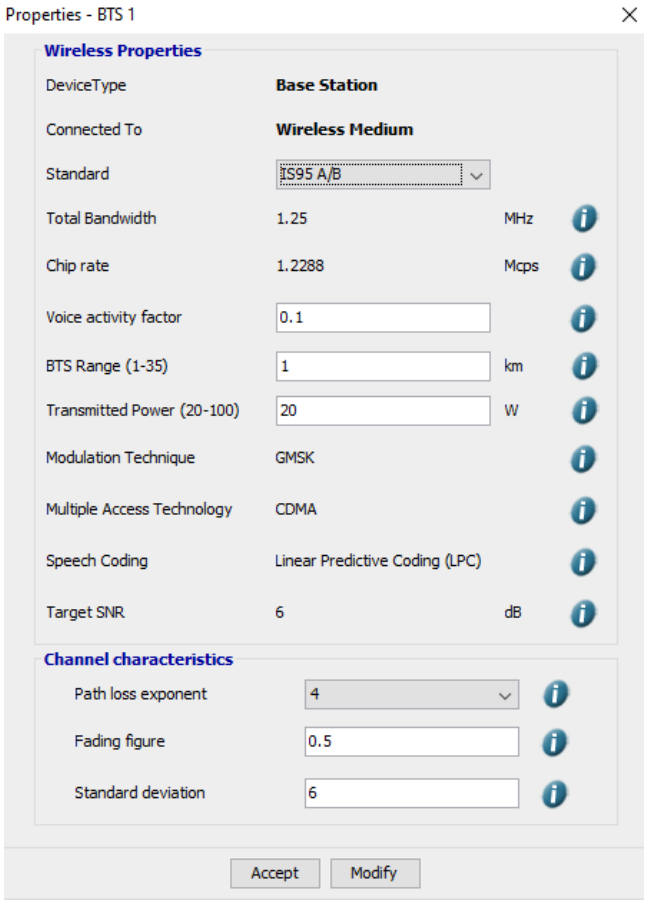
Kaplesh Mulchandani
D12A 45

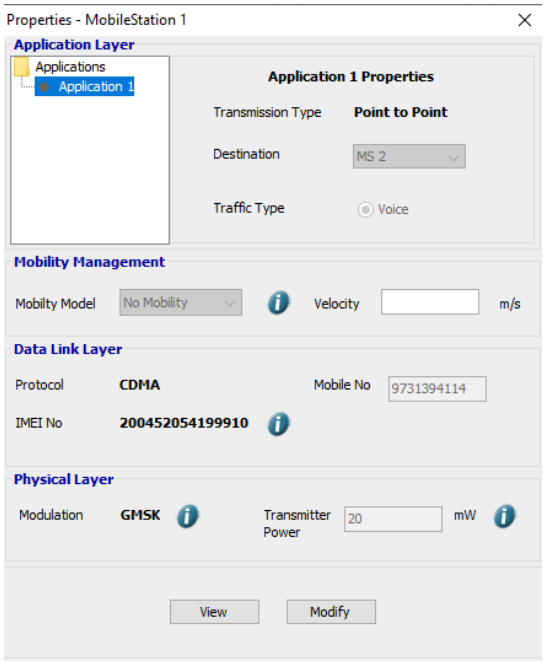
MC Experiment

Setting up BTS and MS:

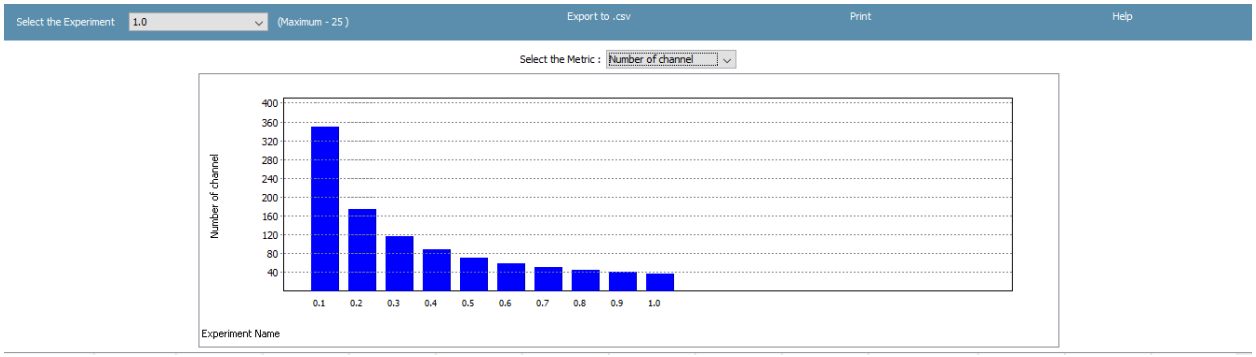
Changing BTS values:



Selecting the voice option is all the MS:



Number of Channels:



Experiment: 10

Aim : Wireless Network Security: Kismet, Wireshark and Netstumbler

Objective : study of Kismet, Wireshark and Netstumbler.

