International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2013): 6.14 | Impact Factor (2014): 5.611

Ground Rules of Wireless LAN Security

K. Senthamarai

HOD (2010-13) ,CSE, P. R. Engineering College, Vallam, Thanjavur

Abstract: ***Wireless Local Area Networks (WLANs) are cost effective and desirable gateways to mobile computing. They allow computers to be mobile, cable less and communicate with speeds close to the speeds of wired LANs. These features came with expensive price to pay in areas of security of the network. This paper identifies and summarizes these security concerns and their solutions. Broadly, security concerns in the WLAN world are classified into physical and logical. The paper overviews both physical and logical WLANs security problems followed by a review of the main technologies used to overcome them. It addresses logical security attacks like man-in-the-middle attack and Denial of Service attacks as well as physical security attacks like rouge APs. Wired Equivalent Privacy (WEP) was the first logical solution to secure WLANs. Towards perfection in securing WLANs, IEEE802.11i emerged as a new MAC layer standard which permanently fixes most of the security problems found in WEP and other temporary WLANs security solutions. This paper reviews all security solutions starting from WEP to IEEE802.11i and discusses the strength and weakness of these solutions.***

Keywords: WLAN, wireless LAN, security, IEEE802.11, Physical Attacks

1. Introduction

Wireless Local Area Networks (WLANs) succeeded in providing wireless network access at acceptable data rates. The Institute of Electrical and Electronics Engineering (IEEE) have set standards and specifications for data communications in wireless environment, IEEE802.11 is the driving technology standard for WLANs . WLANs are deployed as an extension to the existing fixed/wired LANs and due to the fact that the nature of WLANs are different from their wired counterparts, it is important to raise the security of WLANs to levels closer or equal to the wired LANs. In general IEEE802.11 can operate in two network topology modes, Ad hoc and Infrastructure modes. This paper discusses WLANs in infrastructure mode. In the infrastructure topology, wireless stations (STAs) communicate wirelessly to a network access point (AP) which is connected to the wired network, this setup forms a WLAN. The establishment of connections between STAs and AP goes through three phases; probing, authentication and association. In probing phase, the STA can either listen passively to AP signals and automatically attempts to join the AP or can actively request to join an AP. Next is the authentication phase, the STA here is authenticated by the AP using some authentication mechanisms described later in the paper. After successfully authenticating, the STA will send an association request to the AP, when approved, the AP adds the STA to its table of associated wireless devices. The AP can associate many STAs but an STA can be associated to one AP only at a time. A breach of the security of the

WLAN will eventually harm the security of the wired LAN. The propagation of air waves can not be blocked or locked in a room so there is a big risk of eavesdropping and Man-in-the-middle-Attacks The situation is different in wired LANs where critical servers can be locked in a special room and data transmission is carried out by cables that can be monitored and controlled to some extent. When dealing with WLANs it is important to keep three security goals in mind, Authentication to the WLAN, Confidentiality and Integrity of the data transmitted.

Confidentiality means hiding high sensitive data during information transmission between STAs and AP.

2. Literature Survey

Wireless LANs are everywhere these days from home to large enterprise corporate networks due to the ease of installation, employee convenience, avoiding wiring cost and constant mobility support. However, the greater availability of wireless LANs means increased danger from attacks and increased challenges to an organization, IT staff and IT security professionals. This paper discusses the various security issues and vulnerabilities related to the IEEE 802.11 Wireless LAN encryption standard and common threats/attacks pertaining to the home and enterprise Wireless LAN system and provide overall guidelines and recommendation to the home users and organizations.

Over the last twelve years, 802.11 Wireless LAN's have matured and really reshaped the network landscape. 802.11n is now rapidly replacing Ethernet as the method of network access. The rapid proliferations of mobile devices has led to a tremendous need for wireless local area networks (WLAN), deployed in various types of locations, including homes, educational institutions, airports, business offices, government buildings, military facilities, coffee shops, book stores and many other venues. Besides, the facilities of flexibility and mobility of wireless devices has been attracted by most organizations and consumers all over the world. Low cost of hardware and user friendly installation procedures allow anyone to set up their own wireless network without any specialist knowledge of computer networks.

