Using Wireless Fidelity (Wi-Fi) Technology For Urban Navigation

Dewayne R. Brown and Derrek B. Dunn
N.C. A & T State University
Greensboro, NC 27411 dbrown@ncat.edu, dbdunn@ncat.edu

Abstract **- As cities and towns grow, consumers, entrepreneurs, and tourists can benefit from a technology that will help them to find their location or destination in an urban environment. By using Wireless-Fidelity technology, people can use commodity laptops, Personal Digital Assistants and cell-phones to navigate within access points of any city or town. The purpose of this research is to navigate around Greensboro, North Carolina using Wireless-Fidelity technology to investigate the efficiency of using the access points in the city. This process is called War-Driving. This research will also address some security issues that affect urban navigation using Wireless-Fidelity.**

Index Terms – Global Positioning Systems, Place Lab, Navigation, War-Driving

1. INTRODUCTION

We live in a world which is constantly changing, and the way individuals adapt to any particular change will eventually determine if they succeed or fail. In essence, the same can be said regarding wireless networks; if older technology is not upgraded, replaced, or reconfigured, the potential for unauthorized users to access networks and perform malicious acts simply increases. There are numerous ways individuals can better equip their wireless network to withstand the onslaught of potential hackers, and one way is to make sure wireless security measures are in place. The act of War-Driving plays a significant role in the efforts to expand the knowledge of securing wireless networks. Understanding War-Driving and how it operates with various programs such as NETSTUMBLER, WiGLE, etc., increases the awareness of individuals who simply believe they have a secure wireless system once they take the equipment right out of the box.

War-Driving has been around for quite some time, and actually the overall process has been quite successful. War-Driving, in conjunction with another familiar application, PLACE LAB will prove to enhance the knowledge of individuals worldwide as well as assist in the future efforts of Wireless-Fidelity (Wi-Fi) and its need to be deployed out on a broader scale.

PLACE LAB is a geo-positioning system [1]. PLACE LAB provides a locating system which will have the ability to work in areas where individuals will spend most of their time, which is indoors. PLACE LAB provides a low-cost of entry for both users and the application developers.

The research provided in this paper will look at data pertaining to War-Driving, GPS logging, and Access Point (AP) placement. Additionally, this research was conducted in an effort to determine if existing access points were still in existence, and GPS tracking was used to log the recorded data.

While working on this project, it was imperative to identify both the Wired Equivalent Privacy (WEP) and the Service Set Identifier (SSID). WEP encryption method was designed to provide wireless networks with the same security available in wired networks. SSID is the name assigned to a wireless network. Usually, the SSID comes by default using the vendor's name and should be changed to something nondescript. With information about whether or not WEP is disabled and SSID default settings, an unauthorized user could access your documents, financials or other sensitive information.

2. RESEARCH PROCEDURE

The equipment needed in order to conduct this experiment was a GPS receiver, laptop computer, NETSTUMBLER, WiGLE, and PLACE LAB. NETSTUMBLER, WiGLE, and PLACE LAB were used as the software requirement. Researchers had to register at these sites in order to have access to them. A GPS receiver and laptop were used for the hardware requirement. Maps were downloaded from the WiGLE website which covered the Greensboro area. War-Driving was done to verify that the access points are still there. GPS technology was used to find out the locations of the researchers and the access points. Extensive details about the experiment and data gathered were formulated in charts.

The wireless LAN detection tool NETSTUMBLER was downloaded. This handy software addition facilitated the detection of WLANs around the targeted research area. NETSTUMBLER was used in the research to find locations with poor coverage in the research area, detect unauthorized or "rogue" access points which may cause interference to existing networks, assist War-Drivers in their efforts to increase the knowledge of wireless issues related to security, placement, and overall deployment of wireless networks on a much larger scale.

