Advances in Computer Science and Information Technology (ACSIT)
Print ISSN: 2393-9907; Online ISSN: 2393-9915; Volume 2, Number 6; April-June, 2015 pp. 573-579

http://www.krishisanskriti.org/acsit.html

Cracking and Hardening Hidden-SSID of Wireless Access Point

Neeraj Kumar Gupta[1], Mridul Kumar[2] and Md. Zeeshan[3]

[1,2,3]Galgotias College of Engineering & Technology Greater Noida, U.P.
E-mail: [1]neeraj26493@gmail.com, [2]mridulinlko@gmail.com, [3]zeenu811@gmail.com

Abstract—*WLAN system has become an important part, to provide mobility and feed increasing number of users, in an organization. WLAN access-point radio waves cannot be restricted to four walls of room, creating privacy and security concern to organisation. Hidden-SSID is the feature provided by WLAN access-point manufacturers to minimize the privacy and security concern of organisation. In this paper, the present protection scheme is analyzed thoroughly and it is explained how it can be cracked. It is also shown that how this feature can be made harder to crack.*

1. INTRODUCTION

With increase in the number of handheld devices and demand for mobility, wireless local area network has become important. WLAN access-point (AP) discovery based on IEEE 802.11 standard suffers from privacy problem[2,5]. WLAN access-point (AP) uses several Frames and Headers for its operation and none of them are encrypted. Hence they can be easily sniffed, for exploitation analysis, and injected in the network. Due to plain text nature of IEEE 802.11 frames and headers, several protection mechanism become useless.

WLAN clients can probe for networks in two possible ways[2]:

1. Directed Active Probing*:* The client sends a probe message on each radio channel and gets a response only from APs that serve the requested SSID.These directed active probes contains the name of networks to which the client has already been connected. The continuous probing is necessary for fast handoffs when the signal from a previous AP fades.
2. Undirected Active Probing: The clients sends an undirected probe message that do not specify the SSID and to which all APs respond. This has the problem that it uses more bandwidth and could be slower if there are multiple responses.

An alternative to probing is passive scanning, in which theclientwaitsfor Beacon frames oneachradiochannel. Thisis muchslowerthanprobingandmayresultinlowerquality ofservice.

In case of active probing, the directed active probes reveals the name of client's list of preferred network identifiers, SSID, to anybody listening creating privacy issues for the clients. Hence it can be seen that there is unbalance between the performance and privacy in current 802.11 network discovery schemeWLAN APs creates the privacy concern for the organisation as the radio waves generated cannot be restricted to four walls. APs announces its presence by broadcasting the SSID, which is human-readable and often contain name of organisation, companies or government departments. Hidden networks restrict APs point from broadcasting the SSID, gives organisation some privacy. The clients need to send directed active probe to every AP they encountered. This creates the tradeoff between the privacy for the network and for the client. Many organisation gives importance to their infrastructure security rather than that of the client. They seehidingthenetworkasdefenseindepthwhenused in combination with other mechanisms such as link-layer encryptionandMAC-addressfiltering.

In this paper, we present the logical flaws present in the IEEE 802.11 network discovery scheme which render the Hidden-SSID protection mechanism useless. Finally, we propose an added security mechanism in order to spoof the automated tools which gives a false sense to the attacker that he/she has cracked the Hidden-SSID feature.

2. IEEE 802.11 AND PRIVACY

IEEE 802.11 standard is part of a family of standards for local and metropolitan area networks, providing specification for Medium Access Control (MAC) and Physical Layer. Wireless local area network based on IEEE 802.11 standard operates in two mode: Ad hoc mode and Infrastructure mode. Ad hoc network composed solely of stations within mutual communication range of each other via the wireless medium. Infrastructure mode consist of one or more access points (APs) and some client stations (STA). Access point (AP) is an entity that has station functionality and provides access to the distribution services, via the wireless medium (WM) for associated stations. Each client station is identified by a hardware MAC address, which is globally unique identifier of their network card. In the same way, AP is identified by a basic service set identifier (BSSID), which is equal to the

hardware MAC address of the AP's wireless interface.The network, also called an extended service set (ESS), is identified by a human-readable name called a serviceset identifier (SSID).