However, the increased development of Wireless LAN has increased the potential threats to the home user, small businesses and the corporate world. Unlike a wired network, a WLAN uses radio frequency transmission as the medium for communication. This necessarily exposes layer 1 and layer 2 to whoever can listen into the RF ranges on the network. Wireless insecurity has been a critical issue since

Wired Equivalent Privacy (WEP), an IEEE standard security algorithm for wireless networks, was compromised. To address the significant security flaws in the WEP standard, the Wi-Fi alliance developed the 802.11i standard, called Wi-Fi Protected Access (WPA) and WPA2 . However, many researchers have shown that the IEEE 802.11i standard cannot prevent eavesdropping, various denial of service attacks including de-authentication and disassociation attacks. Moreover, 802.11i's pre-shared key mode of WEP for flexibility and backward.

Compatibility has made it easier for most hackers to perform a Dictionary and Brute force attack.

This paper discusses the vulnerabilities and security issues pertaining to the IEEE 802.11 security standard and describes major well known attack/threats to the home and enterprise wireless LAN system.

3. Problem Approach

There are many security threats and attacks that can damage the security of WLANs. Those attacks can be classified into logical attacks and physical attacks.

3.1 Logical Attacks

3.1.1 Attacks on WEP

Wired Equivalent Privacy (WEP) is a security protocol based on encryption algorithm called "RC4" that aims to provide security to the WLAN similar to the security provided in the wired LAN . WEP has many drawbacks like the usage of small Initialization Vector (IV) and short RC4 encryption key as well as using XOR operation to cipher the key with the plain text to generate cipher text. Sending the MAC addresses and the IV in the clear in addition to the frequent use of a single IV and the fact that secret keys are actually shared between communications parties are WEPs major security problems. WEP encrypted messages can be easily retrieved using publicly available tools like WEP Crack.

3.1.2 MAC Address Spoofing

MAC addresses are sent in the clear when a communication between STAs and AP takes place. A way to secure access to APs and hence to the network is done to deny other users from listening to the communication. Integrity means preserving the accurateness and the correctness of information transmitted between STAs and A. Any security solution should achieve these three goals together.

The security and management problem become huge as more APs are installed in the network. So there is a need to centralize and manage security issues in small WLANs as well as large ones and a need to develop techniques to counter security threats. As WLANs applications like wireless Internet and wireless e- commerce spread very fast, there is a need to assure the security of such applications.

3.2 Denial of Service Attack

Denial of Service attacks or DoS is a serious threat on both wired and wireless networks. This attack aims to disable the availability of the network and the services it provides . In WLANs, DoS is conducted in several ways like interfering the frequency spectrum by external RF sources hence denying access to the WLAN or, in best cases, granting access with lower data rates.

Figure 1: Representation of the famous Man-in-the-middle attack for both wired and wireless networks

3.2.1 Man-in-the-middle attack

This is a famous attack in both wired and wireless networks. An illicit STA intercepts the communication between legitimate STAs and the AP. The illegal STA fools the AP and pretends to be a legitimate STA; on the other hand, it also fools the other end STA and pretends to be trusted AP. Using techniques like IEEE802.1x to achieve mutual authentications between APs and STAs as well as adopting an intelligent wireless Intrusion Detection System can help in preventing such attacks.

3.2.2 Bad network design

WLANs function as an extension to the wired LAN hence the security of the LAN depends highly on the security of the WLAN. The vulnerability of WLANs means that the wired LAN is directly on risk. A proper WLAN design should be implemented by trying to separate the WLA from the wired LAN by placing the WLAN in the Demilitarized Zone (DMZ) with firewalls, switches and any additional access control technology to limit the access to the WLAN. Also dedicating specific subnets for WLAN than the once used for wired LAN could help in limiting security breaches. Careful wired and wireless LAN network design plays important role to secure access to the WLAN.

3.3 Physical Attacks

3.3.1 Rogue Access Points

In normal situations, AP authenticates STAs to grant access to the WLAN. The AP is never asked for authentication, this raises a security concern, what if the AP is installed without IT center's awareness? These APs are called "Rogue APs" and they form a security hole in the network.

An attacker can install a Rogue AP with security features disabled causing a mass security threat. There is a need for mutual authentication between STAs and APs to ensure that both parties are legitimate. Technologies like IEEE802.1x can be used to overcome this problem.

3.3.2 Physical placement of APs

The installation location of APs is another security issue because placing APs inappropriately will expose it to physical attacks. Attackers can easily reset the APs once found causing

the AP to switch to its default settings which is totally insecure. It is very important for network security administrators to carefully choose appropriate places to mount APs.

