Analysis of Wireless Network Use in the Twin Cities Metropolitan Area.

Gabe Emerson
University of Minnesota, Minneapolis.
emers089@umn.edu

May 2007

Abstract

Wireless Internet (WiFi) networks are growing in popularity across the United States. Despite the availability of secure methods to encrypt network traffic and handle access control, many networks are left without protection, or with outdated and insecure encryption schemes. This research investigates the use and encryption of wireless networks in different demographic areas of the Twin Cities of Minneapolis and St. Paul. A number of scans were conducted from building rooftops to limit coverage to identifiable socioeconomic regions. The results indicate that land use and zoning, rather than income, is a better indicator of encryption use. While the Twin Cities shows a surprising degree of secure-encryption use, insecure networks comprise the majority of those seen. Another significant finding is that change over time in regional network statistics is a difficult metric to recover.

1. Introduction

This project examined the prevalence, variation, and evolution of wireless network (WiFi) security in Minneapolis and St. Paul, Minnesota. A series of on-site surveys were conducted from various elevated locations in the Twin Cities Metropolitan area. Based on the collected data, a number of statistical comparisons and generalized conclusions were made regarding the popularity of wireless networks and the prevalence of encrypted or open networks as compared to regional zoning, income, or other demographic factors. By repeating several surveys, trends of encryption technology adoption for certain areas were noted and examined.

This paper is organized as follows. Section 1.1 describes motivations for the study in more detail. Section 2 discusses the state of the art for wireless networking and each of the currently-accepted standards for encryption schemes. Section 3 describes the methodology and implementation of wireless network surveys, and the various areas in which they were performed. Section 4 examines the results of these surveys, and section 5 discusses related work in the field. Appendix A gives additional details about the areas selected for wireless surveys, and Appendix B contains statistics collected during the study.

1.1 Motivation

While there have been large-scale surveys of wireless network use in many cities [1],[2],[3], there are no such studies for Minneapolis or St. Paul currently published. Statistics on wireless use are generally gathered only for small areas, with the only wide-scale statistics being collected by private “wardrivers”, and not made publicly available. With Minneapolis and St. Paul currently moving into a post-industrial economy, the use of wireless technology could be a very useful statistic for urban planners, businesses, and university researchers. For example, a proposed Minneapolis municipal wireless network would cover 59 square miles and service over 150,000 households [4]. Similar projects have been proposed for St. Paul and outlying suburbs. In order to estimate cost recovery for such a project, planners could find it useful to know the numbers of Twin Cities residents already using wireless networks. Planners would also be interested in specific neighborhoods whose residents are likely to adopt such technology

The use of WiFi among different populations is also an interesting factor to consider. While overall use of wireless networks may be income-dependent, research conducted by Hottell, Carter, and Deniszczuk [1] indicated that encryption use is largely unrelated to household income. Their work shows that the default settings on consumer WiFi hardware is a bigger factor. Thus far, the relationship between encryption use and regional zoning has largely been ignored. Such a comparison could show whether individual, commercial, or institutional networks are more likely to use encryption, and which types of users seem to be using "good" vs "poor" encryption methods.

Rooftop scanning was preferable to traditional "Wardriving" (scanning from a moving vehicle), since it can cover well-defined wide areas in a short time. Sites can be selected which exemplify a certain type of land use, economic prosperity, or other interesting characteristics. Commercial wireless ISPs usually attempt to locate access point nodes on tall buildings for greater coverage, so by scanning from locations which are potential antenna sites, we can show estimated existing usage in the vicinity of each site. Many of the sites visited are already equipped with microwave, UHF, and VHF repeaters for various services, as they are usually the highest points in a given area. It is interesting to note that other studies such as [2] have used similar methods of high-altitude surveying to cover large areas.

One potential drawback is that high-elevation scanning may detect long-range wireless links from directional antennas outside the target area. Such signals would be blocked by trees or buildings during traditional surface wardriving. However, nearby neighborhood signals which would also be blocked tend to be more "visible" from above the target area, and so the benefits are considered to outweigh the potential for contamination by outside signals.

2. The State of WiFi Security

The most common security measure for 802.11 networks is data encryption using one or more protocols. Encryption can provide multiple layers of protection by requiring clients to posses a secret key in order to read network content . To many institutional users, encryption such as WEP is implemented solely to prevent unauthorized use of network bandwidth. Encryption also provides an implied firewall between outsiders and local area networks which might not otherwise separate their wireless and wired elements. Data privacy from passive eavesdroppers is the most basic layer of projection, but sometimes the most overlooked. A user with the correct wireless credentials (encryption key) is assumed to have the same insider access as a desktop or laptop user plugging into the LAN. Such access allows one to eavesdrop on other users, inject malicious or spoofed data into the network, or attempt to escalate access through insecure systems. Passive-only adversaries can gather wireless packets undetected with almost any consumer client hardware and easily-obtained software.

Many "open" (unencrypted) systems use a layer of security between the wireless access point and the rest of the network. Such systems can include firewalls for protocol filtering, proxies and authentication services for access control, and payment verification servers for on-demand access to public networks. While such systems can prevent unauthorized users from using network resources directly, they do not prevent eavesdropping on plaintext packet data transmitted over the wireless network. If users exchange sensitive data over insecure channels, they risk giving away information such as passwords, email messages, or records of online activity.

Unencrypted networks with some other form of authentication can be compromised via "Phishing", or impersonating a legitimate service to solicit information from a user. An attacker could trick users into providing him with their access credentials by configuring a client or access point to pose as a legitimate access point. By impersonating the real login screen from an HTTP server, he could then gather passwords from deceived users.

Another method of protecting wireless networks is to "cloak" or attempt to hide the existence of an access point. This is done by disabling broadcast packets, which access points use to advertise their existence and identity to clients. Clients must then be pre-configured to use the known SSID, since they cannot select it through the typical discovery process. When used alone, such a method is akin to security by obscurity, and does not provide much protection in typical use. When clients are communicating with a cloaked access point, their packets are just as visible as any other, and can reveal the existence of the network to a passive eavesdropper.

While many wireless users are unaware of the potential for eavesdropping on open networks, others are apparently unaware of the potential for eavesdropping and phishing on poorly-implemented encryption systems (described in this section). From the results laid out in section 4, it is obvious that a large percentage of users are trusting the flawed Wireless Equivalent Privacy standard for either access control, data privacy, or both.

The next parts of section two discusses the original WEP encryption specifications for 802.11 networks, some of the identified weaknesses and attacks on WEP, and replacement encryption methods and their vulnerabilities.

2.1 WEP Standard

When initially developed, the 802.11 family of wireless protocol standards did not natively offer encryption or routing robustness. The decision was made to develop a "Wired Equivalent Privacy" (WEP) system, in which data packets would be encrypted to protect user data from eavesdropping, checksummed to provide integrity, and authenticated for access control [5]. Under WEP, stations (wireless nodes) share a common secret key, known as the root key (Rk). Network packets are encrypted with a one-time key consisting of a unique per-packet initialization vector (IV) concatenated with the root key. The IV is transmitted in cleartext at the beginning of the packet, and the receiving station uses this with the shared key to perform packet decryption. The shared key can be generated a number of ways, including manually, randomly, and algorithmically based on a human-memorable passphrase to simplify setup. The encryption method used is the RC4 stream cipher [6].

Despite being based on a number of proven cryptographic techniques, the initial design of WEP had a number of implementation flaws. Fluhrer, Mantin, and Shamir (FMS) [6] were the first to identify and publish the insecurities in WEP's use of the RC4 algorithm. Stubblefield [5] later demonstrated a practical attack based on these weaknesses. From his research, a number of user-friendly exploits and WEP cracking utilities arose, leading to the widespread loss of WEP effectiveness. While most online cracking tools offered a variable rate of success based on platform-specific WEP implementation and key strength, Newsham [7] demonstrated a slower but more effective offline brute-force attack. Other attacks such as chosen-plaintext showed mixed practical success, but demonstrated additional problems with the standard.

In (2005), Klein [8] developed an improved attack on RC4 as it is used in WEP, and in 2007 a new practical exploit was published by Tews et all [9]. Due to these developments, the Wireless Equivalent Privacy standard is essentially worthless for masking content or controlling access on 802.11 networks. Attacks are very fast when using active methods described by Klein, but slow passive scanning can eventually recover keys while remaining invisible to network intrusion detection systems.

2.2 First Generation WEP attacks

The first-generation WEP attacks took advantage of two major weaknesses in the system. First, the Key Scheduling Algorithm (KSA) used for RC4 encryption generated a large number of output key bits based on a small subset of the initial secret key. This “Invariance weakness” led to easily-guessable patterns in the per-packet keys used between network stations. The second weakness followed from the use of Initialization Vectors for one-time keys. Because part of each packet's key (the IV) is visible in plaintext, observing a large enough sample of IVs and encrypted messages gives attackers a basis from which to re-derive the secret key [6].

