International Journal for Multidisciplinary Research (IJFMR)
ISSN: 2582 – 2160, Volume - 1, Issue - 2

Attacks on Wireless Network and Basic Tips for Securing Wi-Fi Zone

[1]Mr. Abhijit S.Bodhe, [2]Dr.Bhagwan Shree Ram, [3]Dr.A.S.Umesh

[1]Assistant Professor, Department of computer Engg.,SRES COE,Kopargaon(MS)
[2]Associate Professor, Department of Engineering, VTU,(KA)
[3]Director &.Professor, Department of computer Science & Engineering, SJVIT, Banglore(KA)

***Abstract*: Wireless attacks now a day's becomes a very common security issue when it comes to wireless networks and its security. Such attacks can really get a lot of information from one network that is being sent across a complete wireless network and use it to commit some crimes in may be same or other wireless or wired networks. Every wireless network is very exposed or vulnerable to such kinds of attacks and then it's very important that all the necessary security measures are taken to prevent the mess that can be caused by such attacks or at least know which type of attack we are under to find preventive measures. These attacks are normally carried out to target information that is being shared through the wireless networks. It is therefore very important to know of such attacks so that one is in a position to identify it in case it happens under network of same or different subnet. Some of the common network attacks have been outlined below in this paper. Also we discussed some general tips to prevent from such attacks for naive users which can be under such wireless attacks and could be easily prevented.**

I. Introduction

A wireless technology now a day's growing day by day with vast speed and also attacks on same are also increasing in same rate. This paper will focus on different types of attacks on wireless communication especially on wireless communications. So that anyone using this technology must know what kind of attacks can be possible and under which attack the system is.

Wireless network Attack Categories with types of attacks

- **Access control attacks-5**

These attacks attempt to penetrate a network by using wireless or evading WLAN access control measures, like AP MAC filters and 802.1X port access controls.

1. War Driving

Discovering wireless LANs by listening to beacons or sending probe requests and thereby providing launch point for further attacks.War Driving also defined as the act of searching for Wi-Fi wireless networks by a person in a moving vehicle, using a portable computer or PDA. The term War Driving is derived from the 1980s phone hacking method known as war dialing. War dialing involves dialing all the phone numbers in a given sequence to search for modems. The War Driving gained popularity in 2001, because that time wireless network scanning tools became widely available.

Some people do War Driving as a hobby and map out different wireless networks. But hackers will look for wireless networks and then break into the networks to steal data or to perform malicious activities.The initial war driving tools included simple software coupled with the WNIC (Wide-area Network Interface Coprocessor). Many organizations are not worried about their wireless networks because they could spot the war drive attacker inside their parking space and have onsite security pick and throw them out. But recent wireless technology developments enable a network to extend far beyond the parking space of an office building. In some cases, a wireless network has the ability to span several miles. Now an attacker can stay far away from the building and still catch a strong signal from the network.

2. Rogue Access Points

Installing an unsecured AP inside firewall, creating open backdoor into trusted network. Rogue Access Point is an Access Point that has either been installed on a secure company network without explicit planning, permission or authorization from network administrator or has been installed by a hacker to produce a man-in-the-middle attack. If the hacker is able to find the SSID (Service Set Identifier) in use by the network and the rogue AP has enough strength, it is easy for them to perform a man-in-the-middle attack and the wireless users will have no way of knowing that they are connecting to a Rogue Access Point.

The rogue access points are normally installed by employees who need additional freedom to move about at work. These types of rogue access points can be very dangerous since most users are not aware of all the security issues associated with wireless devices.

3. Ad Hoc Associations

Connecting directly to an unsecured station to circumvent AP security or to attack station.Wireless ad hoc networks are self-configuring, dynamic networks in which nodes are free to move. Wireless networks lack the complexities of infrastructure setup and administration, enabling devices to create and join networks "on the fly" – anywhere, anytime [3].

4. MAC Spoofing

Reconfiguring an attacker's MAC address to pose as an authorized AP or station.MAC spoofing is a technique for changing a factory-assigned Media Access Control (MAC) address of a network interface on a networked device. The MAC address that is hard-coded on a network interface controller (NIC) cannot be changed. However, many drivers allow the MAC address to be changed. Additionally, there are tools which can make an operating system believe that the NIC has the MAC address of a user's choosing. The process of masking a MAC address is known as MAC spoofing. Essentially, MAC spoofing entails changing a computer's identity, for any reason, and it is relatively easy.