Description :

What is Kismet?

• Kismet is an 802.11 layer2 wireless network detector, sniffer, and intrusion detection system.

• Kismet will work with any wireless card which supports raw monitoring (rfmon) mode, and (with appropriate hardware) can sniff 802.11b, 802.11a, 802.11g, and 802.11n traffic.

• Kismet also supports plugins which allow sniffing other media such as DECT.

• Kismet identifies networks by passively collecting packets and detecting standard named networks, detecting (and de-cloaking) hidden networks, and inferring the presence of nonbeaconing
networks via data traffic.

Features

• 802.11b, 802.11g, 802.11a, 802.11n sniffing
• Standard PCAP file logging (Wireshark, Tcpdump, etc.)
• Client/Server modular architecture
• Multi-card and channel hopping support
• Runtime WEP decoding
• Tun/Tap virtual network interface drivers for real-time export of packets
• Hidden SSID de-cloaking
• Distributed remote sniffing with Kismet drones
• XML logging for integration with other tools
• Linux, OSX, Windows, and BSD support (devices and drivers permitting)

Reference Lab Manual / Mobile Communication and Computing /CMPN/Sem VI/VESIT

Kismet UI

The main Kismet window consists of

- The network list which gives a list of the connected devices and provides information like name, BSSID, Frequency, number of packets and size of the packets of these devices.
- GPS information which gives details about the GPS connectivity.
- A summary of the current server statistics and packet source status which gives the total number of networks, the total number of packets, the packet rate and the time elapsed.
- The status panel where errors and announcements are printed.

Additional components of the main window may be turned on with the 'View' menu.

Reference Lab Manual / Mobile Communication and Computing /CMPN/Sem VI/VESIT

Network View:

Preferences

Configuration of the Kismet UI is done entirely inside the UI via the 'Kismet->Preferences->...'
menus. Preference changes are (for the most part) immediate and do not require restarting. By default, the Kismet UI will prompt on startup to launch the Kismet server; this behavior (as well

as auto-connection and server setup) can be changed via the Startup and Shutdown preferences (Kismet->Preferences->Startup and Shutdown):
Reference Lab Manual / Mobile Communication and Computing /CMPN/Sem VI/VESIT
• Open Kismet server launch window automatically Kismet will open the server startup window when the UI is loaded, if the default server is not running.
• Ask about launching server on startup Ask to start a server (instead of just opening the server window)
• Show Kismet server console by default Automatically open the Kismet server console window after starting the server
• Shut down Kismet server on exit automatically Kill locally started servers and issue a shutdown command to remote servers when the UI exits
• Prompt before shutting down Kismet server Don't kill servers without confirming
Kismet menus support shortcuts, for e.g. '~Wl' is the same as navigating to the 'Windows->Client List' menu option.

Sound and Speech

The Kismet UI handles sound and speech playing for most users. Sound playing is straightforward (WAV
files are installed, by default, to /usr/local/share/kismet/wav) and can be played with any sound player compatible with your install.
Speech is supported on Festival and Flite. Any other text-to-speech program should work as long as it accepts plain text on standard in. Speech text is encoded depending on the type of speech event,
where %1, %2, etc. are replaced with data by Kismet. The supported events and replacements are:

• New network:

- Network SSID encoded to speech encoding setting (spell, nato, plain)
- Network channel
- Network BSSID

Reference Lab Manual / Mobile Communication and Computing /CMPN/Sem VI/VESIT
• Alert:
- Alert type
• GPS Lost, GPS Lock:
- No replacement options

Tagging networks

Kismet can add custom data to a network in the form of tags. In the Kismet UI, networks and clients can both have tags added to them. These tags are displayed in the UI under network details, and logged to XML and TXT output.
Tags can be set as permanent; by checking the "Remember note when restarting Kismet" checkbox in the Network and Client Note windows, the note is saved and will be re-applied to networks every time Kismet loads. Client tags are applied to a specific client in a specific network; currently there is no mechanism for adding a note to every instance of the client.

Sorting

Kismet defaults to "autofit" mode, where it tries to put as many of the currently active networks on the screen as possible. Because autofit mode is so variable, it doesn't make sense

to try to allow selecting networks in autofit. To select a network and view details, first sort by another method (such as channel, time, etc) via the Sort menu, then select a network.
Reference Lab Manual / Mobile Communication and Computing /CMPN/Sem VI/VESIT

NetStumbler

What is NetStumbler?

• NetStumbler (also known as Network Stumbler) is a tool for Windows that facilitates detection of Wireless LANs using the 802.11b, 802.11a and 802.11g WLAN standards.

• It runs on Microsoft Windows operating systems from Windows 2000 to Windows XP.

