International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 03 , March 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

SECURITY MECHANISM IN WIRELESS LOCAL AREA NETWORK (WLAN)

Dr. Vikas Kulshreshtha[1], Sh. Abhishek Soni[2],

[1]*Asst Prof. Government Engineering College Jhalawar (India)*
[2]*Asst Prof. Government Engineering College Jhalawar (India)*

ABSTRACT

Wireless Network system is basically a distributed system which helps to communicate between different machines. Wireless communication is needed to enable mobility of communicating devices. Several types of wireless networks are in use for mobile communication. Wireless communication takes place over an "open" wire and is relatively easy to tap. It may seem that traditional techniques of cryptography can be used to secure wireless communication. However, the main problem is that these secure techniques are designed for wired networks and are computation and communication intensive. Attempts to reduce these overheads lead to security schemes that are relatively easy to break. Security schemes for wireless local area network will be discussed in this paper.

Keywords: security, wireless, local area network (LAN), mechanism, protocol

I INTRODUCTION

This paper discusses the security techniques used in local area network, specially the IEEE 802.11 standard (IEEE, 1999). In this paper we discuss the security, mechanism and focus on the flawed wired equivalent privacy (WEP), covering its intentions and shortcomings, as well as the ways to get the best protection given limited coverage, WiFi Protected Access (WPA), an interim protocol to fix the shortcomings of WEP, and 802.11i, the IEEE standard to provide strong encryption, key management, and support for authentication.

Wireless Local Area Network (WLAN) has a radius of around 100 m typically. Many wireless access points work directly "out of the box" requiring no configuration. The user simply plugs them in the network and a power outlet, and they work. The downside is that most devices default to being very open, with most security features disabled; these features often are overlooked for an "out of the box" installation. Moreover, user may not know that some of the security features are either limited or flawed.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

IEEE 802 is the LAN/ metropolitan area network (MAN) standard committee that has numerous subgroups within it. IEEE 802.11 is the wireless Local Area network (WLAN) standard sub-committee. And within it, there are several sub-committees for different 802.11 standards.

Basic Architecture of Wireless Local Area Network (WLAN)

The wireless station (WS) is the remote and mobile unit. The access point (AP) or base station is the non mobile unit that connects the wireless network into a wire-based network. The AP acts as a bridge or router and usually has some protection mechanisms built in 802.11 networks can be organized in two different ways: infrastructure or ad-hoc. The basic service set (BSS), identified by a 6-byte string, is a network formed by an AP and the wireless station that are associated with it.

An external service set(ESS) is two or more BSSs that form a single logical network. When they move wireless stations can switch seamlessly from one AP to another with no disruption of service. The APs coordinate the handoff among themselves via an Ethernet connection. Figure 1.1 shows an example of two BSSs forming an ESS.