5. **802.1X RADIUS Cracking**

Recovering RADIUS secret by brute force from 802.1X access request, for use by evil twin An attacker sets up a fake (well, real to the attacker) RADIUS instance. In general case, FreeRADIUS - Wireless Pwnage Edition can used, which is totally embarrassing to say so I'll say use FreeRADIUS WPE from now on. FreeRADIUS WPE is a patch for FreeRADIUS that configures it to automatically allow authenticators (APs) from all private address ranges, automatically accept any EAP-type, automatically accept any user credentials, and automatically log MS CHAP v2 challenges and responses[4].

- **Confidentiality attacks-5**

These attacks attempt to intercept private information sent over wireless associations, whether sent in the clear or encrypted by 802.11 or higher layer protocols.

1. **Eavesdropping**

Capturing and decoding unprotected application traffic to obtain potentially sensitive information. Network eavesdropping is a network layer attack that focuses on capturing small packets from the network transmitted by other computers and reading the data content in search of any type of information. This type of network attack is generally one of the most effective as a lack of encryption services are used. It is also linked to the collection of metadata. Those who perform this type of attack are generally black hat hackers; however, government agencies, such as the National Security Agency, have also been connected[5].

2. WEP Key Cracking

Capturing data to recover a WEP key using passive or active methods. WEP was included as the privacy component of the original IEEE 802.11 standard ratified in 1997. WEP uses the stream cipher RC4 for confidentiality, and the CRC-32 checksum for integrity. It was deprecated in 2004 and is documented in the current standard.

3. Evil Twin AP

Masquerading as an authorized AP by beaconing the WLAN's service set identifier (SSID) to lure users.The evil twin AP is an access point that looks and acts just like a legitimate AP and entices the end-user to connect to *our* access point. that can be used to convert our wireless adapter into an access point. This is a powerful client-side hack that will enable us to see all of the traffic from the client and conduct a man-in-the middle attack later on.

4. **AP Phishing**

Running a phony portal or Web server on an evil twin AP to "phish" for user logins, credit card numbers.A hacker sets its service identifier (SSID) to be the same as an access point at the local hotspot or corporate wireless network. The hacker disrupts or disables the legitimate AP by disconnecting it, directing a denial of service against it, or creating RF interference around it. Users lose their connections to the legitimate AP and re-connect to the "evil twin," allowing the hacker to intercept all the traffic to that device.

5. Man in the Middle Attack

Running traditional man-in-the-middle attack tools on an evil twin AP to intercept TCP sessions or SSL/SSH tunnels.attack where the attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. One example of man-in-the-middle attacks is active eavesdropping, in which the attacker makes independent connections with the victims and relays messages between them to make them believe they are talking directly to each other over a private connection, when in fact the entire conversation is controlled by the attacker. The attacker must be able to intercept all relevant messages passing between the two victims and inject new ones. This is straightforward in many circumstances; for example, an attacker within reception range of an unencrypted wireless access point (Wi-Fi) could insert himself as a man-in-the-middle.

As an attack that aims at circumventing mutual authentication, or lack thereof, a man-in-the-middle attack can succeed only when the attacker can impersonate each endpoint to their satisfaction as expected from the legitimate ends. Most cryptographic protocols include some form of endpoint authentication specifically to prevent MITM attacks. For example, TLS can authenticate one or both parties using a mutually trusted certificate authority

- **Integrity attacks-4**

These attacks send forged control, management or data frames over wireless to mislead the recipient or facilitate another type of attackData integrity ensures that the transmitted data arrives at the destination unchanged. The attack tools focus on frame manipulation, so that an attacker can cause the user to receive the information it chooses. (e.g., DoS).

1. 802.11 Frame Injection

Crafting and sending forged 802.11 frames. An attacker will inject their own Ethernet frames in the middle of the transmission. This can be used in a variety of ways to attack the user. The user can be misled into accepting frames that it did not intend. All the major Internet browsers were vulnerable to a frame injection attack. This vulnerability has been fixed, but it does give an example on how this can be used as an attack.

An attacker could inject frames into a transmission to display their content with the legitimate outer web page frames of another company. For example, a user would access their banking web page and it would look like their legitimate web page, but the attacker has injected Ethernet frames so that even though the web page looks legitimate it is not. When the user attempts to login all the login information can be recorder by the attacker.

2. 802.11 Data Replay

Capturing 802.11 data frames for later (modified) replay.This involves the attacker capturing authentication information and saving it for later use. This can be used for 802.1X Extensible Authentication Protocol (EAP) or for 802.1X Remote Authentication Dial-In User Service (RADIUS) authentications. Once the attacker has captured and saved the authentication information, it will monitor the traffic for another authentication. Then it will inject those frames instead of the legitimate authentication frames and essentially gaining access to a system.

