SEVERAL SECURITY PROBLEMS IN 802.11WLAN

Syed S. Rizvi, *Member IEEE*
Srizv004@odu.edu

Electrical and Computer Engineering Department
Old Dominion University
Norfolk, VA 23517

1. INTRODUCTION

Wireless data communication is one of the fastest growing technologies, and it is used in all sizes of enterprises, small businesses and residential networks. It is being so quickly adopted throughout the world because it provides numerous advantages to its users. Not only are business and residential users enjoying wireless networking features, but governments are now adopting this technology in their organizations. But these advantages come with some quite serious security risks and those who are planning to use this technology should be aware of them. There are several security problems associated with the deployment of wireless networks which are now just coming to light, but as wireless technology prospers, the majority of the security issues will be resolved over the passage of time.

In order to provide stronger security mechanisms, new technologies like Institute of Electrical and Electronics Engineers (IEEE) 802.11have tried to elevate the level of security on wireless networks through *wired equivalent privacy* (WEP). The 802.11 standard **[6]** for wireless LAN communication introduced the WEP protocol in an attempt to address security problems and bring the security level of wireless systems closer to that of wired once. The primary goal of WEP is to protect the confidentiality of user data from eavesdropping. But, unfortunately, the 802.11 standard fails to provide any strong security via the WEP protocol. WEP security is completely broken and offers no real security for wireless networks. Currently several organizations are deploying their wireless networks based on the IEEE 802.11 standard. They consider that the security measures provided by the vendors are sufficient to prevent outsiders from accessing their internal network's resources. But it turns out, this is not the case. All of these organizations, which rely only on their vendor provided security, are open for unauthorized used of their internal resources. The deployment of wireless networks such as 802.11 make the entire network vulnerable to eavesdropping, especially because an intruder does not need to access the network physically. As a result, the attacker can now easily sit near the desired network and capture all the outgoing network traffic.

Unfortunately the WEP protocol is the only security measure taken by 802.11. It has many considerable flaws in its design **[7-8]** which make the entire wireless network vulnerable to any kind of attack. Numerous impressive attacks are possible against the WEP protocol and have been widely publicized **[3].** The majority of these papers revealed how 802.11 poorly implemented the WEP protocol. 802.11 used the WEP protocol to encrypt and decrypt the network traffic. The main problem associated with WEP is the selection of the keys used by encryption algorithm. The mechanism used to generate these keys creates keys that are too closely related to each other **[3].** If an attacker captures adequate network traffic, it can easily establish the set of keys needed to break the encryption. This paper will describe that how IEEE 802.11 addressed security issues through WEP and what the real design problems WEP are. The IEEE 802.11 standard not only failed to provide any adequate confidentiality and privacy through the WEP protocol, but also failed to provide a strong authentication mechanism. IEEE 802.11 does not provide any strong access control technique which prevents unauthorized users from gaining access to the wireless network. The shared key authentication is the only secure authentication mechanism provided by 802.11,

but unfortunately this authentication mechanism has also been proven ineffective. This paper will indicate some of the serious flaws of this security mechanism and will show how this authentication fails to prohibit unauthorized users.

The major problem of wireless networks based on the IEEE 802.11 standard is that the network traffic is not secure during the transmission. The IEEE 802.11 standard does not provide any strong way to secure data during transmission, and therefore allows attackers to make active and passive attacks. The IEEE 802.11 provides security through WEP which only encrypts the data part of the entire frame. The frame header is never encrypted by WEP and therefore always travels in the clear. Consequently the frame header is always viewable to anybody who has a wireless network analyzer. In the same manner, the management and the control frames exchanged between a client station and an access point (AP) are never encrypted and authenticated by the WEP protocol. Thus an attacker has ample freedom to interrupt data frames during transmission or use these frames in order to gain access to a wireless network. In an infrastructure mode station that wants to communicate with another station has to associate itself with an AP. For this reason, APs periodically broadcast beacon management frames with their service set identifier (SSID) to show their existence. Since these management frames containing SSIDs also transmit in the clear, this allows an attacker to easily capture these frames and use them for their own gain. Capturing these frames reveals the key and allows an attacker to access the network.

The paper is organized in the following way: Section 2 presents an overview of the 802.11 WLAN which describes the standard operational modes, authentication methods, and the WEP security protocol of 802.11. In section 3, we describe the possible attacks against 802.11 shared key authentication method. In section 4, we identify the fundamental flaws in the WEP security protocol and the corresponding attacks. Section 5 presents the general problems associating with 802.11 wireless standard. Section 6 summarizes the discussion by identifying more suitable key management and a better WEP encryption architecture. Finally, section 7 offers some conclusions.

2. Overview of 802.11 Wireless Networks

802.11, the first world recognized standard for wireless networks, developed by a working group of the IEEE in 1997. Two years later, the IEEE provided an extension to the original 802.11 wireless LAN standard called 802.11b which is also known as *802.11 high rates* or Wi-Fi. 802.11 specifies the standards for building wireless systems that can provide 1-2Mbps transmission speeds in the 2.4 GHz band. The 802.11 standards provide specifications for the two lower layers of the open system interconnection (OSI) reference model **[6]**: the physical layer and the data link layer. The main objective of IEEE for these standards was to give wireless networks the same strength as that of wired Ethernet networks. A wireless station and an access point (AP) are the two major components through which 802.11 wireless systems are constructed. Any standard PC that has a network interface card which supports wireless communication can be a wireless station. The wireless medium and the radio frequency (RF) are the two possible ways for a wireless system to access an AP. A wireless station can communicate either with the wired system or with another wireless station through an AP. In other words we can say that the AP is a network device or a base station for wireless stations which performs an essential function called *bridging.*

2.1 *Operational Modes of 802.11 WLAN*

According to 802.11 specifications, the wireless stations and access point can be configured in one of the two modes: ad-hoc mode, and infrastructure mode. The IEEE 802.11 defines the ad-hoc mode as the independent basic service set (IBSS), and the infrastructure mode as basic service set (BSS). Ad-hoc mode is a peer-to-peer type of networking, whereas the infrastructure mode requires an AP to communicate between the wireless devices and the wired network.

2.1.1 *Ad-hoc Mode (IBSS)*

Ad-hoc mode is a peer-to-peer type of networking in which every mobile station has a direct communication links to the other mobile stations. Every mobile station that wants to communicate with another mobile station does not need an AP**.** This mode is also identified as IBSS, since all wireless mobile devices communicate with the others directly. In Ad-Hoc mode all the stations within the transmission range are mobile (not fixed) and there is no direct connection to the wired network, which makes it one of

the simplest WLAN configurations. In other words we can say that the IBSS is the entire WLAN and only those stations that communicate with each other directly are the part of this LAN. Since each station or wireless device maintains its own existence, no master/slave relationships exist in this mode. IEEE 802.11 does not specify routing paradigms, data forwarding or exchanging topology information among BSSs **[3].**

2.1.2 *Infrastructure Mode (BSS)*

In infrastructure mode all wireless stations within the BSS connect to an access point. The AP and all the wireless stations within the BSS share the same frequency range. Each station that wants to communicate with another station in the same frequency range must send all of its communication to the appropriate AP. The AP acts as a bridge and forwards the received communication to the destination network that might be the wired LAN or another wireless network. The BSS has a certain geographical area which consists of wireless devices and one or more access points (APs). It is helpful to think of the circle used to describe BSS as the coverage area within which all the stations can communicate with each other as long as they remain the part of the same BSS. If a station changes its membership or move from its BSS, it can no longer directly communicate with other members of the BSS. In order to make a large network or to extend the coverage area of an existing wireless network, we can connect several BSSs through a distributed system (DS). Several BSSs, when combined in a single large geographical area (also called extended service area (ESA) within which members of an extended service set may communicate), makes an extended service set (ESS) **[10]**. A DS is a system used to interconnect a set of BSS is to create an ESS. The IEEE 802.11 specification does not further detail the architecture of a distributed system.

2.2 *802.11 Authentication Methods*

Authentication service is the only way available in the IEEE 802.11standard to control LAN access. The authentication service is used by all stations in order to establish their identity for those stations with which they want to communicate. Those stations that want to communicate with each other need to establish an authentication first. If this authentication has not been established between the two stations, an association will not be established. 802.11 standard does not mandate the use of any particular authentication scheme. The IEEE 802.11 standard defines two types of authentication methods: *open system authentication,* and *shared key authentication.*

2.2.1 *Open System Authentication*

Every station which wants to authenticate itself first sends a request for authentication which is handled by the default authentication protocol for 802.11, called open system authentication. This default authentication protocol does not involve any encryption and decryption methods. This implies that the entire authentication procedure is done in the clear, therefore any client station can associate itself with an AP.