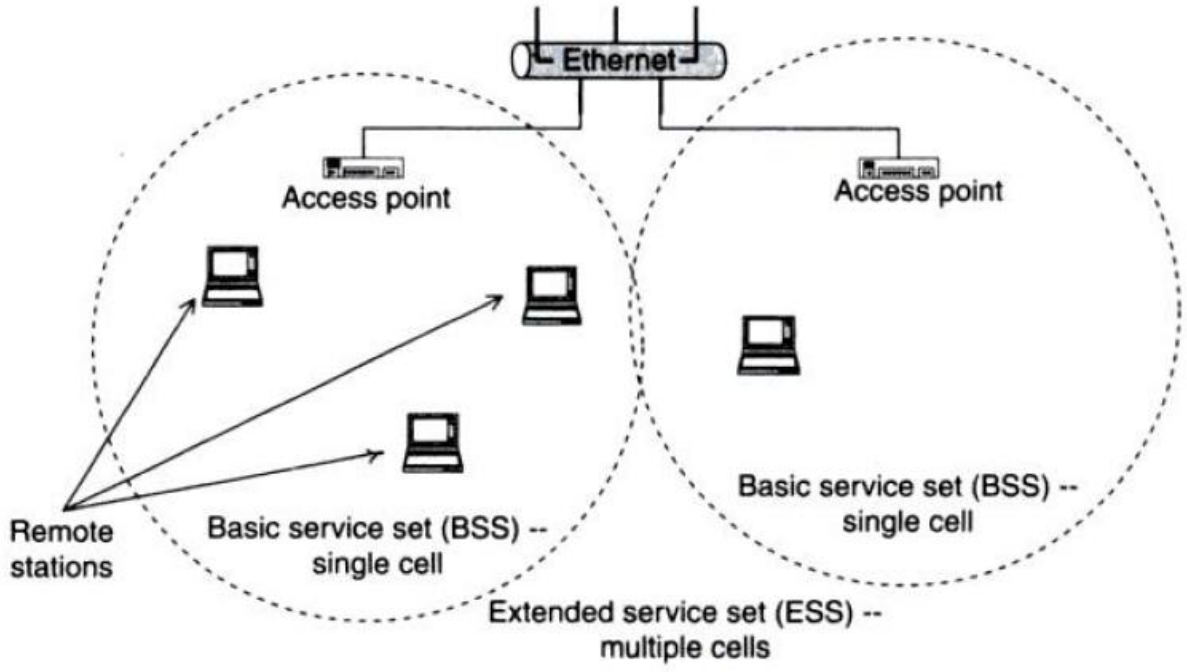

Fig 1.1 Two BSSs forming an ESS

III WIRED EQUIVALENT PRIVACY (WEP)

WEP is the security scheme provided with 802.11b. WEP was designed to raise the baseline security level to be comparable with the standard wired Ethernet. Sniffing packets off a wired network requires a user to physically tap

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

into the network. This paper explains the design goals of WEP, its data frame, and how encryption, authentication, and decryption work.

3.1 WEP Goals

WEP was designed to support a few criteria. Firstly it has to be reasonably strong, secondly stations must be able to resynchronize with the AP without requiring user intervention such as password, because the stations may go in and out of coverage frequently. Thirdly, it must be computationally efficient so that it can be performed in either hardware or software because some processors may be low-power, low-speed device. Fourthly, it had to be exportable.

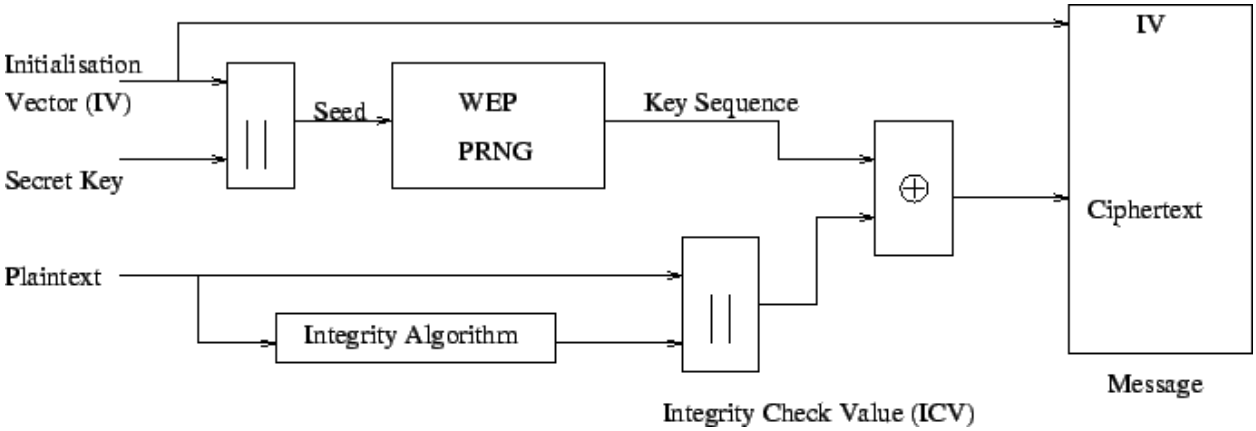

Fig 1.2 Block diagram of WEP encryption

WEP consists of secret key either 40 or 104 bits (5 or 13 bytes) and an initialization vector (IV) of 24 bits. Thus the total protection, as it is sometimes called, is 64 or 128 bits. The key plus the IV is used to seed an RC4-based pseudorandom-number generator (PRNG). This sends the stream of pseudorandom number that is XORed with the data stream to produce the cipher text. In addition, an integrity check value (ICV) indicated if the data stream was corrupted. The ICV is a simple CRC-32 checksum. Figure 1.2 shows a block diagram of WEP encryption.