An AP broadcasts regularly its SSIDs. The SSID is selected by the network administrator. Since SSID is not globally unique, so it only give partial information about the identity of the network. Typical SSID values are derived from the names of businesses, university departments, coffee shops,commercialwirelessoperators,andfictionalnames chosen by home users.But since SSIDs are human readable, this information is often immediately meaningful to a human observer without the need for extensive data collection or correlating observations from different times and locations. Hence, AP operators may feel that the SSID is sensitiveinformationandthatbroadcastingitmakesthem vulnerable to unwanted attention.

For this reason, the AP operator can configure the AP in such a way that it does not broadcast its SSID. This security mechanism is known as Hidden-SSID feature or network clocking. The hidden SSID gives the AP a degree of privacy compared to the usualpublicSSID:theSSIDwillnotbevisibleintheuser interface of wireless clients that come into the range of the AP. Nevertheless, disabling the SSID is a widely recommended practice and many AP administrators heed the advice. This indicates that there probably is a legitimate need for some wireless networks to appear nameless to outsiders.

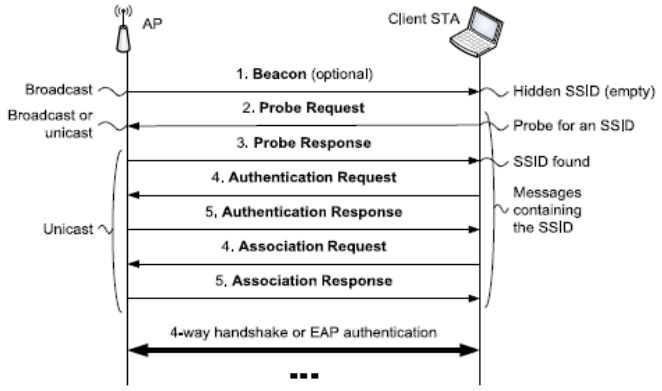

Fig. 1: 802.11 network discovery and association with a hidden SSID or active probing[1,2].

Fig. 1 shows the association process between client and AP. Various Messages (Frames) transmitted during the process are as follows:

1. Beacon Frame[3]: Access point periodically broadcast these frame to announce its presence to all the wireless clients in the vicinity. Beacon frame contains SSID field which contains the network name chosen by network operator.
2. Probe Request Frame: The wireless client searches the network to check if any APs are available. This is done by sending probe request packets. The client can send a broadcast probe request or specific proberequest. In specific probe request either the user enters the SSID or the client uses the previous history or cache of the SSIDs it has connected to in past.If the probe request packet is a broadcast packet then it is known as Null Probe Request Packet. This frame is sent by CLIENT to broadcast its presence to the AP and to ask them for their SSIDs.
3. Probe Response Frame: An AP responds to the Probe Request of the client by Probe Response and tells the client that it is an valid AP and tells client it`s SSID. This frame also include access point's security parameter that is what kind of security access point uses and so on.
4. Authentication Request Packet: In this frame an authentication request packet is sent from the client to AP, to authenticate or verify the connection. In this packet client sends the security key or passphrase which is used for authentication. An authentication response packet is sent from the AP to client telling the client if the authentication is successful or not. The authentication request and response packets are always in sequence. For example. If the authentication request packet SEQ = 0x0001 Then the authentication response packet SEQ = 0x0002.
5. Association Frame: After the authentication is successful by the AP, then CLIENT sends an association request frame. This frame requests the AP to associate or tell the AP to make a connection to share data. The AP responds back to this request with association response frame and AP and CLIENT are associated now i.e. they are now connected and ready to share data. Association response packets contain the parameters and capabilities of the connection.
6. De-Authentication Frame: This frame is not used in the authentication and association process but it is used to deliberately break a connection. This packet can be sent by STA or AP. When the user wants to disconnect the wireless connection and clicks on disconnect option then STA sends a De-Auth frame which breaks the connection. Suppose there is some changes that are made on AP regarding the security or SSID then AP sends De-Auth frame to break all the connections to various STA.