3. 802.1X EAP Replay

Capturing 802.1X Extensible Authentication Protocols (e.g., EAP Identity, Success, Failure) for later replay.

4. 802.1X RADIUS Replay

Capturing RADIUS Access-Accept or Reject messages for later replay

- **Authentication attacks-9**

Intruders use these attacks to steal legitimate user identities and credentials to access otherwise private networks and services[7].

1. **Shared Key Guessing**

Attempting 802.11 Shared Key Authentication with guessed, vendor default or cracked WEP keys. An intruder by use of various cracking tools tries to guess the shared key of a wireless network and gain access to it. These tools make use of brute force technique (trying different combinations in real time) in order to make guessing of a shared key.

2. PSK Cracking

Recovering a WPA/WPA2 PSK from captured key handshake frames using a dictionary attack tool.PSK stands for Pre Shared key. A shared key can be in any format: a pass phrase or anything else. A PSK is a key that has already been shared. The attacker tries to intercept the successful handshake and then uses a dictionary attack to retrieve the shared key.

3. **Application LoginTheft**

Capturing user credentials (e.g., e-mail address and password) from cleartext application protocols. Here, the attackers try to steal the login credentials of a user like email address, username and password from application protocol.

4. **Domain LoginCracking**

Recovering user credentials (e.g., Windows login and password) by cracking NetBIOS password hashes, using a brute-force or dictionary attack tool. Attacking the domain names and retrieving the user credentials like username and password with the help of network sniffing tools. Such tools make use of brute force technique to gain access to user credentials.

5. **VPN Login Cracking**

Recovering user credentials (e.g., PPTP password or IPsec Preshared Secret Key) by running brute-force attacks on VPN authentication protocols.Cracking usernames and passwords by executing brute force attacks on VPN protocols.

6. **802.1X Identity Theft**

Capturing user identities from cleartext 802.1X Identity Response packets.The packets sent by the 802.1x protocol in response is captured by an attacker to crack user credentials.

7. **802.1X Password Guessing**

Using a captured identity, repeatedly attempting 802.1X authentication to guess the user's password also known as 802.1X Password Speculation After an attacker intercepts an identity, he/she continuously guesses the password in order to pass authentication.

8. **802.1X LEAP Cracking**

Recovering user credentials from captured 802.1X Lightweight EAP (LEAP) packets using a dictionary attack tool to crack the NT password hash The attacker captures the LEAP (Lightweight Extensible Authentication Protocol) packets and then cracks the user credentials from it.

9. **802.1X EAP Downgrade Forcing**

an 802.1X server to offer a weaker type of authentication using forged EAP-Response/Nak packets.Using this technique, an attacker forces the server to offer a weaker type of authentication by issuing continuous NAK/EAP packets in response. NAK stands for Negative Acknowledgement.

Availability attacks-10

These attacks impede delivery of wireless services to legitimate users, either by denying them access to WLAN resources or by crippling those resources.

1. AP Theft

Physically removing an AP from a public space. One of the most common wireless security threats is the rogue access point—it is used in many attacks, both DoS and data theft. Many other rogue access points, however, are deployed by employees wanting unfettered wireless access—these access points are called soft access points. Other rogues are located in neighboring companies using your network for free access. Typically low-cost and consumer-grade, these access points often do not broadcast their presence over the wire and can only be detected over-the-air. Because they are typically installed in their default mode, authentication and encryption are not enabled, thereby creating a security hazard.

2. **Queensland DoS**

Exploiting the CSMA/CA Clear Channel Assessment (CCA) mechanism to make a channel appear busy.also called as A clear channel assessment attack is physical layer DoS attack against Wi-Fi networks. The attack focuses the need of a wireless network to receive the "clear channel assessment"; which is a function within CSMA/CA to determine whether the wireless medium is ready and able to receive data, so that the transmitter may start sending it. The attack makes it appear that the airwaves are busy, which basically puts the entire system on hold. The signal telling the system the airwaves are busy is of course sent through the attacker's NIC, by placing it in continuous transmit mode. The attack can be set up through the use of the Intersil's Prism Test Utility

3. 802.11 Beacon Flood

Generating thousands of counterfeit 802.11 beacons to make it hard for stations to find a legitimate AP. The legitimate AP emits a legitimate beacon signal that the user will look for. The fake AP is emitting many fake beacon signals. The user has a much better chance of trying to connect to one of the fake beacon signals rather than the one legitimate one. This leads to a DoS since the user cannot connect to the legitimate AP