3.2 WEP Data Frame

The WEP data frame is shown in the Figure 1.3 consists of an IV of 4 bytes, the data and protocol data unit (PDU) of 1 or more bytes, and the ICV of 4 bytes. The IV can be further divided into 3 bytes (24 bits) of the actual initialization vector plus 1 byte that uses 2 bits to specify a key and 6 bits of padding. With the 2 bits, the device can store up four different secret keys.

International Journal of Advance Research in Science and Engineering
Vol. No.6, Issue No. 03 , March 2017
www.ijarse.com
IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

3.3 WEP Encryption

The encryption is shown in the block diagram in figure 1.2. It takes the plain text message, the IV, and the secret key as input and produces as output a message consisting of the cipher text message and the IV by performing the following steps:

1. Compute the ICV using CRC-32 over the plain text message.
2. Concatenate the ICV to the plain text message.
3. Choose a random IV and concatenate it to the secret key and use it as input to the RC4 PRNG to produce the pseudorandom key sequence.
4. Encrypt the plain text and the ICV by doing bitwise XOR with the key sequence from the PRNG to produce the cipher text.
5. Append the IV to the front of cipher text.

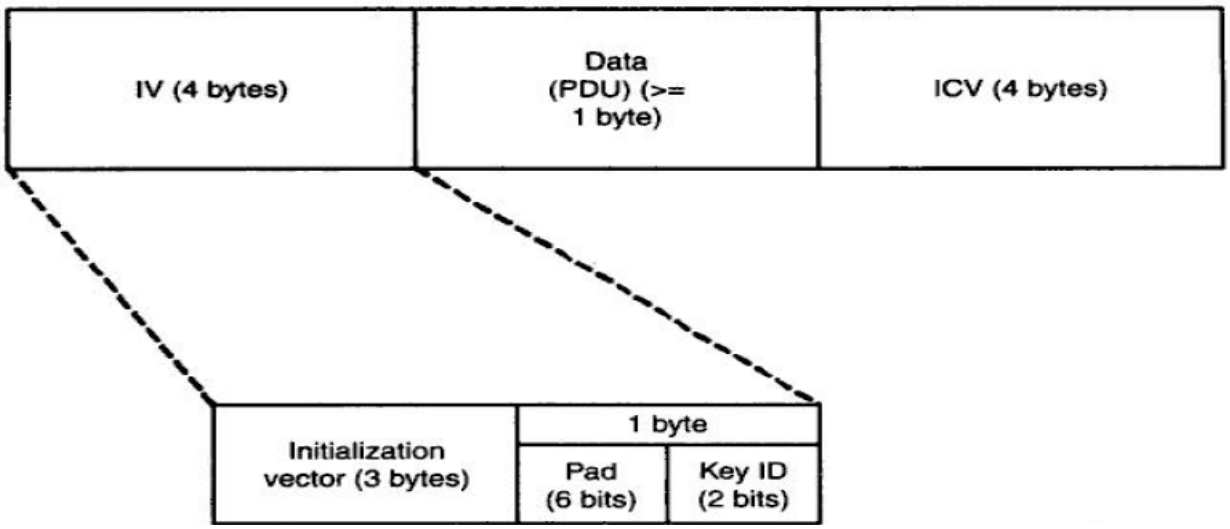

Fig: 1.3 WEP Data Frame

3.4 WEP Decryption

Decryption of WEP is just reverse of the encryption. The algorithm takes the secret key and the message consisting of the cipher text and ICV as input and produces the plaintext message and an error flag as output by performing the following steps:

1. Generate the key sequence k using the IV of the message.
2. Decrypt the cipher text message by doing a bitwise XOR with k to generate the original plaintext and ICV.
3. Verify the integrity of the message by computing the ICV on plain text, ICV', and comparing it with the reversed ICV from step 2.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

4. Trap errors, if ICV is not equal to ICV', by sending an erroe to the MAC management layer and back to the sending station.

