



# International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: [www.ijarcsse.com](http://www.ijarcsse.com)

## Wireless Networking Security ("Secured-Nim": Blocking Misbehaving Users In Anonymizing Networks")

**Mr. Harjit Singh**  
(M.Tech Scholar)  
KSOU, Mysore  
India.

**Er. Gurpinder Singh**  
(Dept of Computer Applications)  
Sant Baba Bhag Singh Post Graduate College,  
Jalandhar, India

---

**Abstract---***Through this paper we are trying to reflect the weaknesses and counter measures that are put forward until recently of the wireless security. We present a structure to help managers appreciate and review the various threats associated with the use of wireless security technology. We also discuss a number of presented solutions for countering those threats. We believe that a thorough understanding of this paper makes the non specialist reader have a complete review of wireless security and vulnerabilities associated with it.*

**Keywords—***Wireless Security, Wireless Hardware, Software Tools, Wireless Network traffic.*

---

### 1. INTRODUCTION

An important factor in the growth of a country is a good communication infrastructure and sees how wireless networks have an important role to play in the development of a country like India. Wireless networks are very common, both for organizations and individuals. Many laptop computers have wireless cards pre-installed. The ability to enter a network while mobile has great benefits. However, wireless networking has many security issues. Hackers have found wireless networks relatively easy to break into, and even use wireless technology to crack into wired networks. As a result, it's very important that enterprises define effective wireless security policies that guard against unauthorized access to important resources. Wireless security is the prevention of unauthorized access or damage to computers using wireless networks. Wireless Intrusion Prevention Systems are commonly used to enforce wireless security policies. The risks to users of wireless technology have increased as the service has become more popular. There were relatively few dangers when wireless technology was first introduced. Crackers had not yet had time to latch on to the new technology and wireless was not commonly found in the work place. However, there are a great number of security risks associated with the current wireless protocols and encryption methods, and in the carelessness and ignorance that exists at the user and corporate IT level. Cracking methods have become much more sophisticated and innovative with wireless. Cracking has also become much easier and more accessible with easy-to-use Windows or Linux-based tools being made available on the web at no charge. We will explore regarding wireless security, Threats to wireless security, Wireless Intrusion Prevention Systems, Wireless Security Best Practices and try to find out some recommendable Security Configurations in practical. A Wireless-Fidelity (Wi-Fi) network will give nearby computer enthusiasts an opportunity to break into the attached wired network. The most critical security vulnerability damaging Wi-Fi was published in 2007 [1], four years after the conception of Wi-Fi, and two years after it became an international standard. Other flaws in Wi-Fi have been apparent for an even longer time. Attacks on them have been improved, refined and combined in software tools that automate portions of the attacks. Poorly secured Wi-Fi networks can be utilized to attack networks and corporations from the inside, instead of attempting to do it externally from the Internet. A badly secured Wi-Fi network can be exploited for other purposes that do not directly threaten the owner of the compromised Wi-Fi network. The wireless intruder can conceal his identity (e.g. from the network owners) and yet, if he wishes, reveal it to others (e.g. authenticate to a public e-mail server). Those who know the identity of the hacker cannot expose him to the owner of the compromised network, they can't even be sure if he has gained access by suspectable means. Many owners of Wi-Fi networks are oblivious to the risks involved and fail to secure their networks adequately. Even large corporations may not be able to secure their Wi-Fi networks as much as they wish. The constraints following a secure implementation will not always enable all of their users to connect with the ease required. More secure systems are complex, and interoperability can become a problem. For this reason, the percentage of vulnerable Wi-Fi networks is high. In the institutions of SBBSEC, Nov 2012, well over 50% of the detected Wi-Fi access points were completely open, and another 15% were secured with inadequate mechanisms[2].