Clients need to get authenticated and associated with AP to access the network. Figure1showsindetailthe802. 11networkattachment procedureforan APthathasahidden SSID. The A Psends a broadcasted Beacon frame which contain SSID field which can be either null or contain network name. In case of hidden SSID, the SSID field is null. After observing the beacon which is optional, the client usually sends several Probe Request. In practice,aclientkeepsalistofknownnetworks. In directed (unicast, specific probe) active probing, the client sends the

Probe Request depending on the implementation. The client will probe either for all known networks (E.g. Windows XP pre-SP2) or only ones for which the probing has been manually enabled (e.g., Windows Vista). In undirected (broadcast, Null probe) active probing, the client will send broadcasted Probe Request (E.g. Android OS). The AP encounter either the broadcasted or unicast Probe Request. In case of broadcasted SSID, the AP return the Probe Response Frame if the AP receives broadcasted Probe Request. If request is unicast, the AP also returns but only when the SSID value in Probe Request should be same as that of AP. If the hidden-SSID feature is enabled, then AP will only respond to the unicast Probe Request containing same SSID as that of AP.

3. 802.11 FRAME FORMAT

Frames used in 802.11 can be broadly divided into three categories: Management Frame, Control Frame and Data Frame. Each of the frame has several defined subtypes. Fig. 2 shows the general frame format.

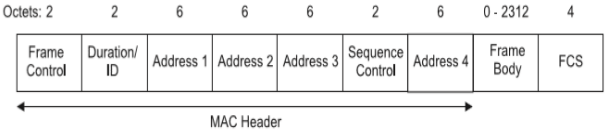

Fig. 2: 802.11 MAC frame format[1]

Generic 802.11 MAC frame is shown in Fig. 2. Frame format contains several fields which are used to control various operations of 802.11. Function of some of these relevant field is as follows:

1. Frame Control Field: It encapsulates various information such as protocol, type of frame (management, data or control), subtype of frame (authentication request, response etc.). The format of Frame Control Field is illustrated in Fig. 3.

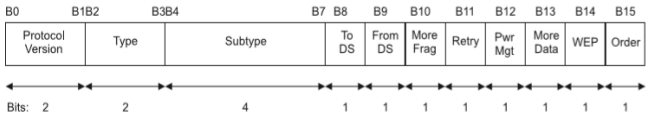

Fig. 3:Frame Control Field[1]

1.1. Type and Subtype Field: The Type and Subtype together identify the function of the frame. Type field identify whether it is a control, management or data frame. Some of the valid combination of type and subtype is shown in Table 1.

Table 1: Valid Type and Subtype combination[1]

Type Value b3b2	Type description	Subtype Value b7b6b5b4	Subtype description
00	Management	0000	Association request
00	Management	0001	Association response
00	Management	0010	Reassociation request
00	Management	0011	Reassociation response
00	Management	0100	Probe request
00	Management	0101	Probe response
00	Management	1000	Beacon
00	Management	1010	Disassociation
00	Management	1011	Authentication
00	Management	1100	Deauthentication

2. Address Fields: There are four address field in the MAC frame format. These field indicates BSSID, source address (SA), destination address (DA), receiver address (RA), transmitter address (TA). It is not compulsory to use all four address at one time. A MAC sublayer address is one of the following type:

2.1. Source address (SA): It identifies the MAC entity from which the data in the frame body field is initiated.

2.2. Destination address (DA): It identifies the MAC entity or entities intended as the final recipient(s) of the data in the frame body.

2.3. Receiver address (RA): It identifies the intended immediate recipient of the data in the frame body.

2.4. Transmitter address (TA): It identifies the station which has transmitted the frame in the wireless medium.

3. Sequence Control Field: This field consist of two subfields: Sequence number and Fragment number. Sequence number is a 12 bit field indicating sequence number of the frame. Each transmitted frame is assigned a sequence number by transmitting station. Fragment Number field is a 4-bit field indicating the number of fragments of a particular frame corresponding to a particular sequence number.
4. Frame Body Field: It contains data specific to individual frame types and subtypes.
5. FCS field: It stands for Frame Sequence Check. It is basically CRC (cyclic redundancy check) over the entire MAC header and frame body. What happens is, CRC is run over the entire MAC header with frame body and the four byte value is stored in FCS.

The frame format for a Management frame is independent of frame subtype and is shown in Fig. 4.