4. **802.11 Associate / Authenticate Flood**

Sending forged Authenticates or Associates from random MACs to fill a target AP's association table. Flooding is overloading the network with a certain type of packet so that the wireless AP is busy serving all the flooding packets that it cannot serve any legitimate packets, Generally When attempting to associate with a wireless network, clients search for an in range access point and request to connect. This authentication process takes place prior to joining the network. Any wireless client must first authenticate to the target network and ensure compatibility before being able to join and forward traffic over a given wireless network.

5. **802.11 TKIP MICExploit**

Generating invalid TKIP data to exceed the target AP's MIC error threshold, suspending WLAN service. The TKIP vulnerability discovered by Erik Trews and Martin Beck is very different from the previous, well-known attacks against WPA-PSK. Previous attacks targeted the method WPA-PSK uses to generate the initial key from the passphrase and network SSID, by brute forcing possible passwords and generating a table of the results. The new attack targets the TKIP data exchange itself, and can affect both PSK and EAP/Dot1X (enterprise) networks. It does not affect networks which use AES encryption (such as WPA2-AES). WPA1 networks using AES encryption are not affected, and WPA2 networks which still use TKIP are vulnerable. By exploiting the fact that packets in QoS queues may arrive out of order, an attacker can defeat the replay protection in TKIP and reuse a captured frame. Applying an older WEP attack known as "chopchop", the plaintext of the packet can be revealed byte-by-byte. However, the maximum rate at which the attacker can guess each byte is limited by the TKIP message integrity check (MIC). If two invalid MIC events occur within 60 seconds, the station will shut down for 60 seconds, and then reassociate with new key.

6. **802.11 Deauthenticate Flood**

Flooding station(s) with forged Deauthenticates or Disassociates to disconnecting users from an legitimate AP

7. **802.1X EAP-Start Flood**

Flooding an AP with EAP Extensible Authentication Protocol -Start.Flood messages to consume resources or crash the target EAP is an authentication framework for providing the transport and usage of keying material and parameters generated by EAP methods.

8. 802.1X EAP-Failure

Observing a valid 802.1X EAP exchange, and then sending the station a forged EAP-Failure message.

9. **802.1X EAP-of-Death**

Sending a malformed 802.1X EAP Identity response known to cause some APs to crash.

10. **802.1X EAP Length Attacks**

Sending EAP type-specific messages with bad length fields to try to crash an AP or RADIUS server.

- **Miscellaneous Attacks-10**

1. Rogue access points

A rouge access point is basically an access point that has been added to one's network without one's knowledge. One totally has no idea that it is there. This is a kind of scenario that can create a kind of back door especially if one is not conversant with it and have complete management of it. This is an access point that can create some very huge security concerns.

One is due to the fact that it can be very easy to plug in a wireless access point in it. If one is not doing any type of network access control protocols on one's network, it becomes very easy for additional workstations and access points to be added onto one's network.

This can be combated by having some network access controls in place or occasionally have some walks around one's building and see if one can come across access points that one have no idea of. One can use some special tools that one can obtain from the internet that will enable one to see all that is happening in one's wireless network.

One might also consider using the 802.1X Network Control Access so that people authenticate to the network every time they plug in a device either in a wireless or wired network. This will not necessarily prevent people from plugging in an access point but it will require the people connecting to that access point authenticate through the methods one have set in place.

2. Jamming/Interference

Wireless interference basically means disruption of one's network. This is a very big challenge especially owing to the fact that wireless signals will always get disrupted. Such interference can be created by a Bluetooth headset, a microwave oven and a cordless phone. This makes transmission and receiving of wireless signals very difficult.
Wireless interference can also be caused by causing service degradation so as to make sure that one denies complete access to a particular service. Jamming can also be used in conjunction with an evil twin.
Combating interference should be one's primary goal in case in happens. One way can be through the use of a spectrum analyzer so as to narrow down to what could be causing the jamming problem. One can use simple software to examine one's traffic. However, using some of the spectrum analyzers might not be so much easy and therefore some training is required.
One can also consider boosting the power of existing access points so that if a different device is causing the interference, then it will be overpowered. One can also try using different frequencies. If the bad guys are creating interference by selecting a narrow band of frequencies to take one's signals down, one can channel one's signals to operate at different frequencies. One can also decide to hunt down where the offending signal is coming from so as to get it out of the network and allow one's network traffic to communicate normally.

