Journal of Mobile, Embedded and Distributed Systems, vol. I, no. 1, 2009
ISSN 2067 – 4074

Issues in WiFi Networks

Nicolae TOMAI
Faculty of Economic Informatics
Department of IT&C Technologies
Babes Bolyai Cluj-Napoca University, Romania
tomai@econ.ubbcluj.ro

Abstract: The paper has four sections. First section is intro in WiFi technology and terminology. The second section shows the security architectures and algorithms used in WiFi networks. Both important mechnisms: encryption/decryption as well as authentication is analyzed within simple IEEE 802.11 aproach in section three and four. The architectures such as WPA or WPA2 are not subject of this paper.

Key-Words: m-application security, WiFi, IEEE 802.11, WEP.

1. WiFi Introduction

The WiFi is common name for wireless local area networks technology compling with IEEE 802.11 standards and owned by WiFi Alliance. The WiFi Alliance promotes standards with the aim of improving the interoperability of wireless local area network products based on the IEEE 802.11 standards. The Wi-Fi Alliance is a consortium of separate and independent companies and it agrees on a set of common interoperable products based on the family of IEEE 802.11 standards. The figure 1 describes the overview architecture of a WiFi LAN.

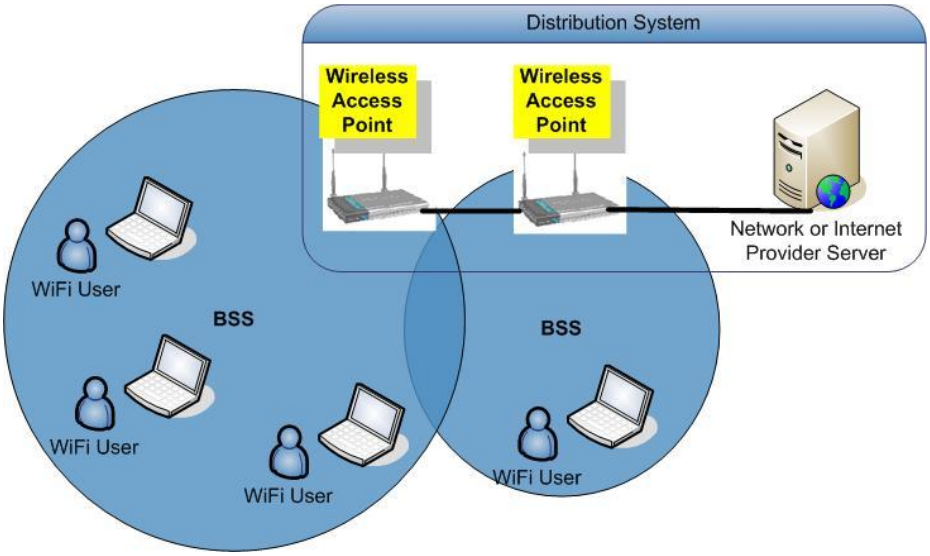

Fig. 1 Overview of a WiFi LAN

A WiFI LAN consists from these components:

- The end-user device with IEEE 802.11 board – radio network interface cards - NICs – it could be PDA, smart-phone or laptop;
- BS/AP – Base Station or Access Point – a device with antenna wich send and receive radio packets over wireless environment from the end-user devices;

ISSN 2067 – 4074

- BSS – Basic Service Set – is the cell coverage formed by radio antenna of the Access Point device;
- DS – Distribution System – is the items that provide Internet to the APs. It is possible to have in the office or home an Intranet without having a distribution system. There is only one AP and all devices communicate and interconnect each other like through a network router.
- ESS – Extended Service Set – contains all the BSSs, APs and Dss from an WiFi LAN and it is seen as a single IEEE 802.11 layer to all the upper layer from OSI Network Model.

An IEEE 802.11 local area network is based on a cellular architecture. Each cell - BSS - Basic Service Set is controlled by a BS - Base Station – called also AP – Access Point. Most of the installations of an IEEE 802.11 LAN are formed from one or more cells and their respective access points. The access points can be connected with Ethernet or in some cases wireless itself in order to provide a DS - Distribution System.

2. WiFi Authentication Mechanisms

In order to supervise a Wireless LAN it is better to use an 802.11 packet analyzer such as OmniPeek or nGenius Sniffer Wireless. The understanding of different 802.11 frame types is a basis for deciphering what the network is or isn't doing. The 802.11 standard provides various frame types that, stations – NICs and access points. Each frame has a control field that shows the 802.11 protocol version, frame type, and various indicators – WEP is on/off, power management is active, and so on. In addition all frames contain MAC addresses of the source and destination station including access point; a frame sequence number; frame body and frame check sequence for error detection.