Open system authentication is considered an unacceptable authentication protocol because it does not provide any security to the wireless LAN. All the plaintext data that exchanged among the stations within the BSS can be listened by any station which makes an association with any AP. In this protocol the wired equivalent privacy (WEP) is set to zero. The open system authentication protocol is frequently implemented where simplicity is the core objective and the network administrator does not want to deal with security issues.

2.2.2 *Shared Key Authentication*

Any station that tries to join the network must authenticate itself by the shared key authentication protocol which provides authentication by means of a standard challenge text and response, along with the shared secret key. In shared key authentication, the client station sends a request to an AP. The AP sends a challenge text packet to the client station. In order to successfully authenticate, the client must encrypt the challenge text with the correct WEP key and send it back to the AP. The client station will not be allowed to associate with the AP if it does not have the proper key. If it has a wrong key or no key at all, it will completely fail the authentication procedure. The same shared secret key is not only used to authenticate the station but also used to encrypt and decrypt the data frames but it is considered a security risk for WLAN.

Four frames are exchanged in the shared key authentication process as shown in figure 3

1 A requesting station sends an authentication frame to the AP with the WEP bit = 1.
2 When the AP receives the initial authentication frame, it replies with an authentication frame containing challenge text generated by the WEP engine.
3 In order to encrypt the received challenge text and to generate an integrity check value (ICV), the new station will then use the shared key and initialization vector (IV). After decrypting the challenge text and producing the ICV, the resulting frame is sent back to the responding AP with the IV and ICV. The AP decrypts the received text using the same key sequence, and compares it to the challenge text sent earlier.
4 If a match occurs, the responding AP replies with an authentication representing a successful authentication. If match doses not occur, the responding AP sends a negative authentication indicating failure.

2.3 Wired Equivalent Privacy (WEP) Protocol

The idea of securing wireless network traffic can best be viewed by comparing it to the security offered in wired networks. The IEEE 802.11 standard makes an effort to accomplish this objective by means of the WEP protocol which includes a mechanism for securing wireless LAN data streams. In order to prevent an intruder from accessing the network and capturing the wireless LAN traffic, the WEP protocol uses Rivest-Code 4 (RC4) and a 40-bit secret key for data encryption. The main intention of the IEEE behind the design of WEP was to provide level of security and privacy comparable to wired Ethernet 802.3. But, unfortunately, the WEP protocol adapted by 802.11 for securing the wireless network transmission is inherently vulnerable to network exploitation. The built in cryptography in 802.11 is by means of the WEP security protocol, which is entirely broken and offers no real security. Many papers have shown the weaknesses of WEP and have proven that WEP does not provide security which meets modern demands. WEP uses a symmetric scheme in which the same key and algorithm are used for both the encryption and decryption of data **[1]**.

2.3.1 *WEP Encryption*

The WEP protocol actually consists of two separate processes which are applied when it starts encrypting data stream. WEP is the framework that enables encryption in the 802.11 standard **[9].** Figure 1 shows the WEP encryption algorithm. The WEP encryption procedure can be divided into four steps, which are as follows:

1. In the first step, a 40-bit secret key is concatenated with a 24-bit initialization vector (IV), resulting in a 64-bit total key size.
2. The resulting 64-bit key is input to the pseudo-random number generator (PRNG).
3. Using an RC4 algorithm, the PRNG outputs a pseudo-random key sequence.
4. The resulting key sequence is then used to encrypt the data by doing a bitwise XOR.

The resulting encrypted bytes are identical in length to the number of data bytes actually transmitted, plus the 4 bytes of integrity check value (ICV). This is because the resulting key sequence is not only responsible for protecting the 32-bit ICV value, but also responsible for protecting data. The WEP protocol produces ICV by applying an integrity algorithm (CRC-32) on the plain text in order to prevent any unauthorized data modification during wireless transmission.

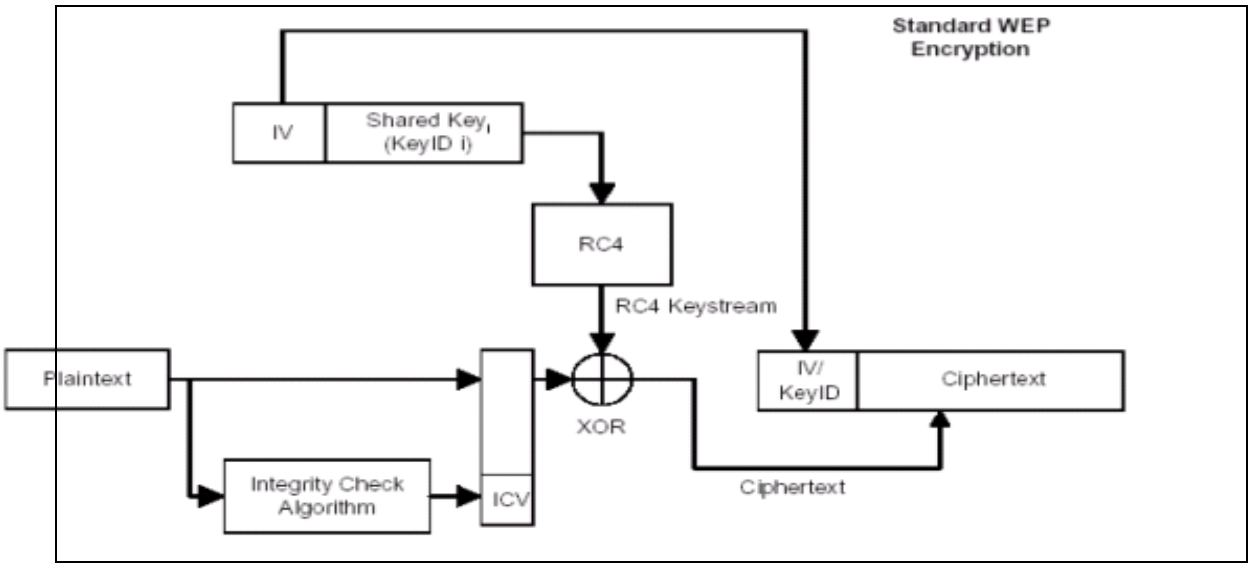


FIGURE 1 WEP ENCRYPTION ALGORITHM **[20]**

2.3.2 *WEP Decryption*

To decrypt the data stream, WEP follows the given four step process. Figure 2 shows the WEP decryption algorithm.

1. The IV (received from the incoming message) along with the shared secret key becomes the input of the WEP PRNG. The PRNG then generates the key sequence (based on the input key) necessary to decrypt the incoming message.
2. Both the cipher text and the generated key sequence together produce the original plain text and ICV.
3. The new ICV is computed by implementing the integrity check algorithm (CRC-32) on the recovered plain text which validates the decryption.
4. If the newly computed ICV is not equal to the one that was sent with the original message, an error is assumed and an error indication is sent back to the sending station.
5.

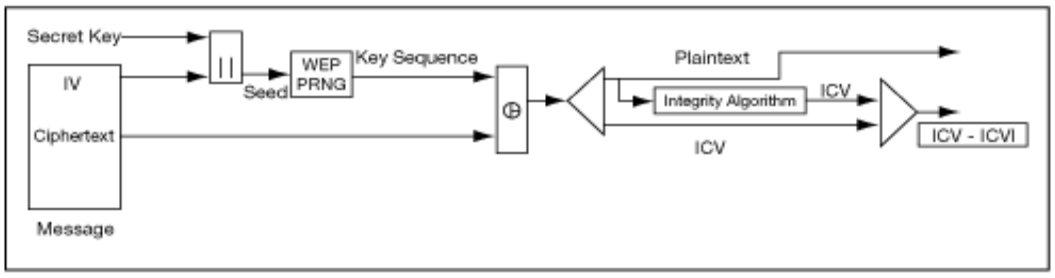


FIGURE 2 WEP DECRYPTION ALGORITHM **[6]**

3 Problems with the Access Control Mechanisms

As discussed in the preceding section, that the WEP security protocol adapted by 802.11 provides no real security for wireless traffic because it has some major flaws in its design. Besides problems in the WEP design, there are also numerous security problems with the access control mechanism. This section describes attacks against the 802.11 standard shared key authentication mechanisms.