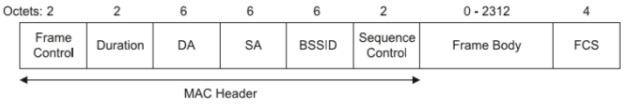

Fig. 4: Management Frame Format[1]

4. CHANNEL AND MONITOR MODE

IEEE 802.11 specifies implementation of wireless local area network in 2.4, 3.6, 5 and 60 GHz frequency band. For instance, IEEE 802.11b, 802.11g, and 802.11n operates on 2.4 GHz band utilizing the 2.400-2.500 GHz spectrum[4,7]. Each spectrum is subdivided into channels. Channel is the

connection, either physical or logical, which is used to convey the information signal. The 2.4 GHz band is divided into 14 channels spaced 5 MHz apart, beginning with channel 1, which is centered on 2.412 GHz. Different countries defines different allowable channels in their country. Most Wi-Fi certified devices uses the permitted frequencies and channel in any nation. Wireless AP based on IEEE 802.11 can be in any one of the permitted channels. In order to communicate, WNIC need to be in the same channel of AP[4].

Table 2: List of permitted channel[1]

Channel	Frequency MHz	North America	Japan	Most of the World
1	2412	Yes	Yes	Yes
2	2417	Yes	Yes	Yes
3	2422	Yes	Yes	Yes
4	2427	Yes	Yes	Yes
5	2432	Yes	Yes	Yes
6	2437	Yes	Yes	Yes
7	2442	Yes	Yes	Yes
8	2447	Yes	Yes	Yes
9	2452	Yes	Yes	Yes
10	2457	Yes	Yes	Yes
11	2462	Yes	Yes	Yes
12	2467	No	Yes	Yes
13	2472	No	Yes	Yes
14	2483	No	Yes	No

IEEE 802.11 wireless network card can operate in one of the six operating mode: Master, Managed, Ad-hoc, Mesh, Repeater, Monitor. Monitor mode causes the wireless network interface card (WNIC) to pass all traffic it receives to the Central Processing Unit[8]. While in Managed mode, when a WNIC receives a frame, it normally drops it unless the frame is addressed to that WNIC's MAC address or is a broadcast or multicast frame. In Monitor mode traffic can be captured without having to associate with an access point. In monitor mode, the cyclic redundancy check values are not checked for captured traffic, so some captured traffic may be corrupted. Monitor mode is used for network monitoring and packet sniff.

5. PROPOSED METHOD OF CRACKING HIDDEN SSID FEATURE

The main logic behind cracking method is that the frame transmitted, during the authentication and association process, is in plaintext. These frames can easily be sniffed and injected for exploitation and there is no method yet to detect out that whether any frame is authentic or forged one by attacker. The Hidden-SSID feature can be attacked actively as well as passively. The proposed cracking method has been divided into two parts to reduce the complexity: Detecting the wireless network, Extracting the hidden network name.

Detecting the wireless network is the process of identifying the wireless network in the vicinity. Figure5 shows the flow of chart of detecting wireless network.

The steps involved in the flow chart are explained below:

STEP 1: Since the AP wireless interface can be in any of the permitted channel. So we need to hop the channel of attacker's wireless interface to sniff data from each permitted channel[7]. For instance, if the AP is on channel 2 and attackers wireless is on channel 5, the attacker's machine will not able to detect the AP because it will not be able to detect the traffic of channel 2.

STEP 2: Capture the Beacon Frame so that we might be able to see the name of available wireless interfaces. Since the Beacon frames are broadcasted frames, so it's not necessary to put attacker's wireless interface into monitor mode.

STEP 3: After capturing Beacon Frames, extract the SSID field value, channel on which AP wireless interface is operating, and the BSSID of AP interface.

STEP 4: If the SSID field is not NULL, then show network name as that of SSID field value.

STEP 5: If the SSID field value is NULL, the show it as "Hidden Network".