The 802.11 data frames contain protocols rules and data from the higher layers within the frame body. A data frame, for instance, could be carrying the XML code from a Web page (complete with TCP/IP headers) that the user is viewing. Other frames that stations use for management and control carry specific information regarding the wireless link in the frame body. For instance, a beacon's frame body contains the service set identifier (SSID), timestamp, and other pertinent information regarding the access point.
For more details regarding 802.11 frame structure and usage, 802.11 standards are a good start. The standards for WiFi are free for download from the 802.11 Working Group Web site [WIMT08].

For protecting data in WiFi LAN, there are many developed security architectures such as ones from figure 2:

ISSN 2067 – 4074

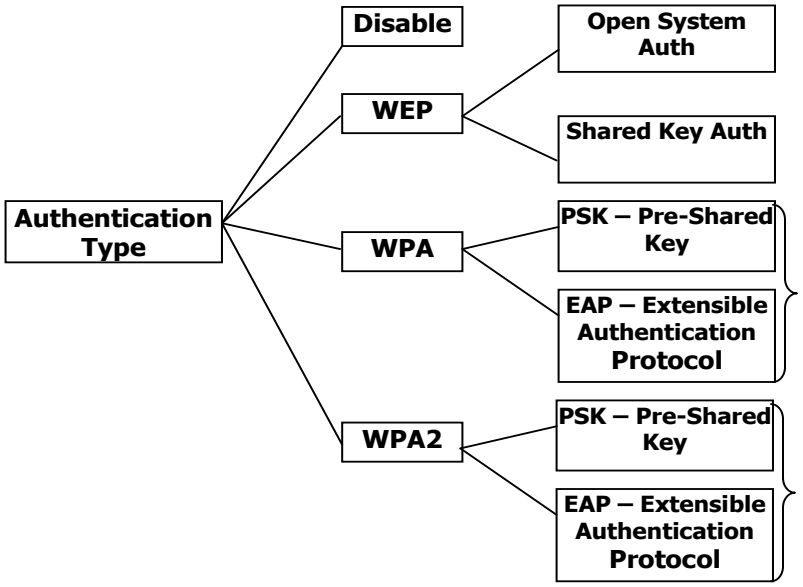

Fig. 2 Wireless LAN authentication type

Table 1 presents the security architectures from figure 2 with various features including the algorithms and techniques that are used:

Table 1 WiFI Security Architectures

Security Architecture	IEEE 802.11	WPA	IEEE 802.1x or IEEE 802.11i-WPA2
Authentication Protocol	WEP – Open System or Shared Key	PSK or EAP	PSK or EAP with CCMP
Encryption method	RC4	TKIP-RC4 or AES	TKIP-RC4 or AES
The Length of the key	40 bits	128 bits for encryption 64 bits for authentication	128 bits
The length of the Initialization Vector (IV)	24 bits	48 bits	48 bits
Key Management	NONE	IEEE 802.1x/EAP	IEEE 802.1x/EAP
The key per packet	The concatenation of the IV	The Mixing of the function	NONE
Data Integrity	CRC-32	Michael	CCM

The encryption, authentication and confidentiality in WiFi networks are ensured using one of the following security archtectures: WEP, WPA or WPA2.

The WEP – Wired Equivalency Policy consists into three main parts: WEP encryption/decryption, WEP authentication and WEP Integrity. WEP Integrity is ensured using CRC-32 algorithm. WEP Authentication use Shared Key and WEP Encryption uses a crypto scheme based on RC4 algorithm. WPA and WPA2 are similar with WEP but a little more complicated.

ISSN 2067 – 4074

3. WEP Encryption and Decryption

All the WEP Encryption/Decryption and WEP Authentication (not Open System) services are based on a password known only by acess points and NIC that will communicate within WiFi LAN. Most operating system provides a user interface to insert the WEP/WPA key like in figure 3:

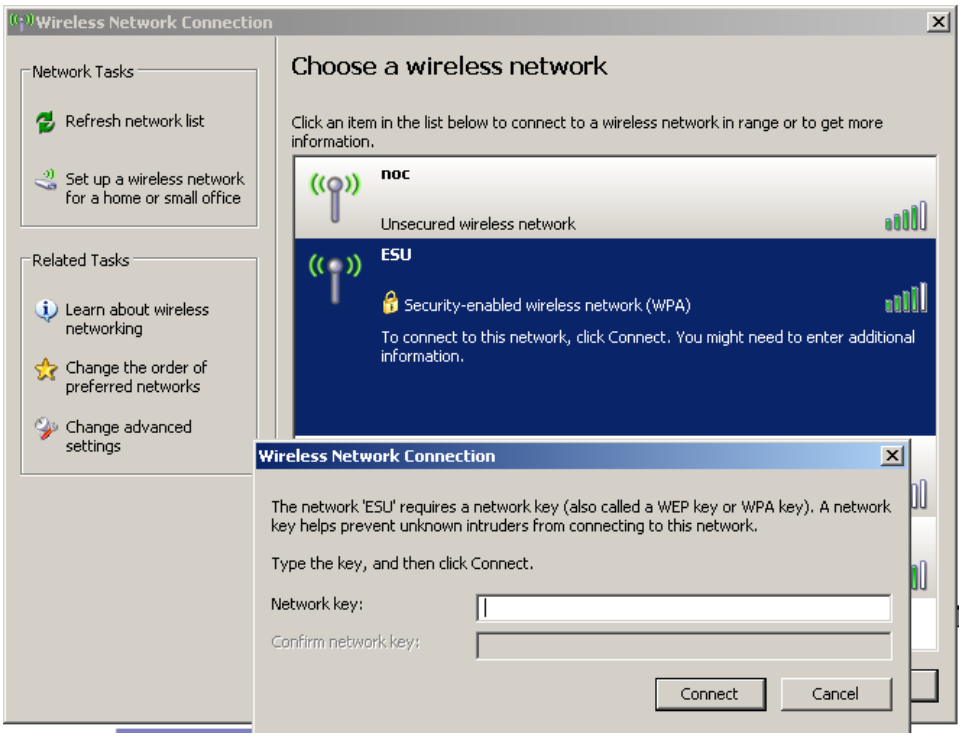

Fig. 3 User interface for entering WEP or WPA key

After the WEP key is introduced (in advanced system this key could stay on a smart card, HSM or a RADIUS Authentication Server), the security of the IEEE 802.11 standard is ensured by WEP – Wired Equivalency Policy. The encryption algorithm for WEP is in figure 4.

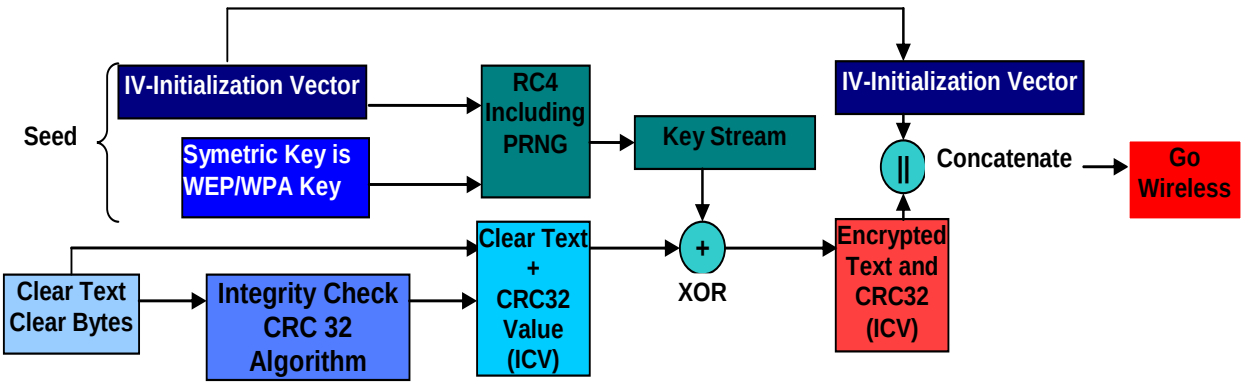

Fig. 4 WEP encryption scheme

ISSN 2067 – 4074

If the device sends a encrypted packet over WiFi using WEP in IEEE 802.11 secure architecture then the user insert a symmetric encryption key (the same as the one from Wireless router set by the network admin) to the application which manage the WiFi stack. The algorithm ARCFOUR (RC4 – see the crypto chapter) is used in order to generate a key stream. The CRC32 function is applied to the clear packet in order to do integrity check. The resulted packet is going into XOR function with key stream and it results the encryption of the clear byte array and CRC32 value – ICV (Integrity Check Value). Before the network packet to go in the air the encrypted packet (which contains ICV) is concatenated with the initialization vector. The wireless router or the wireless receiver gets the initialization vector in clear and the encrypted message. The receiver has the symmetric key for the RC4 encryption algorithm and get from the air the IV value (Initialization Vector) and encrypted packet (which contains the encrypted Text and ICV) as in figure 5.