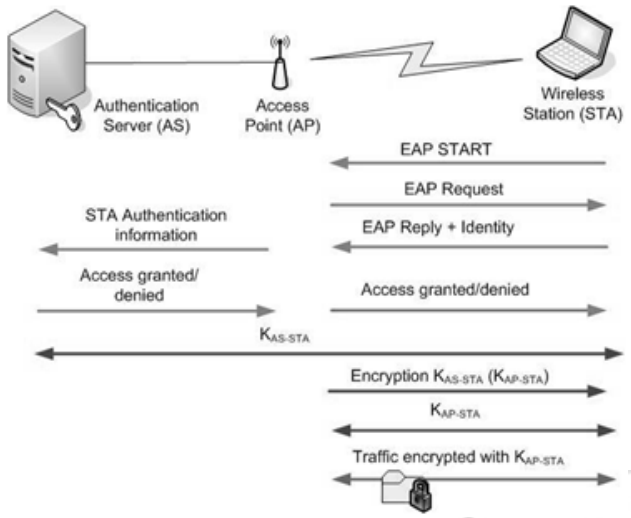

Figure 2: Illustration of IEEE802.1x network access control Protocol

3.4 Wired Equivalent Privacy (WEP)

WEP is the security protocol in use since the early IEEE802.11 standard . It is used to secure communications between APs and STAs and to provide secured authentication schemes; the aim was to provide security to the WLAN similar to the security provided in the wired LAN. It is based on a stream cipher encryption algorithm called "RC4". WEP is used to control access to the WLAN and to encrypt confidential information. To access a WLAN in a shared key authentication scheme, both STA and AP should have the correct shared secret key; this key is used to encrypt confidential information. The length of this key is 40-bits; this is a very short key length. The main drawback of WEP is the use of this 40-bit key even though RC4 encryption algorithm can support up to 104 bit key but 40-bit key is the default key size shipped with WLAN products.

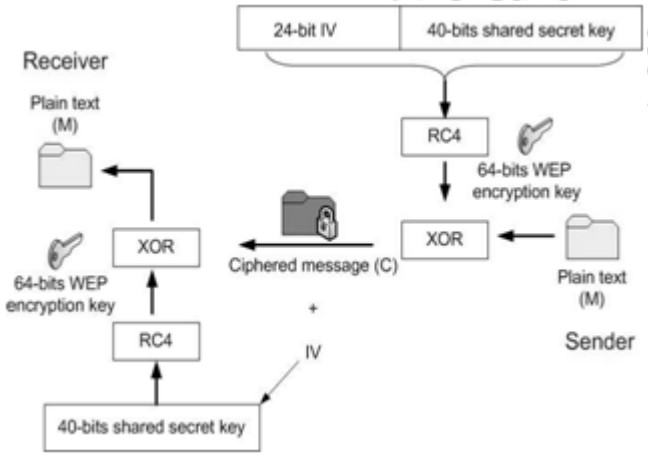

Figure 3: Schematics of the Wired Equivalent Privacy (WEP) protocol used to control access to the WLAN

4. Discussion

To solve the roots of the problems in WEP IEEE specified a new standard that provides enhanced security as well as support to legacy protocols for backward compatibility. IEEE802.11i. is based on IEEE802.11 with security enhancement in the MAC layer; it was approved in July 2004. IEEE802.11i elevates the level of security shipped with WLAN products like APs and wireless network interface cards. A specific task group in the IEEE called "Task Group i (TGi)" developed and still updating this standard, the group tried to specify a standard that will achieve most important security goals, authentication, confidentiality and integrity. RSN IEEE802.11i defines the concept of Robust Security Network (RSN). RSN, according to IEEE802.11i, is the description of the network that can establish an RSN Association (RSNA) between its entities. any communication between entities in WLAN starts with an association, whether an STA associates with AP in an infrastructure topology or an STA associates with another STA in ad hoc topology. With this new framework, IEEE802.11i defines RSNA-equipment which has the capability to establish RSNA. On the other hand, there are pre-RSNA equipments which are equipments that do not have the capability to establish RSNA.