It should be noted that NETSTUMBLER is widely recognized as the application of choice when it comes to access point (AP) locating software [2]. NETSTUMBLER works on networks that are configured as *open systems*. This means that the wireless network indicates that it exists and will respond with the value of its SSID to other wireless devices

when they send out a radio beacon with an empty set SSID. This does not mean, however, that wireless network can be easily compromised, if other security measures have been implemented. To defend against the use of NETSTUMBLER and other programs to detect a wireless network easily, administrators should configure the wireless network as a *closed system*. This means that the AP will not respond to empty set SSID beacons and will consequently be invisible to programs such as NETSTUMBLER which rely on this technique to discover wireless networks. However, it is still possible to capture the raw 802.11b frames and decode them through the use of programs such as Ethereal and Wild Packet's Airo Peek to determine this information. Radio Frequency (RF) spectrum analyzers can be used to discover the presence of wireless networks. Notwithstanding this weakness of *closed systems*, you should choose wireless APs that support this feature. Additionally, it must be understood that NETSTUMBLER is only a tool, and its uses can be for intentions which will help or hinder wireless networks. For example, an individual who wanted to use NETSTUMBLER for malicious means has the ability to do so just as the individual who wants to use NETSTUMBLER for research to increase an individual's knowledge base about wireless networking. Moreover, NETSTUMBLER is highly favored because of it easy user interface, and its ability to provide an enormous amount of data including SSID, MAC addresses, encryption, longitude and latitude information (when used with GPS software), etc.

3. DATA RESEARCH

A Midwest region of the Greensboro area was chosen to conduct this research. We were able to locate this information and download maps from a well know source named Wireless Geographic Logging Engine (WiGLE) [3]. WiGLE is a site which consolidates location and information of wireless networks world-wide to a central database, and has user-friendly java, windows, and web applications that can map, query and update the database via the web. WiGLE currently accepts files in any of NETSTUMBLER'S exported file formats, DSTUMBLER'S text output, Kismets CWDG, XLM, CSV, or GPS formats, Pocket Warrior's text output, as well as via our online form. WiGLE currently has 4,305,518 networks with locations in their database. The website has been in existence for four years, and during that time it has become a well know site to make individuals aware of the security vulnerabilities which are associated with wireless networks.

An effort titled the World Wide War-Drive (WWWD) has been around for four years. WWWD was created by individuals who want to ensure a more secure wireless networking atmosphere [4]. Figure 1 shows show critical data compiled from NETSTUMBLER, WiGLE, and WWWD websites. This information was gathered over a four year period, and proved to be a success because the amount of awareness increased every year. Data recorded was from Sept. 2002 (first WWWD) – June 2004 (last WWWD). Starting at the extreme left of each category is WWWD 4, which represents the fourth year. To the right of WWWD 4 is WWWD3. WWWD2 is located on the right of WWWD3. WWWD1 is on the extreme right or to the right of WWWD 2.

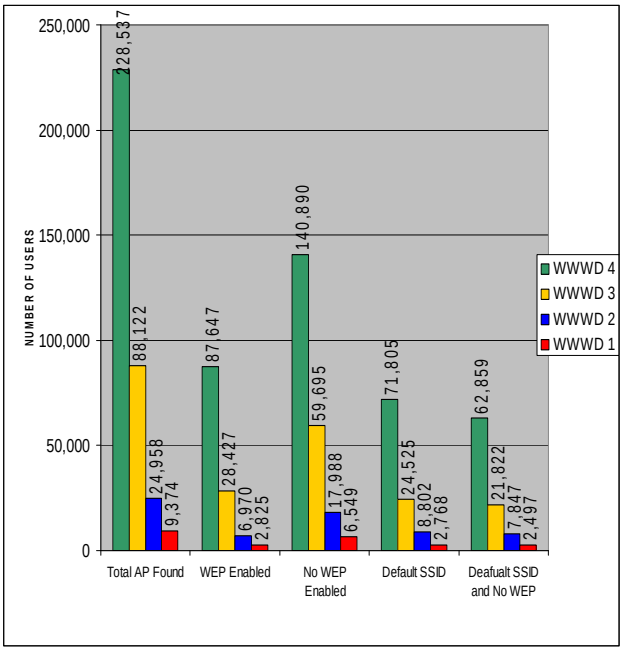

FIGURE 1

The chart shows significant increases in every category due to the fact that individuals were becoming more aware of the prevalence of wireless networks and their ability to provide added mobility. WiGLE'S ability to cover an enormous amount of area has increased its need for consumers and business professionals alike in a time when security is on the forefront of everyone's topic of discussion.