## **II. What is Wireless (Wi-Fi) Security?**

Wi-Fi depends on cryptographic methods to enable security. In this thesis, the Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA) security mechanisms provide the security as defined by [3]:

**Privacy:** Data transmitted in the network should not be readable by anyone but those communicating.

**Authentication:** Only clients who know a shared secret may connect to the network. WEP was the first cryptographic protocol developed for Wi-Fi to enable privacy and authentication. WEP, however, was not secure after all. To rectify the security issues with WEP, the Wi-Fi Alliance pushed a new cryptographic protocol, WPA. Since then, a common practice of securing a WPA enabled network with passwords has been discovered to be vulnerable to an offline dictionary-attack. Even though WPA itself is thought to be secure, apart from the dictionary-attack, it was a quick fix to the problems in WEP. WPA is a subset of a Robust Security Network (RSN) which was introduced in an early draft of a security standard developed by Institute of Electrical and Electronics Engineers (IEEE) denoted 802.11i [4]. Other than the similarities between WPA and RSN, IEEE 802.11i is not covered in this thesis.

## **III How is Wireless (Wi-Fi) Used?**

With the advent of Wi-Fi, wireless technologies have become inexpensive, user-friendly and available to a large number of people and companies. In dense urban areas, access points belonging to different individuals are so closely spaced that their coverage areas overlap. The survey performed in Section 2.6 shows this is true for the Complex of SBBSEC[5]. With its popularity and the availability to anyone within range, many individuals detect Wi-Fi networks as a hobby. War drivers bring their laptops and Wi-Fi gear. With WEP, anyone participating in the network can eavesdrop on other conversations in the network. With the aid of a Global Positioning System (GPS) receiver and an antenna, they explore areas and map the locations and coverage areas of access points. Some do it for the fun, and some with the intent to exploit vulnerable Wi-Fi networks. War bikers and war walkers do the same by other means of transportation.

### **Technical traditional aspect of wireless security**

Wireless security can be broken into two parts: Authentication and encryption. Authentication mechanisms can be used to identify a wireless client to an access point and vice-versa, while encryption mechanisms ensure that it is not possible to intercept and decode data. For many years, MAC access control lists have been used for authentication, and 802.11 WEP has been used for encryption.

### **Wireless LANs in the Home**

Wireless networking has become commonplace, and with prices reduced to a fraction of what they were, it is no wonder that wireless networking products have transitioned from the office and into the home. For the home user, a wireless network provides freedom in convenience and lifestyle to exchange words, data, and music or video with any computer – across the Internet, or around the world. Home users can create a wireless network out of an existing wired network and wirelessly extend the reach of the Internet throughout the home on multiple computers, making it more convenient for everyone to get online.

## **IV. IEEE Wireless Networking Specifications**

The IEEE (Institute of Electrical and Electronic Engineers) released the 802.11 specifications in June 1999. The initial specification, known as 802.11, used the 2.4 GHz frequency and supported a maximum data rate of 1 to 2 Mbps. In late 2008, two new addenda were released. The 802.11b specification increased the performance to 11 Mbps in the 2.4 GHz range while the 802.11a specification utilized the 5 GHz range and supported up to 54 Mbps. Unfortunately, the two new specifications were incompatible because they used different frequencies. This means that 802.11a network interface cards (NICs) and access points cannot communicate with 802.11b NICs and access points. This incompatibility forced the creation of the new draft standard known as 802.11g. 802.11g supports up to 54 Mbps and is interoperable with 802.11b products on the market today. The concern is that the 802.11g specification[6] is currently in development and products will not be available until a later date.

### **802.11 Specifications**

The 802.11 specifications were developed specifically for Wireless Local Area Networks (WLANs) by the IEEE and include four subsets of Ethernet-based protocol standards: 802.11, 802.11a, 802.11b, and 802.11g.

#### **802.11**

802.11 operated in the 2.4 GHz range and was the original specification of the 802.11 IEEE standard. This specification delivered 1 to 2 Mbps using a technology known as phase-shift keying (PSK) modulation. This specification is no longer used and has largely been replaced by other forms of the 802.11 standard.

