committee for many years of support and guidance:

Dr. Joseph Evans
Dr. Gary Minden
Dr. John Gauch

To Matt Dunbar for his guidance, help in collecting data, and the idea of using a GIS to visualize wireless networks.

To Tim Buller for introducing all of us to the concept of “wardriving”.

To Larry Sanders for his assistance with technical issues related to 802.11 networks.

To Michael Hulet for his understanding and patience while I worked on this project over the years.

# Abstract

In what has been deemed the century of wireless, understanding the security implications and usage patterns of 802.11 wireless networking has never been more important. As a general trend, more than half of the world's wireless 802.11 networks are not using any form of encryption and are broadcasting their presence. It has become all too easy to locate and "piggyback" these networks for free Internet access or for more malicious purposes such as identity theft, traffic analysis (sniffing), corporate intrusion, or any illegal activity that would benefit from being anonymous on the Internet. Most people who operate these wireless devices are unaware that their network signals typically propagate much farther than intended and do not understand the security implications of an un-wired, broadcast-style medium. The first part of this paper will present a detailed analysis of wireless networking trends in Lawrence, KS over a three-year period, providing a clear picture of the problem at hand and show how it has changed over time. The second part will detail a visualization and mapping technique that makes use of a Geographic Information System (GIS), providing extremely informative views of signal propagation from wireless networks. The goal of these improved visualizations is to raise public awareness, subsequently increasing general concern regarding the security issues that shroud 802.11.

# Table of Contents

# List of Figures

# Chapter 1 - Introduction

## 1.1 *Motivation*

*In this first decade of the 21st century, the communications industry is at an interesting transition point. The 20th century could be called The Wireline Century, with millions of kilometers of copper wire, cable and glass fiber being installed in homes and office buildings, below and above streets, and under oceans. The 21st century is rapidly becoming The Wireless Century. The motivation for wireless technology is no longer voice, as it was in the last century, but data. This shift has been the impetus for a number of distinct technologies for delivering unique services to users.* [1]

As stated by Dzubeck above, we are in the midst of a wireless revolution. 802.11 wireless networking is largely fueling this revolution, forever changing the face of data networks and allowing for a new set of applications and services never before possible. Wireless "hotspots" are popping up all over and cities are starting to build networks that cover their entire city limits. Businesses and home users are also benefiting from the freedom and flexibility that 802.11 offers, rolling out an alarming amount of wireless infrastructure. Of the estimated 37M home networks worldwide in 2003 [2], half are thought to be using 802.11 wireless networks, with wireless having a three to one advantage for new roll-outs [3]. In Lawrence, Kansas, a medium-sized city, a 200% yearly increase in the number of wireless networks has been observed since 2001. As wireless prices fall, the technology is finding its way into more products such as home appliances, audio/video systems, video game consoles, and of course laptops. It is estimated that by 2005, wireless adapters will be included in 95% of notebooks as a standard feature [4].

The popularity of 802.11 networking can be attributed to the amazing amount of flexibility that the technology offers. With the Internet and other network-based services becoming the norm, there is a desire for these services in airports, coffee shops, restaurants, kitchens, living rooms, and in other public areas. Also, with the adoption of broadband and the fact that families are finding the need for more than one computer, it is convenient to create a small home network that allows the sharing of a broadband connection, files, and printers. Traditionally, a hard-wired network was used for this, interconnecting each network element. Wireless simplifies this process tremendously by eliminating the need to run and terminate cables. Businesses are also realizing that wireless can save money in network deployment, can revolutionize the way they do business, and can offer new work environments for their employees.

Unfortunately, all of this new-found networking freedom comes at a price. Wireless networks broadcast their signals over the air using the electromagnetic spectrum and do not offer the same physical security that wired networks do. Most people who operate these wireless devices are unaware that their network signals typically propagate a lot farther than where they are intended. Home users are finding that they can access their neighbors' networks and businesses are learning that their signals are leaking out into their parking lots and around their buildings. To add to this problem, most users are not implementing the security features built into all 802.11 devices.

The encryption that was designed to maintain privacy (WEP) is easily breakable and from what I have observed over the years, the vendors are downplaying its importance and providing poor instructions to implement it. It is safe to say that on a world-wide basis more than half of the wireless networks deployed are not using encryption, meaning that the signals are broadcast openly over the air for anybody or anything to intercept [5]. Other wireless security practices that security experts recommend such as MAC filtering, disabling "broadcast SSID", using a non-default SSID, updating firmware, and changing configuration passwords are also being ignored.

All of this has led to an explosion in the number of easily accessible access points that are wide open for anybody to use. With this capability, users can "piggyback" or use wireless networks without the owner's permission for anonymous Internet access or traffic analysis. Open network file shares can even be accessed. This ability can lead to both identity theft and copyright violation, and could be a major liability for protecting the nation's cyber infrastructure. Wireless access points are also configured by default in the factory to respond to any request for identification information sent out by another wireless network card. This makes them very easy to locate.

With the potential security risks at hand and explosive growth of open networks, it is important to understand the implications of this technology. The objective of this study is to quantify the growth and security of wireless networks in a typical, medium-sized city. After not being able to locate any controlled studies of

how wireless networking has changed in a typical city, it was decided that a study such as this would be beneficial in explaining, quantifying, and predicting the future trends of wireless. Using the technique of "wardriving", wireless network statistics were collected by scanning a sample set of roads in Lawrence, Kansas over a three-year period. After clearly quantifying the security problems at hand, it became evident that a better method was needed to convey these security issues to the public.

Therefore, the main focus of this study is the development of a visualization and mapping technique that makes use of a Geographic Information System (GIS) to provide informative views and show the propagation of wireless network signals. In 2000, when these techniques were first developed, there were no methods for mapping the propagation of wireless network signals based on data from wireless scans. By providing aerial views of a typical house or business, and showing how far the wireless signals actually propagate, much better visualizations can be generated which a business or a home wireless user can more easily understand. It is my hope that through the images generated by this technique, public awareness regarding wireless signal propagation and security can be raised.

## 1.2 *Project Goals*

This project aims to:

- Provide information on how wireless network data is collected by means of "wardriving"
- Investigate the trends and statistics of a medium-sized city's wireless infrastructure, quantify the growth and security problems at hand, and predict future trends
- Raise public awareness regarding wireless networking by providing meaningful visualizations of wireless infrastructure

## 1.3 *List of Accomplishments*

The following was accomplished with this research:

- A three-year study of wireless networking trends in Lawrence, KS was performed yielding valuable statistics on growth, vendor saturation, and use of security features. This data was then compared to world-wide statistics and used to predict future wireless trends of a typical medium-sized city in the US.
- A technique for visualizing wireless signal fields using a Geographic Information System (GIS) was developed which provides a clearer picture of signal propagation, and helps in explaining to others the potential security risks of unwired networks.

## 1.4 *Layout*

This document is organized into the following sections:

- Background – A thorough description of the 802.11 standard and wireless concepts along with the potential security threats inherent in wireless networking
- Acquisition of Wireless Network Data – A detailed look at how wireless network data is acquired through the use of active and passive scanning
- Case Study: Lawrence, KS – An in-depth look at how wireless networking has changed over the last three years in Lawrence, Kansas, providing a clear picture of the security problems at hand
- Visualizing Wireless Networks – A description of the wireless network visualization methods developed, along with a detailed procedure and several examples of generated imagery
- Conclusion and Future Work – Conclusion and recommendations for further research on these topics

# Chapter 2 - Background

This chapter provides an introduction to the 802.11 wireless networking family of standards, concentrating on the unique features and concepts that 802.11 brings to the IEEE 802 family. It then details the many security threats inherent in 802.11 wireless networking.

## 2.1 *802.11*

In 1990, The Institute of Electrical and Electronics Engineers (IEEE) started working on an official industry standard for wireless networking. In 1997, the 802.11 standard was released allowing for wireless communication at speeds of up to 2Mb/s in the 2.4GHz spectrum. There were few products based on this standard due to its slow data transfer rate and compatibility problems, so in 1999 the IEEE created the 802.11 Working Group which soon released two new standards, 802.11a and 802.11b [6]. It was these new standards (especially 802.11b) with their higher transfer speeds, better interoperability, and lower cost which gained wide acceptance and revolutionized the networking industry. Since then, many other 802.11 based standards have been released that specify enhanced security (802.11i), quality of service (802.11e), and faster transfer speeds (802.11g and 802.11n). Figure 2-1 summarizes some of the 802.11 family standards that are prevalent today.

| Standard | Ratification | Description |
|---|---|---|
| 802.11 | 1997 | The original 2 Mbit/s wireless networking standard which uses the 2.4 GHz ISM Band |
| 802.11a | 1999 | Enhancements to 802.11 which provide 54 Mbit/s in the 5 GHz ISM Band |
| 802.11b | 1999 | Enhancements to 802.11 which provide 11 Mbit/s in the 2.4Ghz ISM Band |
| 802.11e | 2002 | Enhancements include Quality of Service (QoS) and packet bursting |
| 802.11f | 2002 | Defines the Inter-Access Point Protocol (IAPP) for roaming between different vendors' access points |
| 802.11g | 2002 | 54 Mbit/s wireless standard that uses the 2.4 GHz ISM Band (backwards compatible with 802.11b) |
| 802.11i | 2004 | Provides enhanced security and encryption |
| 802.11n | 2006 (Planned) | Not yet standardized but will provide speeds up to 135 Mbit/s (backwards compatible with 802.11g and 802.11b) |

**Figure 2-1: Commonly Used 802.11 Standards [7][8]**

Instead of recreating the entire set of underlying network technologies necessary for wireless communication, 802.11 focuses on the issues surrounding the wireless medium.

A lot of technologies are borrowed from other 802 standards such as 802.3 (Ethernet) which specifies the network layer Media Access Control (MAC) that 802.11 uses. In the rest of this section, the concepts and technologies that are unique to 802.11 will be discussed such as its spectrum requirements, topologies, physical access, authentication, and privacy.

### 2.1.1 Spectrum

Wireless networking relies on the electromagnetic spectrum as its medium for transmission. In the United States, the Federal Communications Commission (FCC) regulates the radio spectrum and has designated three bands for *Industrial Scientific and Medical (ISM)* use. 802.11a operates in the C-Band ISM (5.725 - 5.875 GHz), while 802.11b and 802.11g operate in the S-Band ISM (2.4 – 2.5 GHz) [9]. These bands were chosen for 802.11 since they are less regulated by the FCC, allowing for unlicensed public use at a transmission power below 1 Watt [10]. In 802.11, the ISM bands are split up into several channels to allow for multiple access points to share the resource without interfering with each other.

### 2.1.2 Data Delivery and Reliability

The wireless medium offers many challenges in regards to interference and noise, with other products such as cordless phones and Bluetooth devices competing for the same spectrum. Also, multiple 802.11 networks that are within range of each other can contend for the same spectrum creating transmission collisions. To combat this problem, a more reliable data delivery mechanism was needed. The 802.11 standard defines a more robust data delivery method called Carrier-Sense Multiple Access with Collision Avoidance (CSMA/CA) that listens to the medium before transmitting, thus avoiding collisions. This is different then the CSMA/CD (CSMA with Collision Detection) found in 802.3 Ethernet, which detects transmission collisions after they have happened. CSMA/CA creates more traffic since it has to broadcast a signal onto

the network in order to check for collision scenarios and to tell other devices not to broadcast [11].

### 2.1.3 Wireless Topologies

The 802.11 standard defines two modes of operation: Infrastructure and Ad Hoc. Ad Hoc, which is rarely used, was designed to provide peer-to-peer networking, allowing multiple wireless devices to talk to each other directly. In this scenario, the simplest network possible is between two computers and is typically used as a convenient way to setup a quick network for file exchange. With Ad Hoc, all stations must be in range of each other to participate in a common network. This mode of operation is also commonly referred to as an Independent Basic Service Set (IBSS).

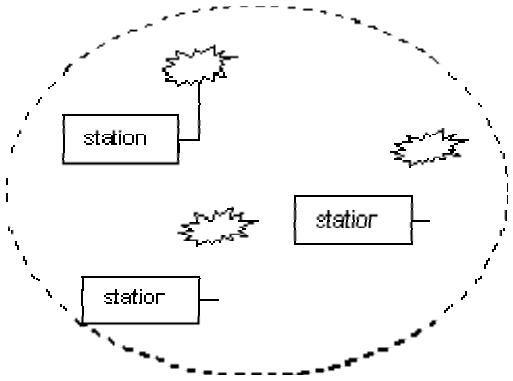


**Figure 2-2: Ad-Hoc Wireless Network Topology [12]**

Most wireless networks use the Infrastructure mode since it allows for a dedicated piece of hardware called an “access point” (AP) to participate in the wireless network. AP’s provide a bridge between wireless and wired Ethernet networks, and provide

mechanisms that allow for clients to roam between access points on the same LAN. This mode of operation is also referred to as a Basic Service Set (BSS).

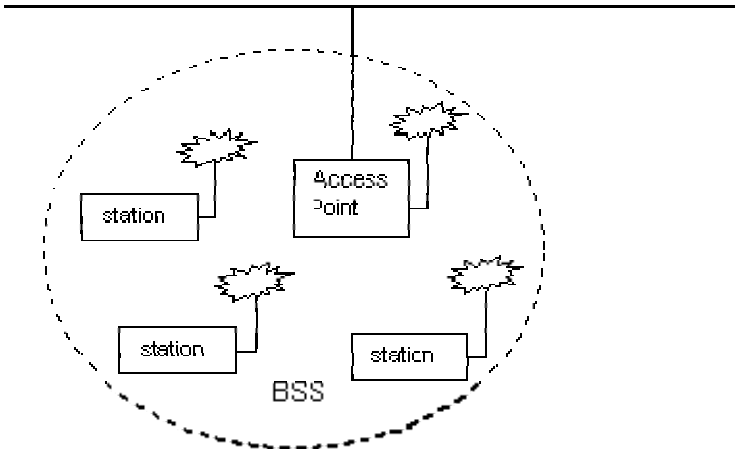


**Figure 2-3: Infrastructure Wireless Network Topology [12]**

A collection of access points that allow for roaming between them is referred to as an Extended Service Set (ESS). In an infrastructure network, all communication between the clients is sent through the access point.

### 2.1.4 Association

In an infrastructure network, association is required before any client can communicate on the network. Mobile stations always initiate the association process and base stations may choose to grant or deny based on the contents of an associate request [12]. Wireless clients can only be associated with one access point at a time.

### 2.1.5 Reassociation

The reassociation service handles the responsibility of managing client "handoffs" between access points. This is typically performed when signal levels indicate that a switch to a different access point in the ESS would be beneficial. This service also makes sure that any frames that never made it to the client from the previous base station are sent to the new base station for transmission to the client.

### 2.1.6 Authentication

Wireless networks have limited physical security and need a mechanism to prevent unauthorized access. 802.11's authentication service defines a set of services to control access to the wireless network. This mechanism is put into place to allow for the identification of one station to the other. Two methods are defined in the 802.11 standard for authentication: Open System Authentication and Shared Key Authentication.

#### 2.1.6.1 Open System Authentication

Open system authentication is based on a very simple two-step process. A special packet which contains the station's identity or Service Set Identifier (SSID) is sent to the authenticating station. The authenticating station then responds with a packet which specifies whether the identity of the authenticating station is recognized. This is commonly referred to as an "open network", and if the authenticating station or access point is broadcasting its SSID, then a client can ask for the SSID by sending a probe request. If the access point or station is not broadcasting its SSID, then the user

must have prior knowledge of the SSID or use specialized scanning software to find it by listening to transmissions from the station.

#### 2.1.6.2 Shared Key Authentication

Shared key authentication is based on the concept of a secret shared key that is known by each station. In the case of 802.11 networks, a secret key is typically configured on a station or access point and then communicated to other users through a secure channel independent of the 802.11 network. Authentication is granted when the keys match between the stations. With Shared Key Authentication, the use of Wired Equivalent Privacy (WEP) is assumed since the same keys are used to encrypt all traffic transmitted between stations.

### 2.1.7 Privacy

With a wireless network, all stations that are in range can "hear" data traffic on the network. This seriously impacts the security level of a wireless link. To combat this problem, WEP, or “Wired equivalent privacy”, was defined in the 802.11 standard to provide encryption between stations. Since many security flaws have been discovered in WEP, newer standards such as 802.11i and WPA have emerged to provide a more robust encryption mechanism.

#### 2.1.7.1 WEP

WEP was originally defined in clause 8.2 of the IEEE 802.11 Wireless Networking Standard to provide encryption that prevents casual eavesdropping. WEP only

protects the data as it traverses the wireless medium and was not designed to provide complete end-to-end protection over a mixed wired/wireless network. Its name implies that it is equivalent to a wired network in its ability to keep information private. Unfortunately, this has been proven not to be true.

WEP uses an RC4-based symmetric encryption where each packet is encrypted using a secret-key to generate the cipher text. RC4 is the most widely used stream cipher in software applications [13]. WEP's implementation of RC4 suffers from many attacks since it was poorly designed from the beginning, but the most damning was described in a 1991 paper by Fluhrer, Mantin and Shamir [13]. Their discovery led to several publicly available tools and more papers describing optimized algorithms for implementing their findings. Their attack relies on knowing the first byte of the encrypted frame and working from there to derive the key. Since 802.11 uses Link Level Control (LLC) encapsulation, the value of the first byte is known (0xAA). Each byte must be guessed since this attack is statistical in nature; each resolved packet gives a 5% chance of guessing a correct key byte and a 95% change of guessing incorrectly [14]. By looking at enough of these resolved cases, a bias toward the true key bytes starts to emerge. Once the early key bytes are narrowed down, it is then possible to test candidate keys by determining if the WEP checksum on a decrypted packet is correct.

Originally, the 802.11 standard defined a maximum WEP key length of 40 bits since in 1997 the 40-bit encryption key was considered reasonable for low level security [9]. 40-bit key technology was not controlled by the US export laws at the

time and the vendors desired world interoperability. Most experts argue that keys should be at least 128 bits now. Almost every vendor has adopted this after the 802.11 standard was relaxed, with some even offering 256-bit keys. When cracking WEP, longer keys only change the analysis time of the dictionary of collected packets, equating to a few extra seconds of CPU time. There have been multiple tools written to exploit the vulnerabilities in WEP and derive keys from a collection of wireless network packets.

#### 2.1.7.2 802.11i / WPA

After realizing that WEP has too many flaws to fix, the IEEE started working on an 802.11 supplement titled "Specification for Robust Security" which has been coined 802.11i. This new system requires completely new hardware since it implements a completely re-worked encryption scheme from the ground up. One of the most important features that 802.11i offers is authentication. This allows for mechanisms to make sure that the data is coming from its supposed source, that it can not be seen, and that it can not be modified [15]. WEP only provides encryption and does not have any mechanism to provide for authentication.

802.11i is based on AES (Advanced Encryption Standard) which is a very robust and well-tested encryption method. One drawback of AES is that it generally requires more computational power than is in today's deployed 802.11 hardware, due to a much more complex algorithm. It solves the problem of key management by using RADIUS (Remote Access Dial-In User Service) and provides authentication by using 802.1X. It also creates fresh keys at the start of a session and changes keys on a

constant basis using the Temporal Key Integrity Protocol (TKIP). 802.11i was approved in July 2004 and is starting to find its way into enterprise grade access points.

Another system has been developed called Wireless Protected Access (WPA) and, according to Walker, all Wi-Fi products manufactured since August 2003 should be WPA ready [16]. WPA version 1.2 was designed as a stepping stone into 802.11i since 802.11i was only just recently finalized. WPA 1.2 is portions of 802.11i and Draft 3.0. It implements TKIP but does not support AES encryption. WPA version 2.0 implements the entire 802.11i specification and can be considered synonymous with 802.11i.

## 2.2 *Wireless Security Threats*

### 2.2.1 Signal Propagation and Packet Analysis

The nature of wireless communication, in its use of the electromagnetic spectrum to send signals through the air, is its biggest threat. Factors such as the transmission power, the receiver sensitivity, and physical obstacles such as walls determine where a signal is propagated, unlike a traditional wire or fiber. These signals have the potential to travel great distances and can usually be found beyond their intended destinations. As long as a receiver such as an off-the-shelf wireless network card is in range, all wireless packets (encrypted or not) can be intercepted.

Without extremely sophisticated tools, it would be almost impossible to detect a station that is passively listening. If a client was actually associated with the network, then it could be tracked by physically walking around looking at how the signal level changes. Some companies do offer specialized wireless security products that use triangulation to determine the location of a station, but they are extremely expensive due to their complexity. The only useful information that might be obtained from the network side would be the MAC address of the card (which can easily be spoofed) or information about the client's operating system (which can easily be hidden through the use of a firewall).

Once wireless network packets are intercepted, they can be directly analyzed with the ability to look for content such as clear-text passwords, web addresses, IP addresses, or any other information transmitted over the network. Web browsers help combat this issue since they typically provide their own end-to-end encryption using the Secure Sockets Layer (SSL) for sensitive information exchange such as bank transactions. Not all web sites use this encryption, and there is a definite possibility of an attacker collecting enough information that could aid them in identity theft. Even if the network is using WEP encryption, packets can still be collected and later analyzed to derive the encryption key.

### 2.2.2 Unsecured Networks and Poor Access Point Configuration

Poor wireless access point configuration is another major issue surrounding the security of wireless networks. A lot of users are not implementing the built-in security measures that are found in every 802.11 access point such as encryption,

MAC address filtering, and disabling “broadcast SSID”. Only about 38% of the networks in the world are using WEP encryption [5]. Even though WEP encryption can be cracked, it still acts as a first line defense against intrusion and packet analysis. The newer encryption standards such as WPA and 802.11i are secure as of today, but nobody knows what the future might hold. WEP was considered secure when it was first deployed, but now can easily be circumvented using several highly published methods.

Access points support the ability to perform MAC address filtering which only allows certain cards with known MAC addresses access to the network. This security measure can easily be circumvented by changing the MAC address on a wireless card, but is still effective as another barrier against unauthorized use. Another security feature commonly overlooked is disabling “broadcast SSID”. This makes it harder for attackers to locate access points since more sophisticated software that implements passive scanning would then become necessary to detect the access point. This is discussed in detail in the next chapter.

