

Wireless LAN Security – Challenges and Solutions

PROF. RATHNAKAR, DR. VITYANATHAN, DR. PETHUR RAJ

Abstract — enabling technologies, tools, languages, frameworks and platforms facilitating the much anticipated convergence of Web and wireless communication started to unfold, the vision of ushering mobile / wireless Internet is all set to fructify and blossom here in a big way in the days to come. Fortunately Mobile Internet / Wireless Web is a larger part of the grand vision of ubiquitous Computing (providing information and services on demand in a secure manner for any one at any time, at the desired quantity and quality, at any place through any device). But one critical, urgent and explosive issue that stands out in making computing and communication ubiquitous, pervasive and invisible is security. As security problem has encompassed the whole IT domain today, there is a serious and focused research on bringing out robust, unbreakable, durable and innovative security ideas and solutions. Thus the requirement of security has come to the center stage of research. In this new, highly important and fast emerging field security is being touted as the main obstacle for extensive proliferation of wireless Internet usage. In this paper, we have explained about the wireless Local Area Network (WLAN) security challenges along with how a hacker is able to break into the wireless network like WEP cracking, MAC attack, Man-in-middle attack, Dictionary attack, session hijacking and DoS followed by the existing and proposed viable solutions such as WEP based security using RC4 algorithms and the issues related to the same.

Key words - IEEE802.11i, RC4 algorithm, TKIP, VPN, WEP, Wi Fi Protected Access, Wireless network MAC layer, WLAN security.

I. INTRODUCTION

Wireless data communications have transformed not only the business world but also the whole human society by improving efficiency, flexibility, convenience and above all productivity besides providing the unique location, device, and time-independent connectivity.

Information security describes all measures taken to prevent unauthorized use of electronic data – whether this unauthorized use takes the form of disclosure, alteration, substitution, or destruction of the data concerned. Information Security is classified as the provision of the three different services such as; message confidentiality,

Prof. Rathnakar Acharya is with the Alliance Business Academy, 19th Cross, 7th Main BTM II stage, Bangalore, India – 560076. Phone-080-26681444, 9448871233

Dr. V. Vityanathan – HOD is with the Computer Science and Engineering Department SASTRA University, Tanjavur, T.N India – 613402. Phone-04362-264101, Fax:04362-264120

Dr. Pethur Raj Chellai – Senior Software Consultant, Wipro Technologies, Bangalore, India. Phone- 9916138511

Integrity, authentication, non-repudiation and availability.

With the arrival of mobile / wireless Internet, the security issue has become all the more important. There are many security issues that deal with securing wireless/ handheld devices, centralized server and gateway systems, and more importantly securing information being communicated via wireless channels in addition to persistent applications and data security. In this paper, we concentrate mainly on the challenges and solutions for providing total and unbreakable security for wireless information being transmitted.

In a traditional wired LAN, all communication is confined to a physical link between the workstations. If we protect the workstations and the physical link, we can prevent unauthorized access to our network. Where as in WLAN, the communication is not through a physical link it is through the wireless channel; hence it is vulnerable to all kinds of security threats. The WLAN requires a software based solution to manipulate the channel and device performance to provide better security for the user applications.

The rest of this paper is organized as follows; in section II we first mentioned the security challenges in WLAN, and explained the typical wireless security attacks with a particular focus on WEP based security solutions. Section III illustrates WEP vulnerabilities. Section IV introduces Wi Fi protected Access (WPA) methods. IN section V we presented the other effective WLAN security solutions. Section VI about the WLAN security components followed with the conclusion.

II. CHALLENGES IN WLAN

A. Seven wireless Networks security challenges – when a wireless network is established, designing a secured network is a concern. Here are the seven key WLAN security challenges are;

- 1) Easy access – Strictly speaking this is not a security threat, but information available about a wireless network is also the information needed to launch an attack on the network.
- 2) 2. Rogue Access Points (AP) – Rogue AP's deployed by end users pose great security risks.
- 3) 3. Unauthorized use of services – Most of the AP's running with default configurations have not activated with Wired Equivalent Privacy (WEP) [1]
- 4) 4. Services and performance constraints – WLAN have limited transmission capacity. If an attacker were to launch a ping flood from a fast Ethernet segment it could easily overwhelm the capacity of an AP.
- 5) 5. MAC Spoofing and Session hijacking – 802.11

networks do not authenticate frames. Like a traditional Ethernet, there is no protection against forgery of frame sources addresses. Attackers can use spoofed frames to redirect traffic and corrupt address resolution protocol (ARP) tables. At a much simple level attackers can observe the MAC addresses of station in use on the network and adopt those addresses for malicious transmission.