Attacks based on the IV weakness are passive ciphertext-only, relying on "resolved" IVs (those which put the KSA into a known state). Each resolved IV leaks information about one secret key byte, and an attacker must correctly guess the current byte before guessing later bytes. A large sample of IVs allows better guesses, and a higher probability of correctly guessing the current byte [5]. Invariance weakness attacks use limited-scale brute force methods based on related-keys. A period of information gathering collects data based on IVs, and a brute force attack is then used on each word of the key [6]. Each of these attacks works faster than pure brute force. The complexity of the IV attack scales linearly with key size (and so is faster for the original 40 bit key standard), while the complexity of the Invariance attack is independent of key size. Because these attacks rely on passive monitoring to collect a suitably large IV sample, the time necessary to crack a given key is dependent on the network activity (the amount of encrypted traffic available).

2.3 Second Generation WEP attacks

The latest methods of WEP cracking use active packet injection and more efficient key-recovery methods to decrease the time and traffic requirements. While the FMS attack typically requires a sample of IV's greater than 1,000,000, Tews' method needs only 40,000 packets to achieve roughly 50% probability of key recovery. A success rate of 95% requires approximately 85,000 packets. The improved efficiency can allow faster recovery when using a passive observtion method, but by actively re-injecting (Replaying) ARP packets, an attacker can force network nodes into generating the necessary volume of traffic in a period of several minutes [9].

Klein's recent RC4 attack improves key recovery by looking at known patterns in ARP packets. This allows key recovery with a smaller number of packets by deriving part of the key stream each time. When combined with the cleartext IV, this extra data makes limited brute force much more accurate with fewer bad guesses for key bytes. In addition, Klein describes an alternate method which does not require waiting for "weak" IV states, but uses new insights into the pseudo-random key generation used by RC4 to improve guesses about key data. As such, both known-ciphertext and ciphertext-only attacks have become more efficient [8].

2.4 WPA TKIP Encryption

As details of WEP insecurity began to emerge, the WiFi Alliance (the agency responsible for developing wireless standards) developed WiFi Protected Access as an interim solution. While the AES algorithm was generally identified as a more secure encryption method than RC4, it was too computationally intensive to be backwards-compatible with existing hardware. WPA was instead implemented as a quick fix until new standards based on stronger protection methods could be finalized. WPA continues to use RC4 for encryption, but increases key length, IV length, and uses IV sequencing and key rotation to prevent packet replay and dictionary-type attacks. WPA also adds some spoofing and packet tampering protections. Most legacy router and access point products can be upgraded to utilize WPA via firmware patching [10].

WPA offers two modes, both using Temporal Key Integrity Protocol (TKIP). The "Enterprise" mode uses an authentication server and per-user keys. "Personal" mode (aka WPA-PSK) uses a pre-shared secret key similar to WEP. In 2004 it was shown that WPA-PSK was vulnerable to key recovery attacks. Although there are so far no published exploits against enterprise-mode WPA networks, they are assumed to be less common than PSK networks due to setup complexity [11].

2.5 WPA2 CCMP encryption.

The long-term replacement for WEP and WPA developed by the WiFi Alliance is alternatively called WPA2, 802.11i, and WPA-CCM. WPA2 is intended to support legacy WEP and WPA equipment while ultimately replacing them with a system considered to be much more reliable and secure. WPA2 uses the Advanced Encryption Standard (AES) algorithm, which is stronger and more complex than RC4. This implementation of AES uses the CCMP security protocol, which computes message integrity checks and message authentication codes using cipher block chaining. Keys are computed using a hierarchy similar to TKIP, where initial administrative keys are used to derive pairwise and session keys. Session keys are generated through a 4-way handshake between client and access point, and can be based on shared keys assigned by an authentication server or by older encryption protocols and distributed via Extensible Authentication Protocol (EAP-TLS) [12].

WPA2 has been formally evaluated and shown to be secure against key recovery in enterprise mode, but vulnerable to DOS attacks under certain circumstances [13]. This is a relatively minor concern, as a dedicated attacker could cause a general DOS simply by jamming the radio frequencies assigned to chosen 802.11 channels. A larger concern is that WPA2 in PSK mode is just as vulnerable as the original WPA to hash attacks if weak keys are used.

2.6 WPA attacks.

In PSK mode, WPA and WPA2 secret keys are created based on user-entered passphrases. These keys and other network-specific variables such as the SSID are used to create pairwise master keys (PMK) between access points or routers and client nodes. Session keys are then created by hashing the PMK many times. The system is intended to introduce additional entropy (randomness) into the key generation, eliminating some of the predictability of WEP keys. However, for short passphrases of low initial randomness (IE, human-memorable passphrases), it has been shown that the eventual session keys are vulnerable to hash-comparison dictionary attack for both TKIP and CCMP. Once recovered, the session keys can then be used to derive the PMK and then the PSK, since the other variables can be obtained from the network. While cracking tools for WPA are still somewhat primitive, they are easily available and usable by attackers of modest experience [10].

Pre-compiled dictionary hashes can make offline brute-force cracking of weak keys very fast, although inefficient in storage space for large keyspace coverages. Human-memorable passphrases shorter than

20 characters and having low entropy can be reverse-engineered from the resulting weak session keys, which can be recovered from analysis of the authentication handshake messages and cracked offline. To maintain security in WPA or WPA2 with PSK, the network must be configured with strong initial shared keys, longer than 20 characters and using a high degree of randomness to prevent dictionary attacks [14].

3. Implementation

This section discusses the methods used for collecting wireless network statistics, the scan sites used, and the selection criteria for sites.

3.1 Scan Procedure

The raw data for this study was gathered through a series of on-site surveys around the Twin Cities. Hardware used for 802.11 scanning consisted of a laptop with a Symbol Technologies LA-4121 Spectrum24 PCMCIA card. An external cylindrical waveguide antenna was connected via low-loss pigtail. Data was collected with the Linux application Kismet, run under the Backtrack 2 live CD distribution. Log files were saved to a flash card for later analysis. Other client cards and software were tested but proved to be incompatible with Linux, or suffered from other problems. Kismet uses both active and passive scanning to find the maximum number of networks within range. Active scanning sends out probes requesting a connection, and passive scanning receives SSID broadcasts and packet data from clients and access points.

Repeat scans were conducted from building rooftops in the regions listed in section 3.3. To maximize repeatability for scan locations, several consistently-accessible rooftops were chosen. In addition, several locations were chosen for one-time scans due to unreliable access. (For example, downtown skyscraper roofs can sometimes be visited via social engineering, but this method does not always work twice). The single-scan locations are listed in section 3.4. Figure 1 shows the approximate locations of all scan sites used.

At each site, the directional antenna was rotated through 360 degrees in both horizontal and vertical orientations to maximize coverage. The majority of access point antennas are assumed to be positioned with vertical polarity (and thus provide a stronger signal to client antennas in the same orientation), but some are given horizontal polarity due to mounting methods or other factors. For high-angle locations such as urban canyons with nearby low-altitude signal sources, the antenna was also swept through various angles between the horizon and ground. At the Minneapolis campus of the University of Minnesota, two scans were necessary to cover the entire area, and results were combined to eliminate duplicate hardware addresses.

All scans were conducted with the same 802.11 hardware and software, using the same technique. While better equipment became available which could have increased the effective range of later scans, consistent methodology was preferred in order to maintain consistent statistics.

An issue that became apparent during repeat scans was that a number of unpredictable factors influence the "visibility" of a given network. Changed access point locations, rearranged furniture, number of users on the same channel, or even open doors and windows can all alter the signal strength reaching the scan site, meaning that changes in network density and encryption statistics over time do not necessarily indicate an increase or decrease in actual use. We attempted to look more closely at the repeat results, to determine if individual access points had changed their security methods during the survey. Those findings are reported in the results section.