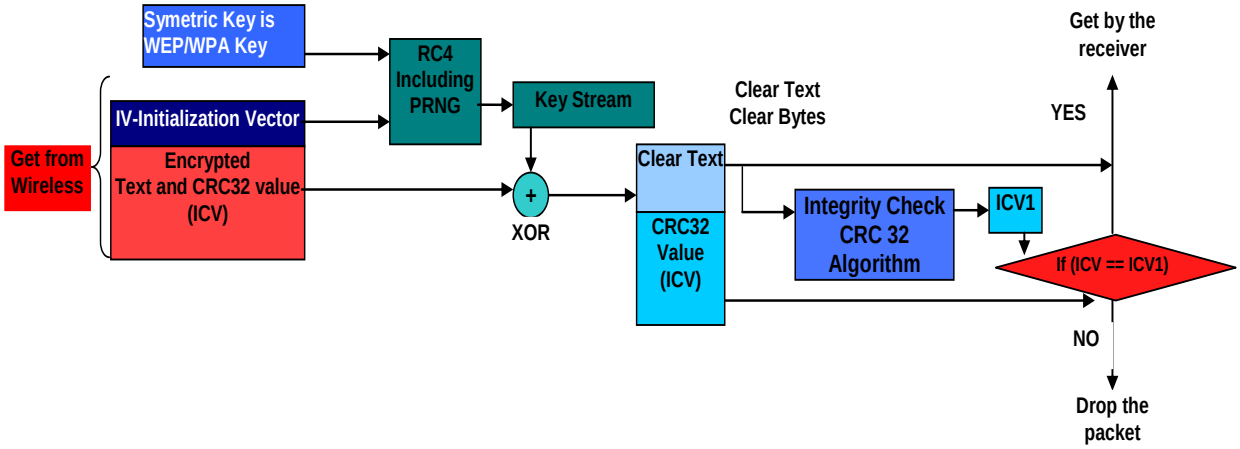

Fig. 5 WEP decryption scheme

The receiver is now able to rebuild the key stream for decryption. The encrypted text and the ICV – Integrity Control Value is decrypted with the obtained key stream. The decrypting module is able to get the ICV and clear text. The CRC32 algorithm is applied to the clear text and it is obtain 4 bytes of the ICV1 – Integrity Control Value. If ICV1 and ICV is the same then the clear text was corectelly decrypt so the module of decryption send the clear text to the receiver application. The explained flow is detailed in figure 6.