3. Evil twin

A wireless evil twin mainly comes into play when criminals are trying to create rogue access points so as to gain access to the network or access to information that is being put through a network. Coming up with an evil twin is very simple since all one need to do is purchase a wireless access point, plug it into the network and configure it as exactly as the existing network. This is possible in open access points that do not have any passwords associated with them. Once one comes up with one's access point, one plugs it into the network so that it becomes the primary access point thus overpowering other existing access points. With this, one's evil twin will tend to have a stronger network signal and therefore people will choose it. Through this, the individual controlling the access point will be in a position to see all the information being sent around the network.
One way through which one can protect one's self from an evil twin is through encryption of one's data. Through this, people who have set up the evil twin cannot read one's information even if they capture it.

4. Bluejacking

Blue jacking is a kind of illegal activity that is similar to hacking where one can be able to send unsolicited messages to another device via Bluetooth. This is considered spam for Bluetooth and one might end up seeing some pop-up messages on one's screen. Bluejacking is possible where a Bluetooth network is present and it is limited to a distance of ten metres which is the distance a Bluetooth device can send a file to another device. It rarely depends on antennae. Bluejacking works on the basis that it takes advantage of what is convenient for us on our mobile devices and the convenience is being able to communicate and send things back and forth between devices. With this, one can easily send messages to other bluetooth devices since no authentication is required. Some third party software can also be used to carry out Bluejacking.

5. War chalking

War chalking is another method that was used so as to determine where one could get a wireless access signal. In this case, if an individual detected a wireless access point, he or she would make a drawing on the wall indicating that a wireless access point has been found. However, this is not currently used.

6. Initialization Vector attack

An IV attack is also known as an Initialization Vector attack. This is a kind of wireless network attack that can be quite a threat to one's network. This is because it causes some modification on the Initialization Vector of a wireless packet that is encrypted during transmission. After such an attack, the attacker can obtain much information about the plaintext of a single packet and generate another encryption key which he or she can use to decrypt other packets using the same Initialization Vector. With that kind of decryption key, attackers can use it to come up with a decryption table which they and use to decrypt every packet being sent across the network.

7. Packet sniffing

Packet capturing and sniffing is a very big challenge when it comes to wireless networks. In this case, an individual is in a position of capturing a packet that one are sending across a network and see the kind of information that one are sending to a particular individual. Packet sniffing is possible due to the fact that most of the information that we send is clear and does not have any encryptions in it. This makes it very easy for an individual to read its contents. With capturing of information being sent across a network very easy, it becomes incredibly easy to hear or see everything that is going through the network.
To be successful in packet sniffing, one has to ensure that one's network card is silent. This means that one need to make sure that one's card is not sending information to the network if the network is busy.
In this case, it therefore becomes very important that one take all the necessary measures to ensure that data that one is sending across a network is encrypted. One can decide to use WPA2 or WPA to encrypt one's data. With such encryption types, it becomes very difficult for packet sniffers to obtain the decryption keys and read the information in the packets.

8. Replay attacks

Replay attacks are some form of network attacks where an individual spies on information being sent between a sender and a receiver. The individual can also spy on conversations between the two people. Once the individual has spied on the information, he or she can intercept it and retransmit it again thus leading to some delay in the data transmission. In such kind of an attack, a network attacker can use this kind of information to fool around with the computer so as to gain access to it without detection. In

addition, an attacker is in a position to get information such as an encryption key which he or she can later use in the replay attack to prove his identity and authentication.

9. WEP/WPA attacks

WEP attacks are very common wireless network security problems that normally result due to the general weakness of the WEP encryption methods and systems. This is considered a very poor way to encrypt one's data and in some other cases, one's access point may not allow for the use of WEP as a method of encryption. If one see a legacy wireless access point that is encrypted with WEP, one should try as much as possible not to trust it owing to the fact that it is a very weak way of encryption. Access points encrypted with such methods become very vulnerable to WEP attacks from the bad guys who want to acquire access to a particular access point.

10. WPS attacks

WPS attacks are some other wireless network attacks that can be very dangerous. With the major flaws present in the protection of wireless networks an individual with a WPS password guessing tool is in a position to launch such an attack on a particular network. With the password guessing tool, an attacker is in a position to retrieve the wireless network passwords and use the password to gain access to data and information that is on one's network. To avoid being a victim of such an attack, it is very important to make sure that one's WPS protocols are strong so as to prevent an individual from retrieving one's password information.