3.2 Site Selection

Wireless survey sites were chosen to reflect a diverse range of land uses and economic prosperity levels. In several cases there were overlaps in zoning, but efforts were made to chose representative samples from primarily industrial and commercial areas, as well as low, medium, and high-income residential neighborhoods. The approximate coverage areas of each scan are shown in figure 1. Not every detected network can be guaranteed to be within the socioeconomic boundaries of a particular neighborhood, but it is assumed that most networks detected in a certain area are located in or near that area. Land use maps for each scan site are available in appendix A. In some cases, the boundaries of city planning districts and census areas were different than the coverage areas available from scan sites in those neighborhoods. In such cases, I have made every effort

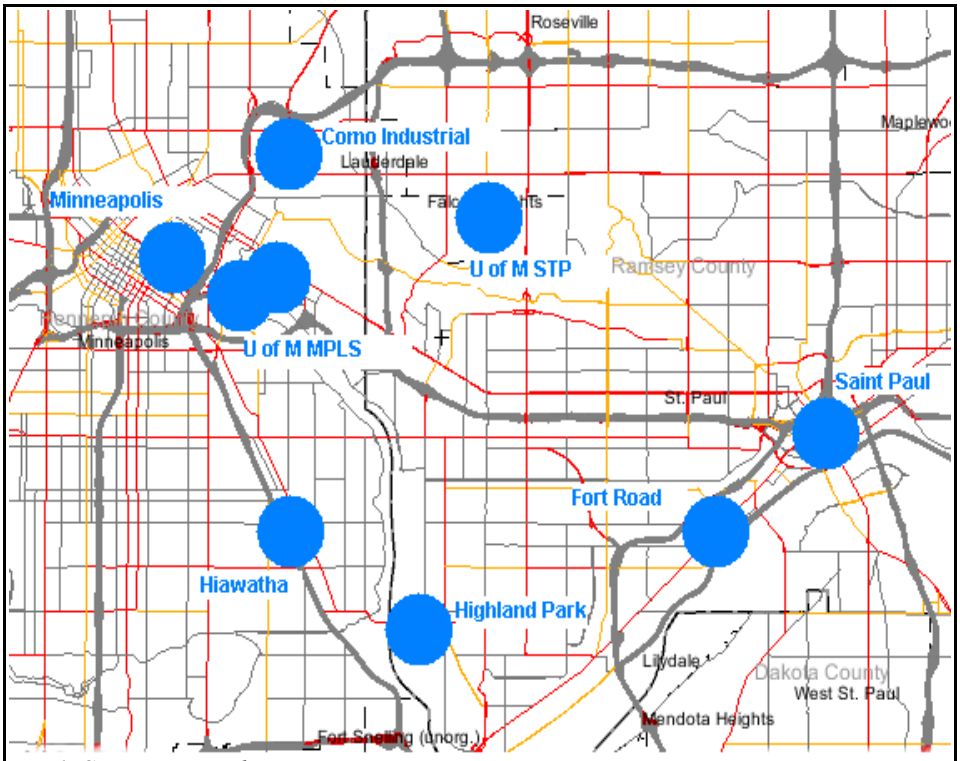

Fig 1. Scan areas and approximate coverage.

to identify discrepancies and suggest factors which could lead to the observed differences.

Target areas for this study required elevated locations where a directional antenna could detect a wide range of access points. These high points also had to be far enough apart to prevent significant overlap from adjacent sample areas. Fortunately, there are enough abandoned or otherwise accessible rooftops in the Twin Cities to support such conditions. Rooftop survey positions included university office and research buildings, abandoned grain elevators, downtown office towers, and vacant industrial buildings.

Efforts were made to avoid potential legal complications. Minnesota law states that a person is not trespassing on a property unless they force entry, ignore posted signs, or ignore requests to leave. By accessing sites in ways which did not encounter signs or barricades, no laws were broken. Only once was I asked to leave a rooftop by building staff, unfortunately before completing a survey at that location.

3.3 Repeated Survey locations and demographics

Those sites at which repeated surveys were made are listed first. Sites which had only a single scan performed are listed in section 3.2.

Downtown Minneapolis.

This survey was conducted near the Mill City Museum on the Northeast edge of downtown Minneapolis. According to the Metropolitan Council [15] this area consists primarily of commercial businesses as well as dense residential housing. Firsthand observations note that many buildings in the vicinity of the scan site were residential condominium towers catering to wealthy residents.

As of early 2007 this eastern downtown area (especially the riverfront) included a number of under-construction housing projects which will serve primarily high-income residents. Many of the blocks in this area indicated as "industrial" in the Metropolitan Council's land use maps (Appendix A, figure A.1) are in the process of being converted into housing. Existing conditions should be a good indication of the demand for, and use of, wireless Internet technology among future residents.

University of Minnesota, Minneapolis Campus.

This public university campus is oriented towards science and technology, business, language, medicine, and the arts. As mentioned before, this area required scans at two sites due to the geographically

divided nature of this campus. The Mississippi River separates the East and West bank buildings by approximately one-quarter mile and the tallest buildings by approximately three quarters of a mile, making a single high point ineffective at scanning wireless signals on both banks. To overcome this, statistics were gathered from the tallest building on each bank and later combined and filtered to eliminate duplicates visible from both sites. Most dormitories, research buildings, and classroom buildings were visible from the scan sites, as well as a significant number of nearby houses, apartment buildings, and businesses.

Residential properties in the area of this campus tend to be primarily multi-family rentals. Facilities are tailored to and priced for single or coupled students, usually in the low to middle income range. The 2000 Census indicated that 30-60% of families in the area are considered to be "low-income" or less than $31,800/year, which is a high ratio compared to the rest of Minneapolis [16]. Businesses within the coverage area are mainly targeted at students, and include coffee shops, fast food restaurants, bars, and light retail. It has been observed that the incentive for businesses to provide free wireless access is higher among a college population than elsewhere.

Highland Park, St. Paul.

In the absence of a single tall site, this survey was conducted from two relatively low locations to maximize coverage of affluent neighborhoods. As with the U of M, scan data was combined to eliminate duplicates. The first location was a public park on top of the Highland reservoir. A nearby water tower would have offered optimal coverage, but was avoided for legal reasons. While line-of-sight from the reservoir included most of the Twin Cities metro area, actual WiFi signal coverage was somewhat limited due to the greater-than-average concentrations of trees around nearby homes. A nearby public building with an accessible roof was also used as a scan platform, and offered coverage of some houses otherwise blocked by vegetation.

Highland Park is primarily high-income single-family homes in the area studied. The neighborhood as a whole also includes some mixed income housing, with industrial development limited to one vehicle assembly plant (Ford Motor Co). Commercial use is light and includes restaurants and small retail stores. Several private colleges are located near the survey site [15]. Median income for the area was $47,217 in 1999, with 29% of households earning above $75,000 a year. Among residents age 25 or older, 92% had a high school education and 71% had at least a 4-year college degree [17].

Fort Road / West Seventh Neighborhood, St. Paul.

The low-income Fort Road neighborhood extends along West Seventh street from downtown St. Paul to the Highland Park area, and is sandwiched between the Summit Hill neighborhood and the Mississippi river. The area saw a great deal of industrial use in the recent past, but economic decline has followed the close of most manufacturing in the area.

Scans for this neighborhood were conducted from the roof of a vacant industrial building, and encompassed mostly single-family homes and small rental properties. Existing industrial use is limited to bulk storage. Commercial use is limited to restaurants, bars, and small retail stores. Wilder Research, contracted by the city of St. Paul, reported that this area had a median income of $34,363 in 1999. They also show 83% of residents over age 25 with a high school education and 27% with at least a 4-year degree [17]. The potential for economic growth in this area is currently in question, although attempts are underway to develop former manufacturing sites into housing and retail space.

3.4 Additional survey sites.

In addition to the areas above, several locations around the Twin Cities Metropolitan Area were each visited once during the period of this research. Those sites are described below.

University of Minnesota, St. Paul Campus.

This branch of the University of Minnesota is technically located in the suburb of Falcon Heights. Research and instruction is oriented towards agriculture, biology, and veterinary studies. Large tracts of the campus are devoted to crop research, and the campus abuts the Minnesota State Fairgrounds. Land use off-campus is primarily light rental residential, with very little commercial use in the immediate vicinity (see figure A.5). Nearby neighborhood income is likely comparable to the Minneapolis campus due to student rentals, although the entire suburb of Falcon Heights had a higher median income of $51,382 in 2000 [18].

The scan for this area was done on the highest roof on campus (excluding water towers), and encompassed the majority of classroom and research buildings. A few residential buildings on campus were also visible from the scan site, but line-of-sight to most dormitories was blocked by other structures.

Hiawatha Neighborhood, Minneapolis.

Similar to the Fort Road neighborhood in St. Paul, this area was previously a major industrial and transportation corridor, and at first glance appears to be in the same state of economic decline. At the present time there are only two large industrial users operating in the area (grain mills), as well as a spur line of the Minnesota Commercial Railroad. The neighborhood is almost entirely low and medium-income single-family homes, as shown in figure A.6. Most industrial sites shown along the Hiawatha rail corridor are vacant or abandoned, one of which provided an ideal scan location.

The scan coverage included areas of the Hiawatha, Howe, and Standish neighborhoods. Income statistics for this region show an interesting skew due to the boundary locations of these districts. According to the 2000 census, median household income for Hiawatha was $43,912. Howe's median household income was $45,270, and Standish had a median of $45,031 [16]. These relatively high figures seem to conflict with the observed conditions at the intersection of the three neighborhood, but it should be noted that each includes expensive near-waterfront and parkfront properties along the Mississippi River and Lake Hiawatha.