ISSN 2067 – 4074

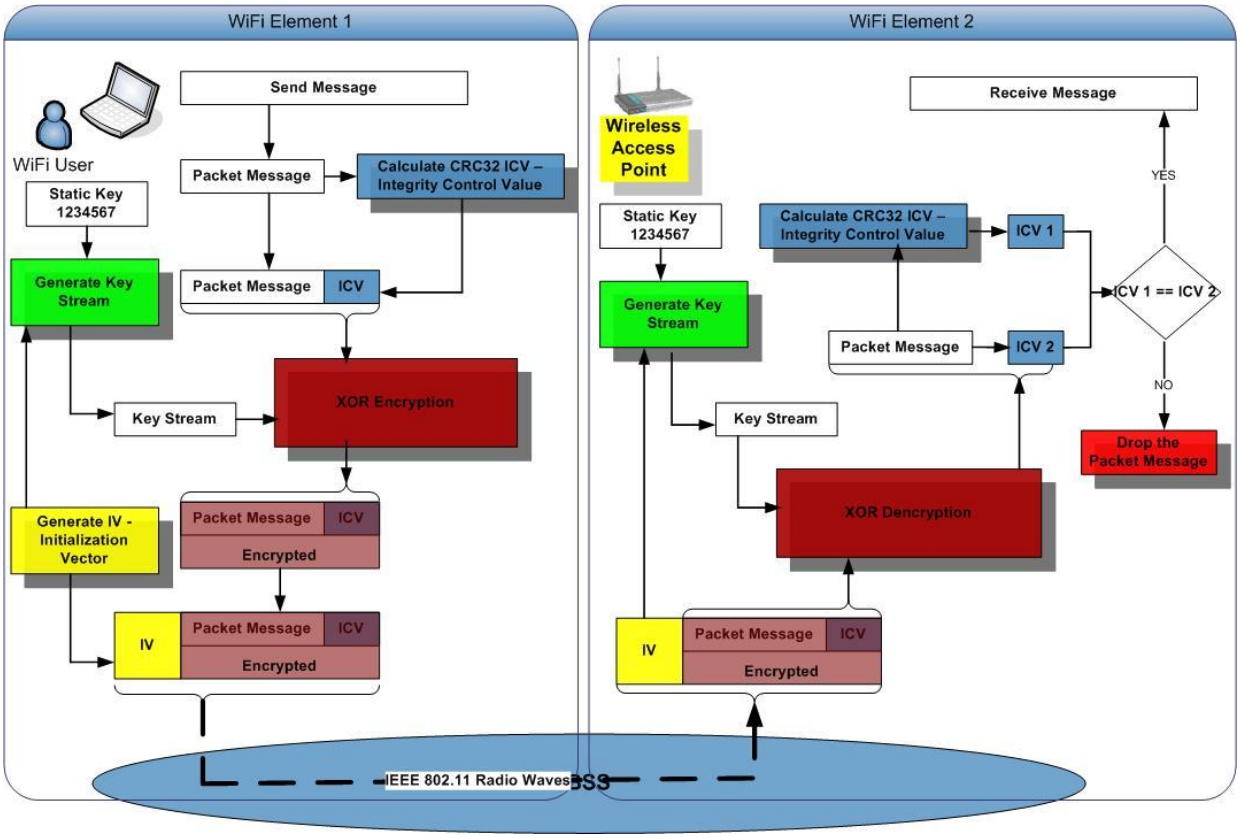

Fig. 6 Logical flows for the encryption and decryption in WEP

The details of the structure of wireless packet in the air are in figure 7.

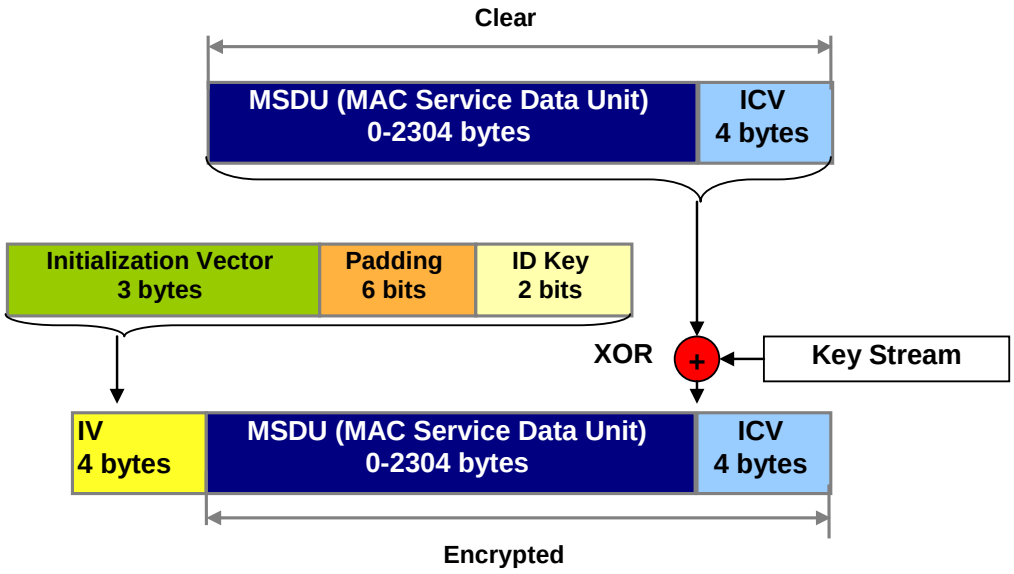

Fig. 7 The structure of the wireless packet in the air

The flow of the encryption is depicted in the left side of the figure 6. The message is divided into many messages. For the each obtained message's packet is made the calculation of the ICV – Integrity Check Value on 4 bytes using CRC32 algorithm. Each packet is concatenated with its own ICV. For each packet transimission in the air is generated an IV – Initialization Vector which has 4 bytes. The IV contains 3 generated

ISSN 2067 – 4074

bytes, a 6 bits section for padding and 2 bits for key identification as in figure 10. The IV on 4 bytes goes in clear together with the encrypted packet message. The IV 4 bytes value is used with symmetric static key in RC4 algorithm and the PRNG – Pseudo Random Number Generated to generate the key stream. The key stream encrypts the message packet using XOR bits function.