Figure 2 shows a broad area of the Midwest region of Greensboro, North Carolina, which is the chosen research area. The red dots symbolize access points recorded on WiGLE.

Figure 2 shows the numerous access points located throughout this area of the city. It should be noted that these access points are more prominent in areas located around college campuses, restaurants, etc. Studies indicate heavily populated areas are more likely to have wireless networks set up because of the simple fact that they provide added mobility to the business minded individuals and the average consumer alike.

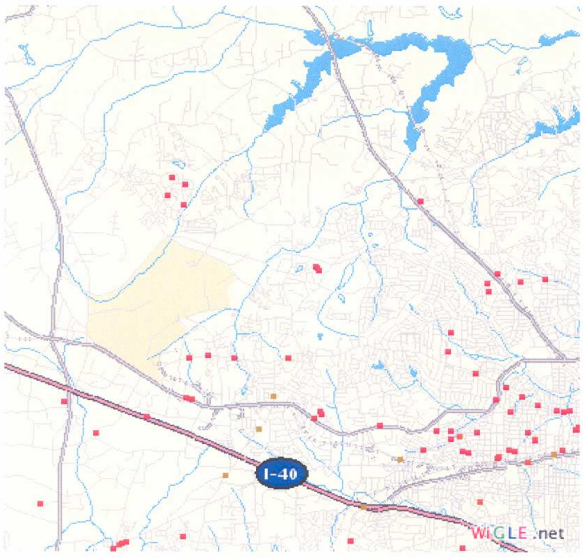

FIGURE 2

Figure 3 is a magnification of Figure 2, revealing more details.

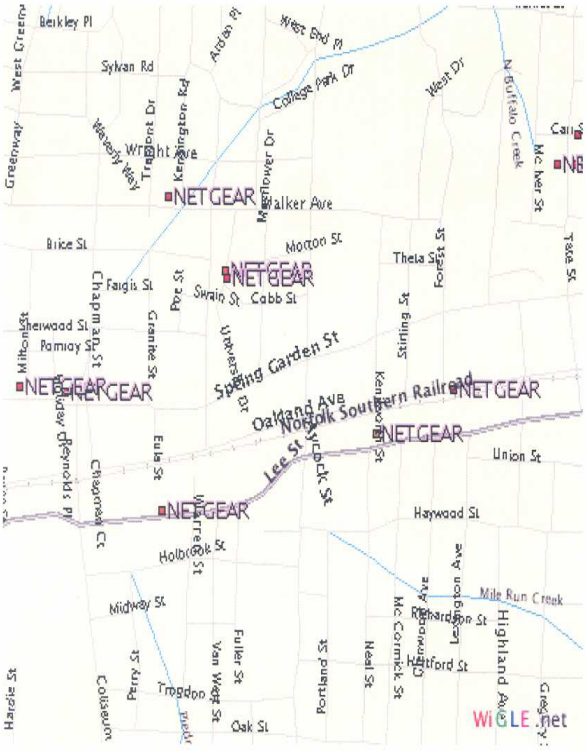

FIGURE 3

Figure 4 shows the most detailed map achieved. Many of the street names are able to be viewed. The red circle in Figure 4 was our targeted research area.