The actual income for the area along the Hiawatha corridor is probably closer to that of the nearby Corcoran and Longfellow neighborhoods, which lack such desirable property. Year 2000 income for those neighborhoods was $33,393 and $34,156 respectively [16]. Educational background figures were not available.

Southeast Como / Mid-City Industrial Area.

The Mid-City Industrial Area is comprised of a redeveloped rock quarry between I-35W and Minnesota 280 north of Hennepin Avenue. A large core of light industry includes freight and shipping companies, warehouses, light manufacturing, recycling, and bulk material handling operations. Several former industrial buildings are being remodeled into residential and artist lofts, and the area is bordered by single and multi-family residences. Much of the housing to the immediate south (the Como neighborhood) is rental property catering to University of Minnesota students, typically offering lower rent than neighborhoods closer to the Minneapolis campus. This scan site included both the northern boundary of Como and the southern section of the Mid-City Industrial area, as shown in figure A.7.

Income statistics were not available for the Mid-City Industrial Area itself, as residential property was nearly nonexistent as of the 2000 census. Data on the Como neighborhood to the south was provided by the city of Minneapolis. This neighborhood had a median income of $33,895 in 2000, and approximately 15% of residents were in the $75,000+ income bracket [16].

Downtown Saint Paul.

The scan for this area was conducted from a relatively low (18 story) rooftop in the central business district. Despite social engineering attempts and a lack of effective access barriers, an earlier scan from a higher location was interrupted by building staff.

Saint Paul's downtown business district is not as developed as its counterpart in Minneapolis. Buildings tend to be older, and are either rental office space or mixed-use commercial and residential. A few newer buildings are devoted to single organizations. Many older buildings in the former business core have been converted to artist lofts or light-industrial work space. In general, there is no dominating economic use identifiable for this area, and almost every variation was observed in the immediate vicinity of the scan location. (see figure A.8)

Downtown St. Paul also has an apparent anomaly in demographic data as related to annual income. Wilder Research indicates that in 1999, the average household income was $29,359, and that only 13% of households earned more than $75,000 per year [17]. However, the geographic boundaries within which this data was collected include portions of low-income neighborhoods south of the Mississippi River [17]. The balance of the included region is light industrial and dense commercial zones with medium-income artist communities and relatively few high-income condominium residents. It is quite likely that the apparent prosperity level has been skewed in the direction opposite to that seen in the Hiawatha corridor neighborhoods.

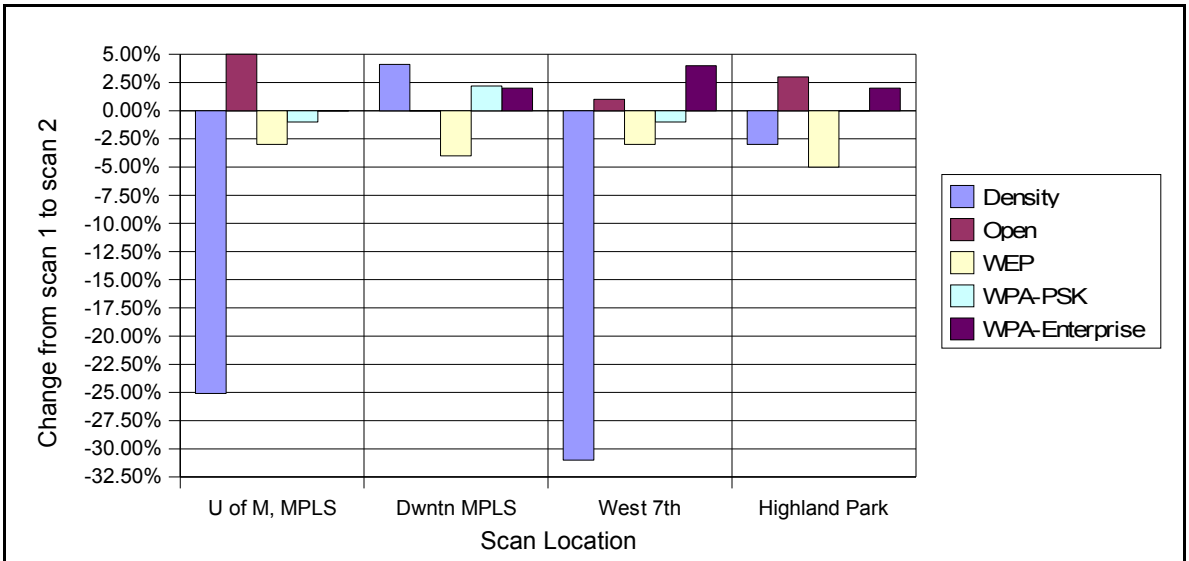

Fig 3. Changes observed at repeated scan locations

4. Data Analysis and Results

The collected statistics from single and repeated scans are given in Appendix B. In this section I will attempt to lay out generalized observations and comparisons of the results. All percentages are rounded to the nearest whole number. The combined totals for all areas are shown in figure 2.

4.1 Observed changes in network density and encryption.

The repeated scans produced varying changes in density as shown in figure 3. At Downtown Minneapolis, a slight increase in the number of access points (network density) was noted. As noted earlier, a change in the number of networks does not necessarily indicate an actual change in wireless use. This is especially apparent when considering fine-grained change at the individual network level, as discussed in the last part of this section.

At Highland Park there was a slight decrease in density, and at both the University of Minnesota, Minneapolis campus and the West Seventh neighborhood there was a marked decrease in available networks during the second round of scans. The University showed 25% fewer networks, and West Seventh had 31% fewer than observed initially. It seems unlikely that a large number of users would cease operation of their wireless networks on the University campus, but it is possible that many users switched to other connection methods in the approximately 6-week interval between scans. Likewise, it is possible that a large number of West Seventh users switched ISPs or simply stopped using wireless. It is also possible that interference from multiple networks on the same channels, or outside interference from some other RF microwave source, caused a drop in the number of networks visible.

When considering changes in encryption use, the U of M showed the largest change. During the second round of scans, 62% of the observed networks had no encryption at all, while the first scan showed 57% without encryption. Highland Park also had an increase in the number of open networks, changing from 30% to 33%. The West Seventh neighborhood showed the largest increase in the percentage of enterprise-level WPA, going from 11% to 15%. However, it must be pointed out that the actual number of observed WPA-enterprise networks in this area (8) did not change, merely the ratio between these and the total number of observed networks. The use of WEP appeared to decrease between 2% and 5% in every area. The use of WPA with pre-shared keys (the potentially insecure version of WPA) increased slightly in downtown Minneapolis and decreased slightly in West Seventh and at the U of M.

I attempted to look deeper into the apparent trends by examining individual networks which changed encryption standards in the interval between scans. At the U of M, Minneapolis, I found that two networks had changed from using no encryption to using WEP, and two had changed from WEP to none. All other networks were either unchanged, or appeared during only one of the scans. At West Seventh / Fort Road,

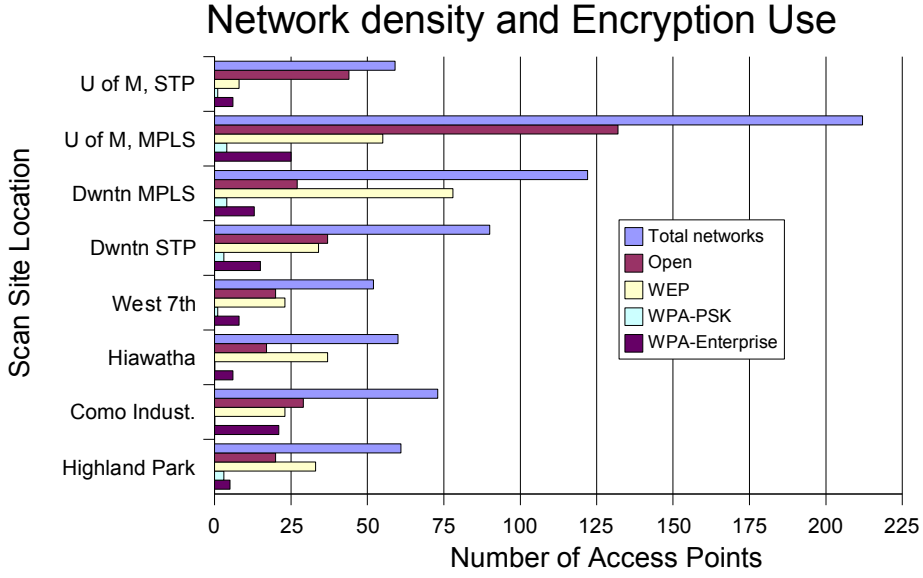

Fig 4.Results from most recent scans

one network changed from no encryption to WEP. In Highland Park, one network changed from using WEP to using WPA (enterprise mode), and in Downtown Minneapolis there was no change among networks observed both times. This leads me to believe that the change in overall statistics is due more to the change in number of observed networks, and is less related to actual changes over time.