- 6) 6. Traffic analysis and eaves dropping – 802.11 [7] provide no protection against attacks that passively observe traffic. The main risk is that 802.11 do not provide a way to secure data in transit against eavesdropping [2].
- 7) 7. Higher level attacks – Once an attacker gains access to a wireless network it can serve as a launch point for attacks on other systems.

B. Typical Wireless Security Attacks

Here comes some of the possible wireless security attacks, yet there are still more attack types.

WEP Cracking – WEP, the primary security algorithm currently under use, is vulnerable because, the encryption keys remain static[1]. The encryption key used by WEP [1], regardless of its length, never changes unless it is periodically and manually changed by the administrator on all devices. An attacker uses a relatively inexpensive wireless packet sniffer to collect packets. After gathering five to 10 million packets, the attacker runs readily available tools that can determine encryption keys of the cipher message in a few minutes, enabling the attacker to decrypt and read all data passing between the user and access point.

MAC Attack – Media Access Control (MAC) addresses can be cracked in the same way as WEP [1] encryption keys. Once the encryption key is deciphered, all packets including the MAC ID is exposed. If no encryption is used, the MAC ID can be simply plucked from the air. Once a valid MAC address has been obtained, hackers can program their computer to spoof a valid user by programming a computer to broadcast the stolen ID.

Man-in-the-Middle Attacks – A hacker situated between the client and access point, intercepting all traffic, characterizes this type of attack. The hacker captures and decrypts the frames sent back and forth between a user's wireless NIC and AP during the association process. This provides essential information about the Wireless NIC and AP such as the IP addresses for both devices, the Wireless NICs association ID, and the network's SSID. With this information, someone can set up a rogue access point on a different wireless channel closer to a particular user, to force the user's wireless NIC to re-associate with the bogus access point. Both client and server believe they are connected directly each other, but instead are connected to a man in the middle. The attacker has access to all data passed between the two entities including login information.

Dictionary Attacks - This type of attack relies on conventional names and words being used as login names and passwords. The attacker gathers a challenge and response exchange from password-based protocols. Using open source tools based on a dictionary of hundreds of

thousands of words, names and phrases, an offline computer tries essentially every name-password combination, and until the login information is decrypted. Once a name and password have been cracked, the attacker has access to the WLAN with all the rights and privileges of that user.

Session Hijacking – When an attacker is capable of not only listening to network traffic but also inserting their own information, a session is then susceptible to hijacking – redirecting it away from a legitimate end point. A hacker can set up an access point, and unsuspecting wireless LAN clients will try to connect to it by sending their authentication information.

Denial of Service (DOS) - DoS attacks are easily applied to wireless networks. An attacker can flood access points with illegitimate traffic, overwhelming that available bandwidth, slowing or stopping legitimate users from accessing the network.

C. WLAN Security - Processes.

Access Control is the process of ensuring that only trusted users can gain access to network resources and they can see only what they are authorized to see. It comprises two elements: authentication and authorization.

Authentication is the process the user confirms his/her identity to the system and **authorization** involves control over what the user can do on the system once he or she has been authenticated. Authentication systems range from simple name-password pairs, to more elaborate challenge-response systems, such as smart cards and biometrics.

Role based Access control (RBAC) method is one such mechanism, where the access rights to the data and resources are granted based on job responsibilities. RBAC roles are created according to the job functions performed in an organization, permissions are granted to those roles and finally users are assigned to the roles in accordance with their specific job responsibilities and qualifications.

The **confidentiality** or privacy of communications is fundamental to a secure system and the usual way to ensure confidentiality is to employ encryption. WEP [6] algorithm has been the main stay for this encryption.

Integrity is the assurance that data has not been altered by anybody unauthorized to alter it. There are three ways in which access control is provided.