3.1 *Problem with Shared Key Authentication*

An attacker can easily break the protocol used for shared key authentication by a passive attack if he or she has the knowledge of just one side of a mutual authentication which is going on between the client station and an AP. The attacker does not need to have knowledge of both sides. The shared key authentication works well as long as the "shared secret" is well protected and is not compromised **[11]**. The random challenge text is the only difference between different types of authentication messages **[4]** exchanged between an AP and a client station which make rigid or fixed structure of the shared key authentication protocol. The weaknesses of WEP, mentioned in the previous section, and the fixed structure of the protocol together make it possible for an attacker to easily exploit the wireless networks.

The attacker attacks by first capturing the second and third management messages exchanged between a requesting client and an AP. The second message sent by the AP to a requesting client contains the random challenge text in the clear as shown in the Figure 3**.** Remember that these management messages are broadcast in the clear by an AP and a client station, so the attacker can easily capture these messages during transmission. After receiving the second message from the AP, the client station then uses the stream key to encrypt the received challenge text and sends the third message to the AP which contains the encrypted challenge text or challenge response with the corresponding IV.

Let ***K*** be the stream key (based on the shared key plus IV) produced for a specific packet and ***P*** be the packet data in plain text. Then RC4 encryption algorithm produces cipher text ***C*** by XORing the stream key with the plain text. The fundamental property is as follows:

$$C = (K) \text{ XOR } (P)$$

After the exchange of these two messages, the attacker now has the complete understanding of the challenge text ***P*** (plain text sent by the AP), the challenge response ***C*** (cipher text which is encrypted by the client who wants to authenticate) and the public IV (since the IV is public and it is transmitted in the clear). After gaining all these indispensable things, the attacker can now easily derive the pseudo-random stream key using the following formula:

$$K = (C) \text{ XOR } (P)$$

Once the attacker successfully derives the stream key, it has the opportunity to authenticate itself with any target network without even knowing the shared secret key. In order to associate itself with a desired AP, the attacker can now send a request authentication frame. After receiving the request frame from the attacker, the AP responds with the challenge text. The attacker can then produce the required cipher text or challenge response. By XORing the two values together (stream key and the challenge text) it will come up with the valid authentication response frame. The attacker then implements the CRC-32 algorithm in order to compute the new value of ICV. Next, the attacker sends a valid authentication response message (cipher text plus IV) to AP, and finally associates with the desired AP and joins the network.

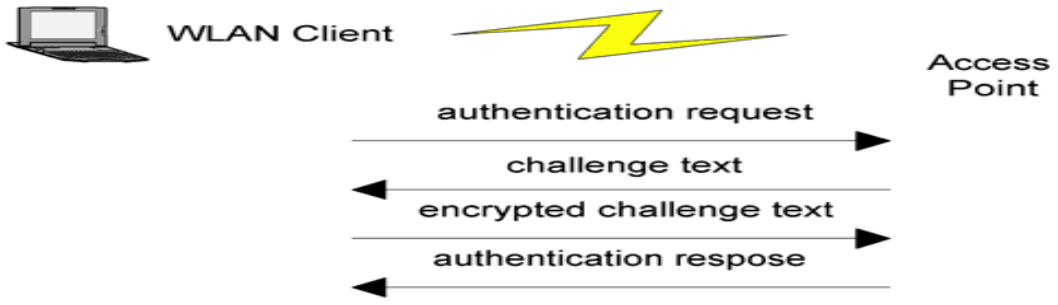


FIGURE 3 WEP SHARED KEY AUTHENTICATION PROCEDURE **[21]**

4 Problems with the WEP Encryption Algorithm

As mentioned earlier (see figure 1 and figure 2), the implementation of the WEP protocol based on the RC4 encryption algorithm, which can be recognized as a stream cipher that takes a fixed length key and

produces a series of pseudo-random bits that are XORed with the plain text to produce cipher text and vise versa. According to Borisov, GoldBerg, and David Wanger **[7],** the usual way in which the WEP protocol operates makes the stream ciphers vulnerable for many different kinds of attacks. The WEP protocol is vulnerable mainly because of relatively short IVs and keys that remain static. The issues with WEP do not really have much to do with the RC4 encryption algorithm [**19**]. With only 24 bits, WEP eventually uses the same IV for different data packets that allows attacker to detect duplicate IVs.

If the same stream key is used to encrypt two different plain text strings and these two cipher texts are forwarded to a certain destination, it can help an attacker recover the original plaintext. If an attacker captures these two cipher texts during transmission, it is possible for an attacker to obtain the XOR of the two plain texts. Once the attacker has the complete knowledge of the XOR by using the captured cipher texts, it can then try to recover the original plain texts by making statical attacks. These attacks become frequent when most of the cipher text is encrypted using the same known shared key. If an attacker successfully recovers one of the plain texts, he can then recover all of the other plain texts. During the transmission, if an attacker changes one of the bits within the cipher text, then at the destination where decryption takes place, the corresponding bit within the recovered plaintext will be changed.
As mentioned earlier, WEP can deal with these two problems by means of an integrity algorithm and an initialization vector. It implements an integrity algorithm (CRC-32) to make certain that a message has not been modified throughout the wireless transmission. For each packet, a new IV is used which results in a different key sequence. Even though WEP has a defense against these two problems, the poor implementation of these two security measures results in poor security. Furthermore, the deficiency in the WEP encapsulation design arises from attempts to adapt RC4 to an environment for which it is poorly suited **[5].**

4.1 *Problem with the (CRC-32) integrity check algorithm*

Whenever a new packet arrives for encryption, the WEP protocol operates the CRC-32 algorithm on plain text in order to produce a new value for the ICV. The ICV is part of the encrypted message and typically consists of four bytes. The CRC-32 algorithm is linear, which means that it is possible to compute the bit difference of two CRCs based on the bit difference of the message over which they are taken. In addition, if an attacker changes ***n*** number of bits within a certain message, it will come up with a deterministic set of bits in the CRC that must be changed in order to produce a correct checksum for the modified message **[2].** In other words, if an attacker successfully computes the bit difference of two CRCs, which are based on the bit difference of two dissimilar messages over which they are taken (since the CRC-32 algorithm operates on the plain text in order to produce the corresponding CRC value), the attacker can modify the ***n*** bits within the original encrypted message. Since an attacker changes ***n*** bits prior to decryption of the encrypted message, this allows an attacker to alter a random number of bits within the encrypted message and properly adjust the checksum so that the resulting message at the destination appears valid.

4.2 *Problem with the initialization vector*

In the 802.11 WEP protocol, the IV is a 24-bit field which is concatenated with the shared secret key in order to produce the random key sequence. The key length of IV (24 bits) is short enough to make brute force attacks practical to individuals and organizations with fairly modest computing resources [**15, 16].** As shown in figure 1 and figure 2, the IV is sent independently in the clear, and it is known to everyone. In other words, we can say that the IV is included in the unencrypted portion of a wireless packet (the WEP protocol only encrypts the payload, that is the frame body and CRC of each frame before transmission) so that the receiver can know what IV to use when deriving the key stream for decryption (the sender and the receiver both should have identical keys for encryption and decryption). The IV is therefore not only available to receiver but also available to attackers. Even though a new IV is used for each packet in order to avoid the same key stream (since the IV is the only part of the total key which changes from time to time, whereas the secret key remains constant), the small space available for generating new IVs does not ensure that a unique key stream is used for each new message. A busy AP which constantly sends 1500 bytes packets at 11Mbps (in the case of 802.11B) will exhaust the space of IVs after 5 hours (1500 x 8/ (11x10^6) x 2^24 = ~18000 seconds = 5 hours). **[2].**The amount of time may be even smaller than 5 hours, since many packets are smaller than 1500 bytes.
One of the reasons of key stream reuse is the improper IV management. Since most of the vendors implement static shared secret keys which remains constant during the entire network life. In other words,

the static nature of the shared secret keys emphasizes this problem. Furthermore, 802.11 standard does not provide any function that supports the exchange of keys among stations. Consequently, users and system administrators usually use the same keys for weeks, months, and even years. This gives attackers plenty of time to monitor wireless traffic and detect duplicate IVs. The reuse of IVs always results the reuse of key stream (in this situation, when we have static shared secret keys, the key sequence entirely based on IV). If an attacker captures two cipher texts during transmission which are encrypted by using the same key stream, it is possible for an attacker to determine the XOR of the two plain texts. Once the attacker has the complete understanding of the XOR by using the captured cipher texts, it can then attempt to recover the original plain texts. This situation becomes worse if the majority of the stations within the BSS make use of the same key for encryption and decryption.