4.1 CCMP

IEEE802.11i mandates the use of a protocol to protect confidentiality and integrity of data transferred, named Counter mode with CBC-MAC Protocol (CCMP). CCMP provides confidentiality and integrity of the data transferred and authenticity of the sender. It is based on the Advanced Encryption Standard (AES) block cipher. AES is the most reliable block cipher to date, it uses a minimum of 128-bit key length and text blocks of 128-bits as well . This is a great advancement over traditional WEP protocol which is based on weak RC4 stream cipher. CCMP consists of two important protocols, Counter Mode AES encryption (CTR-AES) and Cipher Block Chaining – Massage Authentication Code (CBC-MAC) based on AES. CTR-AES encrypts data transferred (i.e. achieves confidentiality) and CBC-MAC provides integrity of data and authentication of the sender by calculating the Message Integrity Code (MIC) of the message. Figure 11 shows how MIC is calculated using CBC-MAC based on AES block cipher.

4.2 Key Management

Key management was a major problem in WEP; one of the biggest drawbacks of WEP was key abuse by using the same key over and over again. With the help of IEEE802.1x/EAP, a novel key management scheme was developed. This key management scheme can be used with TKIP and IEEE802.11i security standard. IEEE802.11i names this key management scheme the “4-way handshake”. Initially the STA listens to AP signals passively or actively probes for it. Then the STA authenticates using open system authentication method. Then STA associates with the AP. When the association is established, they both authenticate themselves using IEEE802.1x authentication.

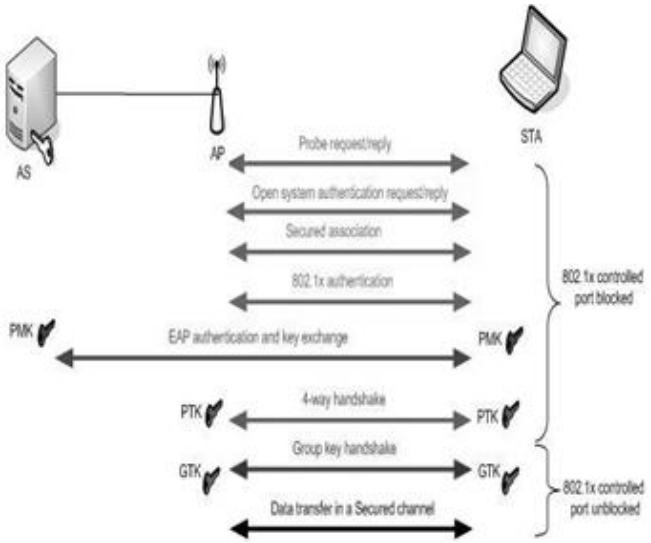

Figure 4: Key management structure in IEEE802.11i protocol.

4.3 CBC-MAC Protocol (CCMP)

IEEE802.11i is optionally supporting TKIP to provide backward compatibility with legacy systems and with systems that does not support AES hardware. TKIP keys are obtained from PTK and GTK, 128-bits minimum, TKIP will benefit from the key management scheme offered by IEEE802.11i to solve key distribution problems. IEEE802.11i offers extra features like pre-authentication capabilities for secured roaming, pre-authentication can only be used when the 4-way handshake is completed.

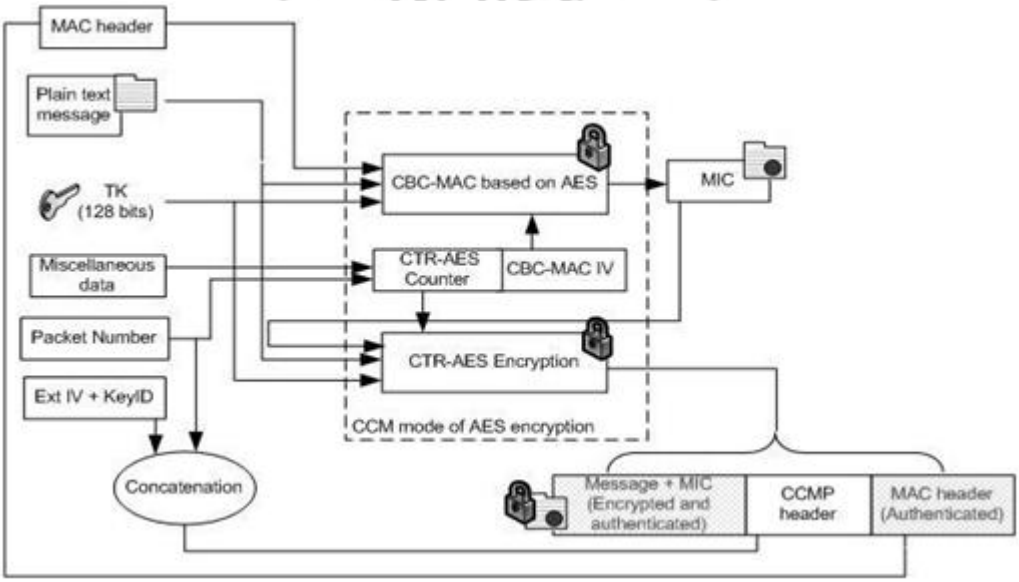

Figure 5: Block diagram of CBC-MAC Protocol (CCMP)