After the detection of available wireless network present in the near vicinity, now SSID of the hidden network can be retrieved in the following way:

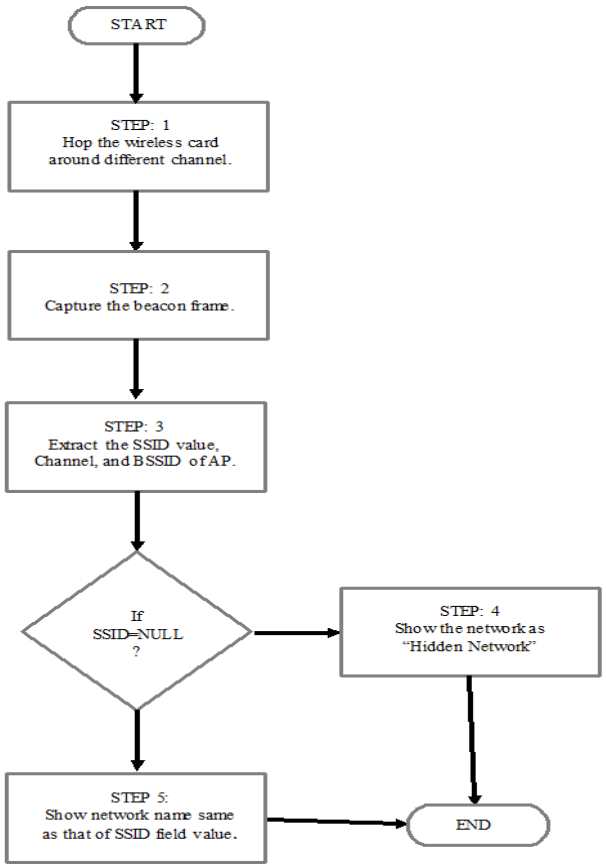

Fig. 5: Detecting wireless network

STEP 1: It might be possible that more than one hidden network would be available in the near vicinity. So in that case, we have to identify the network using the basic service set identifier (BSSID) or MAC address of the AP.

STEP 2: The wireless card must be put into the monitor mode. This is done so that all the traffic in the medium can be sniffed.

STEP 3: The attacker's wireless interface must be in the same channel as that of the "Hidden Network" AP. This is done to ensure that no traffic must be skipped off in the current channel. If the channel of attacker's wireless interface hops or is in different channel, then it might be possible that attacker might losses the Probe Response(s).

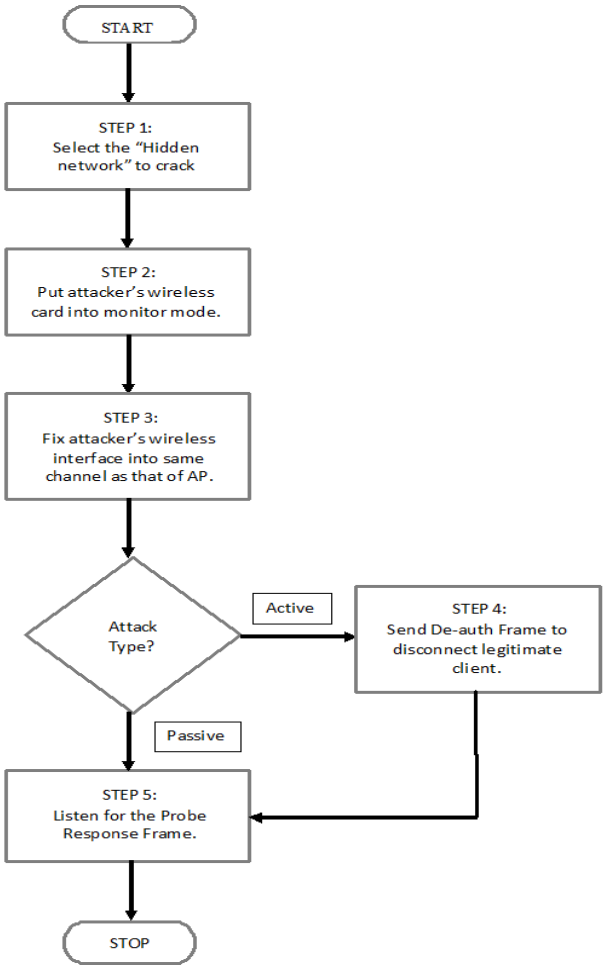

Fig. 6: Extracting Hidden-SSID

STEP 4: In active attack, De-auth frames are injected into wireless medium from attacker's machine as if it were generated by the AP. Since the client, does not have any mechanism to authenticate the frame. So the client will be disconnected from AP. After client get disconnected, it will try to reconnect due to active probing or it will manually try to connect. In the process of authentication and association, the Probe Response will be generated by AP which will be captured by attacker's machine. Since Probe Response contains SSID which can easily be retrieved. The active attack is very fast if at least one connected client is present in the network.