Service Set Identifier (SSID) - Network access control can be implemented using an SSID associated with an AP or group of access points. The SSID provides a mechanism to segment a wireless network into multiple networks serviced by one or more access points. Each AP is programmed with an SSID corresponding to a specific wireless network. To access this network, client computers must be configured with the correct SSID to access the AP, the SSID acts as a simple password and thus provides a measure of security.

MAC Address Filtering - The second method is to use the unique Medium Access Control (MAC) identifier that is part of every Ethernet device. While an AP or group of access points can be identified by an SSID, a client computer can be identified by the unique MAC address of its 802.11 [2] network card. To increase the security of an 802.11 network, each AP can be programmed with a list of MAC addresses associated with the client computers to

access it. If a client's MAC address is not included in the list, the client is not allowed to associate with the AP. This procedure is very effective for smaller operations where the MAC address list can be efficiently managed. Each AP must be manually programmed with a list of MAC addresses and the list must be kept up-to-date.

WEP-based Security - The third way is to use WEP security protocol to provide encrypted communication between the client and an AP. WEP employs the symmetric key encryption algorithm, Ron's Code Pseudo Random Number Generator (RC4 PRNG). The shared secret is typically a 40-bit key or a 104-bit key shared between many stations. A key shared between the AP and its many stations is called a default key. A key shared between the AP and only one other station is called a key-mapping key. Both default keys and key-mapping keys are subsequently used to protect communications between associated stations.

The WEP protocol is primarily used to protect (MAC Protocol Data Units) MPDUs. It uses the default key or key-mapping key and the RC4[5] algorithm for encryption, and it uses CRC-32 to compute an Integrity Check Value (ICV) over the MPDU data. The resulting 32-bit ICV is appended to the MPDU prior to encryption. The RC4 [4] key is composed of a 24-bit Initialization Vector (IV) value concatenated with the default key or key-mapping key to form a per-packet key. The MPDU data and ICV are then encrypted under the per-packet key. The IV and a key identifier are pretended to the encrypted MPDU data field, forming the complete WEP protocol data unit. The receiver, which knows the shared key, is able to reproduce the key stream and to decrypt the message. If the ICV matches, the message is assumed to be authentic.

The WEP [6] has been designed to ensure the following security properties:

- 1) **Confidentiality:** only stations that possess a key, usually shared by all stations participating in a wireless LAN, can read messages protected with WEP.
- 2) **Data origin authentication / data integrity:** malicious modifications of WEP protected messages can be detected by checking an integrity code
- 3) **Access control in conjunction with layer management:** if set so in the layer management, only WEP protected messages will be accepted by receivers, so that stations which do not know the key cannot send to such receivers usually all the base stations.

III. WEP VULNERABILITIES

As discussed above, WEP [1] have two generic limitations;

First, use of WEP is optional and as a result, many real installations never turn on encryption.

Second, by default, WEP [1] uses a single shared key common to all users of a WLAN and this common key is often stored in software-accessible storage on each device. If any device is lost, stolen, or compromised, the only recourse is to change the shared secret in all of the remaining devices. Since WEP does not include a key management protocol, distributing the new secret to all users is a boring and tedious process.

The most serious problem with WEP is its encryption keys that can be recovered through cryptanalysis. WEP uses a common stream cipher, RC4 [3] in a non-standard way. WEP concatenates a base key with a 24-bit per packet, called the WEP Initialization vector (IV) and uses the result as a per packet RC4 key.

An eavesdropper who can obtain several million encrypted packets whose first byte of plaintext is known can deduce the base RC4 key by exploiting properties of the RC4 key schedule. Also as this attack is purely passive and can be done using off-the-shelf hardware and software, the detection is nearly impossible. With efficient equipment, it is possible to eavesdrop on WEP-[3] protected networks from distances of a mile or more from the target.

Also the small IV size creates a serious risk of key stream reuse, a condition that allows an eavesdropper to recover plaintext traffic. In addition, an attacker without fear of detection can modify encrypted messages freely. Thus it is possible to decrypt any chosen packet in a few hours time.