4.2 Comparisons between Scan Areas.

As one might expect, the science and technology-oriented Minneapolis campus of the University of Minnesota offered the greatest wireless network density in the Twin Cities. The less technical St. Paul campus had significantly fewer networks available in the campus core, offering approximately the same density as typical residential neighborhoods. Downtown Minneapolis also showed a higher number of networks than St. Paul, likely due to the growing popularity of high-density residential property near the scan site. It is also worth noting that Minneapolis is currently testing a city-wide WiFi system, and that the test area lies on the southeastern boundary of Downtown. Nodes affiliated with this test system are named "USI Wireless", and appeared several times in scans from the downtown and university sites. Despite being around 50% industrial, the Southeast Como area had a high network density and a larger percentage of open networks than other residential areas, likely due to its student population.

Among mostly-residential areas, Hiawatha showed the highest percentage of WEP use, but West Seventh showed a slightly greater use of WPA-enterprise. Highland Park had the largest incidence of PSK WPA use. The University campuses had the highest percentage of unencrypted networks. There are several University-affiliated networks which include hundreds of unencrypted nodes requiring html-based authentication, but which do not protect data traffic against eavesdropping. Downtown Minneapolis showed the highest rate of encryption with only 22% open networks, although most users seem to prefer WEP over more secure standards.

When considered from an economic prosperity standpoint, it does not appear that average income is a significant factor in the adoption wireless technology as a whole. The number of networks seen in both high-income, medium-income, and low-income residential neighborhoods was nearly the same. While there were slightly fewer networks seen in West Seventh than elsewhere during the second scan, this neighborhood actually had more during the first scan than did Highland Park.

Stealthed networks appeared very rarely, once each in downtown ST. Paul, the Minneapolis campus of the U of M, Highland Park, and Southeast Como. It is possible that more cloaked access points exist in each area, as the apparent number of stealth networks is actually a factor of their network traffic. A stealthed network with no clients transmitting packets during the scan would not have appeared in the list of detected networks.

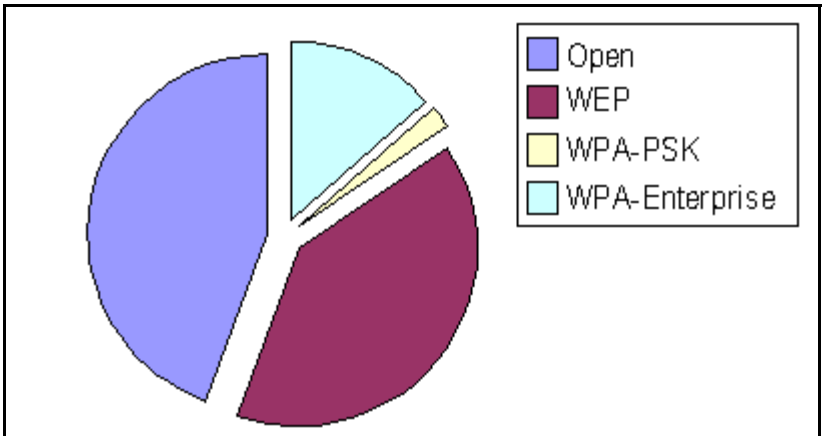

Fig 2.Combined totals from most recent scans (Out of 729 networks)

4.3 Conclusions

Annual income and education may be a factor in the use of wireless encryption, but precisely how is not readily apparent from these results. For those neighborhoods where education statistics were available, it appears that the wealthier and more educated Highland Park neighborhood was more likely to use WEP than was West Seventh. However, West Seventh showed a slightly higher tendency to use enterprise mode for WPA networks, while Highland Park used more of the less secure pre-shared key mode. Downtown St. Paul had about the same occurrence of enterprise-level WPA use as Minneapolis, but had far more unsecured networks, both in number and overall ratio (41%). This may be due to the generally smaller size and budgets of businesses operating in downtown St. Paul.

Non-broadcasting or cloaking access points did not seem to be a popular security measure. This is likely due to the relative inconvenience of accessing cloaked networks from clients, and the minimal benefit in terms of security and privacy.

As noted in section 4.1, apparent change in the interim between repeat scans may have little if any relation to real changes. If there was indeed a significant change in network density between each scan, the concurrent change in encryption use statistics may still be valid. However, if the density changes were due simply to more or fewer networks being visible, the encryption use statistics would be skewed towards the larger sample.

WEP remains disturbingly popular across all zoning types and income levels, as seen in figure 2. While the use of WEP encryption appeared to decrease slightly during the interval between repeat scans, it continues to account for 70% of all encrypted networks. From the data gathered, it appears that WPA is slowly replacing WEP, but the results are too preliminary and the changes are too small to be given much weight at this time.

The most surprising finding was that WPA networks in pre-shared-key mode are quite rare in the Twin Cities. The majority of users with WPA networks in all areas seem to be using enterprise mode with authentication servers. While WPA in general still makes up only 30% of encrypted networks, it appears that most users are willing to take the extra step of avoiding PSK mode to ensure higher security.

5. Related and Future Work

There have been a number of user interface studies to determine the difficulty of implementing wireless security measures [1],[19],[20]. Factors such as relative ease of encryption configuration and overall difficulty of using wireless networks are often considered. It would be very interesting to see the relative ease and prevalence of encryption use on various brands of consumer WiFi hardware as mentioned by Hottell [1]. Such a study was not performed as part of this research due to the repeat-task learning problem and the difficulty of finding a suitably diverse demographic sample within a limited area and time.

Wide-range wardriving surveys have been conducted in numerous cities, although rarely as a controlled academic study. A demographic comparison study similar to this was conducted in 2006 by Matthew Hottell [1]. Some informal studies such as [21] have combined wardriving with GIS data to produce context-

enriched maps of urban hotspots. Industry researchers and private consulting firms such as WirelessMaps.com [22] sometimes offer advice for wireless ISP placement based on demographic data as well as site geography and population density. In locations outside the Midwest that posses terrain and greater vegetation cover, geographic features are often as or more important than details of the population being served, but regardless, most providers will have a vested interest in the likelihood of residents to use their service.

A more detailed method for locating wireless network nodes can be performed via triangulation. A scanning system located in a vehicle and equipped with GPS can gather signal strength data from the same network in multiple locations, and calculate an approximate position based on the data. Such data can be used to find gaps in network coverage which could be due to poor access point placement. To date this method is not very accurate, with a margin of error estimated to be about 32 meters [23].

Advanced analysis of existing large-scale wireless networks can be useful as models for other networks, or as a basis for effective future expansion. Henderson et al discuss the evolution of just such a network at Dartmouth college in their series of network analysis papers. They provide a wealth of detailed information on changes in service and protocol usage trends, client types, and user mobility [24]. Data such as this would be vital to a commercial or institutional network provider who wished to tailor service performance to accommodate a large user base. It would be very interesting to see usage statistics and changes among different types of institutions such as hospitals and corporate offices.

Kim and Kotz discuss models of user mobility among access points, and the ability of networks to behave like cellular telephone systems in client-node hand off. They discuss the potential for tracking individual users via signal strength triangulation and packet routing, but note that gaps in coverage and connection delays inherent in most networks prevent precise single-client tracking over more than short time periods [25]. Gruteser and Grunwald discuss ways to avoid triangulation by clients wishing location privacy, primarily through the use of disposable address identifiers [26].

Other information which could have been gathered by a project such as this includes the number of access points with default administrative passwords left in place. This statistic should be independent of encryption use, as encryption assumes that an outsider cannot access the access point via HTTP in order to log into the administrative functions. With more location-specific data (street level wardriving) one can examine details of neighborhood "clustering" mentioned by Wei [27] or the ratio of hardware brands to encryption use discussed by Hottell [1].

6. Conclusion

This research shows that for prevalence of WiFi and use of encryption, land use and economic activities in an area are stronger determining factors than is local income. The results indicate that commercial and university areas have a higher density of networks, and that active business districts such as downtown Minneapolis have the highest percentage of encryption. Colleges and nearby student neighborhoods tend to have the most unencrypted networks. While WPA is becoming slightly more popular, and a surprising number of networks use the stronger enterprise-level WPA, the majority of encrypted networks are still using the insecure WEP standard. The difference between large-scale apparent changes and small-scale network-by-network changes show that data from repeated scans is not very accurate. WiFi remains too prone to interference and arbitrary signal strength factors to be reliably evaluated for change over time.

Works Cited.

