2-2006

Evaluation and Illustration of a Free Software (FS) Tool for Wireless Network Monitoring and Security

Victor A. Clincy
Kennesaw State University, vclincy@kennesaw.edu

Krithi Sitaram Ajay
Kennesaw State University

EVALUATION AND ILLUSTRATION OF A FREE SOFTWARE (FS) TOOL FOR WIRELESS NETWORK MONITORING AND SECURITY*

Clincy, Victor
College of Science and Math
Kennesaw State University
Kennesaw, Georgia 30144
770-420-4440, vclincy@kennesaw.edu

Sitaram, Ajay Krithi
College of Science and Math
Kennesaw State University
Kennesaw, Georgia 30144
asitaram@students.kennesaw.edu

ABSTRACT

Wireless communication provides users many benefits such as portability, flexibility, reduced hardware need and lower installation costs. Wireless local area networks (WLANs) for example allow users the ability to carry their laptops from place to place without any physical wires and without losing network connectivity.

However, some amount of security risk is always associated with wireless networks. The most significant security risk for wireless technology is the potential outsiders have in gaining access to the communications medium, the communications medium being the air waves. Though WLANs provide the users with the option of roaming, this convenience is facilitated by broadcasting packets to anyone with compatible equipment within range of a transmitting device. This broadcasting of packets induces a compromise between convenience and security. Having an unsecured WLAN can result in a loss of service, or can be used as a staging area to launch attacks against other networks. The significant challenges faced today in securing wireless LANs are maintaining privacy, data confidentiality, and preventing unauthorized access using proper access control mechanisms.

As wireless networking and security become more prevalent in the market, more and more computer science programs are incorporating courses in

---

wireless networks or at the least, devoting a significant percentage of the advanced networking courses to wireless topics. As a result, in addition to industry practitioners, there is a growing interest among university researchers and faculty regarding tools used in monitoring and assessing security threats for wireless networks.

This paper will demonstrate and evaluate a free and open source software tool, called Network Stumbler, used for monitoring and assessing security threats for wireless networks. Network Stumbler is a Windows-based tool that allows you to detect Wireless Local Area Networks (WLANs) using 802.11b, 802.11a and 802.11g. It has many uses:

- Verifies that your network is set up the way you intended.
- Find locations with poor coverage in your WLAN.
- Detects other networks that may be causing interference on your network.
- Detects unauthorized "rogue" access points in your workplace.
- Helps aim directional antennas for long-haul WLAN links.
- Can be used recreationally for WarDriving.

Keywords: Wireless Networks, Security Issues, Free Software, Advanced Topics in CS, Pedagogy

I. INTRODUCTION:

Wireless networks are classified into three main categories: WWAN (wireless wide area network), WLAN (wireless local area network), and WPAN (wireless personal area network). WWAN includes technologies such as 2G cellular and Global System for mobile communication. WLAN includes 802.11g standards and others. WPAN includes bluetooth and IR devices. Wireless communication uses the wavelengths from the radio frequency (RF) band up to the IR band. For this paper, the main area of concentration is on wireless local area network (WLAN) monitoring and security.

The WLAN connects the computers and other network devices via an access point (AP). The access point (AP) acts like a transceiver that provides devices a certain amount of mobility. Access point devices usually have a coverage area of up to 300 feet. This area of coverage is called a cell and users roam within the cell with their wireless laptops. Although wireless networks are flexible and easy to implement, wireless networks must be efficiently monitored and there are some important security issues to be aware of.

Some of the important security factors deal with the way the wireless network is set-up and configured. Generally with wireless networks, one of the first thing to do is set up the access point.. Since the access point is the link between the wireless and wired Worlds, the service set identifier (SSID) features should be configured in the access point for security reasons. Some SSID features entail Wired Equivalent Privacy (WEP) and MAC. Other important security factors considered for wireless networks deal with detecting whether other networks are causing interference and detecting unauthorized rouge access points. Since wireless networks' signals are transmitted via radio frequency waves, it is important to find the locations with poor coverage and properly position

directional antennas for long haul links. Network Stumbler is a free software tool developed to analyze and detect the various important security issues previously mentioned.

II. NETWORK STUMBLER: A BRIEF OVERVIEW:

Network Stumbler was developed by Marius Milner and runs in a Windows environment. Network stumbler is an easy to use graphical interface and good amount of information about the tool is given in the website www.netstumbler.com.