#### **802.11a**

802.11a operates in the 5 - 6 GHz range with data rates commonly in the 6 Mbps, 12 Mbps, or 24 Mbps range. Because 802.11a uses the orthogonal frequency division multiplexing (OFDM) standard, data transfer rates can be as high as 54 Mbps. OFDM breaks up fast serial information signals into several slower sub-signals that are transferred at the same time

via different frequencies, providing more resistance to radio frequency interference. The 802.11a specification is also known as Wi-Fi5, and though regionally deployed, it is not a global standard like 802.11b.

#### **802.11b**

The 802.11b standard (also known as Wi-Fi) operates in the 2.4 GHz range with up to 11 Mbps data rates and is backward compatible with the 802.11 standard. 802.11b uses a technology known as complementary code keying (CCK) modulation, which allows for higher data rates with less chance of multi-path propagation interference (duplicate signals bouncing off walls)[7].

#### **802.11g**

802.11g is the most recent IEEE 802.11 draft standard and operates in the 2.4 GHz range with data rates as high as 54 Mbps over a limited distance. It is also backward compatible with 802.11b and will work with both 11 and 22 Mbps U.S. Robotics wireless networking products. 802.11g offers the best features of both 802.11a and 802.11b, but as of the publication date of this document, this standard has not yet been certified, and therefore is unavailable

### **V. How to Identify Wi-Fi Networks**

This chapter serves as a guide to getting started with hacking Wi-Fi networks. The ability to gather intelligence on a network is crucial to anyone attempting to attack a Wi-Fi network. After reading through the chapter, knowledge on how to construct a descent platform for further hacking should be in place. Basic understanding of the operation of Wi-Fi is provided, and hints on how a network may be manipulated is explained.

#### **Introduction**

As stated in Chapter 1, there is a surprising amount of Wi-Fi networks in populated areas. Locating most of them is as trivial as following the instructions manual of any wireless card. It will explain how to locate an accompanying access point. The same instructions will work for locating a neighbor's access point. To automate the task of searching for access points, many software tools have been developed. Some of the tools contain quite a lot of features, even the ability to find so-called "hidden" networks. By combining coordinates from a GPS receiver and measurements of signal strengths, it is possible to calculate an estimate of the range of the network and even the center where the access point may be found. To create a visible picture of the distribution of the Wi-Fi networks, the coordinates are used to plot detected access points on a map. This makes for some interesting maps which may be used by engineers when designing or extending a Wi-Fi network. However, it may also be maliciously used to enlighten fellow hackers where they may obtain access to open or poorly secured networks. Wi-Fi networks give crackers one of the most anonymous methods to obtain access to the Internet. Going a step further than simply locating Wi-Fi networks by capturing packet traffic, is analyzing the contents of the packets. Quite a lot of useful information can be extracted. Even encrypted data packets have plaintext headers. In the case of Wi-Fi, a whole category of command and control packets must be transmitted in plaintext. Naturally, decrypted packets reveal more details, probably details that engineers already know, but that crackers will go to great lengths to obtain.

#### **Availability**

The infrared based IEEE 802.11 devices are virtually non-existent,<sup>3</sup> as will they be in this thesis. Products with 802.11b (without g) are still common in new devices, mostly in small embedded devices such as smart phones (Q-Tek 8310), handheld computers (iPAQ), printers (HP), video projectors, cameras, etc. High-end notebooks often have all of 802.11 b, g and a. Entry and mid-level notebooks have 802.11 b and g, but not a.