Another common mistake made in the configuration of access points is in the use of a descriptive or default SSID. It is fairly common for home users and businesses to use descriptive SSID’s such as their business name, department name, first/last name, or their address when configuring their networks. This aids a hacker by giving them more information on the potential use of the network, parties responsible, or an exact location. Almost every access point comes preconfigured with a default SSID. A lot of users do not change this from its default setting,

signaling the distinct possibility of a poorly configured access point that does not have the security features mentioned above enabled.

A lot of other basic and fundamental security measures such as changing the access point password and applying firmware updates are also commonly overlooked. Some users do not change the password that is required to gain access to the configuration of their access point. The default passwords for each of the manufacturer's equipment are well-known and published all over the Internet. By not changing the default password, it would make it very easy for an intruder to reconfigure or hijack the access point. It has also been discovered that some of the firmware versions running on the various manufacturers' access points suffer from major security flaws. This could allow an attacker to gain access to the access point configuration. People typically do not upgrade the firmware unless they are having a non-security related issue.

### 2.2.3 Un-authorized Use

Without the use of any of the basic security features listed above, any client can freely associate with a wireless network. "Piggy-backing" or using another's private network without permission is becoming a major issue. Home users are accidentally associating with their neighbors' networks or knowingly using them for any purpose they see fit. Typically, this is done for free Internet access or for more malicious activities that would benefit from anonymity such as illegal file sharing. Since most ISP's implement quotas on their broadband subscribers, this could lead to billing problems or termination of the victim's service. To add to the problem, the

implementation of DHCP servers found on most networks make it even easier for a client to associate with a wireless network and immediately receive an IP address. The Dynamic Host Configuration Protocol (DHCP) is designed to make administration easier by dynamically assigning address to devices when they want network access.

Businesses usually have to protect more sensitive information than one would on a typical home network. It is a common mistake to simply plug wireless access points into an internal corporate network which resides behind firewalls or other security measures. In this scenario, the firewall is bypassed, making the access points part of the "trusted" internal network. This could give a wireless intruder less obstructed access to sensitive servers, file shares, etc. The same holds true in home networks, allowing the associated clients to be connected to the network inside the router bypassing the Network Address Translation (NAT). NAT can be helpful in increasing security by not allowing access to open ports inside a network. Almost every security expert recommends isolating wireless networks on a different segment of a network so access can be controlled to more sensitive areas. They also recommend using a Virtual Private Network (VPN) to provide robust encryption between the client and a VPN gateway within the network. In this scenario, all traffic is encrypted with a much more secure algorithm from the client to the VPN gateway, making it nearly impossible for a hacker to analyze the traffic.

According to industry experts, shoddy configuration of wireless local area network (LAN) access points and client software will cause 70 per cent of successful

attacks against business networks through 2006 [17]. Recently, a Michigan man pleaded guilty in Charlotte, North Carolina in his role to steal credit card numbers from the Lowe's chain of home improvement stores by breaking into an unsecured wireless network at a store in suburban Detroit [18]. This gave the hacker access to the Lowe's corporate network, where software running on servers located in a different state was modified to collect credit card numbers. The interesting part of the story is that the suspects were apprehended in the store's parking lot using a laptop and a wireless card to access the network.

### 2.2.4 Denial of Service Attacks

Anybody can overwhelm the spectrum causing the transmitters to wait to send their information. The same technology found in cell phone jammers, which renders cell phones useless, could easily be adapted to the 2.4Ghz and 5Ghz bands.

### 2.2.5 Public Wireless Networks and "Hotspots"

By associating to a public network or "hotspot" without some sort of client security such as a firewall and/or antivirus program, a user is potentially subjecting them self to attack. Public networks are common grounds for "worms", "viruses", and "malware" to propagate. Also, if anonymous network file sharing is enabled, it would be trivial for others to access these shares.

# Chapter 3 - Acquisition of Wireless Network Data

## 3.1 *Wireless Scanning*

Unlike traditional wired local area networks where it is as simple as following wires to determine a network topology, wireless networks use a radio signal that propagates through free space. Wireless scanning is the process of identifying networks by looking for these signals. It is very common for these signals to propagate farther than they are intended for and can typically be detected outside homes and businesses, sometimes up to several blocks away. The coverage area is primarily determined by the power that the signals are transmitted at, the antennas used, and physical obstacles such as walls.

Wireless network data can be obtained with most 802.11 enabled PC's or PDA's running specialized wireless scanning software such as Kismet and NetStumbler. These programs allow you to collect an amazing amount of information from wireless networks such as the MAC Address, SSID, network type, channel, WEP status, and a GPS location. Some software packages even support the ability to log traffic that is traversing the air for later analysis via sophisticated packet-analysis software. Other simple scanning mechanisms are typically found built into operating systems such as Microsoft Windows and Apple OS/X, allowing for easy discovery of wireless network SSID's that your wireless adapter can associate with. A wireless network scan can be as simple as looking for signals in a

stationary location or can take a more mobile approach by scanning much larger areas.

## 3.2 *Wardriving*

Wardriving or "collecting wireless network data by means of automobile," is a term that was coined by Pete Shipley, a computer security expert from Berkeley, CA. He claims he was not the first to search for open wireless networks, but was the first to automate the scanning process and integrate a GPS to provide spatial information [19]. Since his initial "wardrives" in 1999, people have extended the concept of wardriving to planes ("warflying"), sail boats ("warsailing"), and have even developed a method of providing localized wireless network information by chalking special symbols onto a sidewalk ("warchalking").

"Wardriving provides a unique opportunity to gauge the growth of a technology market segment by direct inspection [20]." Using off the shelf technology, a wealth of information can be collected that is not easily accessible with other technologies. This phenomenon has led to great interest in "wardriving" by the research community and hobbyists for studies such as this. On the other hand, malicious hackers are also using "wardriving" as a convenient way to find new, previously unavailable paths into home and corporate networks.

## 3.3 *Legalities of Scanning*

Many legal questions arise when discussing wireless network scanning and packet-sniffing. "The legality of wardriving has not been tested, but few people think that wardriving itself is illegal [20]." This seems to be the general consensus among most people, including the FBI, since it can be used legitimately for security audits and site surveys. Bill Shore, a Special Agent with the FBI, recently stated the following in an official email:

> *Identifying the presence of a wireless network may not be a criminal violation, however, there may be criminal violations if the network is actually accessed including theft of services, interception of communications, misuse of computing resources, up to and including violations of the Federal Computer Fraud and Abuse Statute, Theft of Trade Secrets, and other federal violations."* [21]

One thing is certain; it is definitely illegal to use a network without the owner's permission. This is clearly stated in "§ 1030, Fraud and Related Activity in Connection with Computers", which is part of the National Information Infrastructure Protection Act of 1996. Since the owner of the network is typically paying for an Internet connection, it would be considered theft if his/her connection was used for personal purposes [22]. Another illegality would stem from a person knowingly bypassing the Wired Equivalent Privacy (WEP) security to access the network.

Scanning software like NetStumbler supports a feature where it will automatically try to associate with the networks it finds. If TCP/IP is bound to your network card, and DHCP is enabled, then it will even go as far as trying to acquire an address through a DHCP server. This could be considered intrusion since you are requesting an IP address to use on their network. The authors of NetStumbler recommend unbinding TCP/IP from the wireless network adapter before scanning so there is no accidental use of any discovered network.

## 3.4 *Active Scanning vs. Passive Scanning*

When scanning for wireless networks, two predominate scanning methods have emerged known as active and passive scanning. In active scanning, a probe request is transmitted from the wireless card into the air using a special broadcast SSID. If an access point picks up the request, a probe response is sent back. By looking for these responses and analyzing the information contained in them, network scanning software can gather information from access points in range. This exchange of information is an integral part of the original 802.11 standard and is how access points provide the client with all the necessary information they need to associate, such as the supported data rates and SSID. Active scanning software takes advantage of these responses and logs the information contained in the response packets. NetStumbler (http://www.netstumbler.com), which is one of the more popular scanning packages, implements this type of scanning.

The disadvantage of active scanning is that it only allows for discovery of wireless access points that are configured to respond to probe requests. An access point will respond to probe requests if the "broadcast SSID" configuration option is enabled. Most access points have this feature enabled, since it is usually the default setting. This makes it much easier for a user to get a wireless network up and running out of the box since it allows for the wireless configuration utilities found in most operating systems to discover the SSID of the network. With active scanning you can still detect closed, non-broadcast SSID systems if your wireless adapter is set to the same SSID as the access point before initiating a scan.

Passive scanning uses a special driver to put the wireless card into a mode in which it can see all data that is broadcast through the air. This special mode is typically referred to as "rfmon" and is similar to promiscuous mode in Ethernet except that it can also see management packets such as beacons and probe requests/responses without being associated with the network. Since there are eleven channels defined by the 802.11 standard for the United States, it must rotate or "hop" through these channels and listen in order to detect the presence of any access point in range.

Passive scanning exploits the fact that access points typically broadcast a beacon every 100 ms, which contain the same information offered in a probe response. With passive scanning, any access point can be detected, including non-broadcast SSID closed systems, as long as you happen to be listening on the same channel that it is transmitting on. In theory, this scanning technique can detect all

access points in range, regardless of their configuration. One disadvantage of this method is the fact that you have to use a special driver and that it is possible to miss a transmission when you are not listening on the same channel as the transmitter. The wireless scanning package Kismet (http://www.kismetwireless.net) implements passive scanning, but can be difficult to set up.

## 3.5 *Wireless Network Scanning Software*

### 3.5.1 NetStumbler

NetStumbler is a closed-source, windows-based, wireless network scanning tool that allows you to detect wireless networks using 802.11a, 802.11b, and 802.11g. It was originally released in 2001, and quickly became very popular due to its ease of use and support for a wide range of wireless cards. It works well as a wireless network validation tool by allowing you to check the settings of your network infrastructure, and is also useful for detecting "rogue" access points.

As you can see in Figure 3-1, NetStumbler provides a user-friendly interface and a useful signal strength graphing functionality. A selection window on the left provides a way to filter networks based on criteria such as channel, name, and MAC address, while the window on the right displays the information collected from each access point.

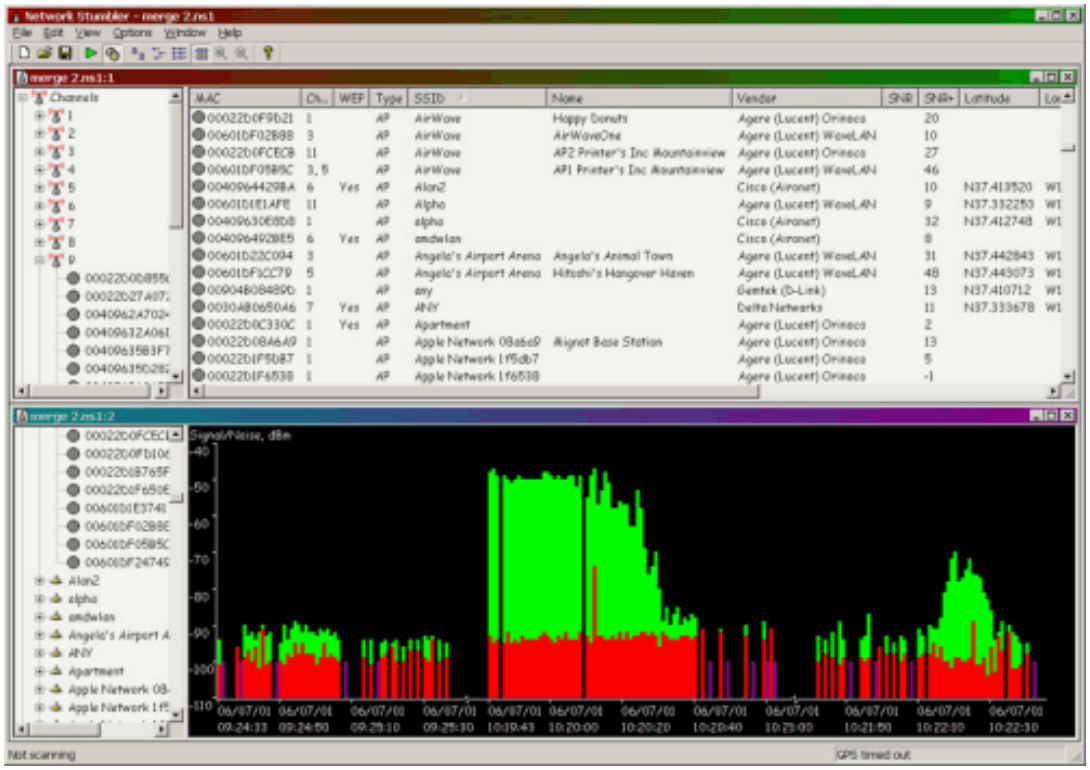


**Figure 3-1: NetStumbler Screenshot**

NetStumbler provides the attributes shown in Figure 3-2 for each access point it receives a probe response from. There are very few configuration options, but one worth mentioning is the scanning speed, which determines the rate at which it sends out probe requests. For the purposes of this study, this was always set to the maximum to increase the number of data points obtained.

| | |
|---|---|
| MAC Address | The registered device address which is also known as the Basic Service Set Identifier (BSSID) |
| Channel | The channel the access point is broadcasting on |
| Name | The device's name. In our experience, this is rarely reported and only if "Query AP's for names" is configured |
| SSID | The Service Set Identifier (SSID) of the Access Point |
| Speed | The maximum theoretical bandwidth of the AP; This was never reported with the version of NetStumbler we used |
| Vendor | The registered vendor name based on the MAC address; NetStumbler has a limited vendor database so a post-processing script was written to look up the all of vendor names. |
| Type | The mode the network operates in (Ad-Hoc or Infrastructure) |
| Encryption | Whether WEP was turned on or not |
| Signal | The signal level in dB |
| Noise | The noise level in dB |
| SNR | The signal to noise ratio which is the signal minus the noise |
| Beacon Interval | The rate at which the access point broadcasts a beacon frame in Kμs |

**Figure 3-2: Access Point Attributes Detected by NetStumbler**

NetStumbler provides a handy export feature that will allows scanning data to be dumped into a tab-delimited text file. Once it is in this form, it becomes much easier to write post-processing scripts and import into programs like Excel, a Geographical Information System (GIS), or other mapping tools. There are three export formats that it supports: "summary", "text", and "wi-scan". The "summary" export option provides a single entry for each AP, based on where the signal strength was the maximum. The "text" option provides every probe response received at a given GPS position. The last export type is "wi-scan" and is a special format compatible with Pete Shipley's original FreeBSD wireless detection script.

NetStumbler provides a powerful method to collect wireless data, with the exception that it implements active scanning and can only detect “broadcast SSID” enabled access points. In order to see all of the wireless access points when scanning, a program that implements a passive scanning technique such as Kismet needs to be used.

### 3.5.2 Kismet

Kismet is an 802.11 Layer 2 wireless network detector, sniffer, and intrusion detection system [23]. It is open source and runs on the Linux operating system. Kismet works with any card that supports raw monitoring (“rfmon”) mode and implements passive scanning. Information is collected by passively listening to the air and it can even detect the presence of non-beaconing networks by looking for data traffic. Kismet has a separate program called “kismet_hopper” which takes care of switching between the channels in a rapid fashion to look for signals. One disadvantage of this program is its “curses- based” text interface as shown in Figure 3-3. Since there is no mouse support, it requires memorizing a series of keystrokes for navigation.

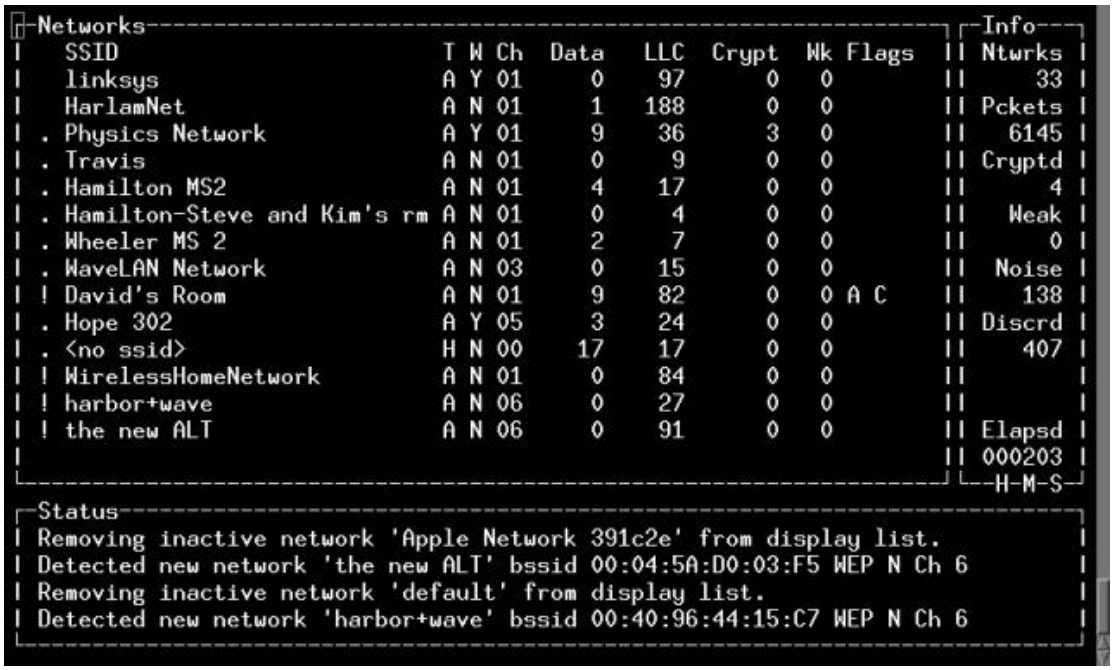


**Figure 3-3: Kismet Screenshot**

In addition to being capable of gathering the same types of information from access points as NetStumbler, it offers a traffic "sniffing" feature. All data traffic that it encounters is logged and can later be analyzed with powerful network analysis software such as Ethereal. Ethereal allows for detailed packet analysis and can recreate HTTP sessions, filter traffic based on any attribute, and provide statistical analysis.

Unlike NetStumbler, Kismet requires special chipset specific "rfmon" drivers which can be a real challenge to get compiled and working. For my laptop running Red Hat Linux 9.0, it required patching the PCMCIA source code and then recompiling the Orinoco (prism2) module. Recently, the "rfmon" functionality has

been included in the CVS version of the prism2 drivers, and will most likely find its way into future Linux kernel source releases. There were several problems with the firmware version of my Orinoco card, so an older version had to be used.

Kismet also provides a basic tool for drawing networks overlaid on downloaded maps called "gpsmap" [23]. It is capable of reading the data files generated from a Kismet scan and can overlay simple network features on top of downloadable maps from sources such as MapBlast, Terraserver, and Earthmaps. This is a nice feature if you want to generate some simple maps, but it provides little control and flexibility with its non-intuitive command line interface.

## 3.6 *Scanning Equipment*

For "wardriving", standard off-the-shelf equipment such as a laptop, wireless card, external antenna, and GPS is all that is typically required. In Figure 3-4, a typical "wardriving" setup is shown.

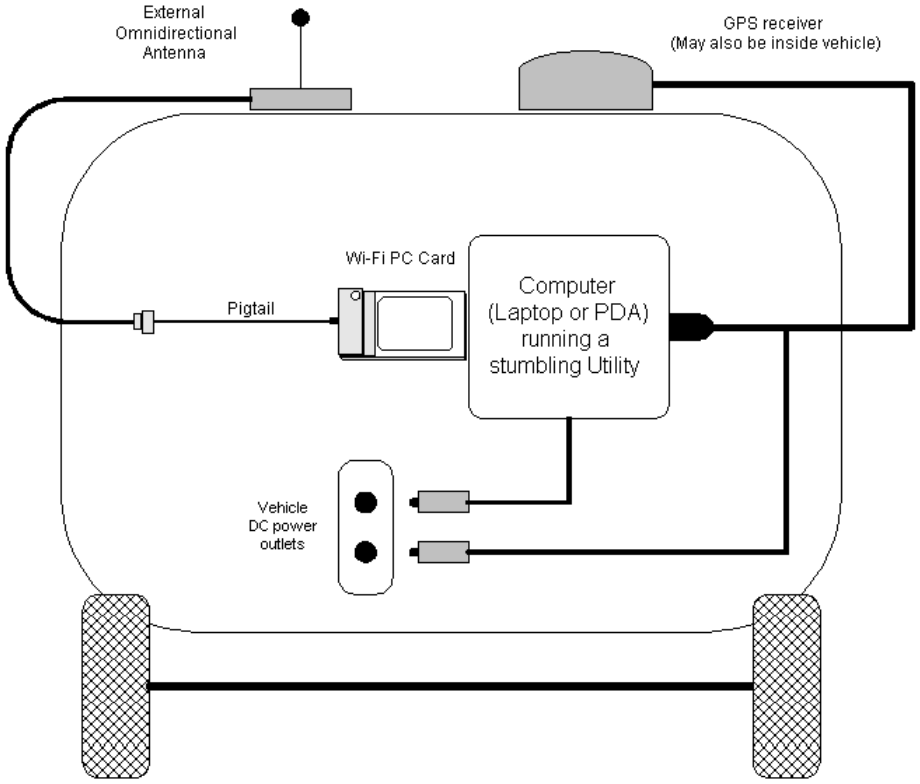


**Figure 3-4: Typical "Wardriving" Setup [20]**

### 3.6.1 Laptop

Most “wardrivers” find it easiest to use a laptop due to its size, low power consumption, and PCMCIA slots (for wireless network cards). A standard Pentium II/266Mhz dual-boot laptop running Windows 2000 and RedHat Linux 9.0 was used for this study. Before obtaining a power inverter, the laptop’s battery was used only providing about 2-3 hours of scanning time. With the addition of a small DC to AC inverter, it was possible to scan indefinitely.

### 3.6.2 Wireless Network Card

The choice of the wireless card is important since there are many factors to consider such as the transmit power, compatibility, and external antenna connectivity. An Orinoco (Proxim) Gold PCMCIA card was used for this study since it is well-supported, has a decent transmit power, and provides an external antenna connector. It was necessary to obtain a special pigtail cable which converts the proprietary MC-Card connector on the wireless card to a standard N-type connector for connection with the antenna.