As a matter of fact, network attacks are network threats that we cannot avoid if we are working on wireless networks or using them. This is because all wireless networks normally have vulnerabilities and loopholes that make it very easy for the bad guys to carry out their network attacks. It is therefore important that we are conversant with the ways of identifying and preventing such attacks.

II. GENERAL TIPS FOR SECURING WIFI

Now that you don't trust anything on the Internet anymore, let's build that confidence back up. There are a lot of ways to make yourself less susceptible to wireless attacks.

- **Use WPA2 security:** This takes enough work to crack that most hackers will look for an easier target. Make sure WPS is turned off!
- **Minimize Your Networks Reach:** Try to position your router in the center of your home or building. There are tools available to measure the reach of your network, and you can adjust the signal level. Try to make it so that the signal beyond your walls is degraded enough that it isn't usable. You may also consider using directional antennae if central placement is not an option.
- **Use Firewalls:** Make sure your APs firewall is enabled. If you can afford a hardware firewall and feel you need the extra security, go ahead and install one. Household networks generally can get away with the standard router firewall, and operating system firewalls.
- **Use a VPN on Open Networks:** If you really must use public WiFi, set up a VPN. Most smart phones have this capability. You can set one up on your PC. This allows you to communicate through an encrypted tunnel back to your home or office. You can even send web traffic through a VPN.
- **Update Software and Firmware:** Keep your system up to date with the latest patches, and make sure any online applications you use are updated as well. Check for AP firmware updates related to security flaws, and implement them as soon as possible. Remember to follow best practices for network modification to ensure you don't interrupt a critical task. Check out your updates in a test lab to make sure that they don't interfere with an important application. Don't perform updates during normal operating hours if possible, and if you must update during work hours make sure everyone is aware that network connectivity could slow down, or be cut off temporarily while you work.
- **Use Strong Passwords:** I recommend you use at least a 15 character password.Use a mix of upper/lowercase letters, numbers, and symbols. Again, don't make it easy. Is the only capital letter at the start? Is there an exclamation at the end? Are there any words in there? These are common bad password practices, and hackers love them.
- **Change the Login Credentials:** Make sure you change the administrative login credentials. This is often something like admin/admin or admin/password by default.
- **Disable your SSID (service set identifier) Broadcast**: This isn't a security measure. The right tools will still find your network's SSID (this is the name of your network in case you didn't know). However, there's a small chance it could help your network fly under the radar.
- **Enable MAC Filtering:** Again, MAC filtering is not security. A knowledgeable hacker knows how to monitor your network and copy the MAC address of a connected device. They can then spoof their own MAC to appear as an authorized device to gain access. However, this is another annoyance for them to deal with [9].

III. Conclusion

In proposed paper we studied various types of attacks on wireless network with general tips to secure the wireless network for such attacks. But these are some simple and basic attacks in reference I shared some papers which helps to understand topic in more detail. After reference 9 check other reference of better understanding of attacks and prevention methods.

Reference :-

[1]http://searchsecurity.techtarget.com/feature/A-list-of-wireless-network-attacks
[2]http://www.omnisecu.com/security/infrastructure-and-email-security/common wireless-attacks.php
[3] https://en.wikipedia.org/wiki/Wireless_ad_hoc_network
[4] https://depthsecurity.com/blog/when-802-1x-peap-eap-ttls-is-worse-than-no-wireless-security
[5] https://en.wikipedia.org/wiki/Eavesdropping
[6] https://www.cse.wustl.edu/~jain/cse571-07/ftp/wireless_hacking/index.html
[7] http://www.brighthub.com/computing/smb-security/articles/53951.aspx
[8] https://en.wikipedia.org/wiki/Clear_channel_assessment_attack
[9] https://phoenixts.com/blog/types-of-wireless-network-attacks/
[10]Dr.Sanjay Thakur Mr.Abhijit S.Bodhe , Dr.A.S.Umesh A Review Paper On Wireless Network Attacks: With Existing Methods to Locate And Eradicate RAPs. 5th international conference on recent trends in engineering science & Management at PGMCOE,Wagholi,Pune Dec 2016.
[11]Abhijit S Bodhe Dr AS Umesh, Rouge Access point: A Threat to Wireless SocietyIAETSD Vol 04 Issue 07, Dec 2017.
[12] Dr.Sanjay Thakur Prof. Abhijit S Bodhe, RAPD Extension with Temporal Traffic Characteristics international Journal of Computer Science and Information Technology Research Vol 3 Issue 2 April 2015