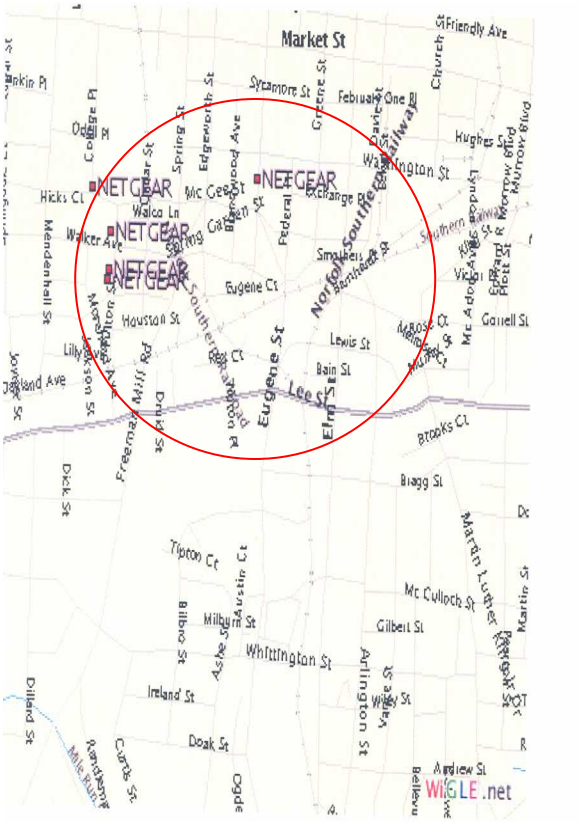

FIGURE 4

A brief overview of the research area has been noted, and now we will begin further research regarding the graphical data of the information gathered.

Additional GPS hardware and software was used in this project in order to better track our data. Delorme, is a company which specializes in mapping software and GPS solutions for consumers and businesses alike. The hardware, *Earthmate GPS LT-20, uses no batteries because it* can be connected via USB from your laptop and provides the actual link to the satellites for tracking information. From a software perspective, *Street Atlas 2006 USA*, proved to be quite beneficial because of the amount of data which was readily available. There were over 4 million points of interest, and with voice activated directions, easy to use interface, and a host of other features, this software is preferred by most over *Microsoft Streets and Trips*. There was an additional Wi-Fi card used in this project by a company name Proxim Wireless. The ORiNOCO 11b/g PC Card gives you the flexibility to connect to any 802.11b or 802.11g wireless network and delivers the utmost in mobile convenience and performance, so that you can move easily between 802.11 networks at work, home or in public spaces. Throughput five times higher than 802.11b speeds network response times and supports bandwidth-intensive applications.

Figure 5 is a screen shot taken of a War-Drive from North Carolina A&T State University to Walker Avenue. Figure 5

shows the number of encrypted access points versus the number of access points which were not encrypted. There were a total of 135 Access Points (APs). Nine of the APs cannot be seen from the screen shot, but they were non-encrypted. 40% or 54 APs were equipped with some sort of encryption, which is labeled with a little lock inside the circle. 60% or 81 APs were not equipped with some sort of encryption, which is labeled a circle without a lock in it.

FIGURE 5

4. DATA RESULTS

From this information gathered, it is clearly understood why so many networks are being invaded by unauthorized users. As prices for wireless networking equipment continues to drop, more individuals will purchase them, increasing the number of users who are not very knowledgeable of wireless network security. Additionally, of the 135 access points detected, nine of them were still using the default SSID (linksys, NETGEAR, Apple Network, etc). This was also a major concern with regards to security issues because more often than not a potential hacker will try the default codes first because he or she realizes that some individuals simply do not change them sometimes.

There were several different methods which could have been used to obtain, track, and log the data; however, the researchers found it beneficial to use PLACE LAB and NETSTUMBLER in conjunction with additional GPS enabled software/hardware to conduct this research. PLACE LAB and NETSTUMBLER integrated well together. PLACE LAB was used as a means to store log files of wireless access points (APs) created from using NETSTUMBLER. This process is necessary because it will assist PLACE LAB in achieving its two primary goals of creating a locating system which will work where individuals spend most of their time as well as providing a low-barrier of entry of for the end user.