### 3.6.3 Antenna

When scanning for networks, it is best to use an antenna that is located outside your car. The body of the car acts as a barrier for radio signals and will severely limit the range at which you can detect networks. According to Jeff Duntemann's "Wardriving FAQ", a roof-mounted omni antenna increases the number of stations sensed by at least 50%, and in some cases 100%, over a PC card's built-in antenna. [20]

There are two predominant types of antennas that are commonly used with 802.11 networks that are classified as omni-directional and uni-directional. Omni-directional antennas are the best for "wardriving" since they attempt to provide a uniform sensitivity and transmit strength in all directions. Although they are not as sensitive as uni-directional antennas, which focus their signal in a single direction, they are still the best choice for scanning because of their directionally unbiased sampling method. Uni-directional antennas allow you to transmit and receive at

greater distances but must be aimed in the direction of the signal. These work poorly for “wardriving” since they are extremely focused and would have to be pointed in the general direction of the access point. For all scans, an Orinoco 9.5db omni-directional antenna mounted in the bed of a truck was used. This provided excellent sensitivity and allowed for the discovery of more networks. Most people will use a smaller magnetic roof-mounted 6db omni-directional antenna since it is easily adaptable to any car.

Another important thing to consider is the antenna cable. At 2.4Ghz, signals degrade quickly when they are being transmitted through a cable. Using a spectrum analyzer, the signal loss of the 2 meter cable and couplers was measured to be about 2db. Using high quality cable, eliminating couplers, and reducing the cable length helps minimize signal loss.

### 3.6.4 GPS

In order to collect the longitude and latitude of where the access point probe responses were received, and to later map them, a GPS is required. Most of the scanning packages require a GPS receiver that emits Garmin, Earthmate, or NMEA 183 formatted data. For our scans, we used a Garmin GPS II Plus which has an external antenna connector. Since GPS units are designed to work outdoors, we found it very useful to use an external antenna located outside the car. This allowed the GPS to always have plenty of satellites to lock onto, providing the most accurate positioning information possible. Without an external antenna, it is recommended that the GPS be placed on the dash as far forward as possible to help it pick up the

maximum number of satellites. The GPS was connected to the laptop using a serial to USB converter.

# Chapter 4 - Case Study: Lawrence, KS

## 4.1 *Case Study Introduction*

In Chapter 3, techniques for acquiring wireless network data were discussed. This chapter takes these methods and applies them to a real-world example, the city of Lawrence, Kansas. After not being able to locate any controlled, localized studies of how wireless networking has changed in a typical city, it was decided that a study such as this would be beneficial in explaining, quantifying, and predicting the future trends of wireless. A city-wide sample set was selected and re-driven in three subsequent years yielding a snapshot of the wireless infrastructure on a yearly basis. From this data statistical analysis was performed, and trends such as WEP usage, growth, vendor saturation, default SSID usage, and channel usage were analyzed. In summary, this chapter will provide valuable insight on the growth of wireless and use of its security features in Lawrence, KS over three years. It will also show that it doesn't differ from the rest of the world in the fact that it has a rapidly growing number of open, insecure access points.

## 4.2 *Demographics*

Lawrence is located in Northeast Kansas, about 35 miles west of Kansas City and about 25 miles east of Topeka, the State Capital. Lawrence has a population of approximately 80,000 and is the home of the University of Kansas which has an

annual enrollment of around 28,000 [24]. One thing that is unique about Lawrence is its high cable modem saturation. Our local cable company, Sunflower Broadband, claims it has an estimated 14,300 cable modem subscribers out of the 42,000 customers its cable service reaches [25]. According to a report by Insight Research Corporation on wireless, there is a strong correlation between wireless and broadband with the two technologies driving each other's prevalence [26]. It is also important to realize that, due to Lawrence's size, it has very few large businesses and that most of the wireless statistics are driven by home users and the university, not large corporations.

## 4.3 *Procedure*

To better understand the implications and trends of wireless networking in Lawrence, KS, a thorough driving scan or "wardrive" was performed each year over a three-year period. Since it was not feasible to drive every possible street, a sample set was chosen that aimed to be as diverse as possible in regards to income, housing type, tenant age, and zoning.

All of the scans were performed using an Orinoco 9.5db omni-directional antenna, an Orinoco 802.11b Gold PCMCIA wireless card, a Garmin GPS II Plus, and NetStumbler running on a Windows 2000 laptop as described in Chapter 3. In 2002, when the first driving scan was performed, NetStumbler was the predominant scanning package and Kismet was in its infancy. Since an active scanning method

was used for the collection of the 2002 data, it was necessary to maintain the same scanning technique in subsequent years in order to provide uniformity. The actual path driven each year is shown in Figure 4-1.

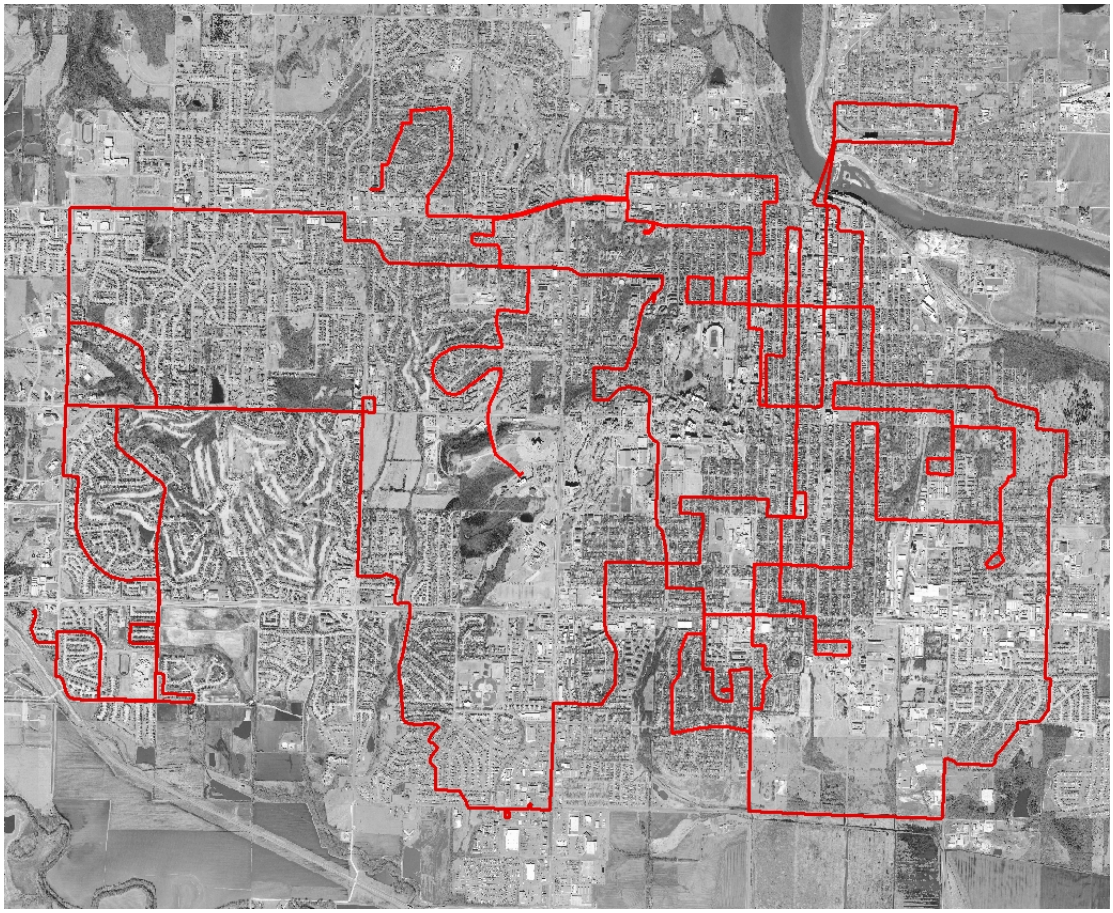

**Figure 4-1: Case Study Sample Set**

As a reminder, all of the data in this study is from "broadcast SSID" enabled access points. Using a GPS mapping tool, great care was taken to drive the exact same path

in the same month of each year. Also, the same hardware and software were used for the three years of scanning.

NetStumbler provides multiple data points for every access point based on the number of probe responses it has receives while the access point is in range. In order to estimate the approximate location of the wireless device, the data point for each network that had strongest signal-to-noise ratio was used. For example, while driving down a street you might see a weak signal from an access point and then observe the signal getting stronger as you approach the actual location of the device. At some point it will reach a maximum, and then start declining as you have passed and moved farther away. It is at this maximum point that the best estimate of the access point's true location is given. NetStumbler provides this information with its "summary" export feature, but since some of the scanning was broken up into multiple days, a method was needed to combine multiple NetStumbler data files. A couple of post-processing scripts were written that determined the maximum signal values for each unique access point and that reformatted the data so it was easier to use in Microsoft Excel (more details on these scripts can be found in Chapter 5). Once the data was combined and reformatted, it was then imported into Microsoft Excel to perform statistical analysis and graph the results.

## 4.4 *Results*

### 4.4.1 Wireless Access Point Growth

The first thing that became evident while scanning the second year was the phenomenal growth in the number of unique access points that were detected. Between 2002 and 2003, the number of "broadcast SSID" 802.11 networks in the sample set rose from 189 to 537, yielding a 184% increase. Then between 2003 and 2004, the number of access points basically tripled again growing 203%, from 537 to 1625. Figure 4-2 summarizes the growth in the number of unique access points found in the sample set over three years.

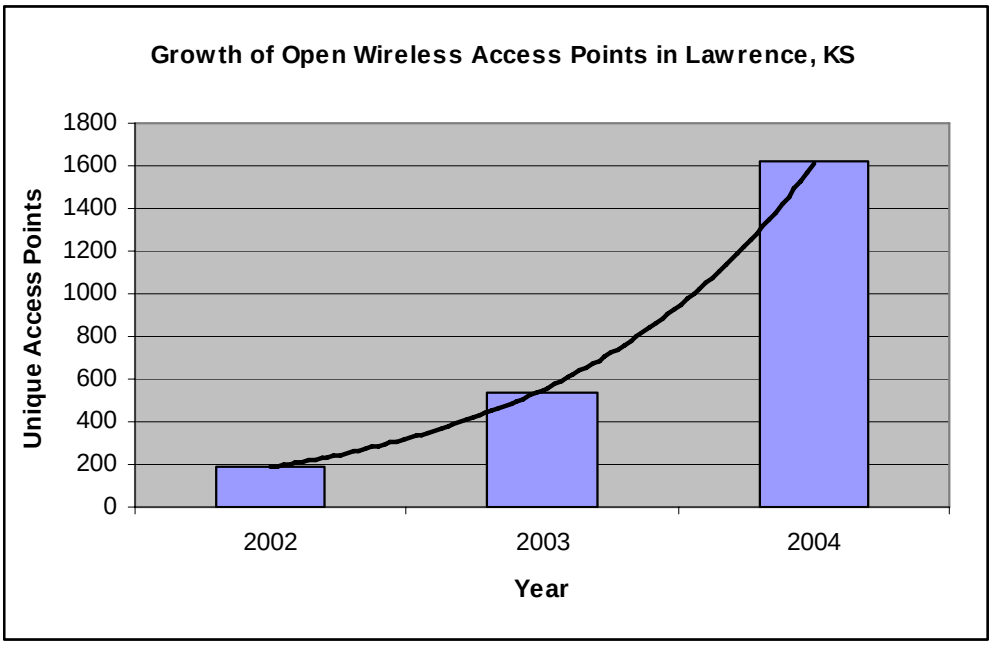


**Figure 4-2: Growth of "Broadcast SSID" Enabled Wireless Access Points in Lawrence, KS**

A January 2004 report released by In-Stat/MDR claims that 22.7 million wireless NIC and AP units were rolled out in 2003, a 214% increase from 2002's 7.2 million [27]. This is very similar to the 184% growth observed in Lawrence, KS during the same time between 2002 and 2003.

Using the visualization techniques discussed in Chapter 5, the images in Figures 4-3 through 4-5 were generated to provide another way of visualizing the growth. In these maps, the approximate location of each access point that was detected is represented with a red star.

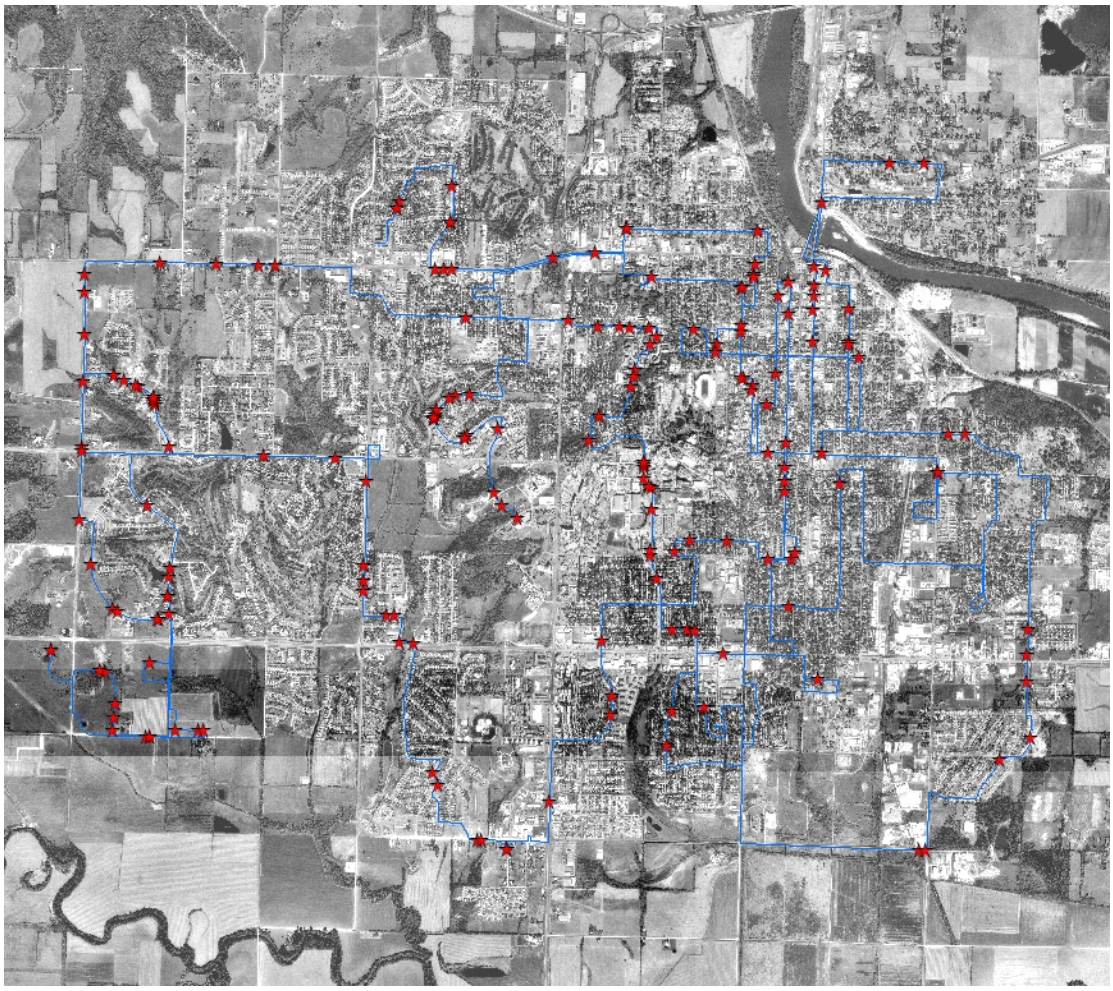

**Figure 4-3: Access Points Detected in Lawrence, KS, May 2002**

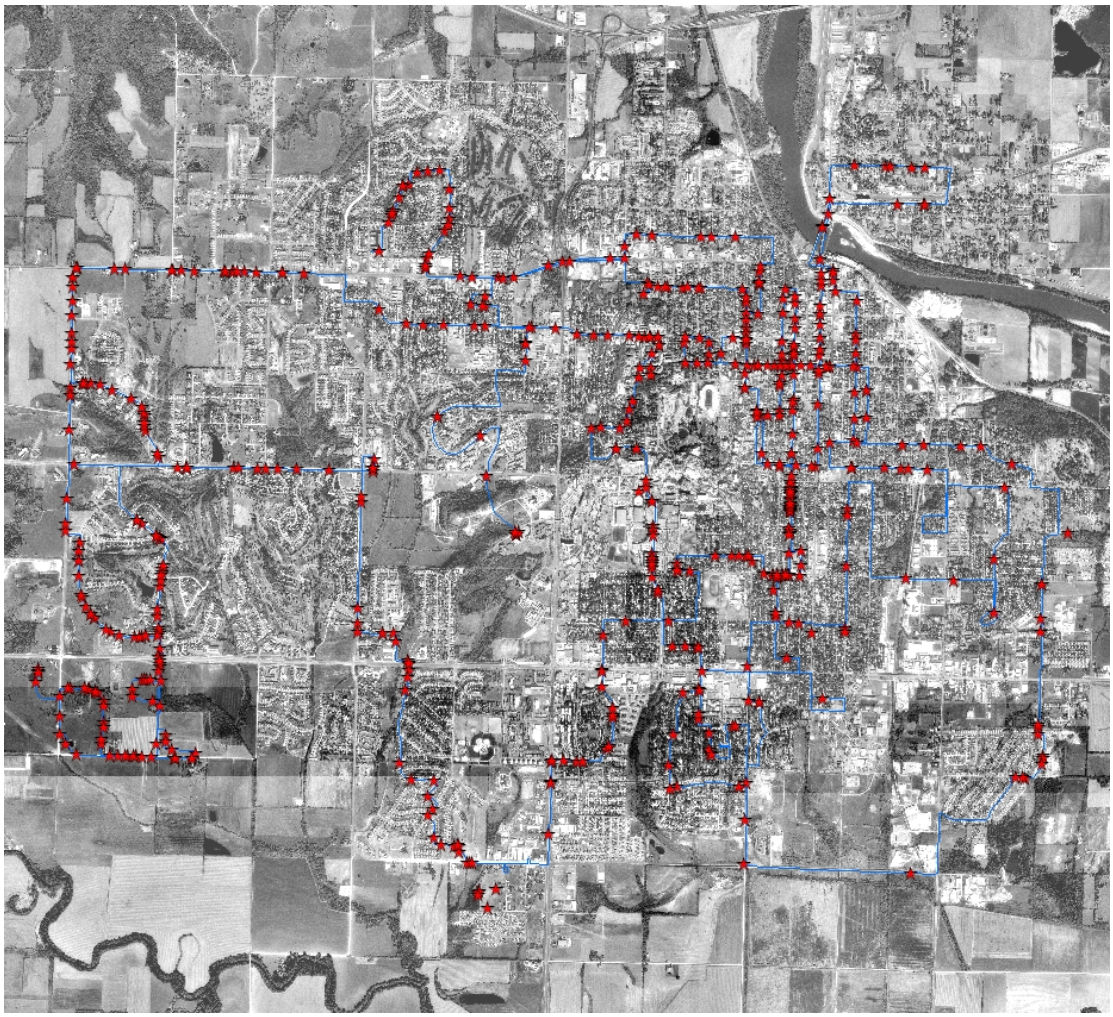

**Figure 4-4: Access Points Detected in Lawrence, KS, May 2003**

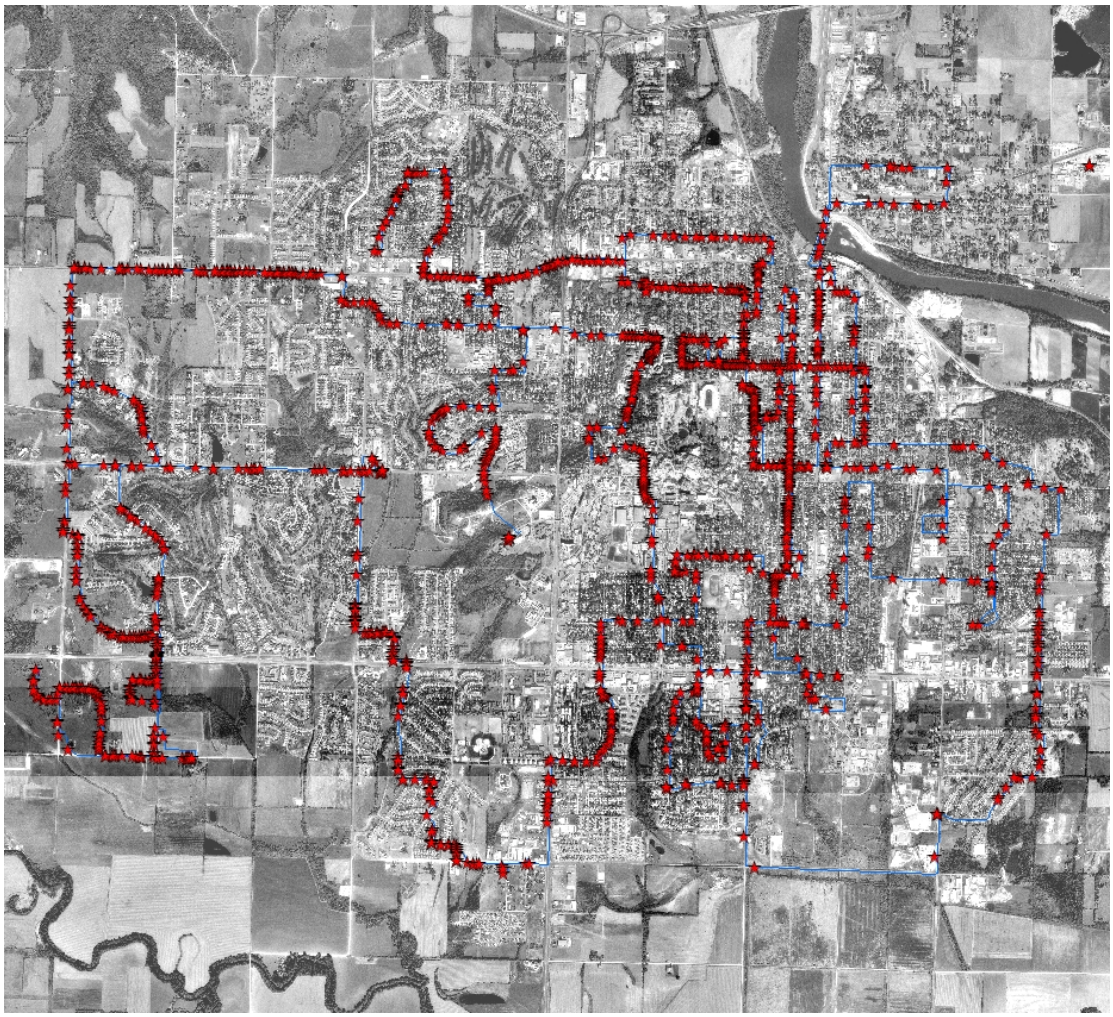

**Figure 4-5: Access Points Detected in Lawrence, KS, May 2004**

Unfortunately, all of this growth directly affects the number of access points that are possible to exploit, since most people are not practicing good wireless security. Based on observations while driving and by later analyzing the maps, it can be concluded that the highest levels of saturation are in regions that have heavy student population or high-income housing. This is a good indicator that home users, and not businesses, are responsible for most of the growth in Lawrence, KS. The

topic of who is using wireless networks and how they are distributed could be the focus of a separate study. It is safe to say that this growth will continue as more multi-computer households adopt broadband and will need a way to share their connection. Other factors such as declining prices, faster speeds, better encryption, and an influx of wireless-enabled products will also fuel this growth for many years to come.