Network Stumbler can actively detect wireless networks by periodically sending probe requests. The probe requests are sent approximately every second. Once a probe requests is sent, Network Stumbler listens for any responding probe response frame from any access points within the range. Network Stumbler works best with network interface cards that use the hermes chipset, this basically refers to ORiNOCO Gold or Silver "Classic" cards or any " re–badged" version. Some of the common hermes chipset cards are listed below:

- Lucent Technologies Wave LAN/IEEE
- Dell True Mobile 1150 series
- Avaya Wireless PC Card
- Toshiba Wireless LAN Cards

This is an abbreviated list. For more information, refer to www.netstumbler.com. The minimum system requirement for Network Stumbler is a 75MHz Pentium 1 with 16MB RAM running windows 95. The tool's executable file is only 532KB and once installed, the entire program consumes only 2MB of disk space.

III. USING NETWORK STUMBLER:

Once Network Stumbler is installed, an icon will appear as illustrated in Figure 1.

Once the icon is clicked, the program starts and attempts to locate a usable wireless network interface card and a GPS receiver. The application also opens a new file with the extension NS1 which simply stands for Network Stumbler 1. The file name is usually a set of numbers as depicted in Figure 2.

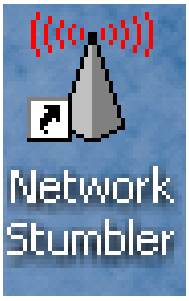

Figure 1: Network Stumbler Icon

The file name is derived from the date and time the program was started and it is usually in the format YYYYMMDDHHMMSS.ns1. If a wireless card is detected, the program immediately starts recording the information to the file.

In Figure 3, Network Stumbler's user interface is displayed. The user interface has two sections. One section of the user interface is the tree view used by the access points. The other section of the user interface is a list view showing all the information about the access point, information like the MAC address, SSID, channel used, speed, and vendor name. If an encryption technique like WEP is used, the list view displays this information as well.