The security risks are categorized as follows:

- 1) The attacker can decrypt intercepted packets and read encrypted traffic
- 2) The attacker can forge new encrypted packets that will be accepted by the access point and join the wireless network or attack other hosts, defeating the WEP integrity and authentication goals.

The problems with the design of WEP are as follows:

- 1) 24-bit IVs are too short and this put confidentiality at risk
- 2) The CRC checksum, called the Integrity Check Value (ICV), used by WEP for integrity protection, is insecure, and does not prevent adversarial modification of intercepted packets
- 3) WEP combines the IV with the key in a way that enables cryptanalytic attacks. As a result, passive eavesdroppers can learn the key after observing a few million encrypted packets
- 4) Integrity protection for source and destination addresses is not provided.

Under WEP, all clients and access points on a wireless network typically use the same key to encrypt and decrypt data. The key resides in the client computer and in each AP on the network. The 802.11 standard [2] does not specify a key management protocol, so all WEP keys on a network usually must be managed manually unless they are used in conjunction with a separate key management protocol. As the same key is used for all devices, and if any device is compromised, then the encryption key must be changed on all of the devices.

WEP does not support key management, which is the automatic exchange of encryption keys between client and access points. To maintain effective security, WEP requires the keys to be changed manually. Stronger security mechanisms such as IPSec and VPN support automatic key management. Thus packets encryption with WEP technique is susceptible to cracking. Because of this, static WEP is only suitable for small, tightly managed networks with low-to-medium security requirements. In these cases, 128-bit WEP should be implemented in conjunction with MAC address filtering and SSID with the broadcast feature disabled.

A. How WEP gets broken?

This can be done by encryption of data with the RC4 encryption algorithm. WEP employs an integrity check field in each data packet to ensure that data is not modified during transmission. A CRC-32 checksum is used for this purpose.

A stream of cipher expands a fixed length key into an infinite pseudo random key stream for the key stream of the purpose of encryption data. In WEP, plain text data is exclusive OR'ed (XOR) with the key stream to produce the cipher text as in fig.1. XOR is a Boolean operator that compares two numbers and determines if they are the same or different. If the numbers are same a value of "0" is returned; if they are different value of "1" is returned.

WEP requires that each wireless network connection share a secret key for encryption purposes. WEP does not define key management techniques such as the number of different keys used within a network or the frequency to change keys. The key stream produced by the WEP algorithm depends upon both the secret key and an initialization vector (IV). The IV is used to ensure that subsequent data packets are encrypted with different key streams, despite using the same secret key.

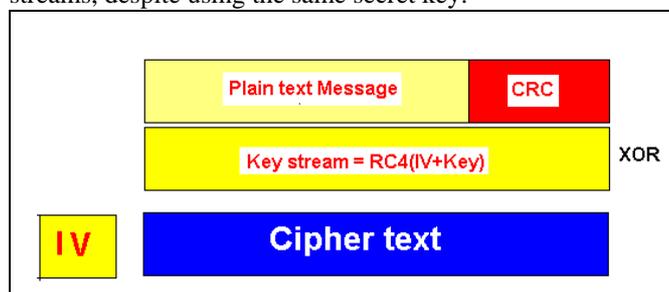


Fig.1. WEP steps using RC4 algorithm

A 24 bit field contains $2^{24} = 16,777,216$ possible values. For a network running at 11 Mbps and transmitting 1,500 bytes packets an IV would be repeated about 5 hours. This time can be reduced under various circumstances. Devices using random IVs also reduce the time required for an IV collusion to occur. Once IV collusion occurs and an attacker has two different cipher plain text messages encrypted with the same key stream, it is possible to obtain the XOR of the two plain text messages by XORing the two cipher text messages.

Example:

Plain text 'a' - 0110 0001
Key 'c' - 0110 0011

XOR - 'a' 0000 0010

Plain text 'b' - 0110 0010
Key 'c' - 0110 0011

XOR - 'b' - 0000 0001

XOR - 'a' 0000 0010
XOR - 'b' 0000 0001

XOR- 'a' & 'b'- 0000 0011(1)
plain text 'a' 0110 0001

plain text 'b' 0110 0010

XOR - 'a' & 'b' 0000 0011(2)

Where (1) == (2)

When using the same secret key, the XORed value of the plain text messages is equivalent to the XORed value of the encrypted messages. Thus if an attacker could then decipher the contents of the plain text messages without any knowledge of the key stream used for the encryption as in fig. 2.