### 4.4.2 Wireless Access Point Growth by Vendor

Since the MAC address was collected for each access point discovered, it was trivial to query it against the IEEE Organizationally Unique Identifiers (OUIs) database [28] to determine the manufacturer of the equipment. Even though it is possible to change the MAC address of a wireless device, it is a very uncommon practice. The graph in Figure 4-6, shows each vendor's market share as a percentage of the total number of access points found in the study of Lawrence, KS over a three-year period.

As you can see from Figure 4-6, Linksys has continually dominated the wireless market in Lawrence, KS (36-40%) with the exception of Orinoco[1] showing a strong percentage in 2002 (30%). Both have continually lost market share to other vendors such as Microsoft, ANI, D-Link, Netgear, and 2-Wire. In 2002, there were far fewer vendors than there are today and vendors like 2-Wire and Microsoft did not even have offerings. Orinoco's sharp decline in market share can probably be attributed to their shift away from the home market into enterprise level wireless

[1] Lucent, Orinoco, and Proxim were combined as one vendor for the purposes of this study since they are essentially the same company due to a spin-off and name change.

products. The same probably holds true with Cisco, since they have always offered enterprise grade products as well.

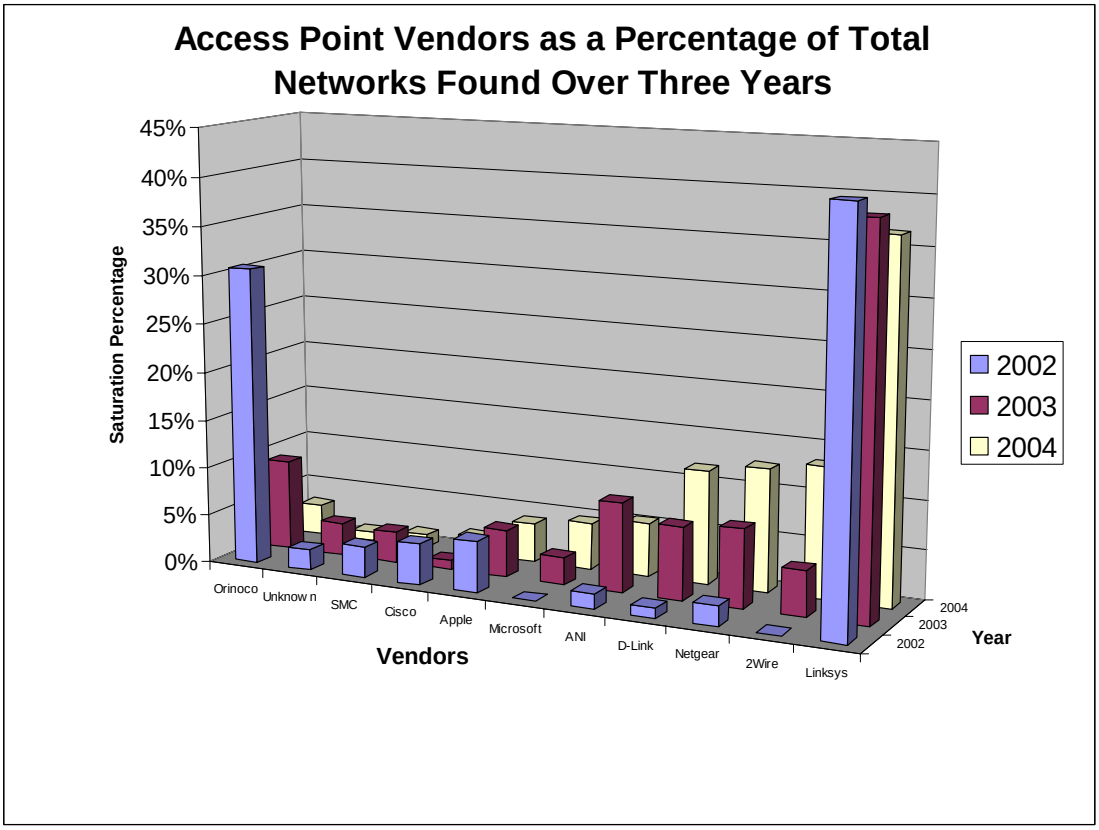


**Figure 4-6: Access Point Vendors in Lawrence, KS**

All of the vendors that have had products available in the local chain electronics stores such as Best Buy, Circuit City, and Comp USA exhibited strong growth, with the exception of Apple, SMC, and 2-Wire. 2-Wire's extremely strong growth is fueled by their exclusive contract with SBC Communications, who provides packaged wireless equipment with their ADSL service.

It is hard to predict the future, but it is safe to say that Linksys will continue to dominate the access point market in Lawrence, KS, and vendors like D-Link and Netgear will continue to gain market share. Microsoft, on the other hand, has recently announced that it will stop offering 802.11 products.

### 4.4.3 WEP Usage

The next important statistic this study looks at is the usage of WEP encryption. WEP provides encryption between wireless devices and derives its name from its ability to provide "Wired Equivalent Privacy". WEP is important to the security of wireless networks since it provides a first-line defense against unauthorized use and the interception of signals. As shown in Figure 4-7, only 25% of the "broadcast SSID" access points found in the sample set were using WEP in 2002. Since then, WEP usage has grown steadily reaching a 38% usage rate in 2004.

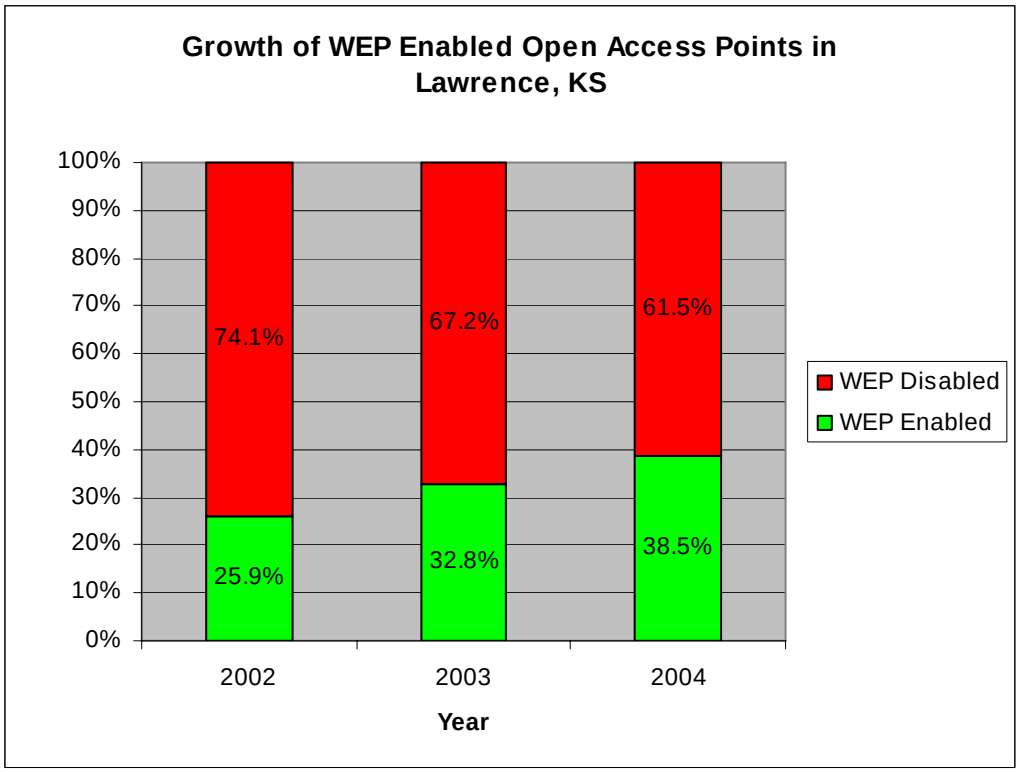


**Figure 4-7: WEP Enabled Access Points in Lawrence, KS**

Currently, Lawrence is no different from the rest of the world in its poor WEP usage rate. When compared to the statistics generated from the Worldwide Wardrive, as shown in Figure 4-8, Lawrence, KS exhibits the same rate of around 38% [5]. The Worldwide Wardrive is a collection of network scanning data submitted from volunteer "wardrivers" all over the world.

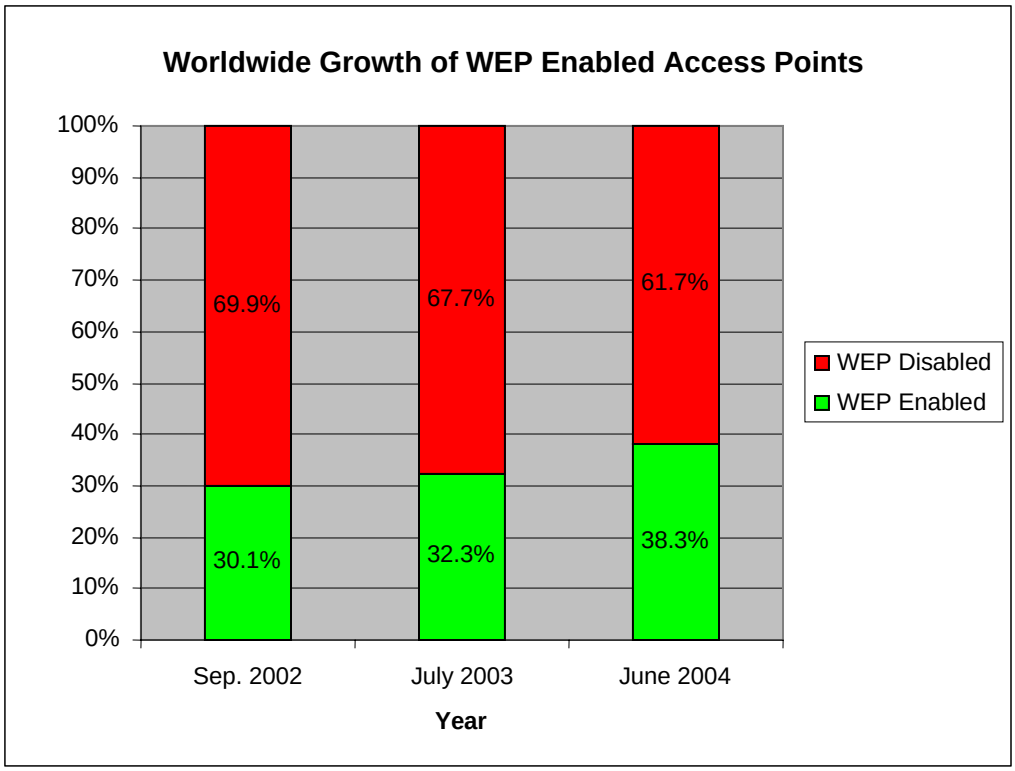


**Figure 4-8: WEP Enabled Access Points Worldwide [5]**

Even though this is a positive trend, as of May 2004, 61.5% or 999 access points in the sample set of 1625 were still wide open. It would be encouraging to see this growth continue since it definitely acts as a first-line defense in thwarting unauthorized use. Most hackers and "piggybackers" are not going to spend their time acquiring the fairly large amount of data needed to crack WEP when there is typically a wide open access point down the street. Another issue that makes WEP harder to crack, is the fact that most wireless networks sit idle, making it very difficult to collect the fairly large amount of traffic required for analysis.

A big factor that contributes to low WEP usage rates is the fact that wireless access points ship with WEP disabled. This is inherent in its design since a unique key must be generated by the user in order to encrypt the wireless traffic. Once an access point is WEP enabled, another layer of complexity is added by having to explicitly enter the WEP key in the client configuration. When intermixing vendors, a user might have to enter the WEP key in HEX on one vendor's device and ASCII on another. Some vendors even generate a WEP key based on a user-specified password. This leads to confusion since it is common for users to accidentally configure their clients with the password instead of the actual WEP key that is generated by the password. Personally, I have heard many accounts of people trying to enable WEP and giving up after having a wide range of problems. Hopefully, there will be better interoperability between the vendors when the newer 802.11i (WPA2) encryption standard takes hold.

It is difficult to understand what is driving the increased WEP usage in Lawrence, KS, but I suspect that it is a combination of a better public understanding of wireless security and better instructions offered by vendors about the importance of enabling WEP. Wireless users are realizing they can easily connect to other networks and are therefore starting to wonder what prevents people from connecting to their own network. WEP usage should continue to increase as the number of wireless networks increase and the public becomes more informed of the benefits encryption offers.

### 4.4.4 WEP Usage based on Access Point Vendor

The next important question to answer was whether certain vendors had higher WEP usage rates over others. As you can see from Figure 4-9 below, vendors such as SMC, D-Link, Linksys, and Netgear have low WEP usage rates. This can probably be attributed to the fact that these are the models typically used by home users who are less concerned and less informed about wireless security.

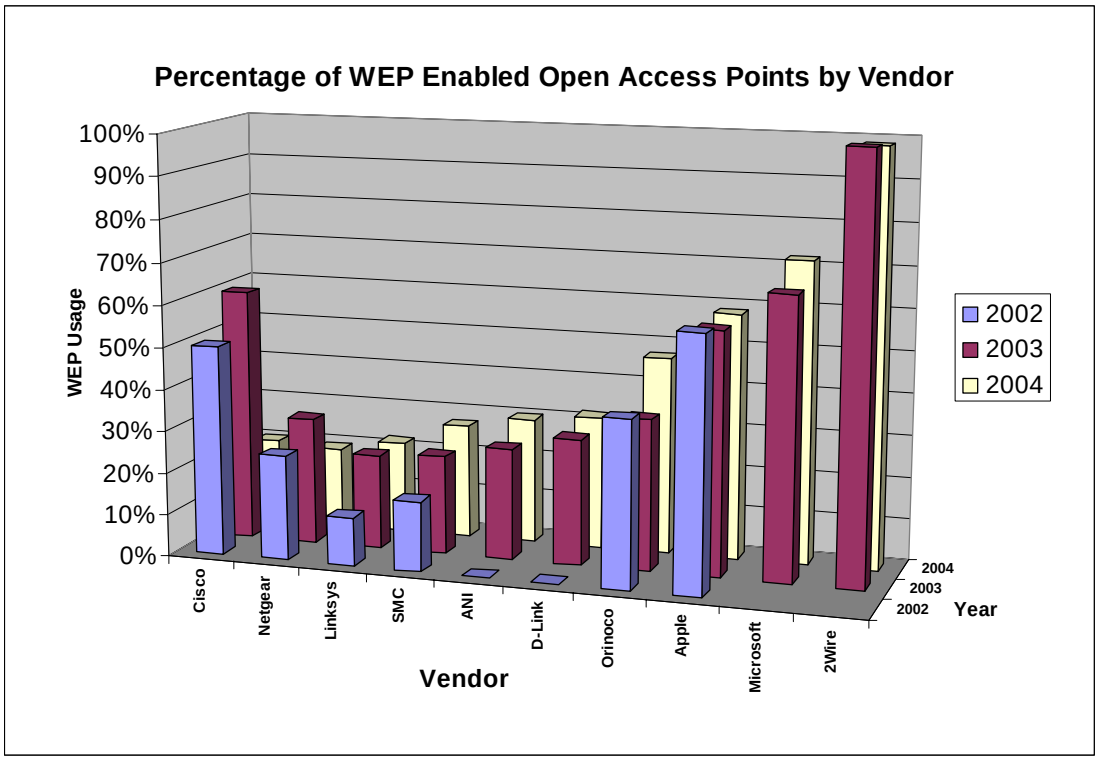


**Figure 4-9: WEP Enabled Access Points by Vendor**

Since Cisco and Orinoco access points are aimed at the enterprise market, their higher WEP usage rates can probably be attributed to better care taken by the administrators.

2-Wire's 98% WEP usage rate is most likely due to the fact that their equipment is professionally installed and configured by SBC as part of a package deal with its DSL service.

Microsoft and Apple have double the rates of WEP usage compared to the rest of the other electronics chain-store competition, which is probably due to better instructions and configuration tools provided by the manufacturer. Over the years, I have seen various vendors' instructions, and there is typically little emphasis placed on the importance and configuration of WEP. In the case of my recently purchased Linksys WRT54G wireless router, the only instructions for enabling WEP were found in an appendix at the end of the manual, making it seem less significant.

Since WEP can be difficult to configure, one might conclude that vendors are purposely downplaying this feature to save on technical support expenditures. This most likely translates to less technical support calls the vendors must field since it is common for the average user to have problems configuring WEP. Unless vendors provide better instructions and stress the importance of WEP, this trend will probably continue to increase at the same rate.

### 4.4.5 Default SSID

All access point manufacturers that I have encountered ship their access points with a default Service Set Identifier (SSID). The SSID is the network name clients use when associating with a network. Default SSID's, or SSID's that have never been changed from the factory default setting, can give intruders a clue that little attention was paid in configuring the access point. When an attacker sees a default SSID they

know it is very likely that the access point has old firmware, has the default password, has no MAC filtering, is broadcasting its SSID, and is not using WEP. Some of the AP's found in this study provide descriptive information in their user configured SSID such as last names, street addresses, and business or organization names. This could give potential intruders information on where the access point is located, the name of the business, or who is operating it.

As you can see in Figure 4-10, as of May 2004, 57.8% of the access points are using a default SSID, up from 50.9% in 2002.

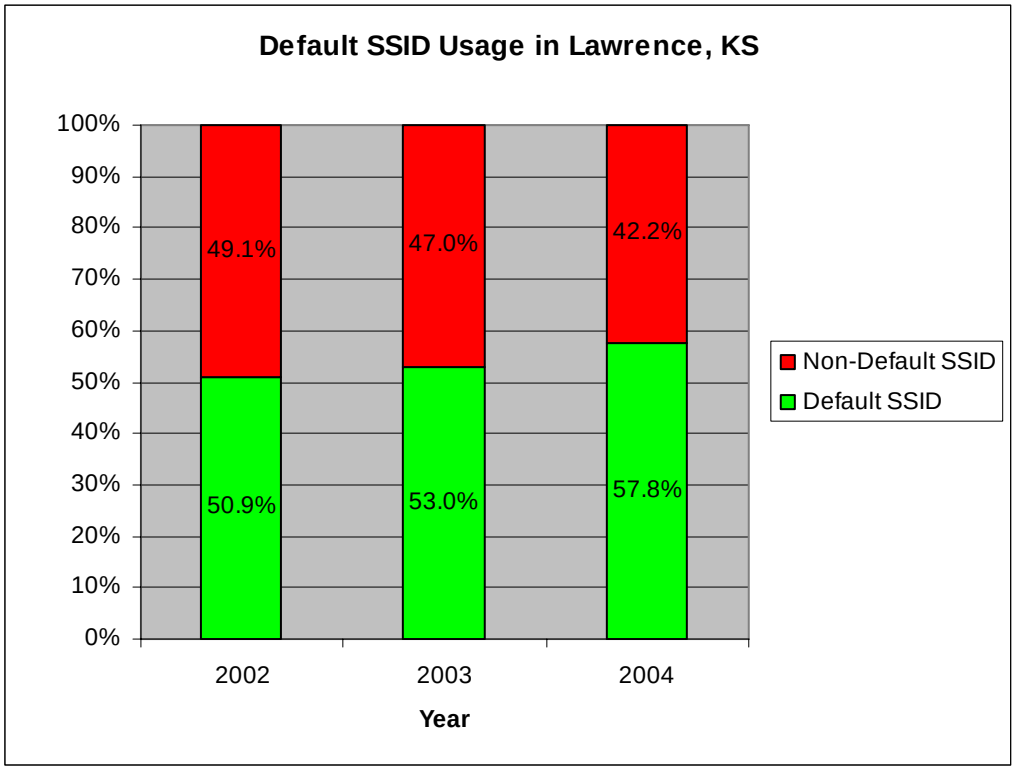


**Figure 4-10: Default SSID Usage in Lawrence, KS**

Figure 4-11 shows the table of default SSID's for each manufacturer encountered in the study. The default SSID's that were not included in the now outdated Wireless LAN Security FAQ [29] were easily derived by looking for trends in the data and verifying that they are known defaults via web searches.

| **Manufacturer** | **Default SSID** |
|---|---|
| Cisco | Tsunami |
| 3com | 101 |
| Orinoco | Orinoco |
| Compaq | Compaq |
| Intel | Intel |
| Linksys | Linksys |
| Netgear | NETGEAR, Wireless |
| Microsoft | MSHOME |
| D-Link | Default |
| Apple | Apple Network XXXXXX |
| SMC | default, WLAN |
| ANI | Default |
| 2-Wire | 2WIREXXX |

**Figure 4-11: Manufacturer's Default SSID's [29]**

When compared to the default SSID statistics from the Worldwide Wardrive as shown in Figure 4-12, Lawrence shows a much higher percentage of default SSID's.