WEP Encryption/Decryption Issues

The major issues for WEP security are releated to the RC4, CRC32 algorithm and IV – Initialization Vector. The RC4 PRNG is producing an infinit byte array for encryption using a small symmetric static key. The sender executes a XOR function over the clear packet frame using the infinit byte array key sequence provided by RC4. The receiver implements the reversal mechanism obtaining the original packet frame.

If
$E1 = C1 \oplus RC4(v,k)$ and $E2 = C2 \oplus RC4(v,k)$
(where C1, C2 = the clear byte array of the WiFi packet frames which have the last 4 bytes the CRC32 value, E1, E2 = the encrypted bytes array, v = the IV – Initialization vector, k = the static symmetric key, $\oplus$ = is the XOR function, RC4(v,k) = the random byte array which represents the key sequence produced by RC4 using v and k as input), then $E1 \oplus E2 = (C1 \oplus RC4(v,k)) \oplus (C2 \oplus RC4(v,k)) = C1 \oplus C2$.

The XOR function applied to the encrypted packet frames (E1 and E2) generates the result of the XOR of the clear packet frames (C1 and C2). If an eavesdropper modify a bit in the encrypted packet frames then that bit is found in the clear packet frames. The only measure in WEP Encryption/Decryption mechanism to avoid such type of attack is to use CRC32 for the message integrity.

The ICV – Integrity Check Value field (4 bytes) is calculated as output of the CRC32 function applied on the clear packet frame. The problem of the CRC32 is that the algorithm is linear. The generator polynom is clear and an eavesdropper can calculate the bit difference between the two ICVs. If the generator polynom of the CRC is known, it is clear which bits in ICV should be modified in order to obtain consistent ICV values.

The IV value in WEP is stored in 24 bits and it is sent in clear in each wireless packet frame. An AP at a 54 Mbps bitrate which is activated for 1500 bytes per packet frame will finish all the possible bits combinations for IV in 5 hours = 1500 bytes * 8 bits / (54 Mbps $*10^6$) * 2^{24} =
[12000 / (54*1000000)] * 16777216 = (12/54000) * 16777216 = 0,00022 * 16777216 = 3690 sec = 1 hour. This means that in one hour, an attacker has time to compare from hour to hour the various encrypted messages (the messages were encrypted using the same key sequence because the IV is the same from hour to hour). It is worst if the WiFi card for an AP starts with IV value zero and increment by one for each packet frame sent into the air. A fast solution is to provide dynamic keys as in CISCO WEP solution from CISCO Aironet solution.

4. WEP Authentication

The WEP Authentication is done in many modes**: Open Authentication** (not use RC4), **Shared Key Authentication** (use RC4), and **MAC filters**. The **SSID-Service Set Identifier** is very important for a mobile station in order to know at which AP – Access Point it will be assigned. The SSID should be assigned to an AP and also to be configured for each station. Once the client mobile station becomes activated in transmission environment, it starts to search APs into the activation area using probe request frames.

ISSN 2067 – 4074

Those probe request frames are broadcasted to all the APs that have the same SSID with the mobile client station. All the APs that have the same SSID respond with probe response frames. The mobile client station determines the AP that will be used in WiFi data exchange taking into account the best bitrate and loading rate. Once the mobile client station established the AP used for WiFi communication, it starts the authentication process. The IEEE 802.11 specification shows **Open Authentication** (not use RC4) and **Shared Key Authentication** as recommended.

The MAC filters are not part of the standard. The MAC filters are very good in practice because the AP can be configured to not accept the WiFi mobile client stations which do not have the MAC from the AP's white list. The major inconvinient for this kind of authentication is the possibility to change the MAC address for an IEEE 802.11 board which is included into a mobile client station. The mobile client station authentication consists in the following transactions:

1 The mobile client station broadcasts a frame request on every channel
2 The AP from client's action area sends a frame response
3 The client decides which the most advantageous AP will be used and sends an authentication request frame
4 The AP sends back the response to the client's authentication frame
5 If the authentication is done with success the client sends an association request frame to the AP
6 The AP responds with an association response frame
7 The mobile client station sends data to the AP using the WEP encryption and decryption mechanism if it is configurated otherwise will send the data in clear.