3.5 WEP Authentication

APs perform an optional challenge style of authentication to the wireless stations as shown in figure 1.4 as follows:

1. The wireless stations (WS) send an authentication request to the AP.
2. The AP sends a (random) challenge text T back to the WS.
3. The WS sends the challenge response, which is text T, encrypted with a shared secret key.
4. The AP sends an acknowledgment (ACK) if the response is valid and NACK if it is invalid.

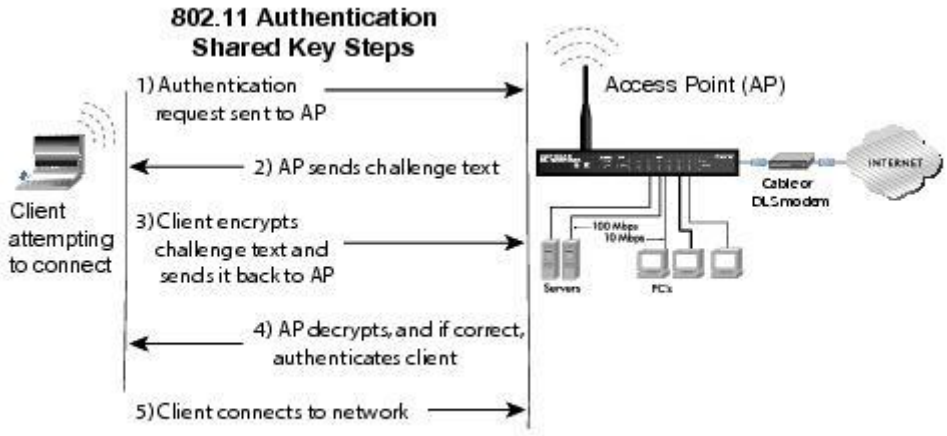

Fig1.4 WEP Authentication

IV CONCLUSION

In today's world digital communication security is a myth. There is a requirement to develop the algorithm for the information security over LAN, WAN, MAN. The information of national importance is at the risk. Information security over LAN, MAN, WAN is the prime area of concern. Today many developers are constantly working to develop some mechanism or algorithm for the information security so that the data over internet should be secure and there will be no national threat. Today is the time of mobile computing, routing algorithm has to be more efficient so that information can be secured from the foreign intrusion.

REFERENCES

[1] Borisov, N., I. Goldberg, and D. Wagner, "Intercepting Mobile Communications: the Insecurity of 802.11," in proceedings of the 7th Annual International Conference on Mobile Computing and Networking, July 2001, Rome, Italy.

IJARSE
ISSN (O) 2319 - 8354
ISSN (P) 2319 - 8346

[2]Cam-Wignet N., R. Housley, D. Wagner, and J. Walker, "Security flaws in 802.11 Data Link Protocol". Communications of the ACM May 2003, 46(5), pp. 35-39.

[3]Cam-Wignet N., T. Moore, D. Stanley, and J.Walker, "IEEE 802.11i Overview," presented at NIST 802.11 LAN security Workshop.

[4]Geier J., "The Guts of WLAN Security Policy" November 12, 2002.

[5]Moy, J., IETF RFC 2328, "OSPF version 2," April 1998.

[6] [Park, V., and M.S. Corson, IEFT Manet Internet Draft.

[7] Perkin, C.E., E.M. Belding-Royer, and Samir Das, IETF RFC 3562, "Ad-Hoc on Demand Routing Distance Vector (AODV) Routing," July 2003.

[8]Walker, J., "Unsafe at any key size: an analysis of WEP encapsulation," Tech. Rep 03628E, IEEE 802.11 committee.

[9]Walker, J., "802.11 Security Consideration and Solution," Intel Developer Forum, Spring 2002.

[10]"WEP Crack, and 802.11 Key Breaker".

[11]"802.1x-Port Based Network Access Control".