STEP 5: In passive attack, the attacker silently listen for the Probe Response. In passive attack, the attacker might need to wait for the new client to connect or wait for already connected client to get disconnected due to some reasons and again try to connect. Due to this reason, passive attack might be time consuming.

In active and passive attack, the attacker look out for the Probe Response. The above method can be used to build the automated tool which will find out the name of hidden network by capturing the Probe Response and hence breaking the Hidden-SSID feature of AP.

6. PROPOSED METHOD FOR HARDENING HIDDEN SSID FEATURE

In this section, a technique is proposed which makes the detection of Hidden-SSID almost impossible for the script kiddies and make it harder for experienced crackers.

Script kiddies uses the automated tools for cracking the hidden-SSID feature. Automated tools basically relies on the Probe response to uncover hidden SSID of network. As IEEE 802.11 does not have any mechanism to check whether the frame is forged or authenticated. This lack of checking can be used to harden the hidden-SSIDdetection by injecting the frames over the wireless network. This will thwart the attempts of script kiddies to penetrate the network. It also increases the overhead of experienced cracker to crack it and might causes the less experienced cracker to fail in penetrating the network.

The main principle of proposed technique is that any forged frame can be injected into wireless network without any checking. So in this technique the forge frames involved in authentication and association process and some data frames are injected in the wireless network. The SSID values used in the forged frames are used apart from real network name. Fig. 7 show the flow chart of hardening the hidden-SSID feature. The various steps involved are as follows:

STEP 1: The virtual interface[8] is created above actual wireless network interface card. This interface behaves as of any real WNIC. Airmon-ng is a utility available in LINUX for creating the virtual interface. By creating virtual interface, we can perform packet sniffing and injection using the virtual interface and can connect to access point using the actual network interface card. Virtual interface reduces the need of extra hardware. Forged frames are injected using virtual interface.

STEP 2: The WNIC card is put into monitor mode. The reason for putting WNIC is that no Probe Response is generated in monitor mode.

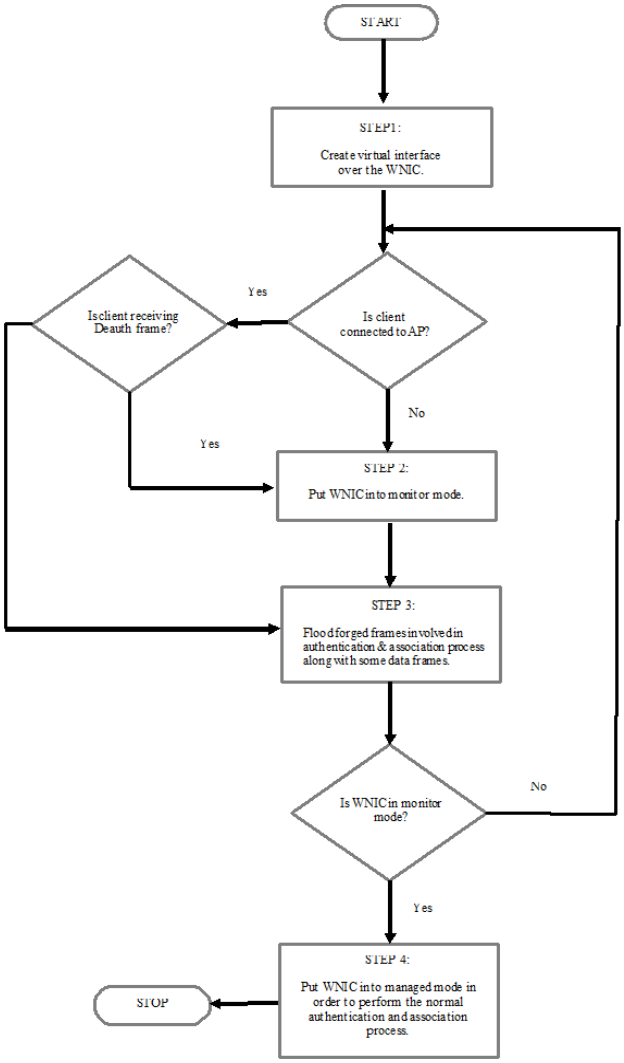

Fig. 7: Hardening Hidden-SSID method

STEP 3: Let us consider the cases:

1. The client is not connected to AP, and the attacker attacks passively and waits for the Probe Response frame. Since our card is in monitor mode so no probe request will be generated and hence there will be no Probe Response. Forged frames are injected in this step which will also contain the Probe Response frame with fake SSID. As soon as the automated receives the Probe response, it will search for the SSID, but the SSID value is spurious.
2. The client is connected to access point and the attacker attacks actively by sending Deauth Frames. As soon the client receives the Deauth frame, it puts the WNIC into monitor mode so that no real Probe Response will be generated due to directed active probing. Since the forged frames are injected which will again fool the automated tool.
3. If the client is connected and it does not receive Deauth frame, the also it sends the forged frame to fool the automated tool attacking in passive mode.

STEP 4: The card is again put into managed mode so that normal authentication and association process can be initiated. The process can be iterated until the client is connected to AP. Since large number of forged frames are generated with spurious SSID value. So an experienced attacker attacking manually using packet analyzer tools like Wireshark will receive a large number of frames with fake SSID. So it will be time consuming for the attacker to filter out the correct SSID value. Forged data frames are generated so that the attacker might not be able to filter out the forged frames based on MAC address.

So the proposed technique, make it almost impossible for the automated tool to penetrate the hidden-SSID feature. It also increases the complexity and time consuming for the experienced attacker to crack it.

7. CONCLUSION

IEEE 802.11 authentication and association protocol was thoroughly analyzed in a most basic way and its basic way of working is explained. Privacy issue related to the protocol were discussed. Working of Hidden-SSID privacy mechanism is discussed along with its shortcomings. The shortcomings are used to penetrate the hidden-SSID feature. The newproposed method fools the automated tools into thinking that hidden SSID has been discovered but in reality only the spurious SSID value which was inserted in forged packet is discovered not the real one. It also increases the job of experienced attacker. Ever method comes with its advantages as well as disadvantages. Some of them are as follows:

1. Spoof the automated tools which give a false impression to attacker that he has cracked the network but might not be able to restrict the experienced attacker.
2. Efficient system in protecting the networks from so called script kiddies but it consume bandwidth.

In future there is vast scope in this field to develop artof penetration testing and securing 802.11networks.

REFERENCES

[1] IEEE Standard for Information technology — Telecommunications and information exchange between systems — Local and metropolitan area networks — Specific requirements — Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. IEEE Std 802.11-2007 (Revision of IEEE Std 802.11-1999), June 2007.

[2] J. Lindqvist, T. Aura, G. Danezis, T. Koponen, A. Myllyniemi, J. Mäki, and M. Roe. Privacy-preserving 802.11 access-point discovery. In Proc. of ACM WiSec'09, Mar. 2009.

[3] Information Embedding in IEEE 802.11 Beacon Frame (http://research.ijcaonline.org/ctngc/number3/ctngc1027.pdf)
[4] R. Chandra, P. Bahl, and P. Bahl. MultiNet: Connecting to Multiple IEEE 802.11 Networks Using a Single Wireless Card. In Proc. of Infocom, Mar. 2004.
[5] Threats to Wireless Local Area Network (WLAN) and Countermeasures" ,A.V.Dhaygude, K.R. Patil, A.A.Sawant ,ICONS'07,January 27-29,2007,Erode,Tamilnadu,India
[6] Wireless LAN: Security Issues and Solutions: http://www.sans.org/reading_room/whitepapers/wireless/wireless lan-security-issues-solutions_1009.
[7] Ms. Swati Jadhav and Prof.SandeepVanjale, Wireless Rogue Access Point Detection Using Clock Skew Method, IJARCCSE, Oct 2013.
[8] OtusileOluwabukola, AwodeleOludele, A.C Ogbonna, AjeagbuChigozirim, and Anyeahie Amarachi, A Packet Sniffer (PSniffer) Application for Network Security in Java, Informing Science and Information Technology, 2013.