### **VI. HARDWARE EQUIPMENT**



Figure 1.1

#### **Wi-Fi Network Card**

The Wi-Fi network card, such as depicted in Figure 1.1, is the link between the computer and the Wi-Fi network, commonly referenced to as the wireless network interface. It contains a radio implementing modulation techniques from IEEE 802.11. Firmware running on the hardware device abstracts the hardware device from the operating systems device driver. Tasks done by the firmware could have been implemented in the device driver but the firmware is a solution to make it very difficult to operate the radio in an unlicensed manner. Whenever an external antenna is required, the wireless network card must have an antenna connector. This is more cumbersome to get than at first thought. Most governments impose restrictive Lawson<sup>6</sup> how radios may operate and be modified. Connecting external antennas may change the density of the radiating signal to limits outside of those allowed, something discussed further in the next section. One of the methods of obstructing modifications has been to require manufacturers to mount only proprietary connectors to their Wi-Fi cards. Thus, restricting the choice of

external antennas to those tested and approved by the manufacturer and the government body. There are many different chipsets available for 802.11a/b/g cards. Not all of them perform equally well, especially in regard to Linux support. Getting the network card to function at all can be difficult. A wardriver will need a card that he can put into a special mode called monitor mode. In this mode, the network card will not try to associate with any access point. All it will do is capture packets and forward all of them to the operating system drivers. The best choice at present is a card with an Atheros chipset where the MadWiFi [8] drivers can be used. More recently, Ralink [9] has been very helpful constructing very good device drivers for network cards based on their Ralink chipset. In monitor mode it has typically not been the intention that the card should be able to transmit frames. This however has recently been rectified in newer device drivers for chipsets based on Prism GT, Atheros and Ralink. A few attacks use this possibility in active attacks with a single network card, [10] Notebooks purchased today usually have an integrated Mini-PCI Wi-Fi card. Currently the common chipset is from Intel, but Atheros also make very good chipsets for Mini-PCI cards. Drivers have been released by Intel themselves that will support monitor mode, but it cannot be used to inject frames concurrently. Most of the time mini-PCI cards have a standard connector that can be used without too much hassle to connect external antennas—such as the one built around a good notebook’s screen. The connector is known as a U.FL connector.

**Antenna**

An antenna is used to focus or restrict the signal sent from the wireless network card into a certain pattern or path. Analogous to the transmit case, it will receive signals in the same path. The main purpose is to increase the strength of the receiving or transmitting signal. It may also be used for the purpose of having the radio sealed or located elsewhere than its coverage area. Antenna construction and design is a major field in its own and requires a fairly good understanding in the behavior of radio waves. Although with the popularity of Wi-Fi, a large number of simple to understand manuals have appeared on the Internet. They make it possible for the layman to experiment with some common designs. The term “cantenna” is a product of this—ordinary household cylinders such as the cylinder with Pringles chips are made into antennas. dBi is an important part of the antenna specifications and in simple terms it translates to how much a signal’s strength has increased when received or transmitted.

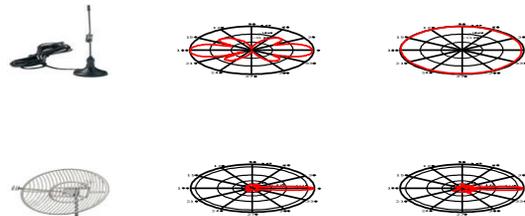


Figure1.2

Volume, this type of antenna is called an “isotropic radiator” and is considered to have 0 dBi gain. It is the basis for the Effective Isotropic Radiated Power (EIRP), which is the amount of power a transmitter would need to produce the same signal strength through an isotropic radiator. Decibel (dB) uses a logarithmic scale. A gain of 3 dBi in effect nearly doubles the signal strength. As such the “antenna” with a 6 dBi gain provides approximately  $263 \text{ dBidBi} = 4$  times more signal strength than an isotropic radiator would with the same input. Antenna designs can be brought down to two main designs directional and Omni directional. With omni-directional antennas such as the one depicted in Figure1.2, the radio signal will spread in 360o, however, the signal is not wasted on birds and earthworms. A directional antenna’s purpose is to concentrate the radio signal into a fairly narrow direction. Anything from 180o to a narrow 7o as the antenna in Engineers will typically want to find the area where it’s possible to connect to the Wi-Fi network. Unless the clients are stationary, it is pointless to use high-gain directional antennas since such antennas are not used by ordinary mobile clients. Crackers on the other hand may only be interested in listening in on the data traffic. As such they would like to know all locations where it is possible to hear the access point. Although a position closer to the access point will most likely result in more captured traffic, it may not be a desirable hiding spot. All good reasons why a cracker has a high-gain directional antenna[11].