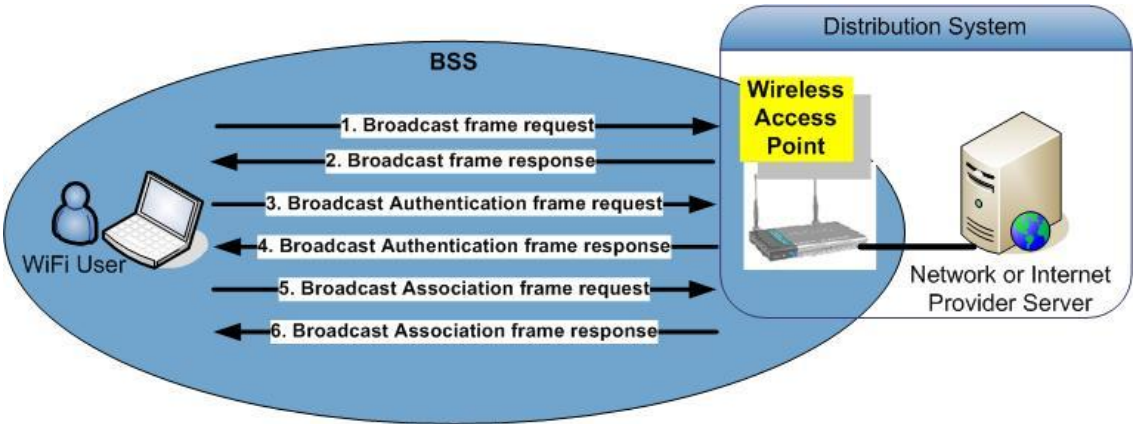

Fig. 8 The client authentication

The authentication can be made between the AP and the mobile client station or between two mobile client stations (ad-hoc networks). So, it is clear the authentication can be done only in case of unicast frames but not multicast frames.

WEP Open System Authentication

The AP accepts any kind of authentication request frame. The connection is made very fast and the authentication consists in two messages: the authentication request frame and the authentication response frame as in figure 9. WEP Open Authentification does not offer the possibility to verify if the mobile client station is valid or not.

ISSN 2067 – 4074

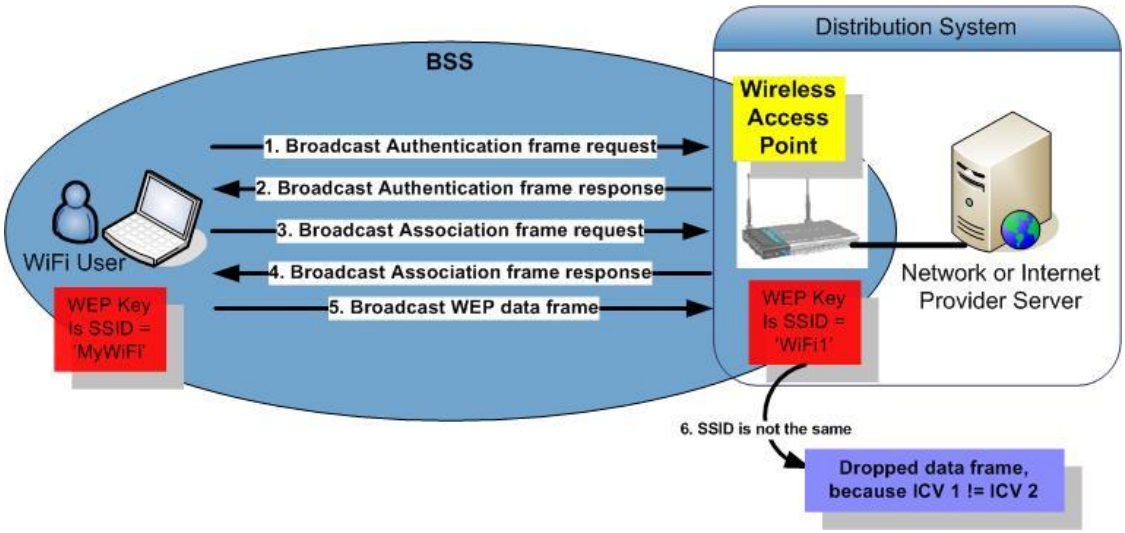

Fig. 9. WEP Open Authentication with different WEP keys (in this case with different SSID)

Practically for Open Authentication, the SSID authentication mechanism is used. The SSID is not encrypted and it is included as "beacon" into information frames of the APs. These frames are not encrypted so with traffic analyzer program is very easy to find out the active SSIDs in an area. So, it is not recommended to use for authentication and confidentiality the SSID mechanism. Thus, any device which has the SSID name of the AP, can connect to the WiFi network. The usage of the WEP Open Authentication without WEP encryption/decryption protocol becomes a major vulnerability. If an AP has the WEP encryption/decryption mechanism activated (this means to have a value for the symmetric static key), the WEP key becomes a modality to control the access to the resources.
If the mobile client station does not know the correct WEP symmetric static key, then the client can not send WiFi frames even if the client knows the AP's SSID (the authentication was successful).