4.3 *Attacks on 802.11 WLAN (Analytical Study)*

The 802.11 standard for wireless networks includes the WEP protocol, used to protect wireless communication from eavesdropping and other attacks. WEP has well-known flaws in the encryption algorithms used to secure wireless transmission. Due to these flaws, a number of attacks are possible, both passive and active, that allow eavesdropping on, and tampering with, wireless transmission. The WEP protocol is intended to enforce three main security goals **[6]:**

Confidentiality: The primary objective of WEP is to protect wireless communication from eavesdropping.

***Access Control*:** A second goal of the WEP protocol is to prevent unauthorized access to a wireless network. The 802.11 standard includes an optional feature to discard all packets that are not properly encrypted using WEP. We have already described the flaws in the shared key authentication mechanism in section 3.1.

Data Integrity: The third and the final goal of the WEP protocol is to ensure that a packet has not been modified in transit. The integrity check field is included in the packet for this purpose.

In the remainder of this section, we will show that none of the three security goals of the WEP protocol are attained. We will also describe the possible attacks against a wireless network.

4.3.1 *Passive Attack*

A passive eavesdropper can intercept all wireless traffic until an IV collision occurs. The attacker can obtain the XOR of the two plaintext messages by simply XORing two encrypted packets that use the same IV. In other words, if an attacker captures two cipher text packets which are encrypted using the same key sequence (the key sequence will be same if an IV is reused), he can obtain the XOR of the two plaintexts by simply XORing the two captured cipher text packets. In other words, we can say that XORing two cipher texts that use the same key stream (a key stream produced by the RC4 algorithm which is used to encrypt the message) would cause the key stream to cancel out, and the result would be the XOR of the two plaintexts. An attacker can infer data about the contents of the two messages by using the resulting XOR of the two plaintexts. Once an attacker gets two cipher texts that use the same IV, several methods of attack can be applied to recover the plaintexts.

For example, if two plaintexts $\boldsymbol{P_1}$ and $\boldsymbol{P_2}$ are encrypted by using the same key sequence ***K,*** the result will be $\boldsymbol{C_1}$ and $\boldsymbol{C_2}$ respectively.

Let (K) = 10011110, (P_1) = 11101101, and (P_2) = 10001111.
Then, (K) XOR (P_1) = (10011110) XOR (11101101) = 01110011= C_1
(K) XOR (P_2) = (10011110) XOR (10001111) = 00010001= C_2

Suppose an attacker does not know anything about the key sequence K and the plaintexts P_1 and P_2. He first captures the two cipher texts C_1 and C_2 which are encrypted using the same key sequence K. By simply

XORing the two captured cipher texts C_1 and C_2, he will come up with the XOR of the two plaintexts P_1 and P_2, as shown below.

(C_1) XOR (C_2) = (01110011) XOR (00010001) = 01100010
(P_1) XOR (P_2) = (11101101) XOR (10001111) = 01100010

Therefore, this verifies that XORing two cipher texts which are encrypted using the same key sequence results in the XOR of the two plaintexts which might be helpful for an attacker to infer data about the contents of a message.

When such statical analysis is inconclusive based on only two messages, the attacker can look for more collisions of the same IV **[2]**. It is possible for an attacker to recover a modest number of messages encrypted with the same key stream in fairly a short time, and the success rate of such analysis grows quickly. Once an attacker gets success to recover the entire plaintext for one of the messages, the plaintext for all other packets with the same IVs can be easily recovered by an attacker, since all the pair-wise XOR's are known. Since the pair wise XOR of every pair of plaintexts can be computed, and many classical techniques are known for solving such problems **[17, 18].**

4.3.2 *Active Attack*

an Active attack is also known as the*" known Plaintext attack"* .In an active attack, an attacker not only intercepts the wireless communication but also modifies the wireless packets in transit. In order to know the plain text of an encrypted message, an attacker can use a host somewhere on the Internet to send traffic from the outside to a host on the wireless network. The contents of such traffic will be known to the attacker, producing known plaintext. An attacker can use this knowledge of plaintext to derive the key sequence. There are also many other ways available to obtain known plaintext.
Once an attacker derives the key sequence, he can change ***n*** bits within the cipher text and construct correct encrypted packets. The procedure involves capturing the cipher text, deriving the key sequence, changing ***n*** bits within the cipher text, and implementing the CRC-32 algorithm to change the value of ICV, so that the resulting modified cipher text appears valid at the destination. The fundamental property is as follows:

K = (C) XOR (P)

Suppose an attacker knows the exact plaintext ***P*** for one encrypted message ***C***. He can use this knowledge to successfully derive the key sequence ***K***.
For example, if key sequence K =10100111 and plain text P =11000101, the resulting cipher text C will be as follows:

Key sequence	K	⟶	10100111
Plain text	P	⟶	11000101
Cipher text	C	⟶	01100010

When an attacker gets the cipher text (C = 01100010), and if he knows the exact plain text (P= 11000101) of the cipher text C, he can easily derive the key sequence K by XORing the two values together.

Plain text	P	⟶	11000101
Cipher text	C	⟶	01100010
Key sequence	K	⟶	10100111

Once an attacker gets the key sequence K, any cipher text $(C_1, C_2, \ldots C_i)$, which is encrypted using the same key sequence (K), can be easily decrypted by the attacker, and an attacker can then recover the corresponding plain text $(P_1, P_2, \ldots\ldots, P_i)$. For example, let K_1 =10101101, P_1 = 10010110, and P2=11100011. By simply XORing the two values together, we successfully encrypt the plain text P_1 and P_2, and get the corresponding cipher text C_1 and C_2, as shown below:

Key sequence K_1 ⟶ 10101101 Key sequence K_1 ⟶ 10101101

Plain text	P_1	⟶	10010110	Plain text	P_2	⟶	11100011
Cipher text	C_1	⟶	00111011	Cipher text	C_2	⟶	01001110

Suppose an attacker knows only about the key sequence K_1 and the two cipher texts C_1 and C_2, which he captures during the transmission. In order to recover the two plain texts P_1 and P_2, the attacker just XORs the two captured cipher texts C_1 and C_2 with the key sequence K_1.

The basic property is that: ***P = C XOR K***.

Key sequence	K_1	⟶	10101101	Key sequence	K_1	⟶	10101101
Cipher text	C_1	⟶	00111011	Cipher text	C_2	⟶	01001110
Plain text	P_1	⟶	10010110	Plain text	P_2	⟶	11100011

Since it is an active attack, the attacker can change bits within the encrypted message and adjust the value of the ICV in order to obtain a correct encrypted version of a modified packet. In addition, there are several well understood methods available which attackers can use to make arbitrary changes to a message, therefore the checksum of the modified message remains same as that of the original. The following few paragraphs not only show the effectiveness of an active attack but also verify that the integrity check algorithm is not enough to assure the integrity of data in wireless packets.

Let the original bits of a plain text ***P*** = 11110101 and the key sequence ***K*** = 01011100101. In order to compute the value of the CRC, the integrity check algorithm produces generator polynomial G(x) for a newly arrived message. Let $G(X) = X^2 + 1$ (for simplicity, we are ignoring the fact that the polynomial generator in the CRC-32 algorithm is different from the one we suppose). The CRC of this message at the source can be calculated as follows:

Generator Polynomial = $G(X) = X^2 + 1 = 101$

Plain text = 11110101

Message after appending two zero bits = 11110101 **00**

```
101 | 11110101 00 | 11000100
     101
      101
      101
       000
       000
        001
        000
         010
         000
          101
          101
           000
           000
            000
            000
            000  ⟶  CRC or Computed ICV
```

After attaching the CRC to the original message, the result will be 11110101 ***000.*** The key sequence (K = 01011100101) is then used to encrypt the plain text (P = 11110101***000***) by doing a bitwise XOR.

K = 01011100101
P = 11110101***000***
C = 10101001***101***

The cipher text (C = 10101001**101**) will then be forwarded to the destination through the wireless medium. In order to successfully change the bits within a message and adjust the CRC, the attacker performs the following three step process:

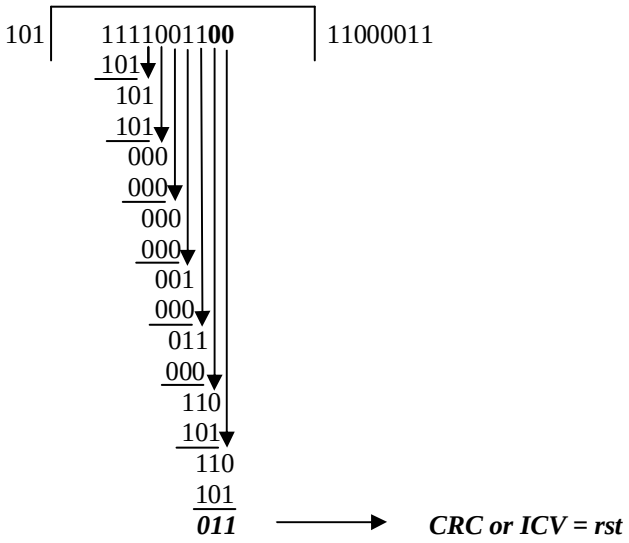
i) Since the medium is wireless, the attacker can intercept this cipher text and change one of the bits.