• A trimmed-down version called MiniStumbler is available for the handheld Windows CE operating system. The program is commonly used for: Wardriving

Verifying network configurations

Finding locations with poor coverage in a WLAN

Detecting causes of wireless interference

Detecting unauthorized ("rogue") access points

Aiming directional antennas for long-haul WLAN links

Finding Access Points

While running NetStumbler, the right-hand pane shows APs currently detected and available under the current view filter. By default, you have no view filter set, so all detected APs are displayed. Each AP listing is marked with a colored dot indicating the signal strength to that access point, alongside its MAC address, the unique identifier assigned to each network device. The colors range from red (signal too low) to yellow (marginal) to green (good). A grey dot marks an AP which had been detected but is now gone. A lock appears on the dot icon when the AP is operating with encryption enabled.

For many NetStumbler users, detecting available APs is the software's primary feature. Typically, the software is run on a mobile computer, which you either carry to some location or drive around with in the car, scanning the air for detected access points. The practice of hunting for access points has come to be known as "war-driving".

Reference Lab Manual / Mobile Communication and Computing /CMPN/Sem VI/VESIT

NetStumbler may better disambiguate access points which share an SSID. But more often, NetStumbler can continuously scan for access points as you roam about an area, presenting a convenient log of its activity, including audio notification. This functionality is typically not available from Windows' or vendor-provided wireless client software.

Exploring Access Points

The left pane of NetStumbler is an Explorer-like interface for navigating available wireless access points. Under the "Channels" heading, all detected access points are listed under their channel frequencies. Under "SSIDs," all detected access points are sorted by their network name and displayed. Two or more APs listed under the same SSID can also be found. This could indicate two separate wireless networks overlapping in range, which could cause problems for clients. Alternatively, it may indicate one wireless network with multiple APs available from the user's current location. In cases where multiple APs sharing the same

SSID are found, the "Subnet" field in the right pane shows which IP network the APs are operating on.

Signal-to-Noise Graphs

Clicking on an AP's MAC address in the left pane will replace the right pane with a live signal-tonoise graph. Note that this graph is accurate only if the user's network card is fully supported by NetStumbler. Signal-to-noise readings can be a powerful tool for troubleshooting the network and optimizing AP or antenna placement.

The graph overlays two sets of values – signal strength (green) and noise (red), measured in dBm. The "taller" the green plot, the stronger the signal; likewise, the taller the red plot, the more noise is present. For the best wireless performance, maximization of the signal and minimization of the noise is required. Typical sources of noise in the Wi-Fi 2.4GHz range include

microwave ovens, cordless phones, wireless video transmitters, and perhaps neighboring wireless networks. The consistency of the graph can be observed to determine the presence of sources of intermittent interference. Partially supported network cards will produce signal strength (green) plots which may or may not be accurate, along with no noise (red) plots.

Access Point Filters

The "Filters" item in the left pane expands to a list of criteria for filtering the right pane list of available access points. On clicking the "Encryption Off" filter, only the open APs will be listed on the right. Some of the filters are quite technical, and are only useful in specialized situations. If an AP is not seen on the right, but it is known that the AP is available, check that such a filter has not been selected which may exclude it from appearing.

Mobile Tracking with GPS

If the NetStumbling PC sports an attached GPS receiver, GPS support can be enabled in NetStumbler to track the location of detected APs. Use the View Options GPS menu to configure the receiver. NetStumbler will fill in the latitude and longitude fields in the right pane, and will record GPS data in logs which can be exported out through the File Export menu.

Extending NetStumbler

NetStumbler exposes a small library of functions which can be accessed through active scripting languages under Windows, including VBScript, JScript, and ActiveState's PerlScript and Python. NetStumbler can be connected to external scripts through the View Options Scripting menu. One popular approach to scripting connects NetStumbler events to text-to-speech output, particularly valuable for so-called "war-driving.

Reference Lab Manual / Mobile Communication and Computing /CMPN/Sem VI/VESIT

Case-study performed

The following was performed as an experiment in the laboratory as a case study on NetStumbler.

1. A wireless router was connected to a computer.
2. Configure the Router, i.e. make modifications in the Settings of the router and set it as an access point.
3. Connect Wi-Fi Dongle to the computer on which the wireless traffic has to be monitored.
4. Install the software required for the functioning of the of the Wi-Fi dongle.

5. Once the software is installed and the dongle is working, open the utility of the dongle and change the Mode to Station.
6. Connect to the infrastructure network created in Step 2 by connecting to the SSID ‘C13’ using the Connect to Site option.
7. Minimize the dongle utility and run the setup of NetStumbler.
8. Go to Start Menu Programs NetStumbler to open NetStumbler IDE.
9. Now the NetStumbler IDE displays all the available networks in its range and also all the stations (devices) which are trying to connect to any of the networks.
On monitoring the NetStumbler window for some time, it was observed that the network (C13) appeared in the list of SSIDs on the left side panel. Also, after a few minutes, some stations which were connecting to C13 network appeared on the left hand side panel of the window under the list of Channel 11 (as C13 was using channel 11