WEP Shared Key Autentication

WEP Shared Key Authentication uses a cryptographic scheme based on chalange-response mechanism for the authentication. The AP and the mobile client station have stored/configured the same symmetric shared key. This authentication method is elementary and does not provide the authentication of the AP, only the mobile client station is authenticated.

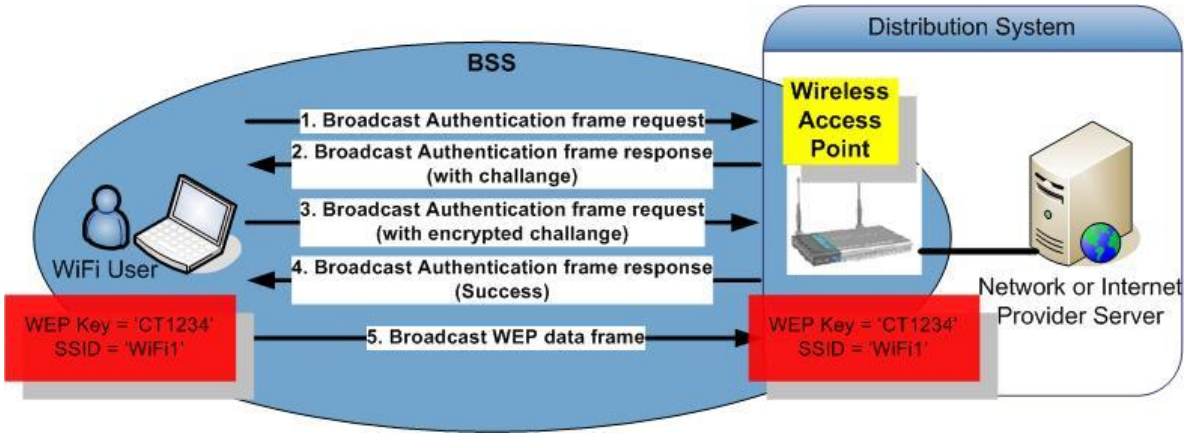

Fig. 10 WEP Authentication with Shared Key – WEP/WPA Key

ISSN 2067 – 4074

The authentication process with shared key has the following steps:

1 The mobile client station sends an authentication request frame to another mobile station or to the AP asking the authentication

2 The AP sends to the mobile client station an authentication response which contains an challenge bytes array using WEP pseudo random number generator

3 The mobile client station gets the challenge bytes array encrypt the frame as in figure 12.10 and sends back to the AP the probe of the authentication request frame

4 The AP decrypts the frame and check out if the decrypted frame contains the same bytes array challenge as the AP sent at step 2. If the bytes arrays are the same then the client is authentified.

The challenge bytes array is generated by AP using RC4 PRNG and it has 40 or 104 bits. In this kind of authentication the client does not authentify the AP. The WEP Shared Key Authentication is better than the WEP Open Authentication and it allow the access to the WiFi resources only if the mobile client station has the symmetric shared key. The shared key bytes array is stored in each station (mobile client or AP) into MIB – Management Information Base in "write-only" mode and it is accessible only to the MAC coordinator. In order to have a good authentication and encryption mechanism the both client station and AP should have WEP encryption/decryption and WEP Shared Key Authentication enabled.

The IEEE 802.11 standard does not specify the key management and distribution for the mobile client stations and AP stations.

References

[1] Zhiqun Chen, "Java Card Technology for Smart Cards – Architectures and Programmer's Guide", Addison Wesley, 2004

[2] Cristian TOMA, Marius POPA, Catalin BOJA, "Solution for Non-Repudiation in GSM WAP Applications", WSEAS Transaction on Computers, UK, 2008.

[3] Cristian TOMA - Security in Software Distributed Platforms, AES Publishing House, Bucharest, 2008, ISBN 978-606-505-125-6.

[4] Wolfgang Rankl & Effing, "Smart Card Handbook 3rd Edition", John Wiley & Sons Publishing House, USA 2004