Bits of an original encrypted message :10101**00**1***101***
After changing two bits of an encrypted message:10101**11**1***xyz***

ii) In order to successfully adjust the CRC of a modified encrypted message (in this example, the CRC of a modified encrypted message is representing as **xyz**), the attacker uses the key sequence (for a direct active attack, the attacker should know at least one of them: plain text or key sequence) to decrypt the modified cipher text. The knowledge of the plain text can be used to adjust the CRC of an encrypted message.

K = 01011100**101**
C = 10101**11**1***xyz***
P = 11110011***rst***

After changing the bits of an original encrypted message and decrypting the modified encrypted message, the attacker then computes the CRC (***rst***) of a recovered plain text by reversing the procedure.



011 is the value of the ICV for the recovered plain text. The attacker uses this value to adjust (or completely change if required) the existing CRC value (101) attached with the cipher text. In other words, attacker uses this value to compute the value of xyz.

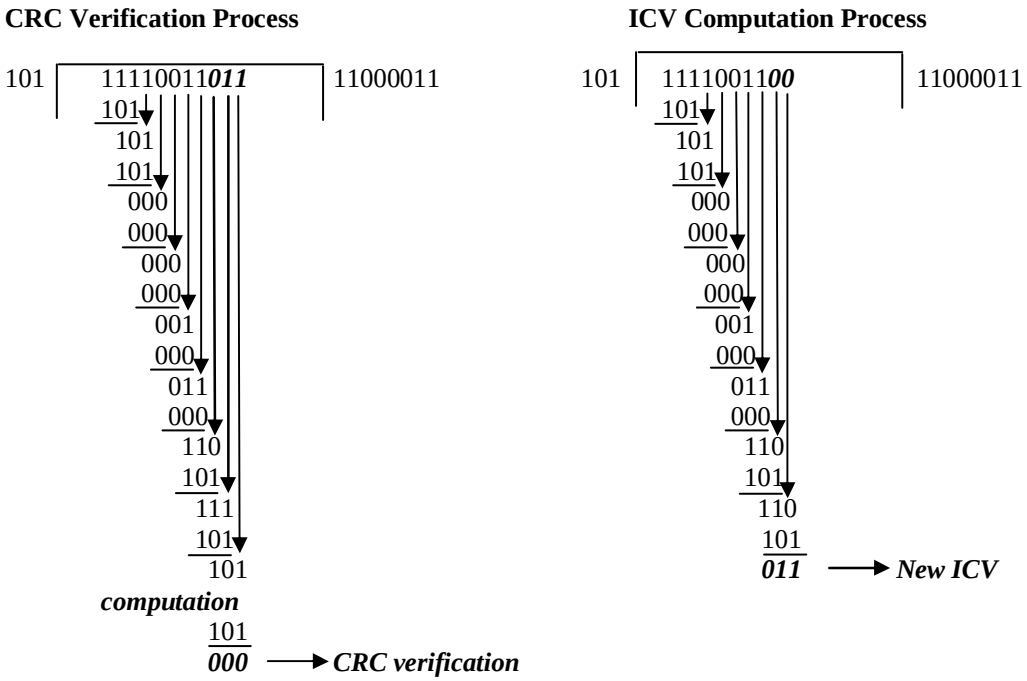
K = 01011100**101**
P = 11110011***011***
C = 10101**11**1***110***

iii) After computing the new value of the CRC, the attacker then attaches it to the encrypted modified message (that is, 10101**11**1***110***) and forwards it to the actual destination through the wireless link.
When this modified message is received at the destination, the WEP decryption engine decrypts the received message by using the key sequence.

K = 01011100**101**
C = 10101**11**1***110***
P = 11110011***011***

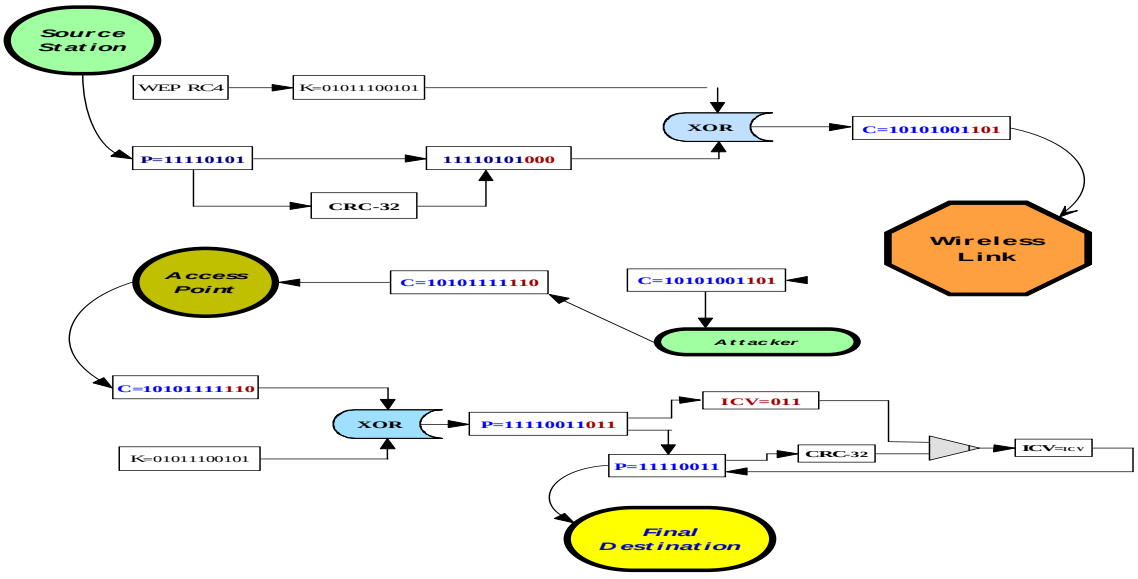
The new ICV is computed by implementing the integrity check algorithm (CRC-32) on the recovered plain text message which validates the integrity of the data. If the receiving station calculates an ICV that does

not match the one found in the received message (here the newly computed ICV should equal to 011 that was sent with the original message), an error is assumed and an error indication is sent back to the sending station.



The result shows that the new value of the ICV (011) is equal to the ICV received with the modified encrypted message. This modified message is successfully received by the receiver. Thus, this data integrity failure not only implies that an attacker can modify any content (for example, the position of a decimal point in a financial document), but it also permits attackers to use the checksum to assure the correctness of their decryption attempts. Thus the WEP checksum fails to protect data integrity, one of the three main goals of the WEP protocol.

Representation of an Active Attack



4.3.3 *Table-Based Attack*

In order to form a family of 2^24 keys, the WEP protocol concatenates the IV, which is 24 bits long, with the shared secret key. Every new transmitted packet selects one of these 2^24 keys and encrypts the data using that key. To prevent eavesdropping and other attacks, the WEP protocol uses a different IV, which results in a different key sequence for every new outgoing packet. Since the stream cipher key can never be reused **[5]**, it obliges the BSS to change the base key (shared secret key) as soon as its members have consumed all of the 2 ^ 24 keys derived from the base key. WEP defines no practical way to accomplish this, so in practice WEP keys are not replaced frequently enough to maintain the level of privacy. As discussed previously, a single AP running at 11 Mbps will exhaust the space of IV's after 5 hours. In other words, the time is inversely proportional to the number of APs. As the number of APs within the BSS increases, it will ultimately reduce the time that it takes a key space to be exhausted.

Key sequence reuse can lead to a number of attacks. Reusing the same key means that the WEP protocol allows different packets to use the same key sequence to produce a cipher text, and this is the reason why it is so important to avoid key reuse in RC4. Once the plain text for an intercepted message is obtained through analysis of IVs collision, the attacker also learns the value of the key stream used to encrypt the message. An attacker can use this key sequence to decrypt any other message that uses the same IV. After capturing enough wireless packets, the attacker can build up a table of IVs and corresponding key sequence In practice, WEP uses the same secret key among all the members of the BSS and since the entire security of the WEP protocol depends on these two keys (secret key and IV), it is clear that WEP requires a different kind of mechanism to prevent one station from using the same IV that is already in use by some other station.