**VII. Analyzing Wi-Fi Network Traffic**

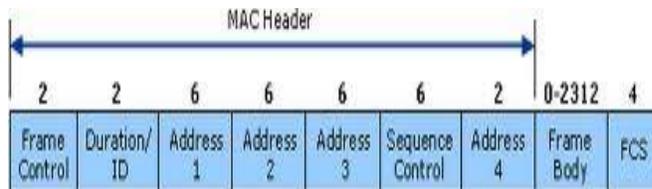


Figure1.3 MAC frame format.

Every packet transmitted in Wi-Fi networks contains bits of information used to maintain the various layers of the communication. Although packets may be encrypted in Wi-Fi networks, they still have plaintext headers. As this section will show, the headers are valuable to anyone analyzing the network. The entire MAC frame displayed in Figure1.3 is easily available to user space tools in Linux. All packets in a Wi-Fi network conform to the MAC frame format. The Frame Control

field specifies which type of payload the MAC frame transports. There are three main types of packets and many subtypes. The main types, in bold, and their subtypes, are

- 1. **Management: Association, Probe, Beacon, and Authentication.**
- 2. **Control: RTS, CTS, PS-Poll, ACK, CF-Ack/Poll.**
- 3. **Data: Data, Data + CF-Ack/Poll and Null-function.**

In the following sections, only the interesting fields of interesting frames are discussed.

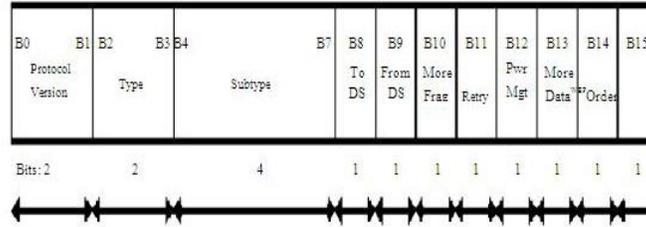


Figure: Frame control field.

- Network is part of a WDS<sup>3</sup>: ToDS = 1 and FromDS = 1.
- Network is in ad-hoc mode: ToDS = 0 and FromDS = 0; and Type = Data.
- Network is in infrastructure mode: ToDS = 1 or FromDS = 1; and Type = Data.

Additionally, every captured frame includes signal-strength measured by the radio receiver. When combining this data with GPS-coordinates, it is possible to estimate:

- Network range: Wherever frames from an access point where received.
  - Access point location: Triangulate from position and signal strength of frames transmitted by the access point and captured in multiple locations.
  - Client location: Same procedure as above, but only on frames transmitted from the desired client.
- Buildings, other obstacles, and multipath fading will reduce the accuracy of the estimations. Moving clients or access points are not handled either and introduce errors.

### VIII. Software Tools

Although, as pointed out, its possible to learn a great deal about a network from its beacon frames. However, an engineer simply listening for beacon frames will not gain much knowledge he didn't already know. An engineer will typically want to know from where it is possible to use and connect to the network. Since it is likely that a client can hear the access point but not the other way around, engineers will want to go as far as associating with the access point under a site-survey. If a cracker associates with the access point he becomes much more exposed. The process of associating requires two-way communication. The second the cracker transmits packets, the attack has become "active". It is well known that active attacks are much more dangerous for a hacker, he may even be located or examined himself.

### Kismet

Kismet [12] is the de facto software tool for wardrivers. It uses most of the information in Section 2.4 and gives the wardriver a simple and user friendly UI with an overview of detected access points.



Figure1.4: Kismet under Linux.