The following three steps provide a very generic approach to completing a Wi-Fi neighborhood navigation project. First, use NETSTUMBLER in conjunction with some sort of GPS software to locate, track, and log wireless network APs. Second, convert NETSTUMBLER'S data into a format which can be used by PLACE LAB (normally "TEXT" format). This information is collected and placed into PLACE LAB'S database. PLACE LAB will use the data to educate individuals on wireless locating systems. Third, WiGLE is used as a means for gathering information and location of wireless networks. It will serve as the basis of data which will be used by PLACE LAB.

PLACE LAB'S approach works quite well because even though the access points discovered were new, there were not necessarily new to PLACE LAB and WiGLE. The reason for this is because there are literally hundreds if not thousands of individuals collecting similar data on a regular basis to log into these and other websites. Once the information is collected and formatted to fit into its corresponding website, only access points which are *new* will show up. Duplicate information will only be kept as a log for the user submitting the data.

Figure 6 shows the actual data depicting the longitude and latitude results NETSTUMBLER discovered while connected to GPS. This data was retrieved from the same War-Drive pertaining to Figure 5. The information was too extensive to include the complete data set, so only a few sample points will be noted. Figure 7 is simply a continuation of Figure 6.

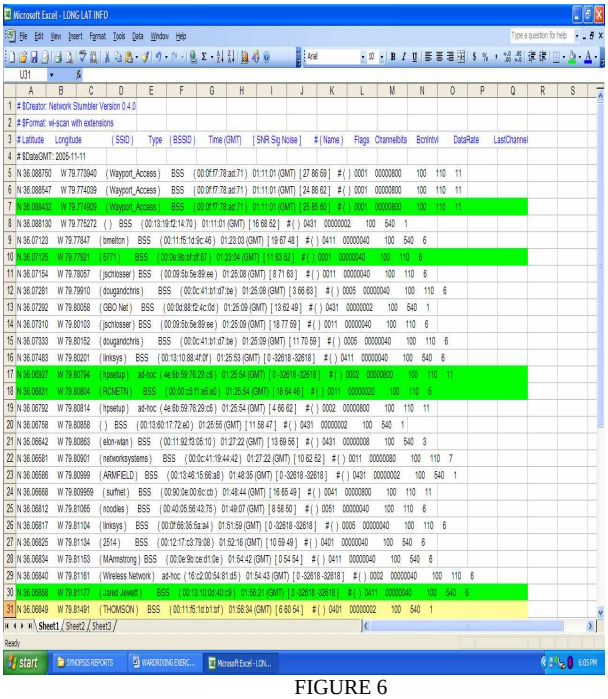

FIGURE 6

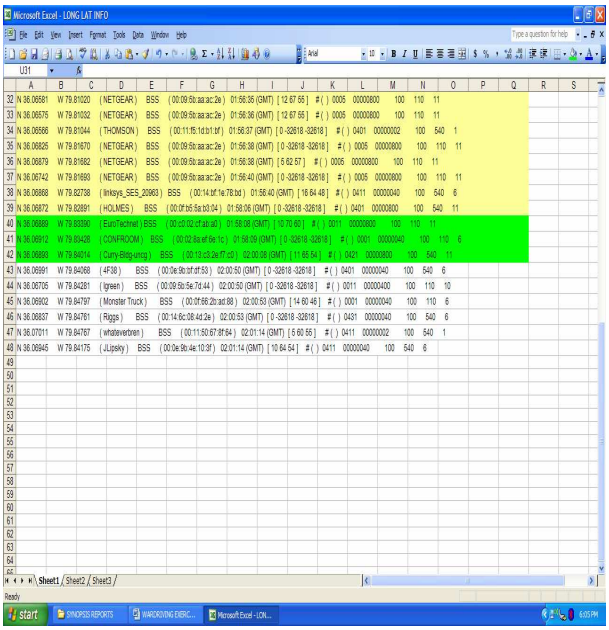

FIGURE 7

Lines 7, 10, 17, 18 and 30 of Figure 6 represent access points which were either newly discovered, or have been altered to increase the amount of security for that particular wireless network. Likewise, lines 40, 41 and 42 of Figure 7 indicated the same results.