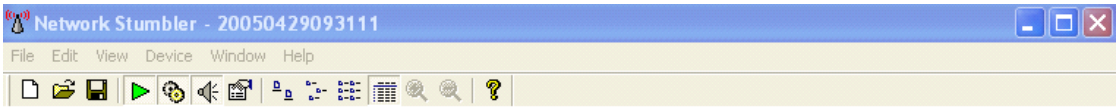

Figure 2: Example of Network Stumbler file name

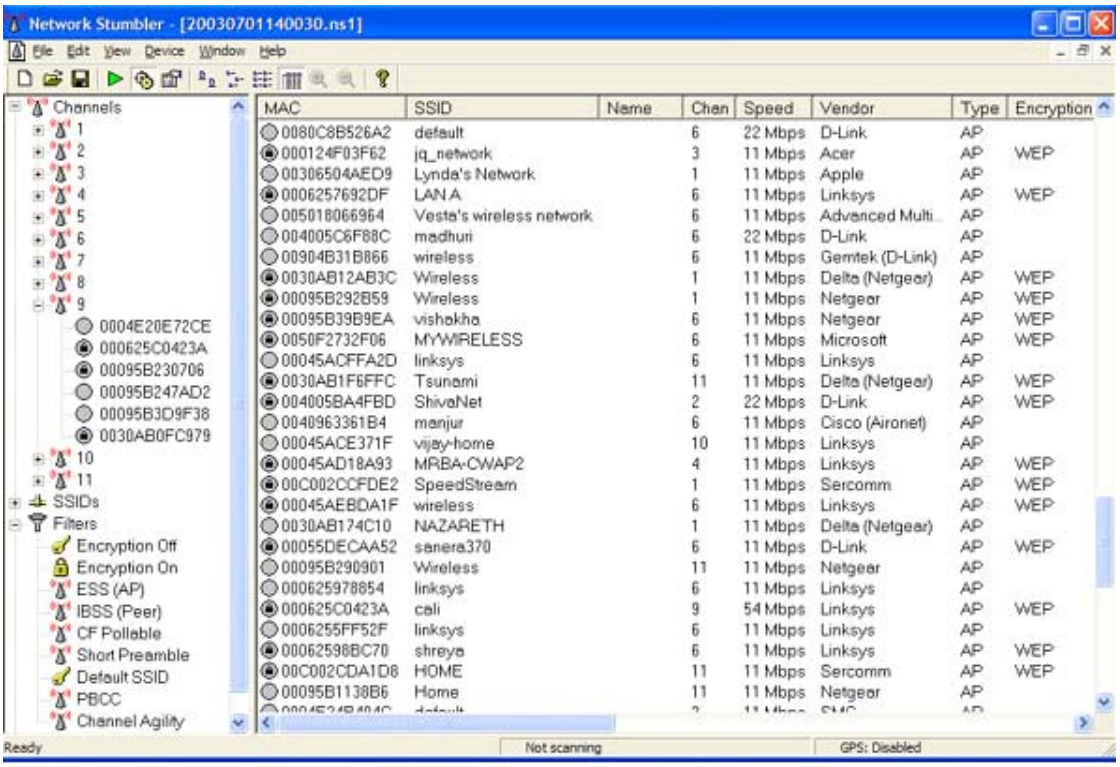

Figure 3: Network Stumbler's User Interface

The list view displays the signal-to-noise ratio at various instances of time. Network Stumbler displays the following information listed in the Table 1 below:

Column	Description
MAC	The text contains the BSSID for wireless devices. The icon shows the signal strength as reported in the last scan: Gray means the item was not detected, or a colored icon ranging from red to green reports the signal strength. A lock appears in the icon if encryption is enabled on the network. For devices on a wired network segment, the icon shows a T-shaped network cable and the MAC address is displayed.
SSID	The reported SSID. This may be blank for access points that report their existence but not their SSID. For wired network items, the SSID is assumed to be the SSID that was associated when the item was discovered. SSID is a network name.

Name	The device's name. This is reported rarely and only if "Query APs for names" is configured.
Chan	All the channels that the device has been seen on. The most recent one is listed first. Before the channel number may be a star (*), which means you are associated with the device, or a plus (+) which means that you were associated with it at some point.
Speed	The maximum reported bandwidth for the device (this is not the actual bandwidth). If you are using an 802.11b device, it may misreport the bandwidth of 802.11g networks as 11Mbps. Some devices are capable of 108Mbps but only report 54Mbps
Vendor	The vendor assigned to the MAC, which may not be the actual equipment manufacturer.
Type	"AP" for a BSS, "Peer" for an IBSS.
Encryption	The word "WEP" will appear on an encrypted network, regardless of whether it is really using WEP.
SNR	The current Signal to Noise ratio, either in dB or arbitrary RSSI units.
Signal+	The highest seen Signal value.
Noise-	The lowest seen Noise value.
SNR+	The highest seen SNR value.
IP, Subnet	The IP configuration of the object, if available.
Latitude, Longitude, Distance	If you are using a GPS receiver, this indicates the estimated position of the object. This position is currently the location where the strongest signal was seen, which is never the actual location. Distance is measured from your current position to the object's estimated position.
First Seen	The time or date when the object was first discovered.
Last Seen	The most recent time or date when the object was seen.
Signal	The current Signal level, either in dB or arbitrary RSSI units.
Noise	The current Noise level, in dB. Not supported by all devices.
Flags	The 802.11 capability flags, in hexadecimal.
Beacon	The 802.11 beacon interval, in Kμs.

Table 1: Information Network Stumbler displays

When the user right clicks on a MAC address that is associated with an IP address and subnet in the list view, a set of options will appear in a context menu as shown below in Figure 4.

If Network Stumbler has determined the IP address or subnet of the selected option, the look up address will appear. When any of the lookup addresses are mouse clicked, a web browser is launched and a query is performed on the registry that assigns IP addresses. The registry used depends on the user's location.

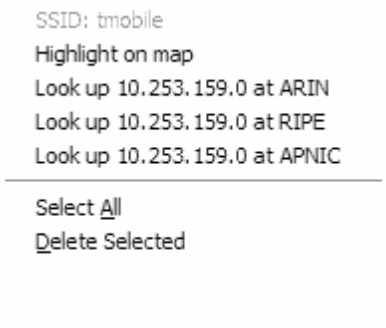

Figure 4: Context Menu

- ARIN assigns number for North America.
- RIPE assigns number for Europe.
- APNIC assigns number for Asia/Pacific region.

The lookup table runs a WHOIS Query. WHOIS is a common network utility that is used to look up domain name and IP address information along with ownership and other information such as any associated organization or customers.

3.1 Wireless Lan Auditing

A network administrator always needs to check that the wireless network is not exposed to unauthorized users. If the security isn't properly configured, the entire organization could be threatened. In order to avoid such security threats Network Stumbler can be used to detect unauthorized rogue wireless LAN as shown in Figure 5.