This table requires a fairly small amount of storage ({(2^24packets) X (1500 X 8 bits/packet) = ~ 24GB}). Therefore, it is possible that a dedicated attacker can accumulate enough wireless packets to build up a full decryption table. If an attacker successfully builds up a full decryption table, the attacker can decrypt every packet that is sent over the wireless link.

4.4 *Migrating Shared Key Size from 40-bit to 104-bit*

The IEEE standards committee for 802.11 accepts that the WEP security protocol fails to meet its design goal, but the committee widely attributes this failure to the use of a 40-bit shared secret key. The committee assumes that migrating from a 40-bit to a 104-bit key could increase the resistance of the WEP protocol. As a result, in 802.11a the size of the shared secret key increased from 40 bits to 104 bits. But unfortunately, increasing the size of the shared secret key from 40 bits to 104 bits does nothing to increase the WEP resistance to many attacks. We identified some of the reported attacks that do not involve the secret key at all. Increasing the number of secret keys that are shared among all the stations within the BSS might play a role in increasing the resistance of the WEP protocol, but just increasing the number of bits in the shared secret key does not make sense. **[5]** has identified significant deficiencies in the WEP data encapsulation that renders its data privacy claims meaningless, regardless of the key size. Increasing the WEP key from 40 to 104 bits does nothing to increase WEP's resistance to attack. This is because the deficiencies are related to how WEP uses cryptography, not the key size. WEP is actually vulnerable because of its relatively short IVs (24 bits) and a shared key that remains static. The issues with WEP do not really have much to do with the size of the shared key. With only 24 bits, WEP eventually uses the same IV for different data packets, which results the same key streams over and over. Once an attacker gets the key stream, he can decrypt any cipher text encrypted by using the same IV. The WEP's usage of encryption is a fundamentally unsound construction **[5].** Thus the WEP encapsulation remains insecure whether its key length is 1 bit or 10000 or any other size whatsoever.

5 General Problems Relating to the 802.11 Standard

The 802.11 standard defines limited support for confidentiality of wireless data through the WEP protocol, whose design contains significant flaws. The 802.11 standard also fails to define strong authentication mechanisms. Beyond these problems, there are some other security concerns that the IEEE standards committee for 802.11 needs to address. In this section, we will discuss some of the general security problems associated with the 802.11 WLAN standard.

5.1 *Service Set Identifier (SSI D) Problem*

The SSID is an identification value programmed in the AP to identify the local wireless network. In other words, the SSID is meant to differentiate networks from one another. In infrastructure mode, any station that wants to communicate with another station or stations, must establish an association with an AP. In order to establish an association with an AP, the client station should know the correct SSID value of an AP. By default an AP will periodically broadcast a beacon frame **[12]**, about 10 frames a second, to show its existence and to announce its capabilities (see figure 4). If a wireless station does not know the correct value of the SSID, it is not able to associate itself with an AP. In other words, the value of the SSID acts as a simple password because when a client station connects to the AP, it provides a kind of security measure.
The fact that an AP broadcasts the beacon management frame at a fixed interval which contains the value of SSID is a problem. These beacon management frames are not processed by any privacy function **[13]**, which means that a wireless network and its parameters are available for anybody who captures these beacon management frames. Therefore, anyone who does not have a correct SSID or has no SSID at all, is able to receive this broadcast and gain access to the AP. Because the SSIDs are widely known and easily shared, unauthorized users are also able to configure their own stations with the correct SSID. Another problem is the fact that most APs use default SSID's provided by the manufacturers. For example, all *Linksys* AP's are set to the network name of "linksys", while Cisco AP's are initially set to "*tsunami*". Because these default SSIDs are well known, not changing it makes your network much easier to detect. This implies that it is quite easy for an attacker to determine a network's SSID and gain access to it. Therefore, it is not a practical approach to implement SSID as a primary security measure.

SSID	Time stamp	Beacon Interval	Capability Information	Supported Rates	Other Parameters

Figure 4 Beacon Management Frame

5.2 *Problems Caused By the Radio Broadcast*

The radio broadcast waves that are used to connect wireless network devices do not simply stop once they reach a wall or the boundary of a business **[1].** Instead, they continue to travel into parking lots, other business, and elsewhere in an expanding circle from the broadcast point. These expanding circles of radio waves create a bubble of transmission radiation. The risk caused by these transmission radiations of radio waves should be obvious. This implies that intruders can eavesdrop on a network from wherever they can set up a laptop to capture these radio signals. The IEEE standards committee for 802.11 WLAN specifies that these radio waves can broadcast up to a 150 to 300 feet distance, but in reality, these radio waves travel much farther.
The point is that eavesdropping is quite easy in the radio environment. When a station sends a message over radio transmission, anyone within the BSS equipped with a suitable transceiver can intercept these radio transmissions. Keep in mind that the 802.11and 802.11b WLAN standards operate in the 2.4 GHz frequency range, which can easily be transmitted through walls at distance of roughly a few hundred feet.
Furthermore, the 802.11 protocol inherently leaves the physical layer header unencrypted. These unencrypted physical layer headers provide critical information to the attacker. An attacker can intercept wireless network traffic by using packet sniffers such as AiroPeek, and AirSnort. These tools capture all conversation on a network segment and provide a wealth of features for dissecting this traffic. Once an attacker captures enough wireless data, he can determine the login IDs and passwords through packet analysis.

5.3 *Denial-of-Service (DoS) Attacks in WLAN*

Properly authenticated and associated clients are often given full access to the wireless network. Even without cracking WEP encryption **[14]**, attackers can access wired networks connected to the wireless one, and perform illegal, embarrassing, or otherwise undesirable acts that reflect badly on the network administration. Attackers can also spread viruses, and perform local or remote Denial of Service (DoS) attacks.
In a DoS attack, an attacker causes a system or a network to become unavailable for a certain time to authorized users, or causes services to be interrupted or delayed for a certain period of time. Wireless networks are also vulnerable to DoS attacks due to the nature of the wireless transmission medium. In DoS attack, enough interference can be generated by an attacker, who is equipped with the powerful transceiver, to prevent wireless devices from communicating with one another. Furthermore, a dedicated attacker

equipped with the proper devices can introduce abundant frequencies with artificial noise and completely disrupt the wireless network operation. The consequences of these DoS attacks are a significant reduction in performance, and sometimes the complete failure of the system. It is quite hard to prevent an attacker from launching a DoS attack, because wireless networks are highly susceptible to interference and interception.

6 Theoretical Recommendations for Known IV Attacks

1 The IEEE standards committee for 802.11 WLAN specifies that the IV should change whenever a new packet arrives for encryption. This implies that the IEEE standard committee does not require that a different IV is used for each packet until it exhausts its key space. In addition, the committee also does not specify how to select IVs, and in fact many implementations use the IV poorly, which makes matters worse. We recommend that the IEEE standard committee for 802.11 makes compulsory the use of a different IV for each outgoing packet until it fully utilizes its available key space.

2 WEP is vulnerable because of relatively short IVs (typically 2^24) and shared keys that remain static. The effectiveness of known IV attacks could be reduced if all of the keys (shared secret keys) and available IV space that WEP originally defines for encryption were utilized. It would ultimately increase the time of IV collision. The IV field used by WEP is only 24 bits wide, nearly guaranteeing that the same IV will be reused for multiple messages. For example, in a large busy network based on 802.11 and 802.11b, this reoccurrence of IV can happen after 5 hours (5hrs is the maximum time an attacker has to wait for an IV collision). But according to our recommendation, this same reoccurrence of IV can occur after 20 hours.
Reoccurrence of IV = [{(2) ^ (24) packets} {(1500 X 8 bits/packet) (4 Shared keys)}/ {(11) ^ (6) bps}] = 20 hours

3 Whenever a new station boots up, WEP hardware initializes the value of the IV to zero. For each outgoing packet, the value of the IV is incremented by one. Initializing the value of the IV to zero and incrementing each time a new packet arrives gives attackers a predetermined sequence of IVs to exploit, and thus increases the chances of known IV attacks. We recommend that whenever a new station boots up the value of IV should initialized with a random number instead of zero. The initialization of the IV by a random value greatly mitigates the chances of attacks and particularly makes it difficult for an attacker to launch known IV attacks and table-based attacks on wireless networks.