In case visual feedback is difficult, come to mind warbikers and warwalkers, Kismet interfaces with a text-to-speech library and may inform its user of events via an earplug. Kismet in Figure1.4 will communicate directly with the GPS receiver and record the position of every single received packet. This enables it to guess the physical location of the access point. An arrow in the user-interface tries to point the user in the right direction to the access point. All currently available commercial Wi-Fi cards are restricted to listen on only a single channel at a given point in time. Kismet instructs the card to jump from channel to channel. It can also use two or more network cards to listen in on multiple channels at a time. Kismet can be locked on to a specific channel to capture as much traffic from there as possible. Kismet compiles interesting statistics such as channel usage distribution and the percentage of WEP or WPA enabled networks. Some access points disable broadcasting of their SSID in beacon frames or probe responses. Hiding the SSID is used to increase the security since only clients that know an access point's SSID are able to associate with it. But because management frames are transmitted in cleartext the SSID is also sent in cleartext when an "authenticated" client associates (authenticated in the sense that it has proved that it knows the "secret" SSID). Kismet will use this packet to display the network name of even so called "hidden" or "cloaked" Wi-Fi networks.

### Wireshark

Wireshark is the world's most popular network analyzer in Figure1.5. This very powerful tool provides network and upper layer protocols informations about data captured in a network. Like a lot of other network programs, Wireshark uses the pcap network library to capture packets.

The Wireshark strength comes from:

- its easiness to install.
- the simplicity of use of its GUI interface.
- the very high number of functionality available.

Wireshark was called Ethereal until 2006 when the main developer decided to change its name because of copyright reasons with the Ethereal name, which was registered by the company he decided to leave in 2006.

If you don't have a graphical interface, you could be interested by "TShark" which is the CLI version of Wireshark. Tshark supports the same functionalities as Wireshark

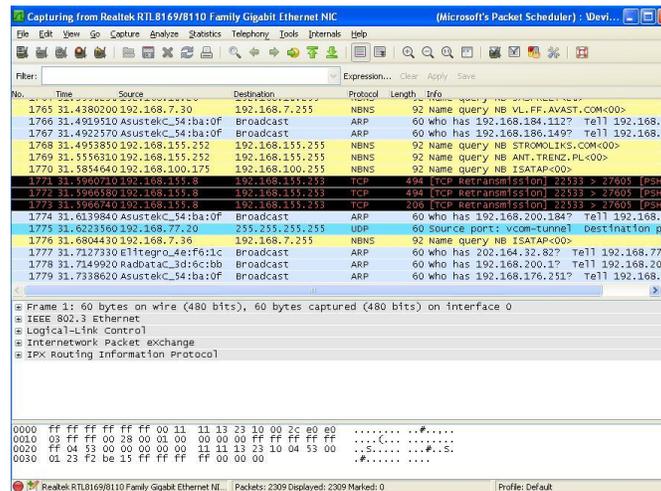


Figure1.5

## IX. Cracking the Security of Wi-Fi

In this chapter the flaws of Wi-Fi security are explained and demonstrated. The differences between WEP and WPA serve to divide this chapter into two parts. Since WEP has the greatest number of vulnerabilities, WEP is where the main focus is directed. WPA is interesting since it replaces WEP in many circumstances, but is still insecure to a limited extent. Trickery on supplemental security mechanisms such as MAC address filters are explained last, until a summary closes the chapter. Wi-Fi has a lot of security vulnerabilities. Unfortunately for Wi-Fi the vulnerabilities and the severity of them became widely known too late. At the time of the famous paper on how to crack a WEP key, early 2009, there were already millions of 802.11 products sold world-wide. At that point, issuing a fix or recalling all products was not feasible. Instead, consumers in need of better security, supplemented WEP with VPN and IEEE 802.1X [13]. New products had to be able to operate with older and broken WEP enabled products. More secure alternatives, such as WPA, were introduced later and could only be made available as an addition to WEP. The complexity of setting up a secure wireless network increased and the percentage of wireless networks that use the best mechanisms to enable security is not as high as it should be. The final replacement for both WEP and WPA; IEEE 802.11i [14], also referred to as Wi-Fi Protected Access version 2 (WPA2) by the Wi-Fi Alliance, is at present considered secure, but is not discussed in this thesis. The practical examples in this chapter are