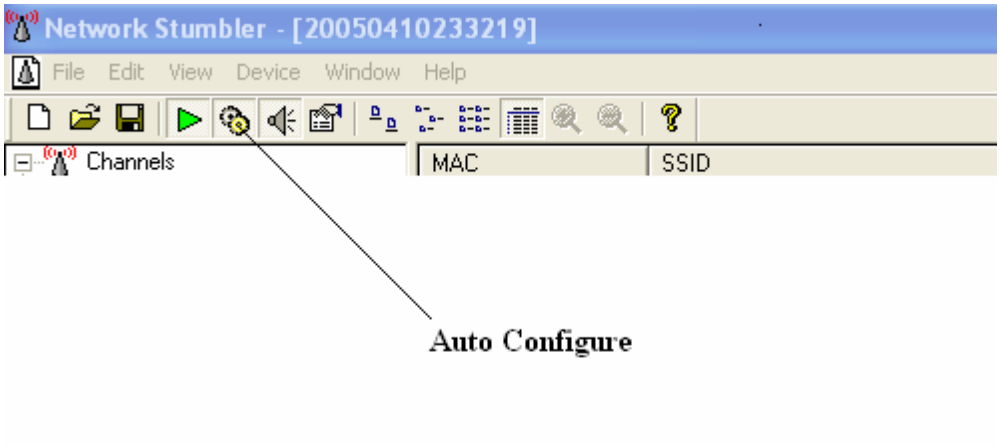

Figure 5: Wireless LAN Auditing

The following settings given below can be performed for wireless LAN auditing.

- Switch on "Auto Configure" to find as many wireless LANs as possible.
- If your LAN uses DHCP then enable DHCP in your wireless card.

3.2 Wireless Lan Coverage Verification

A wireless LAN owner can use Network Stumbler to verify an area that is covered by a good quality signal. The tool can be used to see how far a network coverage area is available beyond the extended boundary.

- Configure the wireless LAN with Service Set Identifier (SSID) and other settings of the LAN to be examined.
- Switch off auto configure so that only the required SSID will be seen.

3.3 Site Survey

The important objective in site surveying in WLAN is to ensure that there is no loss in a connection which leads to data loss as users roam with their laptops. The site survey provides a rough idea of the infrastructure required for a WLAN and can also assist in predicting trends in network traffic. The site survey can indicate high traffic load areas and resolve RF interferences from any neighborhood devices. It is important to pick location and channels so that interference can be minimized. A site survey determines if there are any other devices (Microwave, Cordless Phones, etc.) using the same frequency used by the wireless LAN. A site survey should be done before and after the network has been setup. Figure 6 illustrates Network Stumbler's graphical representation of noise levels.