[1] Hottell M., Carter D., and Deniszczuk M. (2006) “Predictors of Home-Based Wireless Security” In *Fifth Workshop on the Economics of Information Security*, University of Cambridge, England, June 26-28

[2] Professional Information Security Association (PISA), and Hong Kong Wireless Technology Industry Association (WTIA) (2003) “Report on Wireless LAN Wardriving Survey 2003 Hong Kong” www.pisa.org.hk/projects/wlan2003/wd2003full.pdf

[3] RSA Seccurity Inc. (2003) “The Wireless Security Survey of London” Z/Yen ltd. www.zyen.com/Knowledge/Research/The Wireless Security Survey of London.pdf

[4] City of Minneapolis (2007) “Wireless Minneapolis” www.ci.minneapolis.mn.us/wirelessminneapolis/

[5] Stubblefield, A., Ioannidis, J., and Rubin, A. D. (2004) “A key recovery attack on the 802.11b wired equivalent privacy protocol (WEP) In *ACM Transactions on Information and System Security (TISSEC)* v.7 no 2. May. Pp319-332

[6] Fluhrer, S. R., Mantin, I., and Shamir, A. (2001) “Weaknesses in the Key Scheduling Algorithm of RC4” In *Revised Papers from the 8th Annual International Workshop on Selected Areas in Cryptography SAC '01*August, Springer-Verlag.

[7] Newsham, T. (2001) "Cracking WEP Keys". Presentation: Black Hat 2001. www.blackhat.com/presentations/ bh-usa-01/TimNewsham/bh-usa-01-Tim-Newsham.ppt

[8] Klein, A. (2006) “Attacks on the RC4 Stream Cipher” Submitted to *Designs, Codes, and Cryptography 2007.*

[9] Tews, E., Weinmann, R-P., and Pyshkin, A. (2007) “Breaking 104 bit WEP in less than 60 seconds”*Cryptology ePrint Archive, Report 2007/120* http://eprint.iacr.org/

[10] Bergnel, H., and Uecker, J. (2005) “WiFi Attack Vectors” *Communications of the ACM* August. v48, no8.

[11] MacMichael, J. (2005) “Auditing Wi-Fi Protected Access (WPA) Pre-Shared Key Mode *Linux Journal Online* July. http://www.linuxjournal.com/article/8312

[12] He, C., and Mitchell, J.C. (2004) “Analysis of the 802.11i 4-Way Handshake” *Proceedings of the 2004 ACM workshop on Wireless security* pp 43-50. New York, ACM Press.

[13] He, C., Sundararajan, M., Datta, A., Derek, A., and Mitchell, J.C. (2005) “A Modular Correctness Proof of IEEE 802.11i and TLS” *Conference on Computer and Communications Security* pp2-15. New York, ACM Press.

[14] Moskowitz, R. (2003) “Weakness in Passphrase Choice in WPA Interface”*Wi-Fi Net News* November 4. http://wifinetnews.com/archives/002452.html

[15] Metropolitan Council (2007) “Land Use in the Twin Cities Region” *GIS at the Metropolitan Council* http://gis.metc.state.mn.us/

[16] City of Minneapolis (2007) “Minneapolis Census 2000 Information” Census Bureau www.ci.minneapolis.mn.us/citywork/planning/Census2000/

[17] Wilder Research Center (2007) “Saint Paul Neighborhood Census Facts” *Community Dataworks, an online data service of Wilder Research Center* http://www.communitydataworks.org/StPaul/data.php

[18] Leauge of Minnesota Cities (2007) “Census 2000 Update: Expanded Minnesota Profiles” LMC Research and Analysis http://www.lmnc.org/census/census.cfm

[19] Kuo, C., Perrig, A., and Walker J. (2005) "Designing an Evaluation Method for Security User Interfaces: Lessons from Studying Secure Wireless Network Configuration" *Interactions* May/June. New York, ACM Press.

[20] Kuo C., Goh V., Tang A., Perrig A., and Walker J. (2005) "Empowering Ordinary Consumers to Securely Configure Their Mobile Devices and Wireless Networks". *Carnegie Mellon CyLab Technical Report CMU-CyLab-05-005*. February 5.

[21] Gomes, Lee (2004) "San Francisco 94110 Is Really a Hot Spot, My Wi-Fi Tour Shows" *The Wall Street Journal*, May 24.

[22] Webster, B. (2006) "Applying Radio Frequency (RF) engineering as part of your business plan" *Wireless Broadband Internet System Whitepapers*. Wirelessmapping.com.

[23] Kim M., Fielding J., and Kotz D. (2006) "Risks of using AP locations discovered through war driving"In *Proceedings of the Fourth International Conference on Pervasive Computing (Pervasive)*, pp 67-82, Dublin, Ireland, May. Springer-Verlag.

[24] Henderson T., Kotz D., and Abyzov I. (2004) "The Changing Usage of a Mature Campus-wide Wireless Network". In *Proceedings of the Tenth Annual International Conference on Mobile Computing and Networking (MobiCom)*, pp 187-201, September. ACM Press.

[25] Kim M., and Kotz D. (2005) "Modeling users' mobility among WiFi access points" In *Proceedings of the International Workshop on Wireless Traffic Measurements and Modeling (WiTMeMo '05)*, pp 19-24, June. USENIX Association.

[26] Gruteser M., and Grunwald D. (2005) "Enhancing Location Privacy in Wireless LAN through Disposable Interface Identifiers" *ACM Mobile Networks and Applications (MONET),* Vol 10, pp 315-325.

[27] Wei, R. (2006) "Wi-Fi powered WLAN: When built, who will use it? Exploring predictors of wireless Internet adoption in the workplace". *Journal of Computer-Mediated Communication,* 12(1), article 5.

References used but not cited in text.

Jones, R. Kipp and Ling Liu. "What Where Wi: An Analysis of Millions of Wi-Fi Access Points" *GIT-CERCS-06-10* Georgia Institute of Technology 2006.

Majstor, F. (2003) "WLAN Security Threats & Solutions" In *Proceedings of the 28th Annual IEEE international Conference on Local Computer Networks* (October 20 - 24, 2003). LCN. IEEE Computer Society, Washington, DC, 650.

Bittau, A, Handley, M, and Lackey, J. (2006) "The Final Nail in WEP's Coffin"In *2006 IEEE Symposium on Security and Privacy,* May, p386-400

Gurkas, G.Z. Zaim, A.H. And M.A. Aydin (2006) "Security Mechanisms And Their Performance Impacts On Wireless Local Area Networks" *IEEE 2006 International Symposium on Computer Networks* June, p1-5

Wi-Fi Alliance (2004) "WPA™ Deployment Guidelines for Public Access Wi-Fi Networks" http://www.wi-fi.org/knowledge_center_overview.php?docid=4484

Miller, Sandra K (2001) "Facing the Challenge of Wireless Security", *Computer*, vol.34, no.7, pp. 16-18, Jul.

Appendix A. Land Use in Scan Areas.

Each of these maps shows land use (as of 2005) in the approximate area surrounding each scan site. The maps do not indicate the coverage or range of wireless signals. Actual coverage in the regions shown is impossible to estimate accurately due to factors such as urban canyoning and interference from other radio signals. These maps are intended only as a rough guide to nearby land use. All maps are based on Metropolitan Council GIS data, available from [15].