4 Before encrypting each packet, a different value of IV should be used with the secret key in order to try to produce the maximum different key sequences. The same secret key should be used until the available space of IVs is fully exhausted. When the IV space is fully utilized and the IV is reinitialized, the value of the secret key should be incremented. This scheme significantly increases the time of IV reuse and makes it difficult for an attacker to break the WEP encryption. For example, suppose the IV field used by WEP is only 2 bits wide, and suppose WEP uses two shared secret keys with the IV to generate key sequences. The results of our suppositions are summarized in tables 1 and 2. The two shared secret keys and the values of IV are as follows: SSK1= 010 and SSK2 = 100. IV = 2bits = {00, 01, 10, 11}.

Table1:
In table 1, the IV and the shared secret keys are both incremented whenever a new packet arrives for encryption. When the IV and shared secret keys are both incremented upon arrival of a new packet, repetition of the same key will occur just after the sequence number 4. Thus in this technique, the same key gets used after 2^N initialization vectors, where N is the number of bits available for IV.

TABLE 1 Normal Key Sequence Generation

Sequence Number	Initialization Vector (IV)	Shared Secret Key (SSK)
1	00	010
2	01	100
3	10	010
4	11	100
5	00	010
6	01	100
7	10	010
8	11	100
9	00	010

Table 2:
According to our recommendation, only the IV part of the key sequence increments upon arrival of a new packet for transmission. The shared secret key remains the same up to 2^N initialization vectors, where N is the number of bits available for IV. In this way, the reuse of the same key will occur after sequence number 8. This technique ensures that the secret key will be paired up with the entire IV. Thus our recommendation significantly increases the time between key reuse, typically after {2 X (2 ^ N)}.

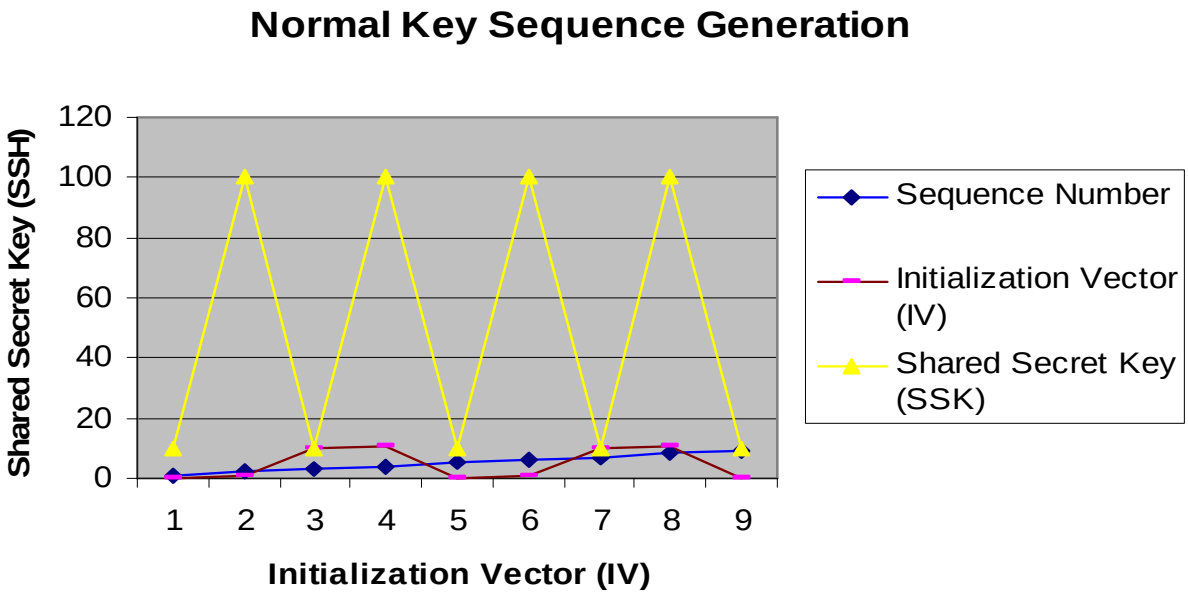
TABLE 2 Recommended Key Sequence Generation

Sequence Number	Initialization Vector (IV)	Shared Secret Key (SSK)
1	00	010
2	01	010
3	10	010
4	11	010
5	00	100
6	01	100
7	10	100
8	11	100
9	00	010

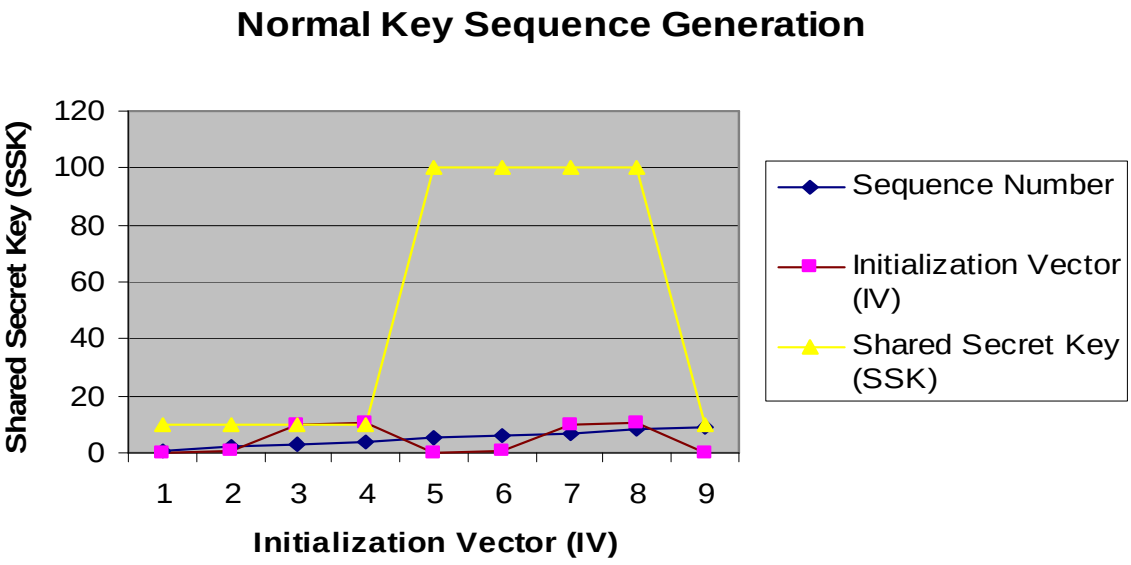
5 Assign a special ID or pointer (a pointer which is not clearly showing that which shared key this pointer belongs to) to each shared secret key and sends it with an IV in clear.

6.1 Simulation Results

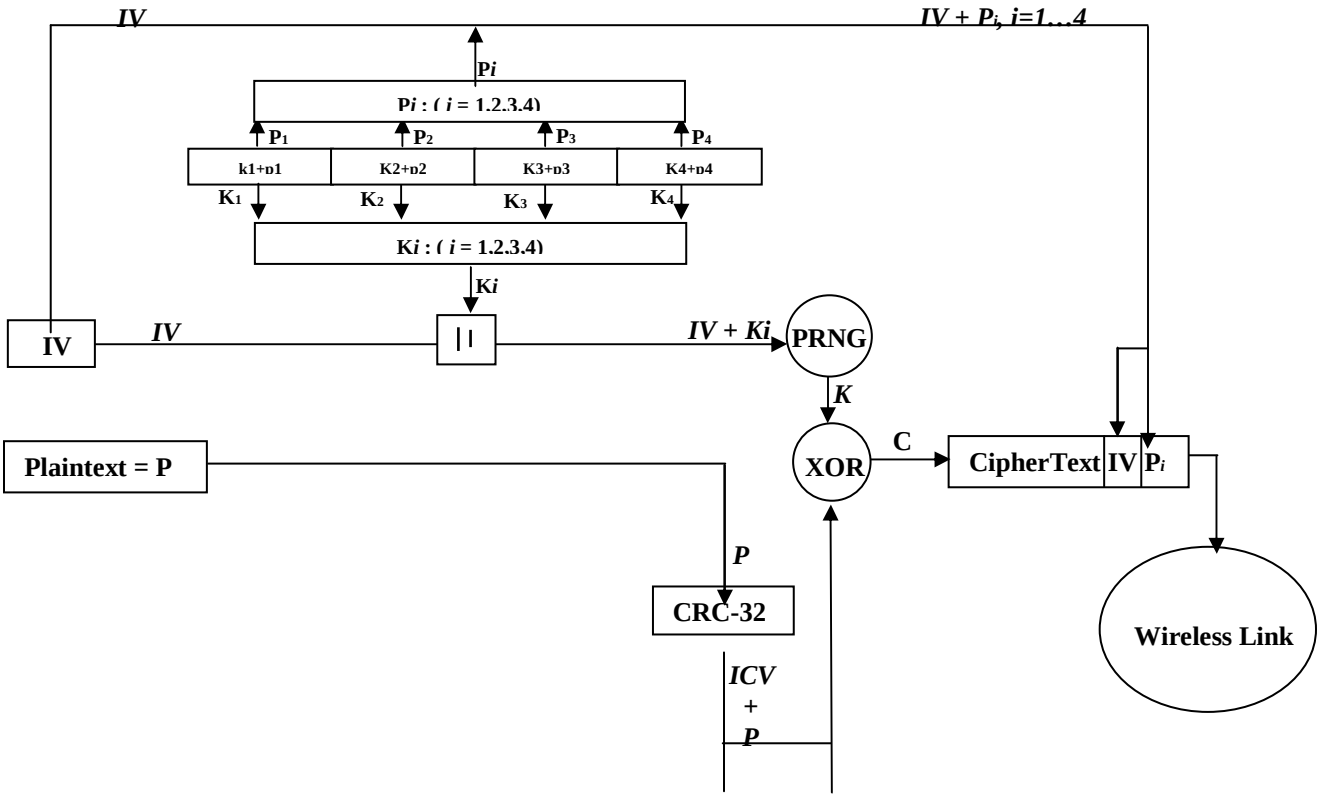
The following graph shows our simulation results based on table number 1.