Line 31 of Figure 6 and lines 32 through 39 of Figure 7 represent access points regarding our target area. This serves as factual data showing that the wireless access points located on our target photo were still in existence.

It is evident that individuals and corporations are realizing the prevalence of wireless networks, and some are even taking the necessary steps to add higher levels of security to ward off unauthorized users. This research experience led researchers to conduct an additional experiment on the information noticed in NETSTUMBLER. At times it was noticed that NETSTUMBLER would provide a result of "Fake" in the VENDOR column. "The value of "fake" in the vendor column is what NETSTUMBLER / MINISTUMBLER fills in when it sees an AP that it cannot determine the brand. This is due to either someone running FAKE ACCESS POINTS or NETSTUMBLER just doesn't have a match for the MAC prefix in the internal database. Additionally, there is a company by the name of Black Alchemy which generates literally thousands of counterfeit 802.11 access points. The real access point is hidden in plain sight amongst Fake AP's cacophony of beacon frames. As part of a honey pot or as an instrument of someone's site security plan, a Fake AP will confuse War-Drivers, NETSTUMBLER, Script Kiddies, and other undesirables wanting to access someone's network.

Additionally, in a comparison analysis, it should be noted that more increased wireless networks are available because of the simple fact, consumers want more mobility. This research indicated 81 out of the 135 wireless access points, detected by NETSTUMBLER were without WEP. The vast majority of them were located in areas where wireless usage is a part of everyday life such as on college campuses, and some fast food dining areas. It should also be noted that there were some default settings on quite a few of the non-encrypted wireless networks, and that could simply be related to the fact that many individuals are not aware of wireless network security measures.

5. CONCLUSION

In this research, the researchers were able to demonstrate some basic data gathering techniques from vulnerable wireless networks which increased the general public's knowledge base, as well as increase their awareness of the need of wireless security. PLACE LAB'S is a vital key to enabling radio-beacon based location and would be widely used because of its high-coverage, indoor/outdoor locating technology. War-Driving is extremely important for the state of wireless security, as it shows how many unprotected WLANs are out there and is therefore directly influencing wireless security awareness. The research conducted in this project serves as a blue print of how to conduct a War –Driving experiment. The research revealed the dangers that lurk for unprotected wireless networks.

All technologies have certain security and privacy issues in common, but newer technologies are more vulnerable because there may not necessarily be measures or standards in place to combat the onslaught of hackers by the time the technology hits the market. It is up to the individual or network administrator to ensure data is kept safe from unauthorized individuals. The future of PLACE LAB will prove to be a bright one because it is addressing the needs of consumers. It will simply be a matter of time before we will begin to notice PLACELAB'S approach become more commonplace in our lives.

The rapid rise and evolution of wireless networking technologies continues to have a profound impact on consumers and companies alike. Some are concerned if wireless networking is worth the risk and the answer all depends on the network administrator. There are literally countless benefits to installing a secured wireless network, and as long as the proper measures are in place, there should not be any issues

6. REFERENCES

[1] Place Lab 2.0, Intel Corporation, Seattle Washington, June 2003.

[2] Milner, Marius, Netstumbler v0.4.0, San Diego, CA, January 2006.

[3] Wireless Geographic Logging Engine (WIGLE), Mimezine Incorporated, Illinois 2002.

[4] Hurley Chris, Thornton Frank, Puchol Michael, "WarDriving: Drive, Detect, Defend", Syngress Publishing, Rockland MA, April 1, 2004.