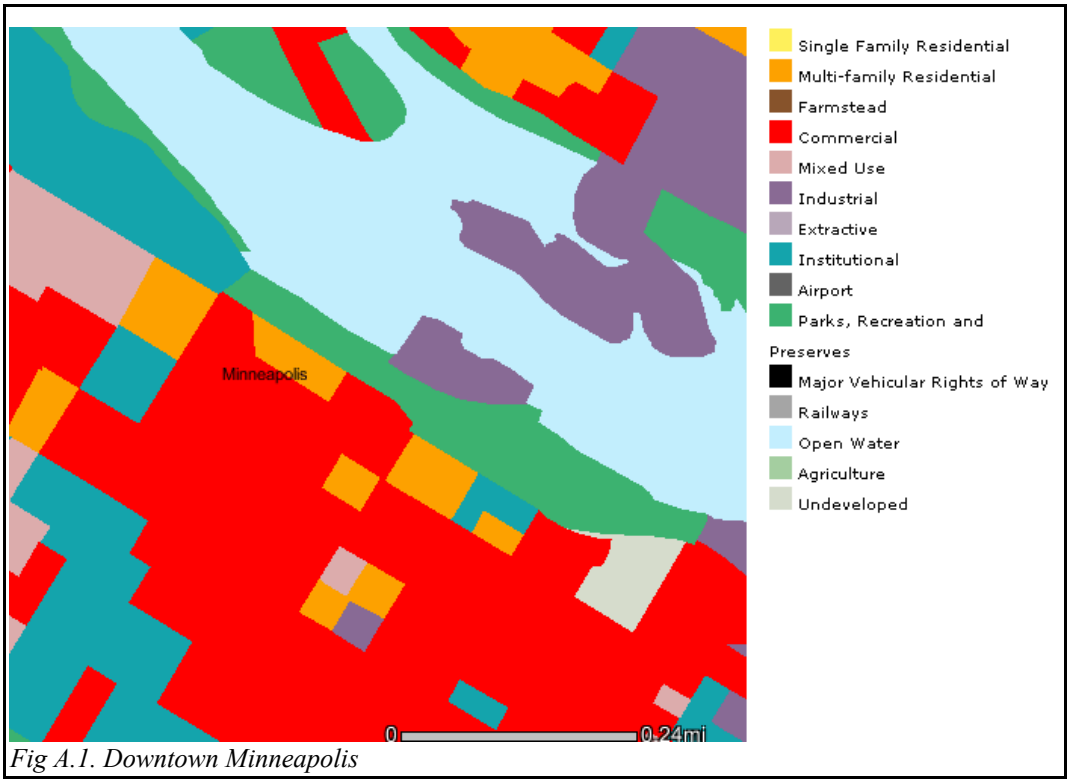

Fig A.1. Downtown Minneapolis

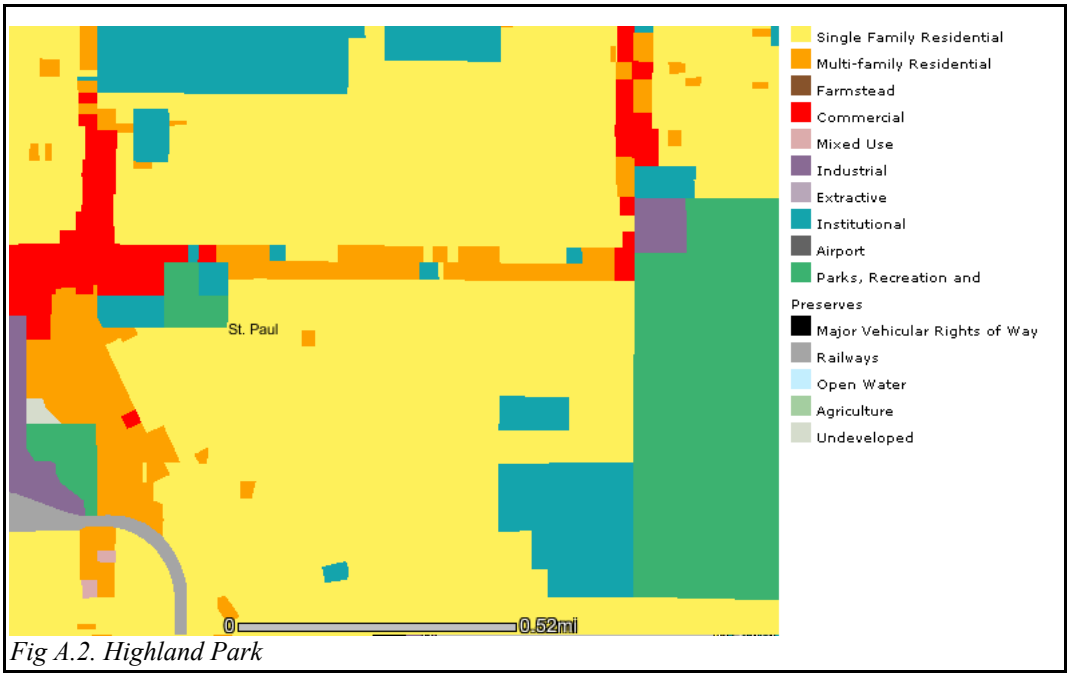

Fig A.2. Highland Park

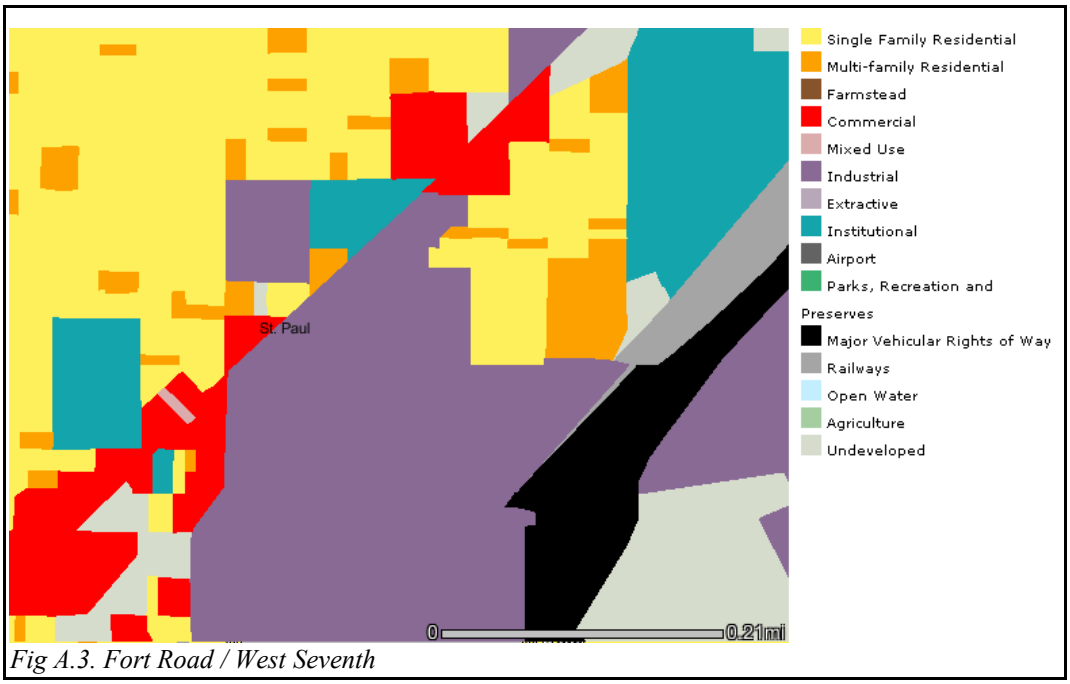

Fig A.3. Fort Road / West Seventh

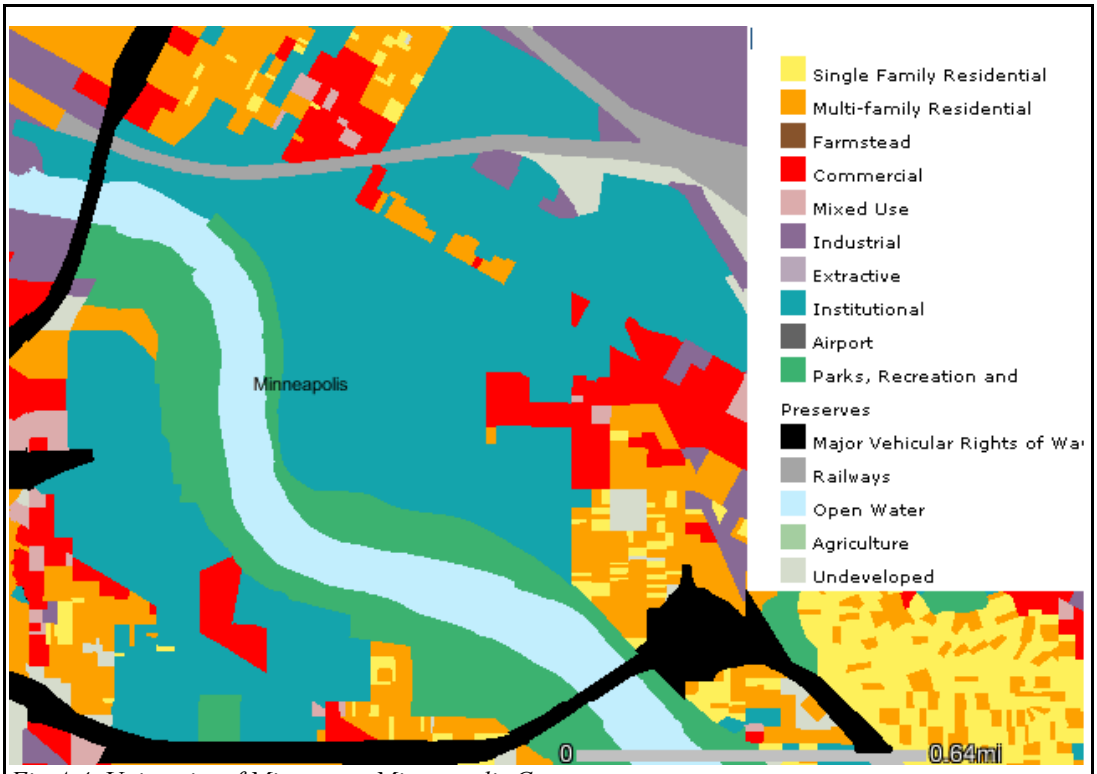

Fig A.4. University of Minnesota, Minneapolis Campus

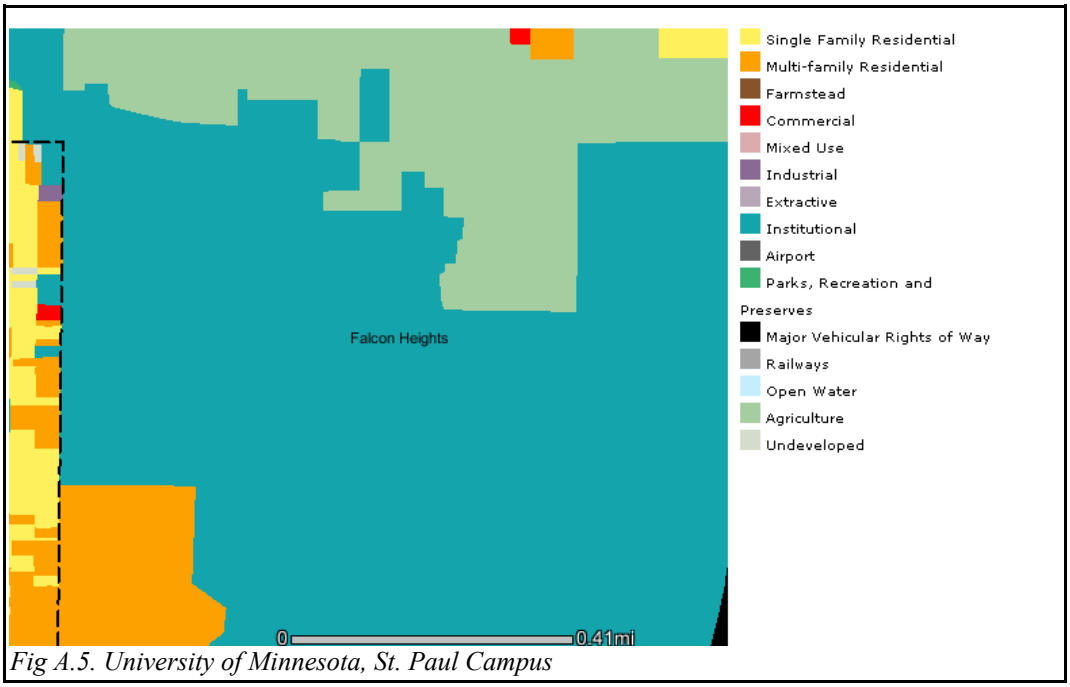

Fig A.5. University of Minnesota, St. Paul Campus

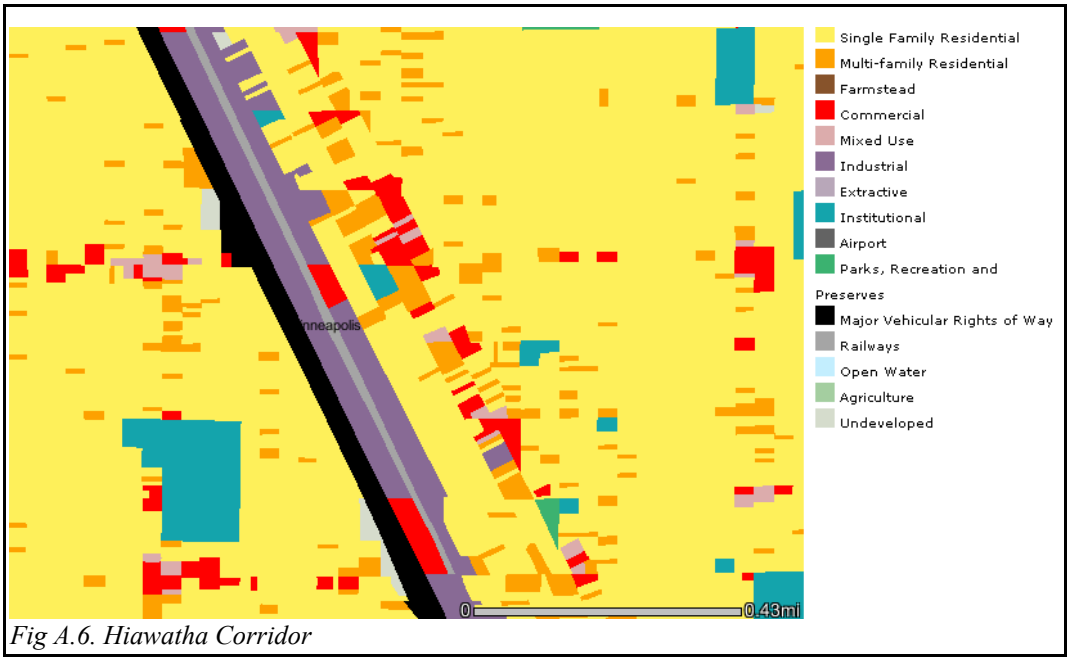

Fig A.6. Hiawatha Corridor

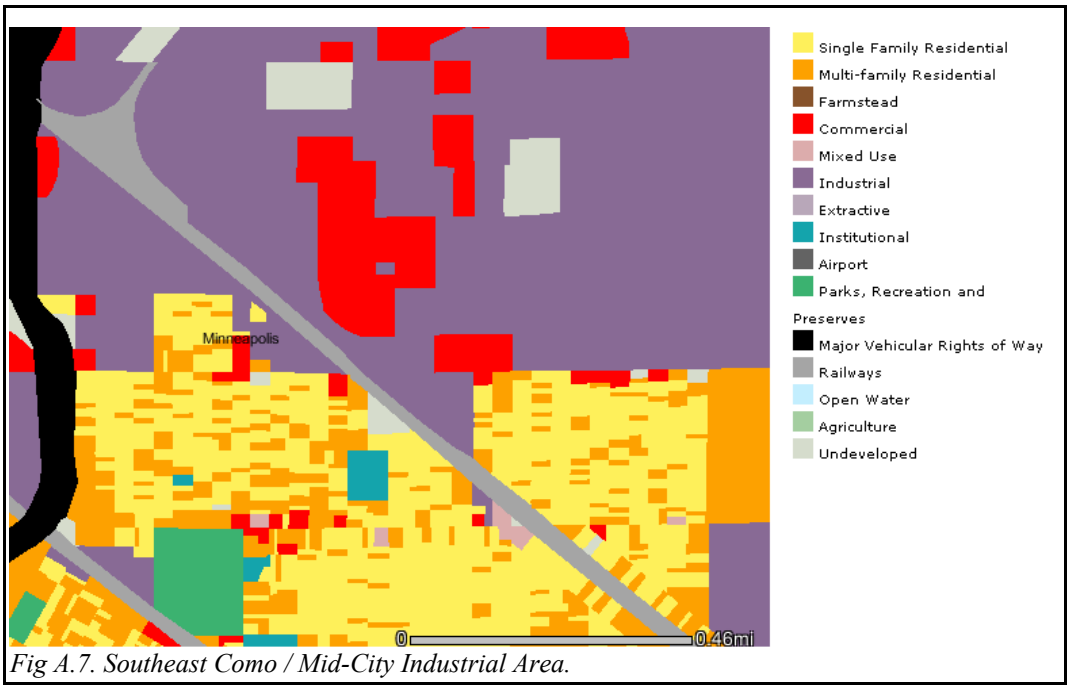

Fig A.7. Southeast Como / Mid-City Industrial Area.

Figure A.8. Downtown St. Paul

Appendix B. Scan Statistics

Site	Data from most recent scans				
	Total networks	Open	WEP	WPA-PSK	WPA-Enterprise
U of M, STP	59	44	8	1	6