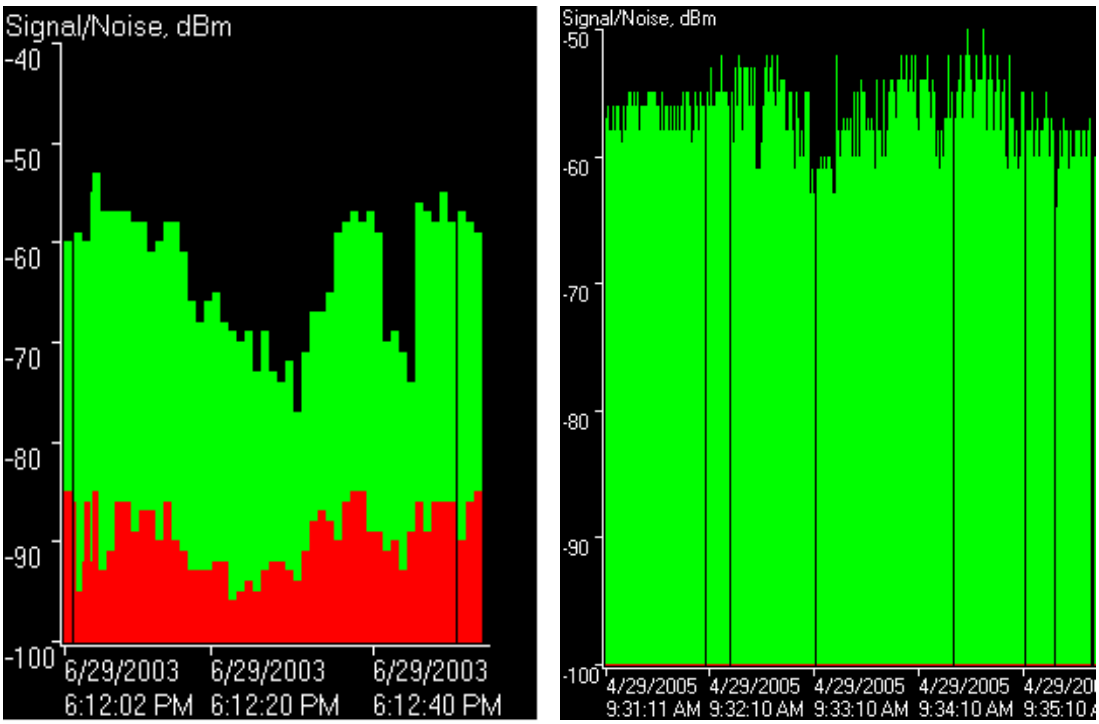

Figure 6: Signal-to-Noise Graphical Representation

The green bars indicate signal strength; the higher the bars the better the signal. The red bars indicate noise level; the higher the bars the higher the noise level. The noise level

indicates interference. The graph between the green and red bars indicates the signal-to-noise ratio. A purple bar, if available, indicates the loss in signal.

The following settings can be performed for site survey:

- The ability to switch on "auto configure" to find as many wireless LANs as possible
- Must use a wireless network interface card that can report noise levels.
- When turning off the auto configure feature, a post installation survey including coverage verification is performed.
- To avoid using others' networks which are not owned, TCP/IP can be un-bind from the network card.

3.4 Antenna Positioning

When setting up an antenna, Network Stumbler can be used to position the antenna to a certain extent. The following steps can be performed in antenna positioning:

- Connect remote antenna to a wireless access point.
- Set up the wireless card with SSID and other settings for remote system.
- Switch off "auto configure" so that only the required SSID will be seen.

3.5 Wardriving

Wardriving is the activity of driving around in a vehicle with a laptop (or PDA) with intent of detecting others' wireless networks. In addition, most wardrivers use Global Positioning Systems (GPS) to track the exact location of the network. A omni-directional or fully-directional antenna is used for better coverage. Network Stumbler is a popular tool for wardriving because GPS can easily integrate. The GPS configuration is shown below in Figure 7.

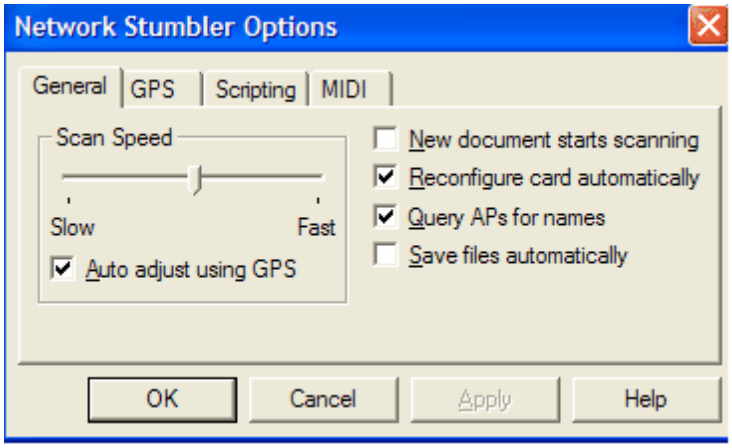

Figure 7: Network Stumbler's GPS Settings

As illustrated in Figure 7, Scan Speed controls how frequent Network Stumbler can probe requests. The scan speed of the program has a internal timer that fires every 0.25 seconds. The timer contains an associated trigger number, for number of cycles needing to elapses before Network Stumbler sends out a broadcast request for the beacon; the default setting is a request sent once every second.

The "Auto adjust using GPS" option allows scanning speed to vary depending on the GPS receiver. If the GPS receiver is not functioning, the previously mentioned setting can be turned off. The scan speed on the faster setting never happens more than four times per second. On the slower setting, the scan happens every 200 feet. The time intervals in seconds between scans are shown in Table 2 below.