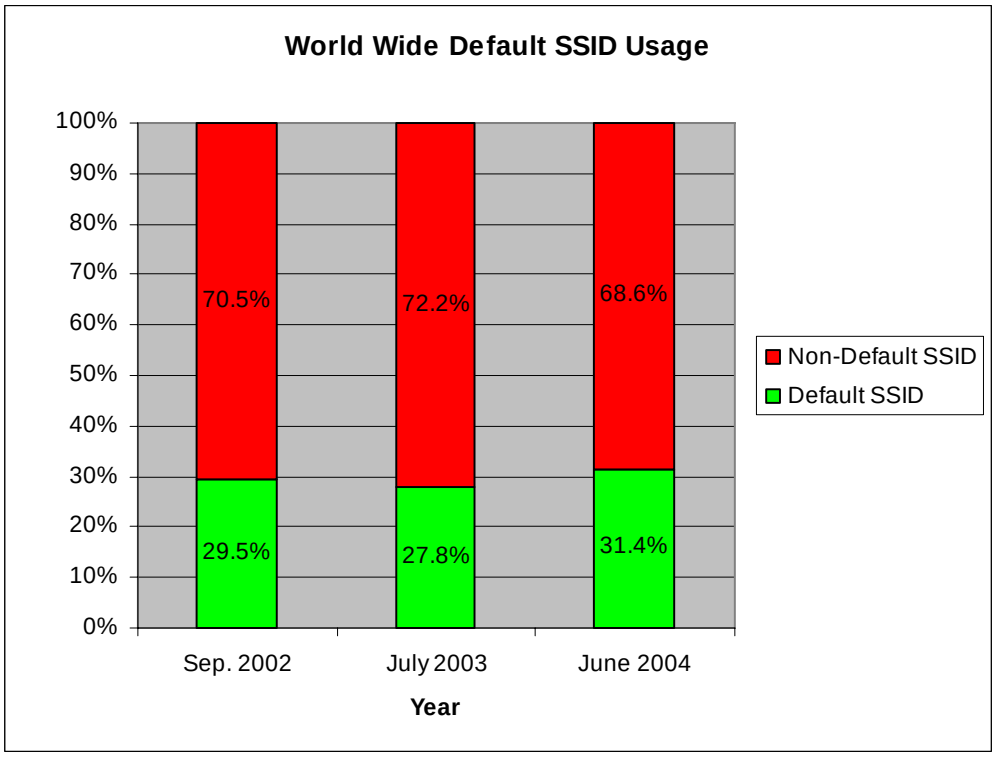


**Figure 4-12: Default SSID Usage Worldwide [5]**

This discrepancy is due to the fact that the list of default SSID's that the WWWD uses is missing several of the more prevalent default SSID's used by manufacturers such as Orinoco, Netgear, and Microsoft. When using their list of default SSID's, the default SSID percentages in Lawrence are similar.

### 4.4.6 Channel Usage

The 802.11b standard defines a total of 14 frequency channels which use about 5 MHz of spectrum each [30]. In the United States, the FCC only allows for the use of channels 1 through 11 since that is all that will fit in the ISM S-band (2.4GHz – 2.5GHz). Since an 802.11b network requires about 30 MHz of bandwidth, the

channel assignment of the wireless equipment specifies the center frequency to use. For instance, if a wireless access point is configured to use channel 6, then it is actually broadcasting on channels 4 through 8 with channel 6 being the center frequency. This means that there are really only three distinct or non-overlapping channels in the United States: channels 1, 6, and 11. Figure 4-13 shows the channel utilization of the surveyed access points in Lawrence, KS.

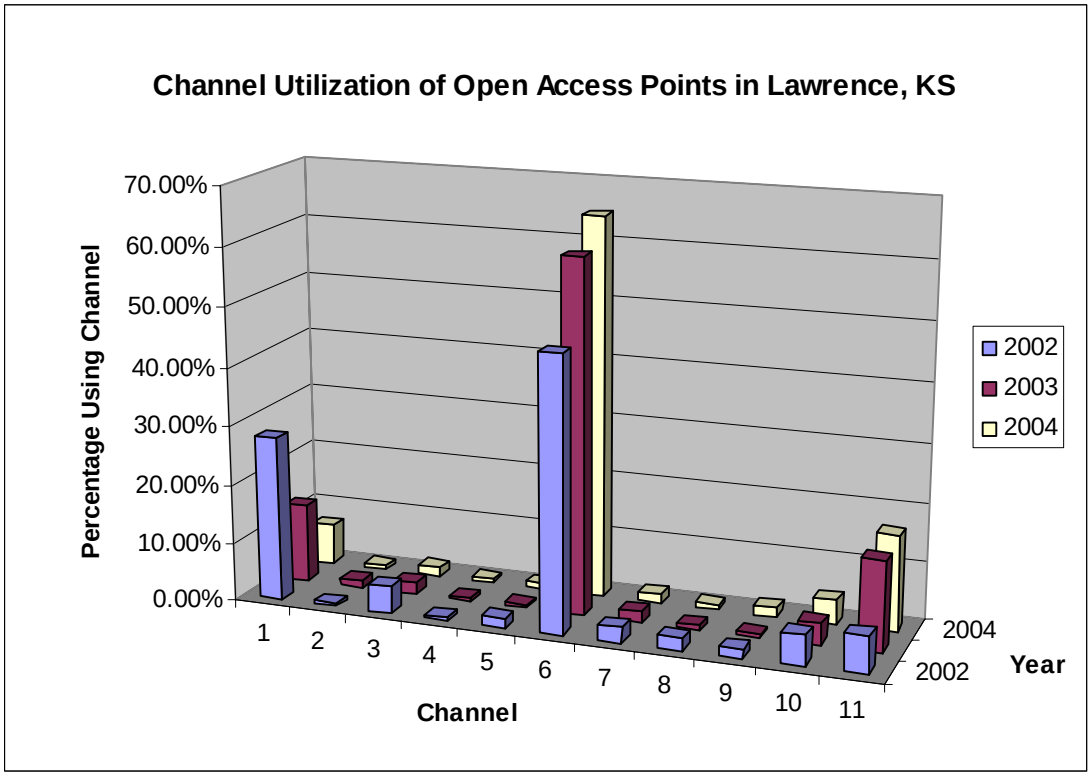


**Figure 4-13: Channel Utilization of Access Points in Lawrence, KS**

From Figure 4-13, you can see that 68% of the AP's in the sample set are using channel 6 and that its usage has increased since 2002. This can be attributed to the

fact that most people do not change the channel on their access point and that channel 6 is a very common default setting used by manufacturers since it is in the center of the ISM S-band. Also, there are a fair amount of AP's using the other non-overlapping channels 1 and 11. It is unknown why the use of channel 1 has diminished while channel 11's usage rate has increased. Figure 4-14 shows the channel usage based on vendor in 2004.

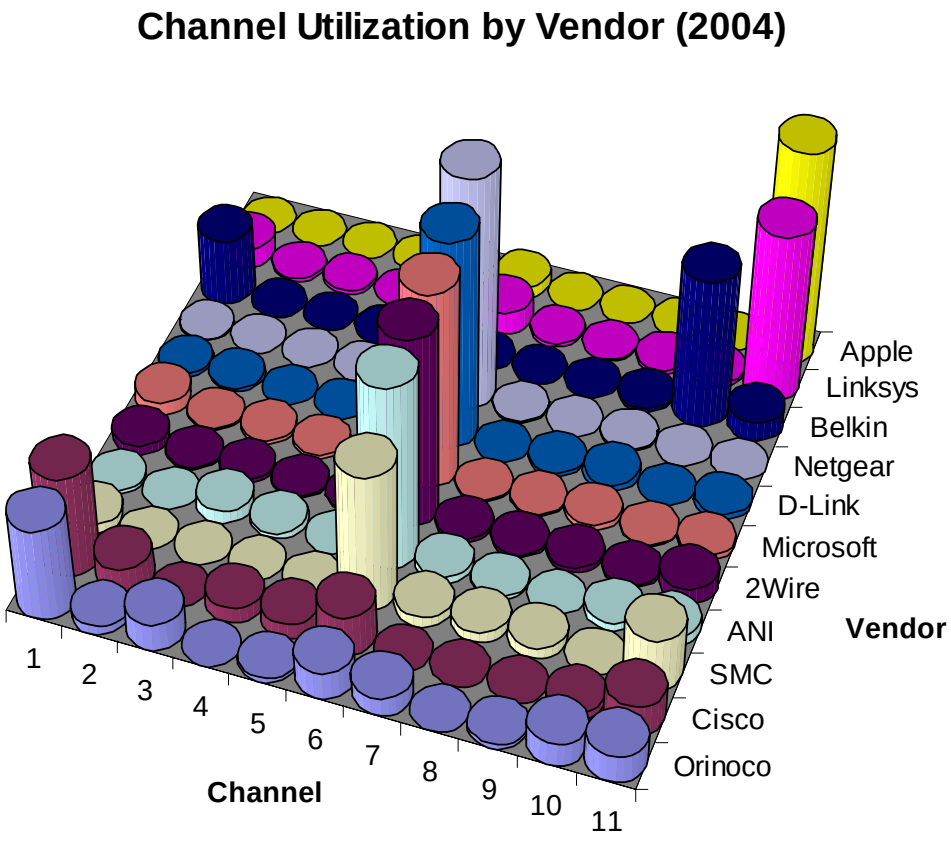


**Figure 4-14: Channel Utilization by Vendor in 2004**

This graph clearly shows that vendors are shipping their access point products using a default channel and that users are not changing this setting. With 68% of the AP's using channel 6, interference among AP's is a big concern.

802.11 is a shared medium collision detect protocol, similar to an old style un-switched or hub-based Ethernet network. A client or station will not transmit until the medium is clear and no other station is transmitting. With other access points broadcasting on the same channel, an access point might have to wait in order to transmit. Non 802.11 sources of interference might not wait for the medium to clear before they send, resulting in collisions and re-transmissions of packets. Besides being subject to interference from other wireless equipment, sources such as HomeRF, Bluetooth, 2.4GHz cordless phones, and microwaves can cause significant performance degradation. Most microwaves emit signals that fall within the same 2.4GHz frequency band that 802.11b access points utilize.

It is my hypothesis that some wireless users are suffering from interference related performance degradation, but are unaware of the problem and not taking action. One reason that some people might change the channel of their wireless equipment is audile interference or what has been described as "weird clicking sounds" in their 2.4 GHz cordless phones. Some access points have an auto-channel setting which allow them to automatically locate the channel with the least noise for use in transmitting. Hopefully, this feature will find its way into more consumer grade access points. The topic of interference and its effect on wireless networks could easily be the topic of another study.

## 4.5 *Case Study Conclusion*

"Wardriving" provides a unique and powerful method for the collection of wireless network statistics. Through the use of this technique, a clear picture is presented showing the sheer growth of wireless infrastructure, and the use of 802.11's security features in Lawrence, KS. When compared to statistics offered by In-Stat/MDR and to the Worldwide Wardrive, Lawrence, KS exhibits almost identical trends. This study shows that due to the wide proliferation of wireless technology, a medium-sized city such as Lawrence, KS can provide localized and detailed statistics that are on par with the rest of the world.

The data collected from the sample set shows that the number of "broadcast SSID" access points has tripled every year since 2002, and will likely continue to grow at the same rate due to the proliferation of broadband and wireless enabled products. The observed growth is similar to the worldwide wireless sales projections between 2002 and 2003 offered by In-Stat MDR.

By looking at the MAC addresses, it was clear that Linksys dominates the access point market in Lawrence, with other vendors that have products in the local electronic chain stores slowly gaining ground. According to the data collected over three years, certain vendors in a group who target their products at the home market have shown higher WEP usage rates and less default SSID's than other vendors in the same group. By looking at these statistics, it becomes clear that vendors with large market shares might directly impact the actual real-world use of wireless security

features due to the varying quality of instructions and tools provided for the configuration of their equipment.

WEP usage has increased in Lawrence, KS from 25.9% to 38.5% over the last three years and will most likely continue increasing as more people learn more about the security risks associated with wireless. There is definite room for improvement with 999 of the 1625 AP's found in 2004 not using any encryption. As far as the use of default SSID's, Lawrence shows a growing trend with 57.8% of the access points using a default SSID. Although less of a concern than not using WEP, it shows that, in general, little attention is paid to the configuration of access points. When compared to statistics obtained from the World Wide Wardrive (WWWD), Lawrence was nearly identical in its WEP usage rate, but much higher in its use of default SSID's. This discrepancy was due to the fact that the WWWD is using an incomplete list of default SSID's when determining their statistics, attributing to a much lower number. Another interesting statistic found is that 72% of the networks are utilizing channel 6, up 22% from 2002. It is unknown if this is causing performance degradation due to interference and would wake an excellent topic for a future study.

This study shows that a lot of useful and informative wireless statistics can be obtained from scanning a sample set of roads every year by means of "wardriving". It also shows that there is a major wireless security epidemic and that something needs to be done to protect consumers from "piggybacking" and eavesdropping. These statistics hold merit, but are not necessarily fit for public consumption. Public

awareness needs to be raised through a more direct and meaningful means of conveying the issues at hand, visualization.

# Chapter 5 - Visualizing Wireless Networks

## 5.1 *Introduction to Wireless Visualization*

Chapter 4 gave a detailed statistical analysis of the wireless infrastructure in Lawrence, KS over the last three years. This chapter will take the statistical analysis a step further, providing an advanced method for the visualization of wireless network data using a Geographic Information System or what is commonly referred to as a GIS. With this method, extremely detailed maps can be generated using aerial photography and interpolation to show signal propagation. These visualizations are aimed at the public to promote awareness of the security issues surrounding wireless networks, providing images that the average wireless user can understand.

Graphics are usually the simplest and most powerful means for communicating statistical results [31]. Statistical analysis provides a simple way to interpret wireless data, but fails to take advantage of the spatial nature of the data typically collected when "wardriving". Spatial data allows for the creation of powerful, real-world representations based on location. Since wireless networks propagate through free space, traditional methods for network mapping such as a simple "wire diagram" are no longer applicable. A direct means, based on observation, is required to show the propagation of a wireless signal due to the many variables that affect its range. It is this issue of propagation that drives most of wireless' security concerns, and in order to increase public understanding, it is necessary to show examples of how signals actually propagate. Most people are

unaware how far their signals travel and underestimate the security risks when their network gear works so well straight out of the box. With this technique, meaningful images of signal propagation can be shown by creating detailed images of wireless networks in typical use scenarios.

## 5.2 *Previous Wireless Visualization Techniques*

At the time our visualization techniques were developed (late 2001), there was little work being done in trying to visualize the spatial data acquired from wireless network scans. The work that was being done revolved around mapping the approximate location of access points on a simple street map. This did a decent job in conveying the number of access points found and their approximate location, but did not show the networks' signal ranges. A lot of this early work was usually done by "freenet" organizations and hobbyists who wanted to show open access points that could be "piggybacked" for public use. Figure 5-1 shows an example map created by KC Wireless, a wireless hobby group based in Kansas City, KS. This map shows the approximate location of several access points in Kansas City denoted by red flags.

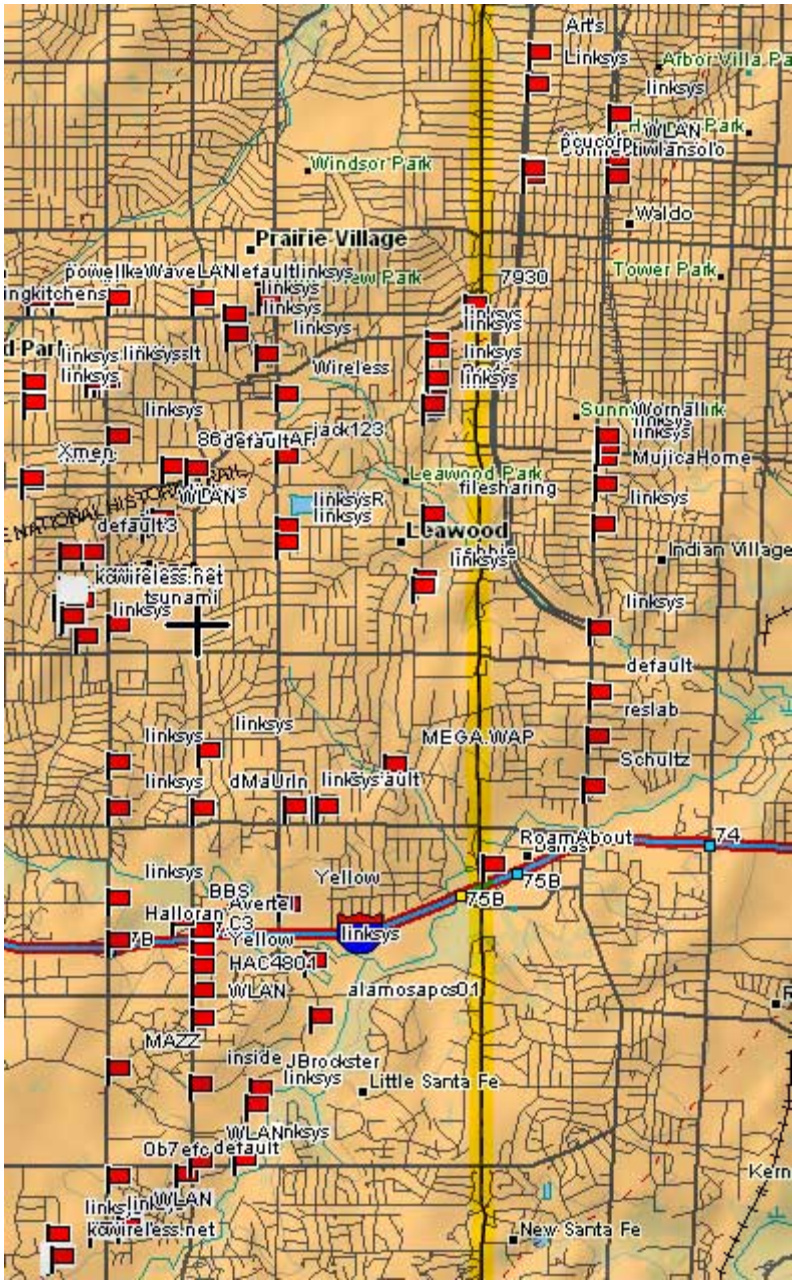


**Figure 5-1: Map of Several AP's in the Kansas City Area [32]**

The map conveys the SSID's and approximate locations of a large number of access points, but does not show the signal ranges or WEP status of each network.

The example in Figure 5-2, takes it a step further by color coding the approximate location of several AP's by their WEP status. This map was generated by Frank Keeney of Pasadena Networks from data collected while driving from Pasadena to San Francisco, California. The green dots denote WEP encrypted networks while red dots denote un-encrypted networks.

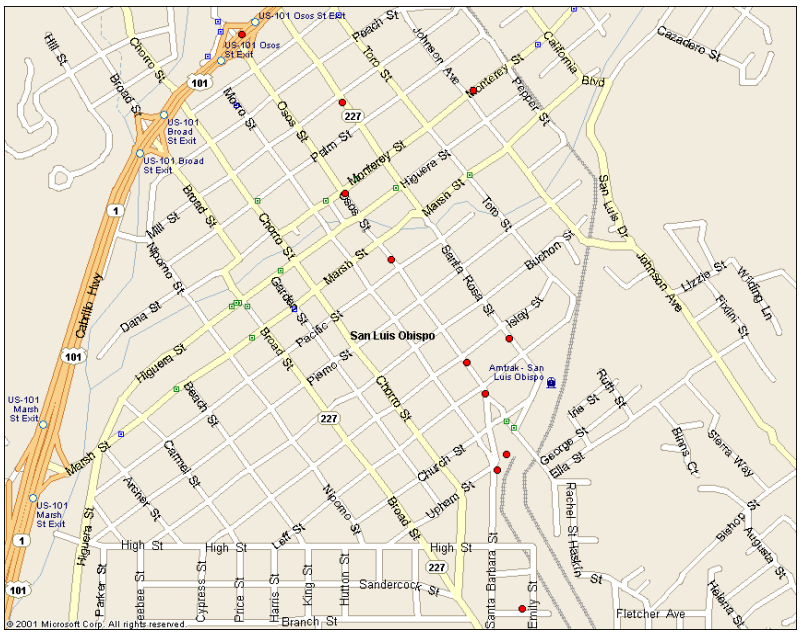


**Figure 5-2: Microsoft MapPoint Map of Several AP's in Berkeley, CA [33]**

Popular tools for creating these visualizations were off-the-shelf mapping and atlas applications such as Microsoft's MapPoint, DeLorme's Streets and Trips, and Autoroute 2001. Unfortunately, these tools offer little flexibility, and were not designed to display custom and complicated external data. All of these programs

severely limit what can be done with the data once it is imported, requiring external manipulation of the data every time a change is desired.

The Consume Project, another “freenet” organization based in the UK, created a dynamic, web-based tool to show the approximate location of their network access points using GPS coordinates to denote position. As you can see in Figure 5-3, they also include an approximate signal range by drawing a fixed-size circle around each radio.

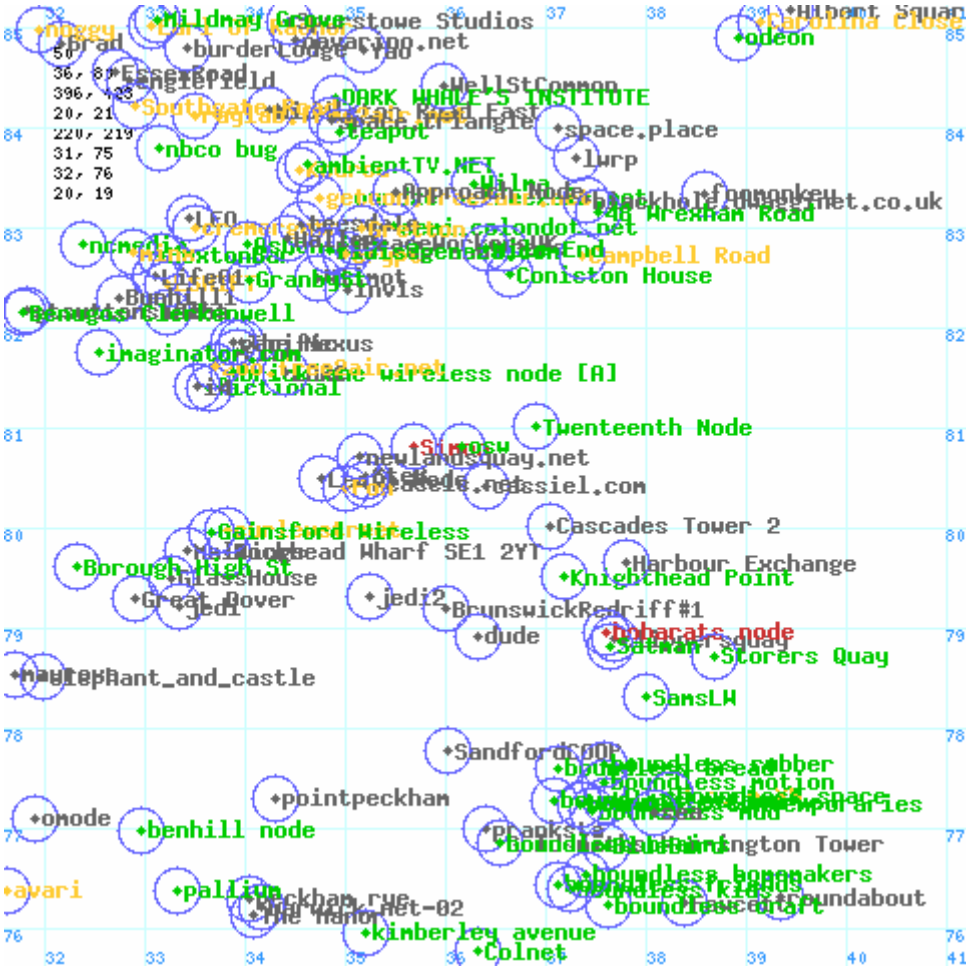


**Figure 5-3: Consume's Dynamic Access Point Mapping System [34]**

Given the fact that the only point of reference offered by the map are longitude and latitude coordinates, the theoretical range shown for each access point has little meaning to the average wireless user. Also, a fixed signal range is never representative of reality due to the many factors that affect signal propagation.