U of M, MPLS	212	132	55	4	25
Dwntn MPLS	122	27	78	4	13
Dwntn STP	90	37	34	3	15
West 7th	52	20	23	1	8
Hiawatha	60	17	37	0	6
Como Indust.	73	29	23	0	21
Highland Park	61	20	33	3	5

		Scan Location			
		U of M, MPLS	Dwntn MPLS	West 7th	Highland Park
Scan 1					
	Total networks	283	117	75	63
	Open	160	26	28	19
	WEP	82	79	35	37
	WPA-PSK	8	1	2	3
	WPA-Enterprise	33	11	8	4
Scan 2					
	Total networks	212	122	52	61
	Open	132	27	20	20
	WEP	55	78	23	33
	WPA-PSK	4	4	1	3
	WPA-Enterprise	25	13	8	5

		Percentage difference between scan 1 and scan 2.			
	Density	Open	WEP	WPA-PSK	WPA-Enterprise
U of M, MPLS	-25.10%	5.00%	-3.00%	-1.00%	0.00%
Dwntn MPLS	4.10%	0.00%	-4.00%	2.20%	2.00%
West 7th	-31.00%	1.00%	-3.00%	-1.00%	4.00%
Highland Park	-3.00%	3.00%	-5.00%	0.00%	2.00%