executed on the Linux operating system, but most of them can also be performed from the Windows platform. Still the instructions executed in Linux will be explained to the point where a Windows-only user can follow the attacks. The basic protocols and flow of frames when connecting to an access point. First the client will detect access points either by sending a probe request and receiving a probe response, or purely by looking at the beacon frames frequently transmitted by an access point. Upon discovery, the client may try to authenticate to the access point. If successfully authenticated, the client may try to associate with the access point by sending an association request. If permitted by the access point the client will receive a positive association response. Whenever WPA is enabled, the shared-key authentication mechanism of WEP is skipped (open system authentication is used), and the real authentication is performed after association.

## X. Security Supplements

### Bypassing MAC Address Filters

MAC address filters are not part of the IEEE 802.11 specification, nonetheless they are found in many Wi-Fi access points as an optional security mechanism. Its purpose is to deny access to any network interface card with an address that is not authorized. A table of authorized MAC addresses are stored in the access point. It is effective at keeping novice neighbors off an open network. However MAC addresses are never kept a secret and a network card may change its address to match someone else's address. All that has to be done to bypass the security is to capture a frame from a client, wait for the client to disconnect, and then change to the client's MAC address and connect.

### Avoiding Interference

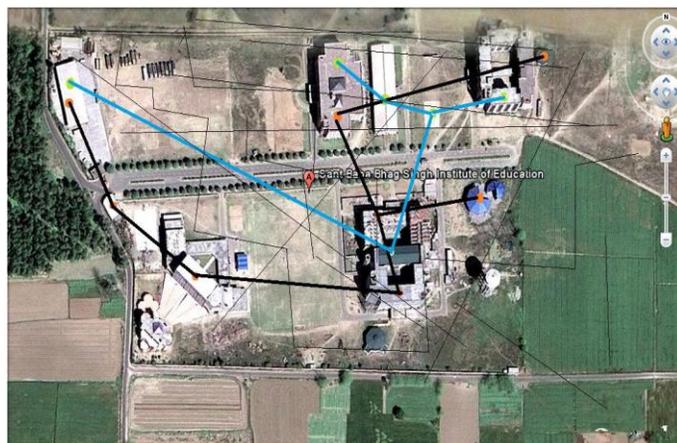
If two computers share a MAC address simultaneously, one for a client, and one for an intruder, they would end up interfering with each other to the point where communications would be disrupted and discontinued. But if the intruder only receives responses which are discarded and ignored by the client, he may tunnel all his communications through the use of only these protocols. To do this, the intruder needs an opening on the other side of the tunnel he must have control of another computer already on the Internet. OpenVPN is a set of tunneling software available for many platforms including Linux and windows. It has the ability to tunnel traffic through only UDP packets or a single TCP connection. Additionally there are features that allow the tunnel to be encrypted and authenticated at both ends of the tunnel. The rest of the section demonstrates how an OpenVPN tunnel is created from Linux. The ifconfig program is a networking tool to configure network interfaces in Linux. Route is a program for configuring network routes, so that network traffic is transmitted over the correct network.

## XI. Results From Warbiking in Institutes of SBBSEC

Several bike trips reveal there are many access points available on the streets SBBSEC. A survey on Dec 2012 from 17:17 to 18:07 revealed 35 access points of which only 33% were setup with WEP or WPA encryption. The access points have been plotted in Figure 1.6. However it does not mean that it is possible to gain access to 67% of the other access points. They may be fitted with Virtual Private Network (VPN) solutions or Captive Portals such as NoCat [15]. When zooming in on the map red and green dots will appear along with labels. The label is the SSID of the access point. The red dots are access points with WEP or WPA enabled, the green dots are those that don't use encryption.