5. Conclusion

IEEE802.11 was initially designed to interconnect wireless devices to wired networks; the aim was to achieve networking with minimum or no security. Security was not an important issue at that stage, however, with the successful of WLANs and the fast adoption of this technology, security became important and achieving security became a primary concern. Wired Equivalent Privacy (WEP) security protocols was the first to be adopted in an attempt to satisfy the need for securing wireless networks, soon WEP became vulnerable and there was a demand for a better security protocol. Industries already invested in wireless devices so any new protocol should consider the hardware capabilities of such devices. TKIP came into picture with promise of a better security using the same hardware. An upgrade in software is what made TKIP more secured than WEP. However, the core encryption algorithm is still the same, weak RC4 stream cipher, with this encryption algorithm and the design flaws it experiences, TKIP believed to be a short-life solution. IEEE recognized the need for a new protocol that is more secure and long lasting. IEEE finally answered the call by working on a new security standard, IEEE802.11i. The standard was approved in June 2004. This new standard addresses new security protocols and introduces the adoption of strong block encryption algorithm, Advanced Encryption Standard (AES), also introduces a new key management scheme. Attacks on privacy, integrity, and authentication can be overcome by IEEE802.11i.

As far as the logical attacks are concerned, IEEE802.11i provides adequate solutions to defend against WEP weaknesses, man-in-the-middle attacks, forgery packets attacks and replay attacks. However, DoS attack is not addressed properly and there are no solid protocols or implementations to stop such attacks basically because the attacks target the physical layer of the TCP/IP stack like interfering with the frequency band. Most research activities in wireless security are done on the data link and upper layers. Researchers are working hand to hand with the industry to provide the best solution for logical attacks but

there is negligence in the area of physical attacks in which human behavior and human interaction with devices takes place. There is no meaning to use IEEE802.11i equipped AP that sits behind a firewall and allocated a dedicated subnet and uses long AES encryption keys to encrypt transmissions if this AP is placed somewhere visible to attackers or placed in such a way that signals propagate outside the premises. As simple as resetting the AP, a catastrophe could happen in the network. The human factor and the way they deal with device settings, placements and overall managements have significant value in wireless security. Education and training in wireless security issues and their differences comparing to wired security issues as well as defining an appropriate wireless security policy are important factors to achieve overall security. Adequate compromise between ease of usability versus security is required in APs shipped today. APs should be easy to implement and use by normal users and at the same time some critical security features should not be left disabled.

All in all, wireless LANs are becoming more and more secure especially with the arrival of IEEE802.11i complaint wireless hardware.

Sensitive information and highly secured communications can be transmitted with a higher confident than few years back that no illicit user around can actively or passively tamper with the data transmitted providing a careful, skilled personnel is in charge of configuring and installing the APs.

6. Future Scope

6.1 Counter Measures

If there are vulnerabilities, then there are their counter measures also, which cannot overcome them fully but can protect to a great extent.

Here are few countermeasures, which can help a lot in retaining security of WLAN.

- Do not trust WLAN and work under the coverage of a VPN (Virtual Private Networks).
- Maintain a good key management system, which changes the key before the sufficient no of packets required for cracking the key are transmitted.
- Increasing the bit length of IV and secret key is also a partial solution.
- Use of strong algorithm like AES
- Making the checksum of the message a keyed function, using algorithms like HMAC keyed Hashing.
- Configuring AP for allowing only few MAC addresses, which are there in his Access Control Lists (ACLs).
- Define the ACL depending upon Signal strength.
- One must take care of the physical security also. You should take care that no unauthorized person gets access of your laptop or any Work Station, which is in the Network because he can just copy the secret key.
- Enable RADIUS or Kerberos authentication for workstation to Access Point.

6.2 Future of Wireless LAN Security

6.2.1 Advanced encryption Standard (AES)

Advanced Encryption Standard is gaining acceptance as appropriate replacement for RC4algorithm in WEP. AES uses the Rijandale Algorithm and supports the following key lengths.