My goal was to create visualizations that better conveyed the security implications and signal propagation of wireless networks. I felt it was important to show real-world examples such as a typical home network or several access points in an office building. It was clear that the maps shown in the examples above fell short in getting the public's attention and meant little to the average tech-illiterate user. My search for a technique to better convey these ideas was unsuccessful. Then, after showing the data to my colleague Matt Dunbar, a technical geographer, he suggested putting it into a Geographic Information System or what's commonly referred to as a GIS. Working together, the collected NetStumbler data was successfully imported into a GIS, and a whole new world of visualization possibilities became evident.

## 5.3 *Wireless Network Visualization in a GIS*

GIS analysis in its simplest form is a tool for looking at patterns in spatial data and relationships between those features [35]. A GIS allows you to combine spatial data layers, such as points in the form of longitude/latitude pairs, areas in the form of polygons, and raster imagery and geo-reference them to a common coordinate

system. This allows for the creation of layers that are geographically aligned such as multiple wireless scans, background imagery, and graphically interpreted layers such as signal fields that can be generated inside the GIS. Another important feature of a GIS is that all of the attributes related to each data point are available inside the software. In our case, this ended up being all of the attributes NetStumbler provided such as the channel, WEP Status, SSID, MAC address, and signal strength. With this functionality, data can be filtered or queried inside the program to quickly generate new views based on any attribute.

### 5.3.1 Early GIS Visualization Efforts

At first, an attempt was made to mimic the maps that were already available, creating simple but effective views of wireless networks. ESRI's ArcGIS software suite was used for all of the analysis since it was readily available and highly utilized by the geography department at the University of Kansas. ArcGIS is the most popular GIS package in use today and has a 72% market share in the educational community [36].

In a GIS, any geo-referenced data source can be used for the background imagery. By using aerial photography obtained from the city of Lawrence, KS instead of street maps, visualizations were created that were more meaningful to the average person. Now, instead of looking at simple lines that represented streets, a wealth of landmarks, including users' own rooftops were visible. This created maps that caught people's attention by bringing a better sense of reality to the visualization.

An early visualization effort, as shown in Figure 5-4, displays a large collection of NetStumbler data points collected while "wardriving" in Lawrence, KS.

In this visualization, the point data associated with each unique access point is denoted by a different color. The dark green and purple colored networks that are represented by a large number of data points are high power, multi-antenna commercial systems that are mounted on towers. Although this visualization technique was a step in the right direction, there was still no way of generating an actual field based on the point data.

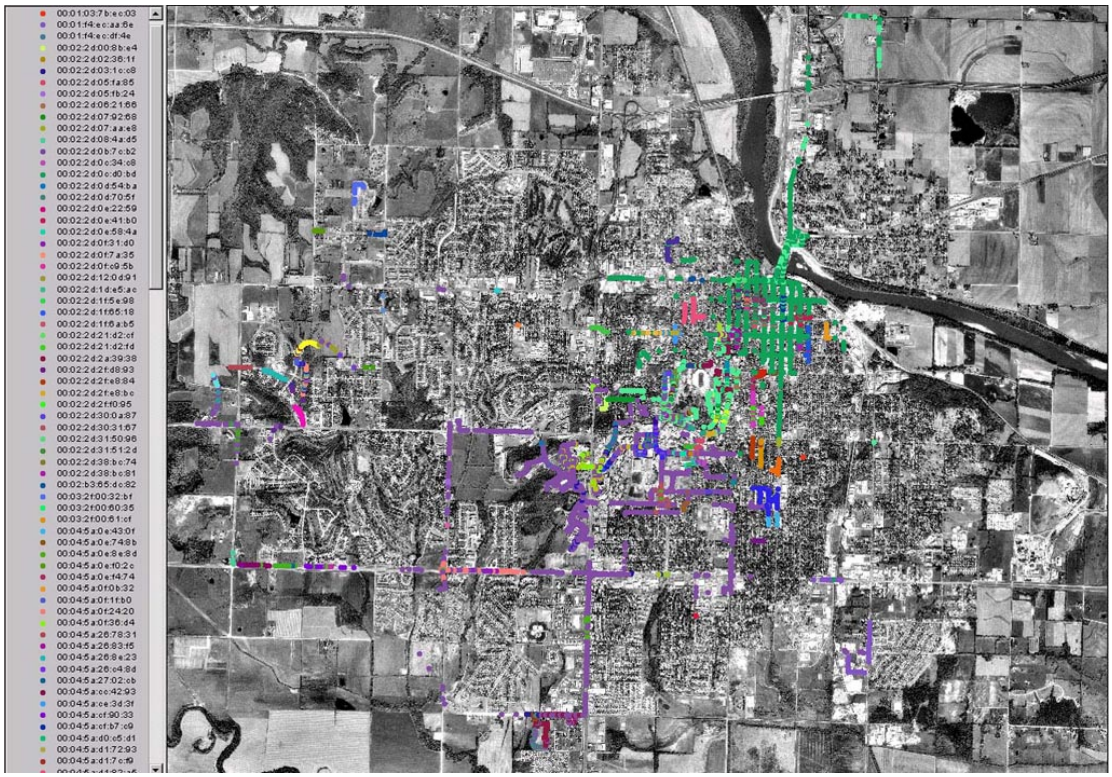

**Figure 5-4: Early Mapping Effort of Several AP's in Lawrence, KS**

### 5.3.2 GIS with Signal Interpolation

The next problem to solve was how to fill in the data points based on the signal to noise ratio and generate a signal field by using interpolation. Interpolation is a procedure used to predict the values of an attribute at locations that lack sampled points [37]. The ArcGIS Spatial Analyst plug-in, which provides a toolset for analyzing and modeling spatial data, provides several interpolation tools. After experimenting with the various interpolation methods in the Spatial Analyst plug-in, it was determined that the Inverse Distance Weighted (IDW) interpolation method proved best since the set of data points were dense enough to convey the variation. IDW also seemed to provide a smoother, more realistic signal gradient than the other techniques such as “Kriging” and “Spline”. IDW determines interpolated estimates based on values at nearby locations that are weighted only by the distance of the interpolation location [38]. The greater the distance, the less influence the data points have on the output value [37].

To verify the idea of using ArcGIS and the Inverse Distance Weighted algorithm to provide a signal coverage field, a simple test was performed. A Linux laptop with an 802.11b Orinoco Gold wireless card running in Ad-Hoc mode was placed in the center of a large flat field. Another laptop running NetStumbler was then walked around the Linux laptop in a spiral fashion collecting point data. Our hypothesis was that fairly uniform signal degradation would be observed in all directions as the roaming laptop got farther away from the stationary laptop. Since

the Orinoco access points at our research center use the same wireless cards, it was felt this would be an excellent representation of an access point.

Figure 5-5 shows the point data obtained from our walk around the stationary laptop which is denoted with a white cross. In order to show where the signal field stops, IDW and the other interpolation techniques included with the ArcGIS Spatial Analyst require data points that have a null signal value. Without these null values providing a barrier, the interpolation would be projected to infinity in all directions.

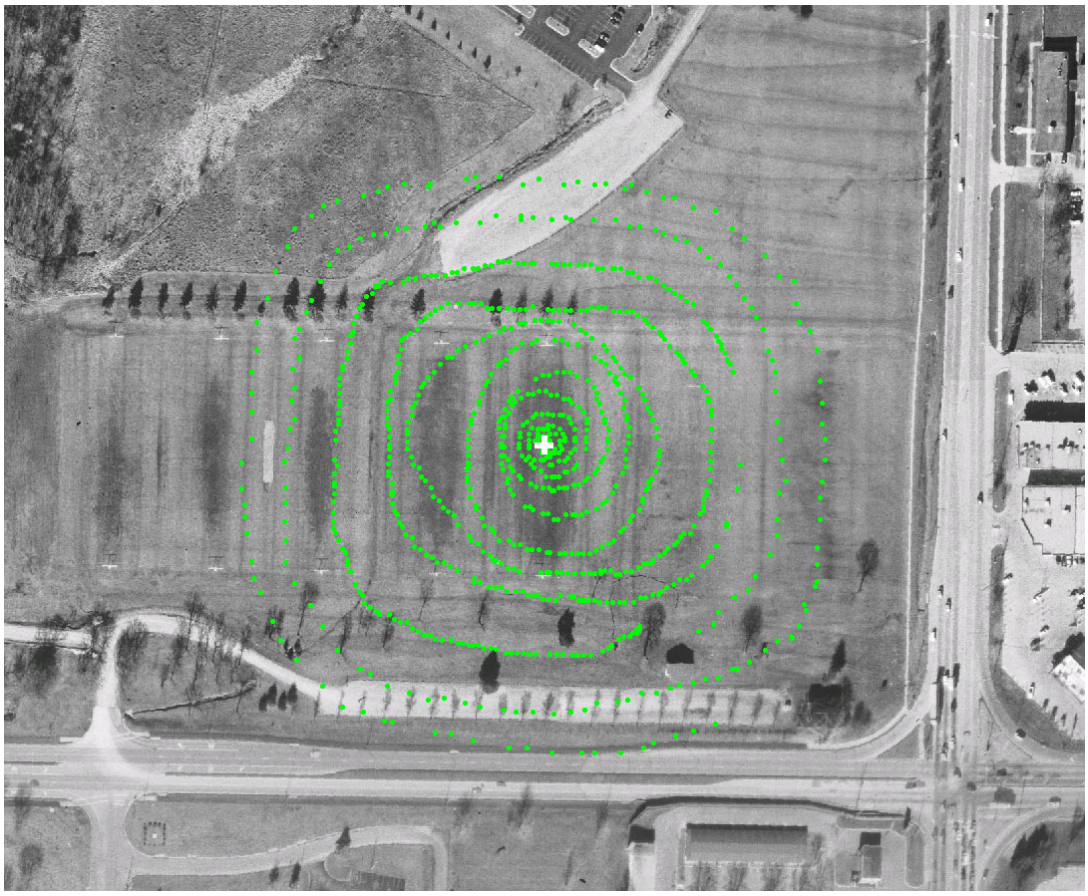

**Figure 5-5: Field Test: Point Data**

Unfortunately, NetStumbler and Kismet do not provide the functionality of being able to log data unless it has a non-null signal value associated with it. This required us to manually bound the NetStumbler data collected with a series of data points that had a signal-to-noise ratio of zero. For the purposes of this example, a simple circle of data points with null SNR values was drawn directly outside the NetStumbler data. The interpolation was then performed inside ArcGIS using IDW and color coded based on the signal-to-noise ratio. Using the visible color spectrum, the data regions with the highest SNR ratio were colored purple with the other regions shifting toward red as the SNR levels declined. The completed interpolation in Figure 5-6 shows a fairly uniform and slowly weakening network signal propagating in all directions, with a slight bias to the north and south.

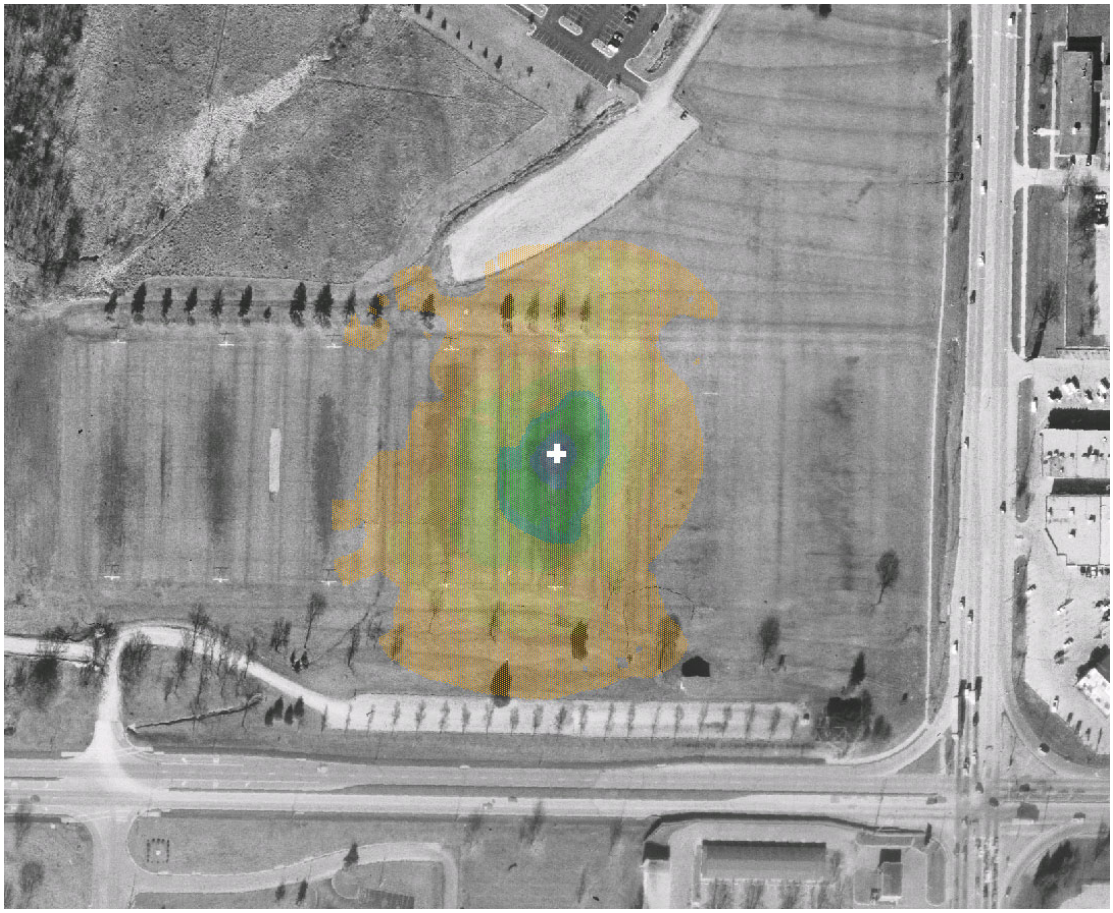

**Figure 5-6: Field Test: Completed Interpolation**

Due to the placement of the stationary laptop, the horizontal polarization plane of the PCMCIA card was measured in this test. The interpolated field observed is similar to the azimuth horizontal component of a generic PCMCIA card as shown in Figure 5-7.

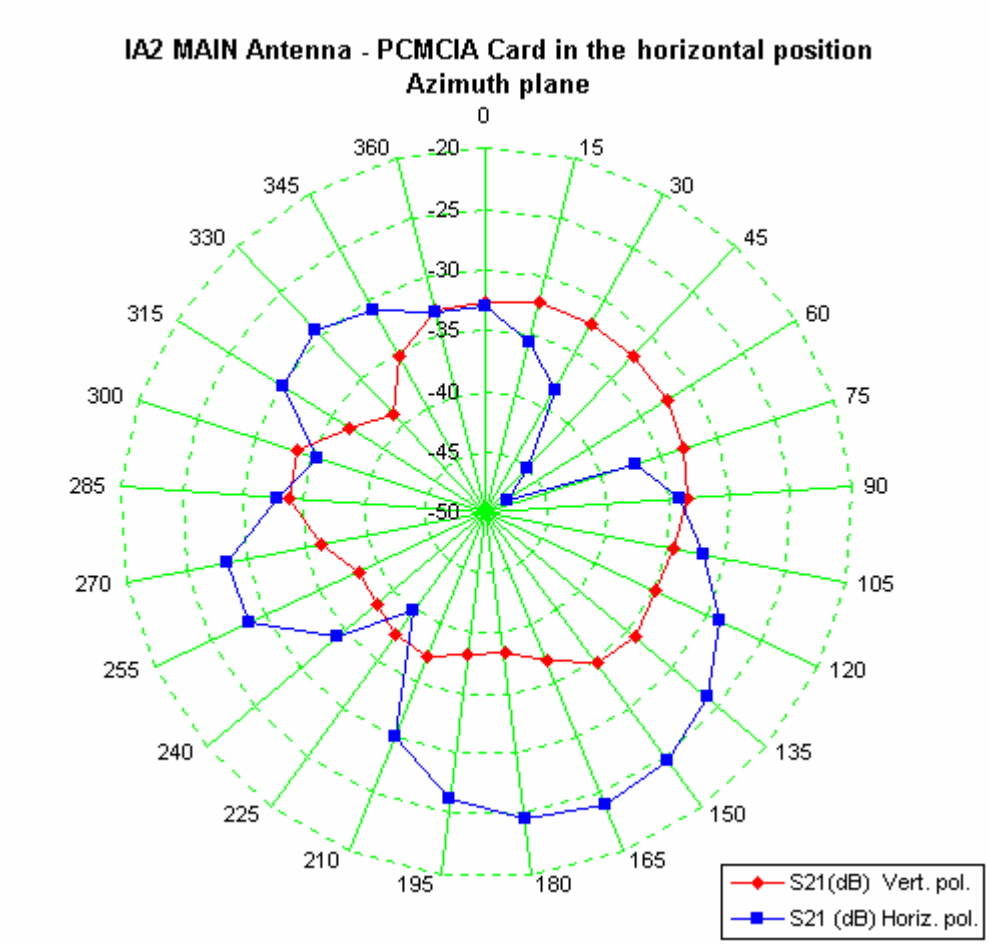


**Figure 5-7: Sensitivity Measurement of a Typical PCMCIA Wireless Card [39]**

This acts as good verification of the results since most PCMCIA wireless cards use a similar internal dipole antenna. Overall, we were extremely pleased with the results this test provided and are confident that IDW interpolation provides a realistic method for showing the propagation of wireless signals.

## 5.4 *Detailed Procedure*

The following section details our technique for visualizing and interpolating wireless data in ArcGIS. The example presented in this section shows how to generate a signal strength gradient from a single access point located in a house using the Inverse Distance Weighted (IDW) algorithm. Using the "wardriving" setup described in Chapter 3, the data was collected by driving the streets and alleys surrounding the target access point.

### 5.4.1 Step 1 - Importing the Data into ArcGIS

The first step in creating the visualization was to import the wireless network data produced by NetStumbler into ArcGIS. Using NetStumbler's "text" export functionality, the raw point data collected from scanning was exported into comma separated value (CSV) data files. Since our data was split between multiple NetStumbler data files, it was easiest to concatenate the exported data together using a UNIX tool such as *cat* and remove any duplicate headers.

Two Perl scripts were written to perform post processing on the CSV data exported from NetStumbler. The first script outputted the individual data point associated with each network that had the highest signal-to-noise ratio. This script was only used when a single data point was desired to represent the approximate location of each network. This step could have also been performed inside ArcGIS with a simple query, but it proved helpful as a sanity check to analyze the "summary" data before importing every data point into ArcGIS.

The second script reformatted the data by splitting the signal-to-noise ratio grouping created by NetStumbler into three separate columns and interpreted the flag and channel bits by creating a column for each attribute. It was also necessary to strip the cardinal directions from the longitude and latitude entries. As an example, the latitude / longitude pair, "N 38.9527833, W 95.2639833", needed to be reformatted to "38.9527833, -95.2639833". Another important function this script served was to determine the vendor based on the MAC address. This information was derived from the partial database Kismet provided and by looking up sample MAC addresses in the IEEE Organizationally Unique Identifiers (OUIs) database on the web [28].

Once a processed set of comma separated values was generated, the next step was to import the data into Microsoft Excel. This step was helpful since it allowed us to analyze the data in a spreadsheet and then export it to a form that ArcGIS can easily interpret. ArcGIS accepts many formats of data, but the best way is to export the data from Excel to a dBase 4 (DB4) style database since ArcGIS can directly import from this format with no user intervention. dBase style databases contain all the necessary information that ArcGIS needs such as the data types, field lengths, and column labels. With this in mind, it was important to set the data types and column widths to accommodate the length and type of each field before exporting from Excel. Once the data was inside ArcGIS, it was thoroughly checked to make sure none of the columns were truncated.

Inside ArcGIS, the .DBF file generated from the previous steps was directly loaded and displayed as a layer using the "Longitude" and "Latitude" fields as X/Y

data. This example only deals with the visualization of one network, so the points that were not associated with the MAC address of the single access point were selected and filtered out. This provided us with a view of all NetStumbler data points corresponding to the single access point as shown in Figure 5-8 below.