## XII. Conclusion

Anyone can obtain equipment necessary to start hacking Wi-Fi networks. Some knowledge is needed to get equipment that is compatible with each other and that has functional software drivers. The software that is available has matured and contains a lot of features that are desirable. The bits of information broadcasted by a Wi-Fi network is of enough interest to create a new term, wardriver.



**Figure 1.6: Warbiking map over the center of SBBSEC.**

Old Wi-Fi products, still occupying a large share of the network installations, are not by any means secure. Even equipment

that can be configured to be secure, are left unsecured, many times due to the increased complexity of access point setups. The attention vulnerable Wi-Fi networks receive from hackers is tremendous, vulnerabilities are not only discovered, but they are refined by others and implemented and combined by a whole on-line community. A compromised network is a great utility for several parties. Neighbors get free broadband access to the Internet, malicious hackers retain strong anonymity, and mobile users get free Internet almost anywhere. Malicious hackers can monitor the users of a network, giving the hackers many opportunities to cause havoc. The risk of getting a visit from someone with bad intentions is currently fairly low, but as it is rather easy to obtain enough knowledge and equipment to compromise a Wi-Fi network, the risks will only rise. The fact that more and more networks become secure means that the remaining insecure network, will be hunted down by malicious hackers and abused. As we see it is possible to bypass this security precaution. And more important if someone monitors your connection they may be able to get crucial information about you. For example we can see what sites the network clients has been surfing around. MAC filtering must not be trusted for securing your network. You must use password protection in order to secure your network.

## References

- [1] Discussion forum surrounding Wi-Fi. URL <http://www.netstumbler.org>
- [2] Kismet Wi-Fi network detector. URL <http://www.kismetwireless.net>
- [3] Jon Edney and William A. Arbaugh. Real 802.11 Security, Wi-Fi Protected Access and 802.11i. 2004. ISBN 0321136209.
- [4] G. Zorn G. Pall. Microsoft point-to-point encryption (mpps). URL <ftp://ftp.isi.edu/in-notes/rfc3078.txt>
- [5] M. Leech, M. Ganis, Y. Lee, R. Kuris, D. Koblas, and L Jones. SOCKS protocol version 5. RFC 1928 (Standard), March 1996. URL <http://www.ietf.org/rfc/rfc1928.txt>
- [6] Peter Palfrader. Live statistics on number of tor routers, May 2006. URL <http://www.noreply.org/tor-running-routers/>
- [7] Jon Postel. Internet control message protocol. RFC 792 (Standard), URL <http://www.ietf.org/rfc/rfc792.txt>
- [8] Jon Postel. Internet protocol. RFC 791 (Standard), URL <http://www.ietf.org/rfc/rfc791.txt>
- [9] Jon Postel. Transmission control protocol. RFC 793 (Standard), September 1981. URL <http://www.ietf.org/rfc/rfc0793.txt>
- [10] Jon Postel and J.K. Reynolds. A standard for the transmission of ip datagrams over ieee 802 networks. RFC 1042 (Standard) URL <http://www.ietf.org/rfc/rfc1042.txt>
- [11] Adi Shamir Ron Rivest and Len Adleman. Rsa data security, inc. URL <http://www.rsasecurity.com/>
- [12] Joshua Wright. Asleap. URL <http://asleap.sf.net/>
- [13] Simmonds, A; Sandilands, P; van Ekert, L (2004). "An Ontology for Network Security Attacks". Lecture Notes in Computer Science. Lecture Notes in Computer Science 3285: 317–323.
- [14] Wright, Joe; Jim Harmening (2009) "15" Computer and Information Security Handbook Morgan Kaufmann Publications Elsevier Inc p. 257
- [15] Security Threat Mitigation and Response: Understanding - CS-MARS, Dale Tesch/Greg Abelar, Cisco Press, Sep 26, 2006