- 128 bit
- 192 bit
- 256 bit

AES is considered to be un-crack able by most Cryptographers. NIST has chosen AES for Federal Information Processing Standard (FIPS). In order to improve wireless LAN security the 802.11i is considering inclusion of AES in WEPv2.

6.2.2 Temporal Key Integrity Protocol (TKIP)

The temporal key integrity protocol (TKIP), initially referred to as WEP2, is an interim solution that fixes the key reuse problem of WEP, that is, periodically using the same key to encrypt data. The TKIP process begins with a 128-bit "temporal key" shared among clients and access points. TKIP combines the temporal key with the client's MAC address and then adds a relatively large 16-octet initialization vector to produce the key that will encrypt the data. This procedure ensures that each station uses different key streams to encrypt the data. TKIP also prevents the passive snooping attack by hashing the IV.

An advantage of using TKIP is that companies having existing WEP-based access points and radio NICs can upgrade to TKIP through relatively simple firmware patches. In addition, WEP-only equipment will still interoperate with TKIP-enabled devices using WEP. TKIP is a temporary solution, and most experts believe that stronger encryption is still needed.

6.2.3 802.1X and Extensible Authentication Protocol

Combined with an authentication protocol, such as EAP-TLS, LEAP, or EAP-TTLS, IEEE 802.1X provides port-based access control and mutual authentication between clients and access points via an authentication server. The use of digital certificates makes this process very effective. 802.1X also provides a method for distributing encryption keys dynamically to wireless LAN devices, which solves the key reuse problem found in the current version of 802.11.

Initial 802.1X communications begins with an unauthenticated supplicant (i.e., client device) attempting to connect with an authenticator (i.e., 802.11 access point). The access point responds by enabling a port for passing only EAP packets from the client to an authentication server located on the wired side of the access point. The access point blocks all other traffic, such as HTTP, DHCP, and POP3 packets, until the access point can verify the client's identity using an authentication server (e.g., RADIUS). Once authenticated, the access point opens the client's port for other types of traffic.

References

[1] IEEE Standard for local and metropolitan area networks, "Wireless LAN Medium Access Control

(MAC) and Physical Layer Specifications", ANSI/IEEE Std 802.11, 1999 Edition (R2003).
[2] Shin, M.; Ma, J.; Mishra, A.; Arbaugh, W.A., "Wireless network security and interworking", Proceedings of IEEE, Volume 94, Issue 2, pp 455 – 466, February 2006.
[3] Wang Shunman, TaoRan, WmgYue and ZhangJi, "Wireless LAN and it's security problem". Proceedings of the Fourth International Conference on Parallel and Distributed Computing, Applications and Technologies, 2003. PDCAT'2003.
[4] Matthew S. Gast, 802.11 Wireless Networks, O'REILLY, 2002.
[5] William Stallings, Cryptography and Network Security, Principles and Practices, 3rd Edition, Prentice Hall 2003.
[6] Matija Sorman, Tomislav Kovac and Damir Maurovic, "Implementing Improved WLAN security", 46th International Symposium Electronics in Marine. ELMAR-2004, Zadar. Croatia, 16-18 June 2004.
[7] Joon S.Park and Derrick Dicoi, "WLAN Security: Current and Future". IEEE Computer Society, October 2003.
[8] WEPCRACK, Software, http://www.sourceforge.net/projects/wepcrack .
[9] AirSnort Software, http://airsnort.shmoo.com
[10] Ethereal Software, http://www.ethereal.com
[11] KISMET Software, http://www.kismetwireless.net
[12] Brown, B. "802.11: the security differences between b and I", IEEE Potentials, October/November 2003.
[13] Joel W. Branch, Nick L.Petroni JR, Leendert Van Doorn and David Safford, "Autonomic 802.11 Wireless LAN Security Auditing". IEEE Security & Privacy, 2004.
[14] War driving website, http://www.wardriving.com/
[15] NetStumbler Software, http://www.netstumbler.com

Author Profile

K. Senthamarai worked as the HOD of CSE Department in Ponnaiya Ramajayam Engineering College at P.R. Engineering College Vallam, Thanjavur.(2010 to 2013).I have completed M.E(CSE) at Kumara guru College of Technology, Coimbatore on 2004.I am a Life Member of ISTE (The Indian Society for Technical Education).