Scan interval (seconds)	Slow	- - -	- - -	- - -	Fast
Without GPS speed	1.50	1.25	1.00	0.75	0.50
GPS, Stationary	3.00	2.50	2.00	1.50	1.00
GPS, 25 mph / 40 km/h	2.74	2.07	1.48	0.98	0.57
GPS, 50 mph / 80 km/h	2.31	1.63	0.96	0.46	0.25
GPS, 75 mph / 120 km/h	1.55	1.20	0.50	0.38	0.25
GPS, 100 mph / 160 km/h	1.16	0.76	0.50	0.38	0.25

Table 2: Network Stumbler's Time Intervals

Regarding the "New document starts scanning" option, a new document is created by either launching network stumbler or creating a new document from the file menu. When a new document is created the scanning starts and the results are received in the new document.

Regarding the "Reconfigure card automatically" option, a large variety of SSIDs can be seen by attempting to keep the adapter in the broadcast SSID mode. In this mode it will disconnect the user from any currently associated access point to perform network scan.

Regarding the "Query APs for names" option, an attempt is being made to capture the name and IP address of access points that contain such kind of information. The option lets the program find out if it is an ORiNOCO or Cisco access points. If the program sees another network with a better signal, it disconnects from the current network in order to get the new access point name.

For the "Save files automatically" option, all modified files are saved every ten minutes without asking for any confirmation.

3.6 GPS in Network Stumbler

The GPS settings window is shown in Figure 8.

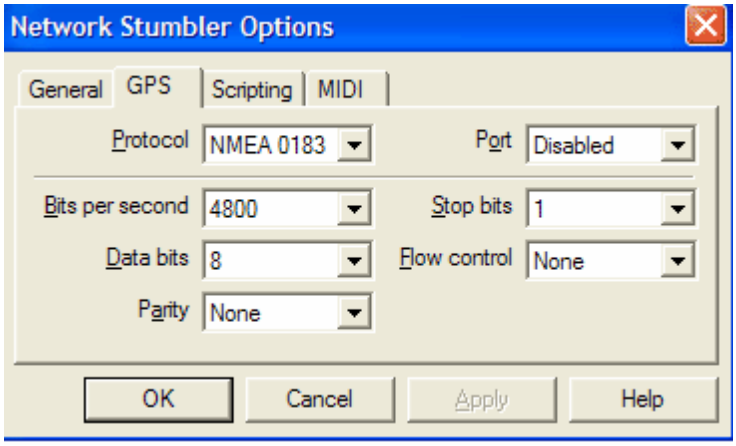

Figure 8: GPS settings in Network Stumbler

As previously mentioned, the GPS setting in Network Stumbler is used for efficient war driving. The GPS tab allows the user to configure the GPS receiver settings. Network Stumbler requires the GPS receiver to use a serial protocol which requires either a hardware serial port or driver that emulates one. The "protocol" option under the

GPS tab allows the user to select the application protocol that is to be used with the GPS receiver. The various choices listed under the "protocol" option are NEMA 0183, Earthmate, Garmin Binary, Garmin Text and Tripmate. The NEMA 0183 protocol is supported by most receivers. The sentences required for position information are GPGGA, GPGLL and GPRMC. The Earthmate protocol is used by serial earthmate device or any other device using Rockwell zodiac protocol . This protocol uses 9600 baud, 1 stop bit, no parity, 8 databits and no flow control. The Earthmate protocol is very rarely used.

The Garmin Binary protocol is supported by devices manufactured by Garmin that uses the protocol called "garmin". The settings uses are 9600 baud, 1 stop bit, no parity, 8 databits and no flow control. Garmin Text is also supported by Garmin and configured to use the protocol "text out". Tripmate is a variant of NEMA 0183 and used by trip mate devices.

The "port" option under the GPS tab is used in selecting the port to which the GPS receiver is connected to; this can be a com port or built in GPS receiver. This setting can be disabled if GPS is not used.

3.7 Scripting

The scripting settings in Network Stumbler are shown in Figure 9.