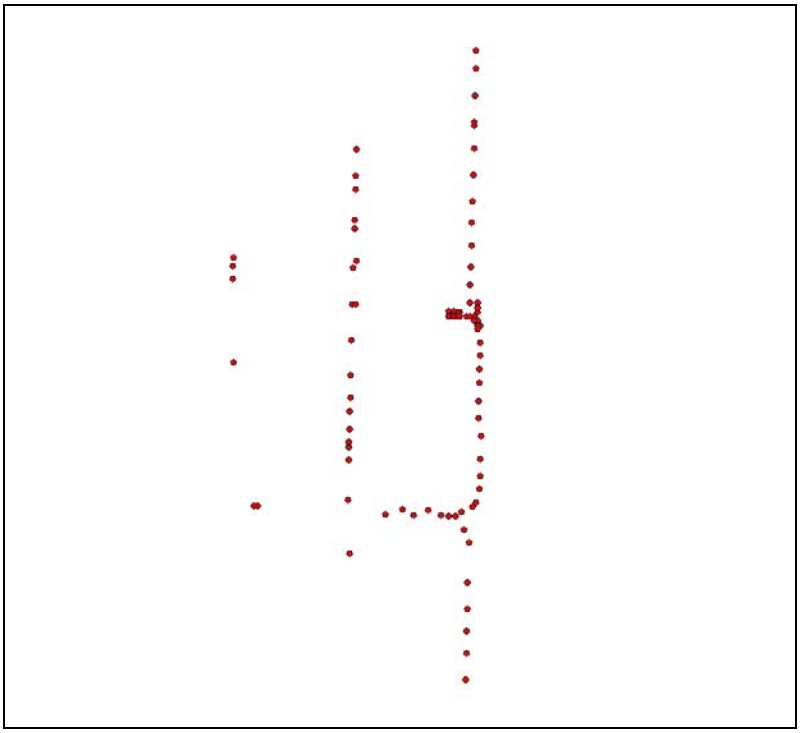

**Figure 5-8: NetStumbler Point Data For a Single Access Point**

### 5.4.2 Step 2 - Obtaining Background Imagery

The next step was to obtain a geo-referenced street map or aerial photo of the study area. The background imagery acts as a reference layer and can be any type of relevant data as long as it is geo-referenced. High resolution 6-inch aerial

photography (flown in 2000) was obtained from the Lawrence, Kansas City Planning Department. This imagery provided extremely detailed images when zooming in on specific areas such as a single house or business. For larger city wide views, where higher resolution data was of no benefit, we used 2001 1-meter resolution Digital Orthophoto Quarter Quadrangles (DOQQ) obtained from the Kansas Geological Survey at the University of Kansas.

Aerial photography's resolution is determined by the smallest unit of length a single pixel represents. For example, 6-inch aerial photography represents approximately a 6-inch area in one pixel. A comparison of 6-inch versus 1-meter resolution is shown in Figure 5-9. At larger distances, as seen in the pair of top images, the difference in resolution is less noticeable, but in extremely tight zooms, the higher resolution makes a dramatic difference.

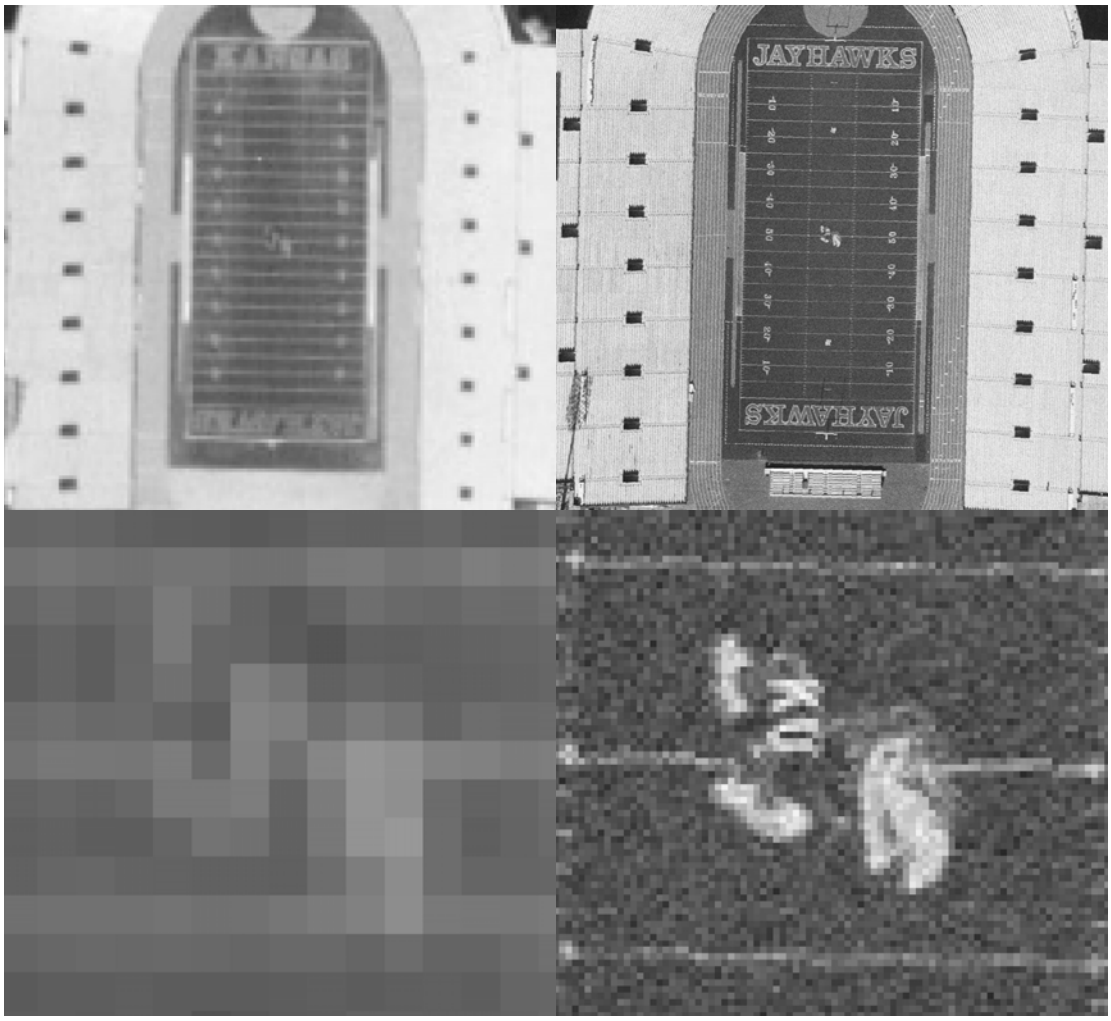


**Figure 5-9: Comparison of 1-meter (left) and 6-inch (right) Aerial Photography**

Many imagery data sources are available on the Internet such as Mappoint, Mapblast, Earthmaps, Terraserver, and the U.S. Census Bureau's Tiger Data. It is very important that the data used is geo-referenced, meaning it contains a pre-defined coordinate system in its metadata.

Figure 5-10 shows the background imagery used for this example. The actual location of the access point that was mapped is denoted with a white cross.

**Figure 5-10: 6" Aerial Photography Background Layer**

### 5.4.3 Step 3 - Re-Projecting to a Common Coordinate System

The goal of this step was to get the wireless point data and the aerial imagery into a common coordinate system so they could be layered and displayed together. All of our NetStumbler data was collected using the NMEA 0183 (National Marine Electronics Association - 1983) format. This is synonymous to "North American

Datum 1983" in ArcGIS. The aerial imagery used for the background was in the NAD 1927 (North American Datum) projection which is synonymous to NAD UTM Zone 15N in ArcGIS. This terminology explains that the Projection is Universal Transverse Mercator (UTM) and is located in Zone 15 North. Zones help to subdivide the projection systems in order to maintain local accuracy by resetting the central meridian. In order to get them in a common projection system, the aerial imagery was converted to NMEA 0183 so it would be compatible with the NetStumbler data. This involved using the "Re-Projection Wizard" in ArcToolbox which is distributed with the ArcGIS suite.

As you can see, this step acted as a sanity check for the process since the point data was aligned with the route driven on the background imagery. In Figure 5-11, you can see that all of the data points correspond to the alleys and streets that were driven to collect the data.

**Figure 5-11: NetStumbler Point Data Layered on Top of the Aerial Imagery**

### 5.4.4 Step 4 – Definition of A Signal Strength Gradient

This was an entirely optional step, but it was helpful to look at the signal gradient of the point data by changing the color of the dots based on the signal-to-noise ratio (SNR). This helps you get an idea of what the interpolation in the next step should look like.

ArcGIS allows you to define a color scheme based on the values of an attribute. By using the “Symbology” tab inside the layer properties, quantities can be represented using color to show values. In this case, the SNR field was used to create a nine segment color gradient based on the natural breaks, or Jenks, of the SNR values. In Figure 5-12, blue is used to show the highest SNR ratios (33.89db – 40.75db) while red shows the points with the lowest values (3db – 5.33db). The rest of the colors represent the signal strength in between.

**Figure 5-12: Colored Signal Gradient of the Point Data Based on SNR**

### 5.4.5 Step 5 - Interpolation Using IDW

In order to perform interpolation in ArcGIS, the Arc Spatial Analysis plug-in was required. This is typically purchased as a separate product from ESRI and includes the IDW interpolation tool used in this study. Before performing the actual interpolation, it was necessary to bound the data with manually created data points

that have null signal-to-noise ratio values. By bounding the data, it let the interpolation algorithm know the extent at which to draw the field. Without this, IDW and the other interpolation techniques in ArcGIS will interpolate to infinity in all directions, creating non-realistic fields that cover the entire canvas. NetStumbler does not log GPS coordinates where networks are absent, so it was necessary to manually add these points. For simplicity, it was decided to surround the data points from NetStumbler with null-valued points just outside the extent of the collected data. In areas where the SNR of the NetStumbler point data was strong, extra zero points were needed to keep the interpolation from leaking. Bounding proved advantageous since in other examples it was possible to draw null-value points around boundaries such as buildings where the signal is impossible to measure with NetStumbler and a GPS.

Figure 5-13 shows the NetStumbler point data in red with the manually added bounding data in green. The null values were created by using the editing toolbar and drawing a few points that had a SNR value of 0. It was then easiest to cut and paste these null-valued points where needed. In the example below, extra bounding points were needed to the east to keep the interpolation from leaking since they were so close to data points that contained high SNR values.

**Figure 5-13: NetStumbler Point Data and Manually Added Bounding Data**

Once the bounding was completed, the actual interpolation could be performed. By selecting the point data layer and clicking on the "Inverse Distance Weighted" option in the "Interpolate to Raster" menu of the Spatial Analyst toolbar, an options dialog is displayed. The "Z-field" selection box specifies the value to perform the interpolation on and, for this example, was set to the SNR attribute. The rest of the values for weight, size, and output layer were left at their default values. A custom

color scheme was used to create a nine segment color bar using the colors of the rainbow. Then, the transparency was set to 50% allowing the background imagery to be visible behind the signal field. The completed interpolation in Figure 5-14 shows a visual representation of a single access point's signal range observed by driving the streets and alleys around the house. The gradient from dark blue to red represents strong to weak signal reception.

**Figure 5-14: Completed Wireless Network Signal Interpolation**

## 5.5 *Example Imagery*

Through the use of our visualization technique, several maps have been generated to show signal propagation. A typical home, a university network, a business, and a hotspot are all offered as examples. The purpose of these visualizations is to show typical-use scenarios and their associated signal propagation, hopefully sparking the general public's interest in wireless security.

### 5.5.1 Home Network

The visualization in Figure 5-15 shows the signal propagation of a single access point located in a typical house. The signal is shown propagating into a school yard to the west and into several small businesses' parking lots to the east. The wide-open space to the northwest of the access point allows the signal to propagate farther than in other directions containing obstacles.

Using a sensitive antenna like the one in our study, it is theoretically possible, barring obstacles, to associate with the network or sniff traffic anywhere within the signal field shown below. With a less sensitive built-in antenna, it is likely that the network signals could only be picked up in the green, blue, and purple regions.

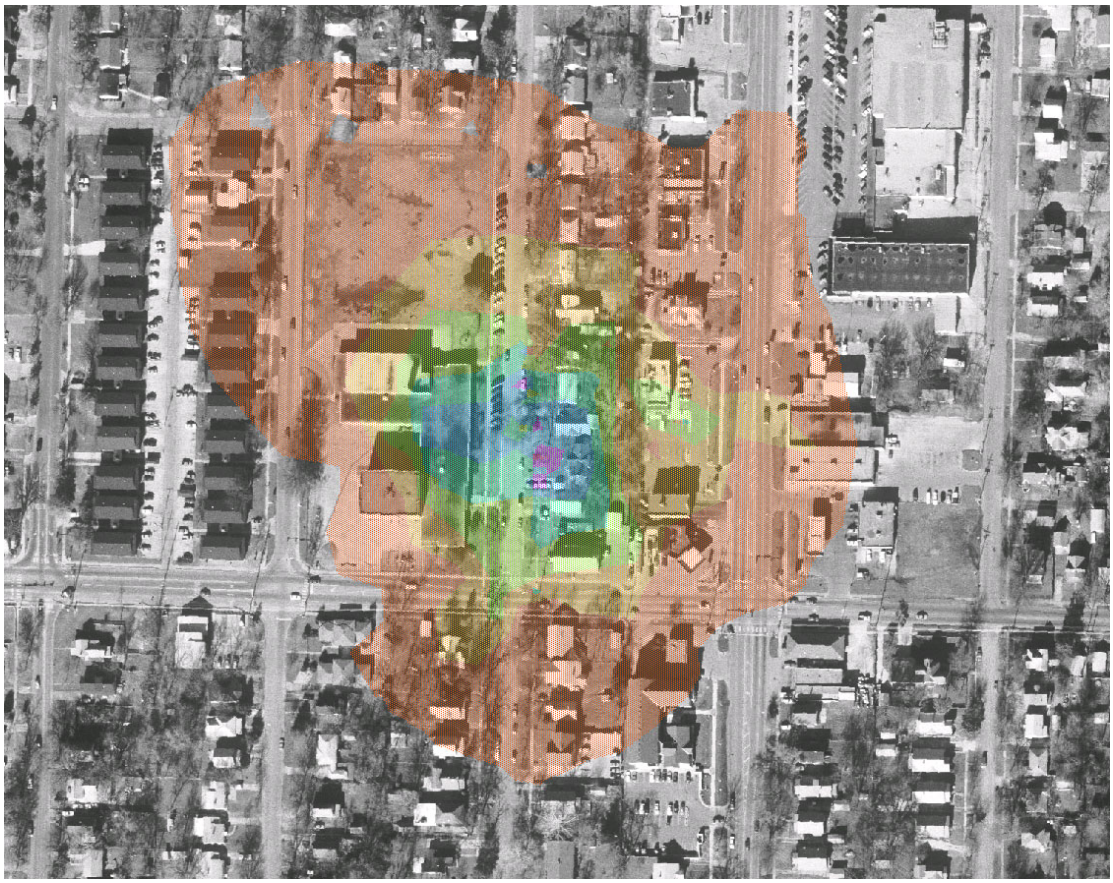

**Figure 5-15: A Typical Home Wireless Network**

NetStumbler provided information on the vendor of the access point, its WEP status, SSID, and channel. The exact location of the access point in this example was determined by its SSID since it was set to the actual street address of the home it was located in. This example clearly shows that a consumer grade access point is capable of broadcasting at large distances, well beyond the owner's property. It is this scenario that has given rise to the practice of "piggybacking" or using another's network without permission.

### 5.5.2 Business Network

In the example in Figure 5-16, our visualization technique was used to look at the nine access points located at the Information & Telecommunication Technology Center, University of Kansas, where I am currently employed. Here, instead of "wardriving", a walking scan was performed to gather data in areas where roads did not exist. By performing a walking scan, much more data was collected providing for a more accurate interpolation. In this example, a color gradient was not used to show the signal strength due to the large amount of overlap.

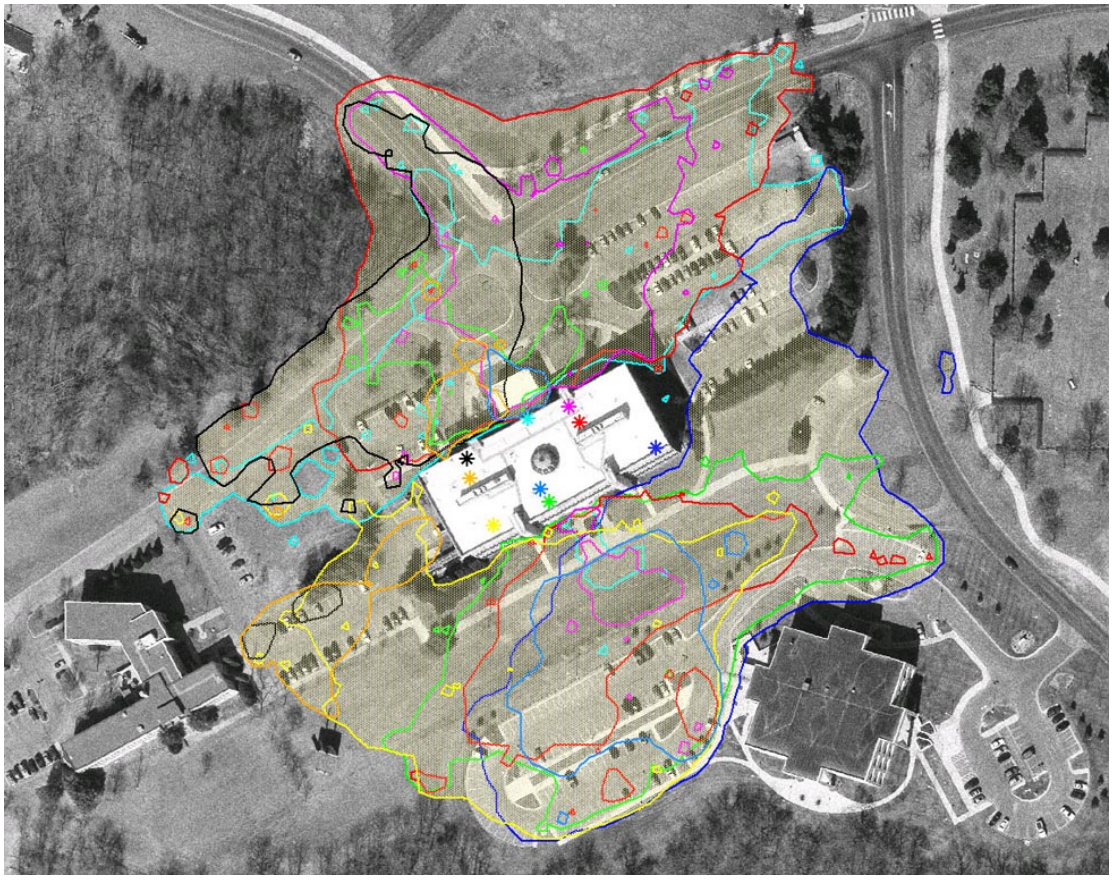

**Figure 5-16: Nine Access Points at ITTC, University of Kansas**

The “Generate Barrier Polylines” option was used in the creation of the fields for this map, providing the solid lines at the extent of each access point’s range. The approximate locations of the nine access points are denoted with different colored asterisks. These were manually added since direct knowledge of the AP’s locations was known. The same colors are then used for the barrier lines to denote the range of each access point. Once again, the signals from the access points are shown propagating well beyond their intended destination of inside the building and on the back patio. This clearly shows that the signals emitted from the building can be intercepted in several parking lots and roads in the immediate vicinity.

In Figure 5-17, only one of the access points is displayed. Its approximate location on the first floor is shown by the light blue asterisk. This picture shows that the placement of an access point affects where its signals are propagated. The signal can be observed leaking out of a bank of windows located in the south part of the building. This shows that the make-up and thickness of physical barriers affect the propagation of radio waves. Through the use of specialized antennas that help focus transmission, the signal leak outside the building could be minimized.

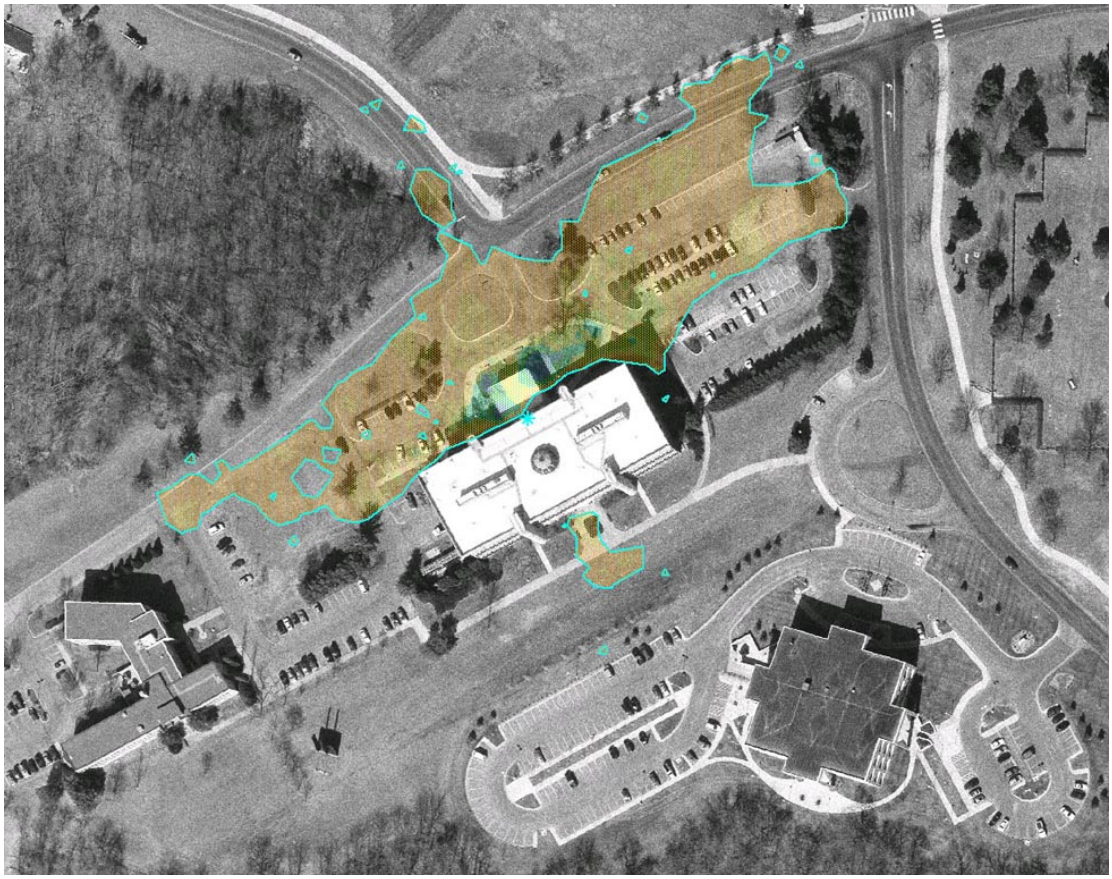

**Figure 5-17: A Single Access Point at ITTC, University of Kansas**

### 5.5.3 Small Business (Hotspot)

The example image in Figure 5-18 shows a coffee shop located in Lawrence, KS with a single 802.11b Apple Airport access point. All accessible roads, alleys, and parking lots were driven to collect this data. The signal in this case is shown reflecting off the buildings to the south and propagating to the northeast. Another interesting thing to notice is that the AP was still detected two blocks to the east. When bounding this

data, the surrounding buildings were used as barriers since GPS data cannot be collected inside enclosed structures.