The following graph is based on the proposed way for the key sequence generation. Our simulation results clearly show the effectiveness of the proposed key generation mechanism. The following graph can be used to observed that how we can improve the security of 802.11 wireless network.



New Architecture of WEP Encryption Based on Above Recommendations:



7 Conclusions

This paper highlights several deficiencies in 802.11 security implementations from the standpoint of authentication methods and WEP security protocol. It should be clear from the above discussion that the design committee of 802.11 WLAN failed to provide robust security through WEP and access control mechanisms. Furthermore, the WEP protocol fails to attain its three security goals: *confidentiality, access control*, and *data integrity*. In addition, the standards committee for 802.11 left many of the difficult security issues such as key distribution, key management, and a strong authentication mechanism as open problems. As a result, many of the organizations deploying wireless networks based on 802.11 standard are at risk of compromise.

Although the 802.11 has been widely accepted in several organizations as a viable replacement to wired LANs, it is still in its infancy as far as security is concerned. Thus the end result of this paper is that most of the deployed 802.11 wireless networks are at risk of compromise and the IEEE standards committee for 802.11 needs to urgently address these open issues.

This paper presents the two access control mechanisms supported by the IEEE 802.11 standard for preventing unauthorized users from accessing the internal resources of a wireless network. One approach is called open system authentication, and is considered a null authentication. The second approach is shared key authentication, which provides a better degree of authentication than the open system approach. However, this authentication mechanism also has some serious flaws in its design, which we described in this paper. We also presented some fundamental equations required to break the authentication process.

We have presented a brief discussion of a protocol called WEP, and identified some related problems that help clarify why the WEP encryption protocol fails to meet its design goals. This paper cites two fundamental problems with the implementation of the WEP protocol. The first is the small space available

for generating new Initialization Vectors. The second problem is the linearity of the checksum used in the WEP protocol. Based on these two fundamental problems mentioned above, there are a number of attacks possible against wireless networks which seriously undermine the security of the system. The possible attacks are: passive attack, chosen cipher text attack, table-based attack, and known plaintext attack (also known as active attack). These attacks are effective against both the IEEE 802.11 standard and the IEEE 802.11 high rates or Wi-Fi (an extension to the original 802.11 standard). In this paper, we have described all of these attacks in great detail and also demonstrated their effectiveness with some analysis.

Another problem was the question of what key size should be used in the WEP encryption algorithm. IEEE 802.11 and IEEE 802.11b use a 40-bit shared secret key with an RC4 algorithm for encryption. However, some papers have suggested that the size of the shared secret key should be increased. They claim that increasing the size of the existing shared secret key would make it more difficult for an attacker to crack the key. As a result, in 802.11a (an extension to the original 802.11 standard) the size of the shared secret key increased from 40 bits to 104 bits. In this paper, we have briefly presented this issue as well and discussed that increasing the size of the shared secret key does nothing to increase WEP's resistance to attack. No matter what size of the shared key being used, the 802.11 WLAN is still as vulnerable to eavesdropping as it is with the original 40 bit shared key,

We also described some of the general problems associated with 802.11 WLAN, such as the service set identifier (SSID) which is periodically broadcast by APs within the beacon management frame. We also discussed the Denial of Service attack and the attacks that are possible due to the broadcast infrastructure of 802.11 wireless networks. Finally we presented some possible solutions to a number of problems discussed.

References

[1] Russell Dean Vine, **"Wireless Security Essential"**, Defending Mobile Systems from Data Piracy. Wiley Publishing, Inc. 2002.

[2] Nikita Borisov, Ian Goldberg, and David Wagner, "**Security of the WEP algorithm**"; http://www.isaac.cs.berkeley.edu/isaac/wep-faq.html.

[3] Tara M. Swaminatha, Charles R. Elden, **"Wireless Security and Privacy",** Addison Wesley Publishing, 2003.

[4] William A. Arbaugh, Narendar Shankar, Y.C. Justin Wan, "**Your Wireless Network has No Clothes"** Department of Computer Science, University of Maryland College Park, March 30, 2001

[5] Jesse R. Walker, **"Unsafe at any key size; An analysis of the WEP encapsulation"** Oct 27, 2000 IEEE P802.11; Intel Corporation 2211 NE 25th Ave Hillsboro, Oregon 97124; doc: IEEE 802.11-00/362 October 2000.

[6] **Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications**. LAN MAN Standard Committee of the IEEE Computer Society. ANSI/IEEE Std 802.11, 1999 Edition.

[7] N. Borisov, I. Goldberg, and D. Wagner, "**Intercepting Mobile Communications: The Insecurity of 802.11 "**7th Annual Int'l. Conf.Mobile Comp. and Net. , Rome Italy, 2001.

[8] W. A Arbaugh, **"An Inductive Chosen Plaintext Attack Against WEP and WEP2",** 2001, IEEE 802.11 Working Group, Task Group I (Security), 2002.

[9] Brian Carter, and Russel Shumay. **"Wireless Security End To End; A Practicle Guide for IT Professionals"**. Wiley Publishing, Inc. 2002.

[10] Com One-The Telecom Expert, "**Wireless LAN 802.11b Technology"** 2002 Com One; http://www.com1.fr, E-mail: info@com1.fr

[11] **Cisco comments on recent WLAN security**;http://www.cisco.com/en/US/products/hw/wireless/ps430/prod_bulletin09186a00800a9e74.html.Cisco Systems, Inc

[12] Trey Azariah, "**Wireless Security Blackpaper**". July 2002, Ars Technica: http://www.arstechnica.com/paedia/w/wireless/security-1.html

[13] Matthew Gast, "**Seven Security Problems of 802.11 Wireless Networks**". May 2002, O'Reilly Network. www.oreillynet.com/pub/a/wireless/2002/05/24/wlan.html

[14] Steve Steinke, **"Security and 802.11 Wireless Networks**". May 2002, Network Magazine. http://www.networkmagazine.com/article/NMG20020606S0011/2

[15] Alan Beck. **"Netscape's export SSL broken by 120 workstations and one subnet**". *HPCwire*, August 22 1995.

[16] Damien Doligez. "**SSL challenge virtual press conference"**. http://pauillac.inria.fr/~doligez/ssl/press-conf.html, 1995

[17] Simon Singh. The Code book: "**The Evolution of Secrecy from Mary**", Queen of Scots, to quantum cryptography. Doubleday, New York, NY, USA, 1999.

[18] W. T. Tutte. "**FISH and I",** 1998. A Transcript of Tutte's June 19, 1998 lecture at the university of Waterloo.

[19] Jim Geier, **"802.11 WEP: Concepts and Vulnerability"**. 802.11 Planet, 2003. http://www.802.11-planet.com/tutorials/article.php/13368661.

[20] Wen-Ping Ying, "**Key Hopping – A Security Enhancement Scheme for IEEE 802.11 WEP Standards**", February 2002. NextComm, Inc. www.nextcomm.com

[21] Jason S. King, "**An IEEE Wireless LAN Security White Paper**" October 22, 2001. www.llnl.gov/asci/discom/ucrl-id-147478.html

.