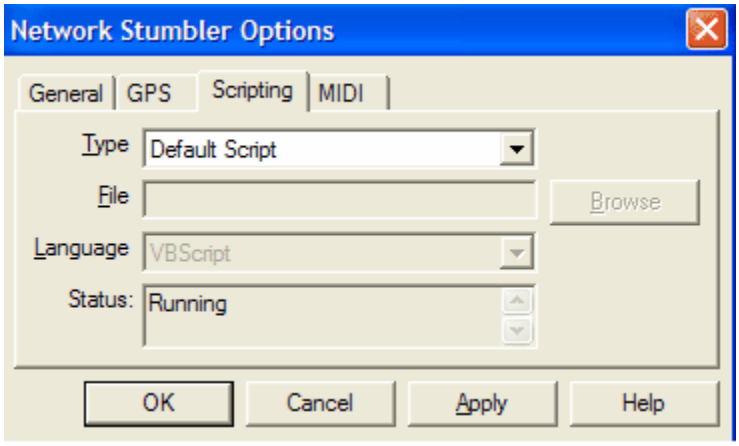

Figure 9: Scripting settings in Network Stumbler

The scripting setting is like an extension for Network Stumbler. Some of the scripting features interface with a mapping or GIS application in sending data to a database for processing. This allows the user to add more functionality in addition to the built in functions. The "type" option allows the type of script to be executed. The "No scripting" choice disables scripting and uses the default Network Stumbler audio feedback mechanism. The "Default script" choice runs Network Stumbler's built-in script and provides complex audio feedback. The "External script" choice runs the script from an external file of your choice; the scripting language must be selected as well in invoking the correct script engine. The scripting languages that can be selected are VBscript, Jscript and Perlscript. The "status" option under the Scripting tab reports the current status of the script and if there are any errors in the script, the status would be displayed. The Network Stumbler website (www.netstumbler.com) has a complete list of scripting functions used by the tool. The only requirement regarding the scripts is that any script written should call the same function names.

3.8 MIDI

All laptops come with a Musical Instrument Digital Interface (MIDI) built in motherboard. The MIDI tab, as illustrated in Figure 10, allows the user to play tones in response to the signal-to-noise ratio readings via this interface. With such a feature, the user can listen for certain signal-to-noise levels. The "Channel" option under the MIDI tab explains which channel can be used, generally channel 10 is used for percussion. The "Patch" option determines the kind of instrument that can be played for selected levels. The "Transpose" option shift notes by specifying the number of semitones. These options are useduring war driving; the tool will play specific sounds as certain actions occur.

The tool comes with 10 built-in sounds for specific events. For example, when a new wireless network is found, a specific sound can be played. When a WLAN signal is lost, a certain sound can be played. In the GPS mode, when there is an error like a timeout, a sound can be played. All of the sounds can also be called from the scripts.

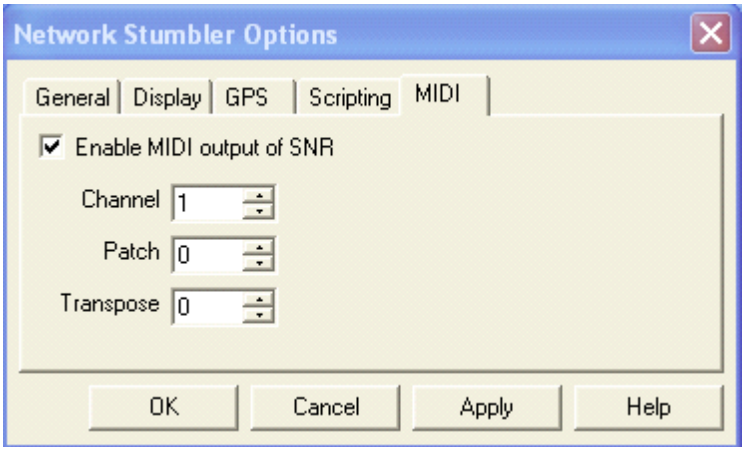

Figure 10: MIDI Function

IV. CONCLUSION

If a user is interested in locating and evaluating wireless local area networks (WLANs) for professional use or interested in the hobby of Wardriving, then downloading and learning Network Stumbler is recommended. Network Stumbler has become the choice of several users because of its simple-to-use interface. Moreover, Network Stumbler is free and can be used for educational purposes such as for in the area of wireless networks.

V. REFERENCES

[1] Milner, Marius, Network Stumbler Tool Help Section, www.netstumbler.com.

[2] Hurley, Chris, Frank Thornton, Michael Puchol and Russ Rogers. Wardriving: Drive, Detect and Defend – A Guide To Wireless Security. ISBN 1-931836-03-5, 2004.

[3] Puchol, Micahel and Russ Rogers. www.simplywireless.com.au/sitesurvey.htm

[4] Flickenger, Rob. Wireless Hacks (Chapter 3). ISBN: 0-596-00559-8, 2003.

[5] Peikari, Cyprus and Seth Fogie. Maximum Wireless Security (Chapter 9). ISBN: 0-672-32488-1. 2002