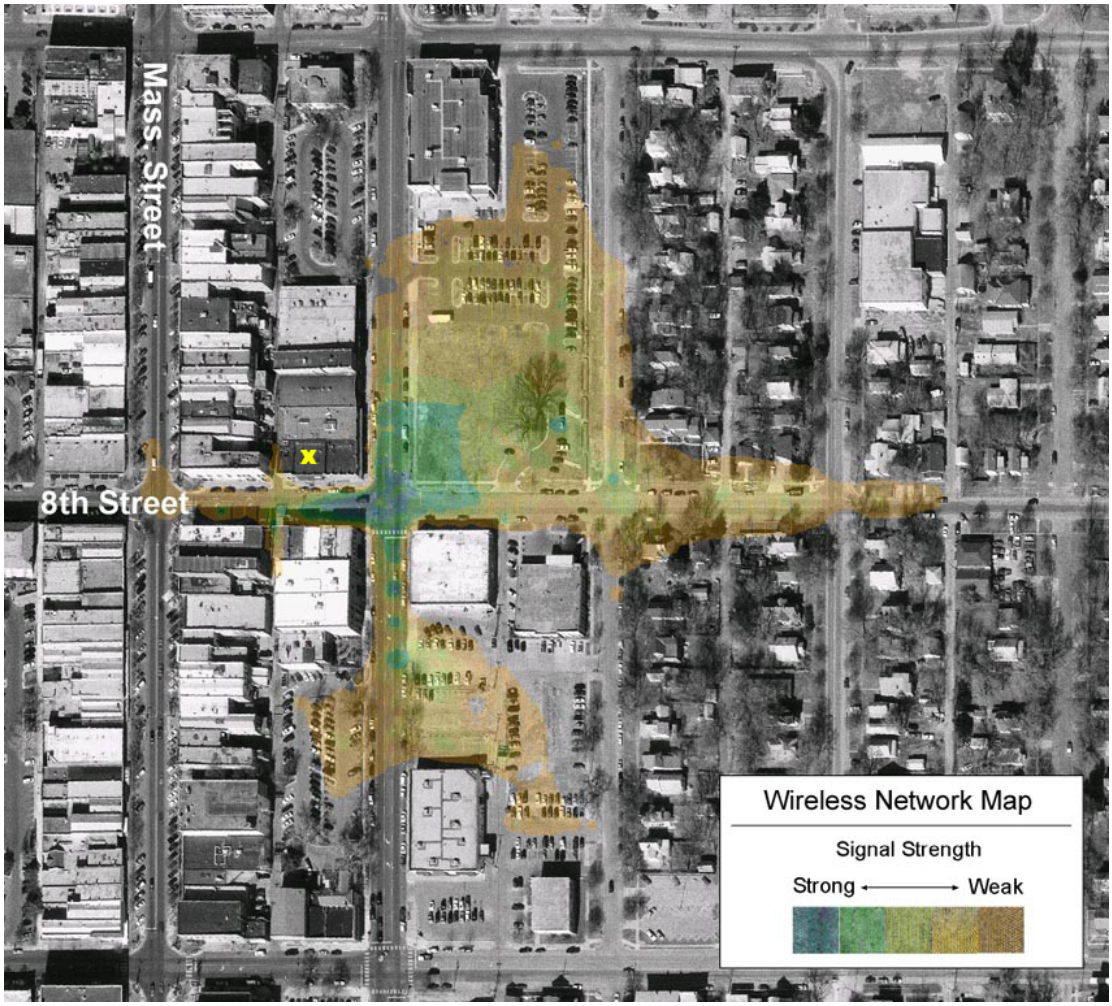


**Figure 5-18: Hotspot Signal Propagation**

### 5.5.4 University Network

The visualization in Figure 5-19 shows a single access point located in Snow Hall at the University of Kansas. This shows how the lack of physical obstacles, or what's referred to as line-of-sight, can greatly extend the range wireless signals will travel. As you can see from the figure, the AP's signal was detected from the parking lot far north of the AP's location.

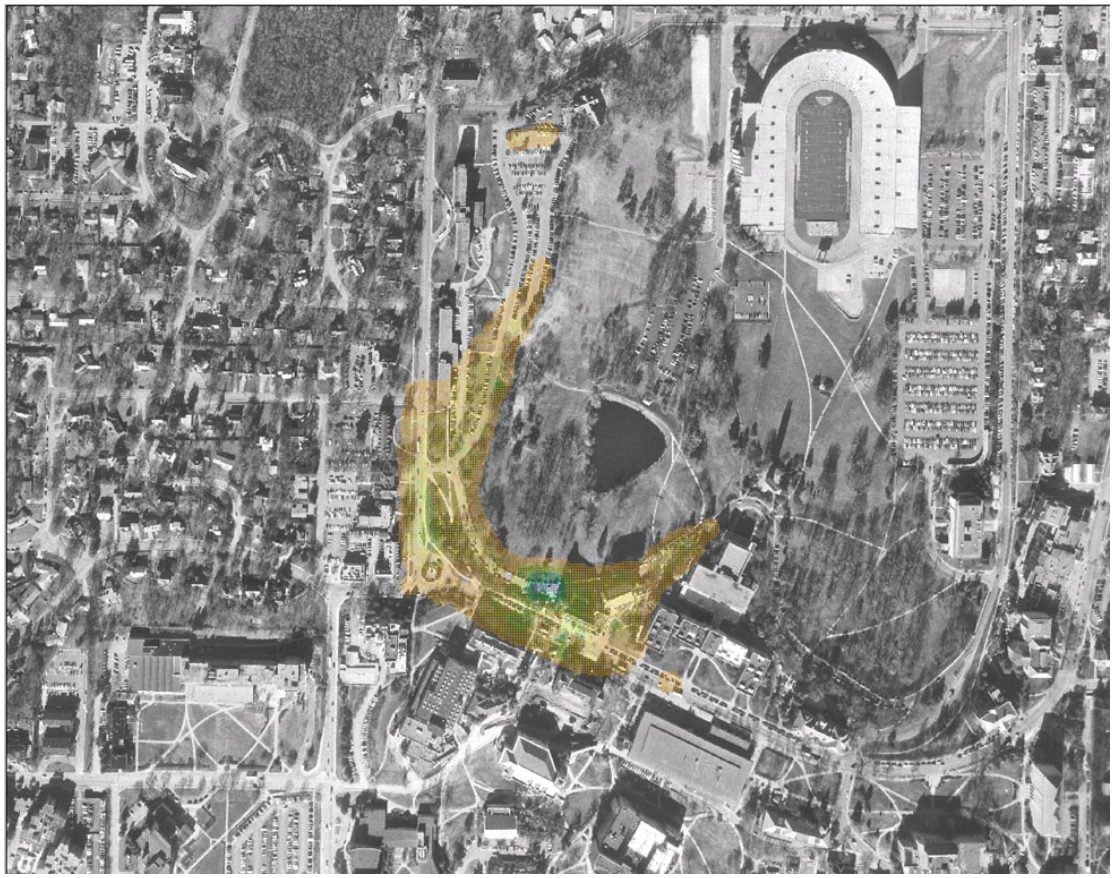

**Figure 5-19: Single Access Point at Snow Hall, University of Kansas**

### 5.5.5 Projected Radiation

A Geographical Information System is not limited to just providing interpolations. GIS's can create all types of features, surfaces, and layers based on any attribute. In this example, the approximate transmission distance of several access points are shown by circle features that were generated in ArcGIS. The radii of these circles were determined by locating the data point of each network with the largest SNR and then calculating the geographical distance to the data point of the same network that was farthest away. This calculation was performed in a script outside ArcGIS and added as a custom field in the point data.

The image in Figure 5-20 shows the estimated radiation of 186 access points in Lawrence, KS. Each network was color coded by its channel to show signal fields that are overlapping and might be interfering with each other.

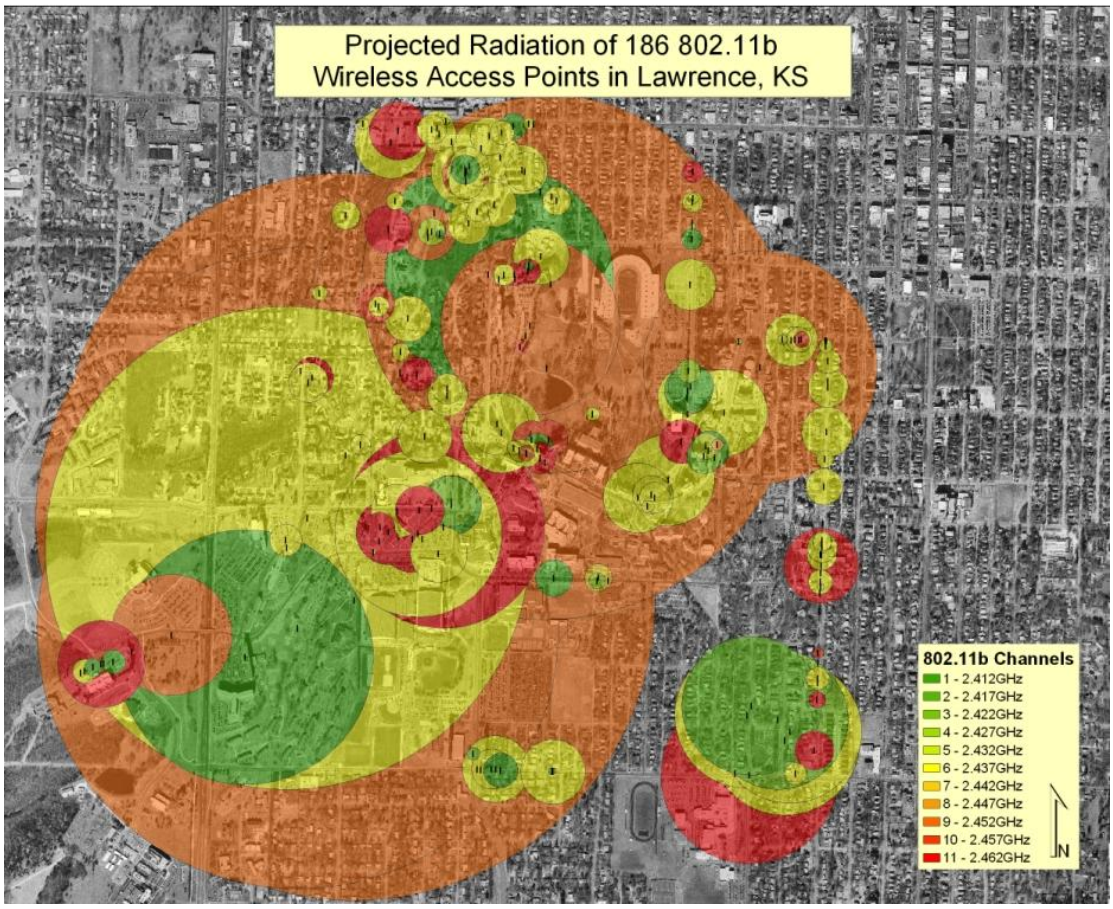


**Figure 5-20: Projected Radiation of 186 Wireless Access Points in Lawrence, KS**

All of these access points were detected on a quick 20 minute "wardrive" around the city. This data was collected using Kismet, which allows for the detection of non-"broadcast SSID" networks. Some of the larger circles are generated by the Lawrence, KS Police Department's wireless infrastructure, which is mounted on top of water towers and large buildings offering increased coverage areas. This example clearly shows the potential interference problems that might exist with so many networks located in close proximity.

# Chapter 6 - Conclusion and Future Work

## 6.1 *Conclusion*

802.11 wireless networks, which broadcast their signal through the air, do not offer the same physical security that wired networks provide. To further this problem, wireless signals are capable of being broadcast at large distances and the signals are usually found beyond their intended destinations. WEP, or Wired Equivalent Privacy, was defined in the original 802.11 standard to help protect against this issue of signal propagation by encrypting transmissions between radios. Unfortunately, very few people in the world are actually using WEP or any of the other security features that 802.11 offers. This leaves a staggering amount of access points wide-open for "piggybacking", packet analysis, or any other malicious activity.

Through the use of "wardriving", the case study presented in this paper shows the explosive growth of wireless and use of its security features in Lawrence, KS over a three-year period. The number of "broadcast SSID" access points in Lawrence, KS has tripled every year since 2002, with drastic consequences. Most users in Lawrence, like the rest of the world, are not practicing good security. Only 38.5% of these networks are using WEP encryption, up 12.6% from 2002. This leaves 999 out of the 1625 networks found in the sample set wide open for anybody to take advantage of. It was also observed that 51.9% of the networks were using a default SSID hinting at poor overall configuration. When compared to statistics offered by

the Worldwide Wardrive [5], Lawrence exhibited statistics that were similar to those observed in the rest of the world.

Statistics provide valuable insight into the trends associated with wireless networking, but are not fit for public consumption. Hence, there was a need for a more powerful method of conveying the security implications inherent in wireless networking, and to show how wireless signals propagate. The visualization techniques developed in this paper provide this missing link, appealing to users' senses through the use of aerial imagery and actual real-world examples.

In late 2001, when our visualization techniques were developed, little was being done in the area of wireless network mapping. The visualizations that did exist used simple street maps and dots to represent access points and their security features, but none showed actual signal propagation. By tapping into the power of a Geographic Information System (GIS) and aerial imagery, much more meaningful representations were created. Using Inverse Distance Weighted interpolation, the point data collected from scanning was transformed into signal fields that were color-coded by signal strength. Several images were created using this technique. The fields generated showed that by using a sensitive antenna, network signals could be intercepted several blocks away. In houses, it showed signals propagating into the surrounding neighbors' homes and in businesses, it showed signals leaking into parking lots. The example images also demonstrated how signals are reflected and affected by barriers such as walls and windows.

Something needed to be done to inform users of their vulnerability. They needed to see how far their wireless signals were being broadcast, and to realize the importance of security features which could minimize the risk. The visualizations created have worked well to convey these security implications of wireless networking. One must remember that visualizations convey meaning in a form that appeals to a human's most powerful sense, sight.

It will be interesting to see what future concerns are raised regarding wireless security. With the poor use of WEP encryption and the general lack of wireless security in the world today, my hope is that these visualization techniques showing signal propagation will encourage people to think more about the security of their wireless infrastructure. The purpose of this study is to provoke a reaction.

## 6.2 *Future Work*

This project provided meaningful data and a methodology to raise wireless networking awareness, but there is always room for improvement. The following is a list of tasks that could improve and/or extend the work of this project:

- Continue collecting and analyzing the sample set on a yearly basis using both active and passive scanning techniques
- Investigate more advanced interpolation techniques and see if the bounding process can be eliminated through the collection of data where networks were not found
- Create a plug-in using the Visual Basic for Applications API provided in ArcGIS to automate a lot of the tasks required in visualizing wireless network data
- Study the effects of wireless interference as the number of wireless networks using the same channel grow
- Analyze the quality of the various vendors' instructions over time and provide hard evidence of the effect this has on the use of wireless security features
- Extend the mapping technique to an indoor environment
- Collect and map data in 3D

# References


1. Dzubeck, Frank. "The Dawn of a Wireless Century." Network World. May 10, 2004. <http://napps.nwfusion.com/columnists/2004/0510dzubeck.html>

2. Tilak, John. "Number of Home Networks to Reach 111M in 2008." DMEurope.com – Digital Media News for Europe. February 9, 2004. <http://dmeurope.com/default.asp?ArticleID=2941>

3. Wolf, Michael. "The Home Network Owner 2004: A Survey of Current and Future Home Network Owners." In-Stat/MDR. May 2004. <http://www.instat.com/abstract.asp?id=99&SKU=IN0401401RC>

4. "Wi-Fi Standard by 2005, In-Stat/MDR Says." Electronics News. August 8, 2003. <http://www.electronicsnews.com.au/articles/d2/0c018dd2.asp>

5. "Worldwide Wardrive 4 Stats." Worldwide Wardrive. June 2004. <https://wigle.net/gps/gps/GPSDB/stats/?eventid=1>

6. Flickenger, Rob. "802.11b Tips, Tricks, and Facts." O'Reilly Wireless Devcenter. March 2, 2001. <http://www.oreilly.com/lpt/a/wireless/2001/03/02/802.11b_facts.html>

7. "IEEE 802.11." Wikipedia. October 16, 2004. <http://en.wikipedia.org/wiki/IEEE_802.11>

8. Geier, Jim. "802.11 Alphabet Soup." WI-FI Planet. August 5, 2002. <http://www.wi-fiplanet.com/tutorials/article.php/1439551>

9. Gast, Matthew S. 802.11 Wireless Networks: The Definitive Guide. Sebastopol: O'Reilly & Associates, Inc. April 2002.

10. Poulsen, Lars. "FCC Rules for ISM Band Wireless Equipment." Wireless Data Communications. January 11, 2000. <http://www.beagle-ears.com/lars/engineer/wireless/fccrules.htm>

11. "CSMA/CA." Webopedia. <http://www.webopedia.com/TERM/C/CSMA_CA.html>

12. “Introduction to IEEE 802.11.” Intelligraphics. <http://www.intelligraphics.com/articles/80211_article.html>

13. Scott Fluhrer, Itsik Mantin, and Adi Shamir. “Weaknesses in the Key Scheduling Algorithm of RC4.” <http://www.drizzle.com/~aboba/IEEE/rc4_ksaproc.pdf>

14. Adam Stubblefield, John Ioannidis, and Aviel D. Rubin. “Using the Fluhrer, Mantin, and Shamir Attack to Break WEP: Revision 2.” AT&T Labs Technical Report TD-4ZCPZZ. August 21, 2001. <http://www.cs.rice.edu/~astubble/wep/wep_attack.pdf>

15. Alan Cohen and Bob O'hara. “802.11i Shores Up Wireless Security.” Network World Fusion. May 26,2003. <http://www.nwfusion.com/news/tech/2003/0526techupdate.html>

16. Lawson, Stephen. “Wi-Fi Security Gets a Boost.” PC World.com. February 24, 2003. <http://www.pcworld.com/news/article/0,aid,109482,00.asp>

17. Jaques, Robert. “Hackers Exploit Poor Wi-Fi Security.” Computing. June 10, 2004. <http://www.computing.co.uk/News/1155759>

18. Poulsen, Kevin. “Wardriver Pleads Guilty in Lowes WiFi Hacks.” SecurityFocus News. June 4, 2004. <http://www.securityfocus.com/news/8835>

19. Shipley, Peter M. “About Pete Shipley.” <http://www.dis.org/shipley/>

20. Duntemann, Jeff. “Jeff Duntemann's Wardriving FAQ.” Wardrive.net. April 26, 2003. <http://faq.wardrive.net/>

21. Shore, Bill. “Wireless networks - Warchalking/Wardriving.” [Email] Available Email: From billshore@fbi.gov and posted to <http://www.stumbler.net/fbi.php> July 8, 2002.

22. “18 U.S.C. 1030. Fraud and Related Activity in Connection with Computers.” Computer Crime and Intellectual Property Section (CCIPS) of the Criminal Division of the U.S. Department of Justice. U.S. Department of Justice. <http://www.usdoj.gov/criminal/cybercrime/1030_new.html>

23. Kershaw, Mike. “Kismet Readme.” Kismet Wireless. October 1, 2004. <http://www.kismetwireless.net/documentation.shtml#readme>

24. “About Us.” City of Lawrence Home Page. <http://lawrenceks.org/about.shtml>

25. Sanders, Larry M. "Re: Sunflower Saturation Data." [Email] Available Email: From lsanders@sunflowerbroadband.com To bbecker@ittc.ku.edu. February 17, 2004.

26. Newman, Anthony. "Europe grows WiFi faster than North America." InfoSync World. October 24, 2003. <http://www.infosyncworld.com/news/n/4224.html>

27. "In-Stat Saw 214-Percent Growth In NIC And AP Unit Shipments From 2002 To 2003." TMCNet.com. January 14, 2004. <http://www.tmcnet.com/usubmit/2004/Jan/1022757.htm>

28. Landron, Angela. "IEEE OUI and Company_id Assignments." Institute of Electrical and Electronics Engineers (IEEE). November 8, 2004. <http://standards.ieee.org/regauth/oui/index.shtml>

29. Klaus, Christopher W. "Wireless LAN Security FAQ." Internet Security Systems (ISS). Version 1.7. October 6, 2002. <http://www.iss.net/wireless/WLAN_FAQ.php>

30. Geier, Jim. "Assigning 802.11b Access Point Channels." Wi-Fi Planet. February 11, 2002. <http://www.wi-fiplanet.com/tutorials/article.php/972261>

31. Tufte, E.R. "The Visual Display of Quantitative Information." Graphics Press. Chesire. 1983. Page 197.

32. Crocker, Glenn. "Wardriving Maps." KCWireless. May 15, 2002. <http://www.kcwireless.net/index.cgi?WarDriving>

33. Keeney, Frank. "Vacation War Driving From Pasadena, CA to San Francisco, CA." Pasadena Networks. 2001. <http://pasadena.net/vacation/vacslolarge.gif>

34. "Consume NodeDB." Consume. <http://consume.net/nodedb.php>

35. Sue Spielman and Tom Whitehill. "Java and GIS, Part 1: Intro to GIS." Java.Net. February 16, 2004. <http://today.java.net/pub/a/today/2004/02/16/gis.html>

36. "A-Z of Service Providers: ESRI (UK)." S-Cat. <http://www.s-cat.gov.uk/atoz/tmp1.asp?ID=1297&SPID=133>

37. Childs, Colin. "Interpolating Surfaces in ArcGIS Spatial Analyst." ArcUser. July-September 2004. <http://www.esri.com/news/arcuser/0704/files/interpolating.pdf>

38. "Inverse Distance Weighting (IDW) in GS+." Gamma Design Software. <http://www.gammadesign.com/OverviewIDW.html>

39. Marshall, Trevor. "Antennas Enhance WLAN Security." Byte.com. October 1, 2001. <http://www.trevormarshall.com/byte_articles/byte1.htm>