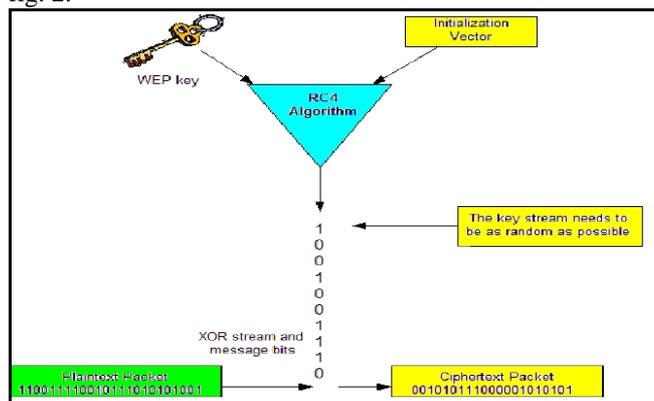


Fig. 2. XOR operations using RC4 algorithm

B. Cyclic Redundancy Check (CRC)

Cyclic redundancy check enhances the integrity of transmissions by calculating a checksum that is included with each data packet. The recipient calculates the same checksum for each data packet. If the checksum are equivalent, WEP provides assurance that the data has not been changed during transmission. In CRC the transmitted message are divided into predetermined lengths and are divided by a fixed divisor. The remainder is one bit smaller than the divisor and serves as the checksum. In the case of the CRC-32, the remainder is a 32-bit number and this checksum is then appended onto the message sent. CRC-32 is not appropriate integrity check for the WEP as it is a linear checksum. Therefore, modifications could be made to cipher text and the original message and modified checksums could be calculated. An attacker may adjust the checksum appropriately, and a recipient would not be aware of the data has been altered.

Attacks - Once the XOR of two plain text messages is obtained, at least partial knowledge of one of the plain text message can be used to decrypt the other plain text message. Determining one of the plain text message is for the attacker to implement a known plain text attack by creating messages and injection them into the network.

802.1X - The protocols, algorithms, and techniques involved with improving the current 802.11 standard's security are complex and very interdependent. The 802.1X standard is a port based network access control that provides a framework for user authentication and dynamic encryption key distribution.

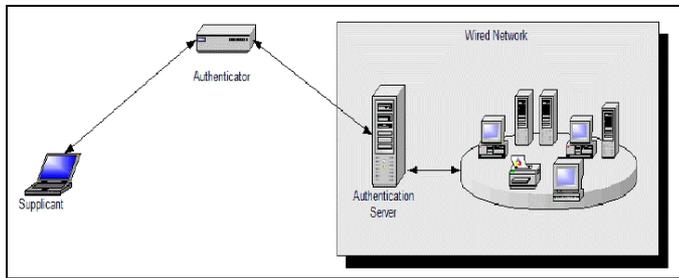


Fig.3. Authentication process

There are three entities that are involved with this approach to authentication as in fig.3;

- 1) The supplicant - software resides on the wireless device
- 2) Authenticator – is the access point (AP)
- 3) The authenticator server – is most likely the RADIUS server

The first goal of 802.1X is to require a successful authentication of a user before a full network connection can be established. When the wireless device initiates connection with the AP, the AP creates a logical port that works in an unauthorized state until the user has been properly authenticated. The unauthorized state means that no traffic, other than authentication frames is allowed to pass. An analogy is having a chain on the front door, which will allow identifying a person who knocks before, allow him to enter into the house. The AP acts basically as a middleman between the wireless device and the authentication server; it just passes the information between the two entities. The AP will only allow the wireless device to communicate with the authentication server until the entire authentication steps are completed successfully. After this the wireless device can then participate with the full network and its resources.

IV. WI-FI PROTECTED ACCESS (WPA)

WPA addresses the security vulnerabilities found in WEP-enabled 802.11 [4] WLANs. For example, WPA-compliant products will include dynamic key generation, as well as an improved RC4 data encryption scheme that uses Temporal Key Integrity Protocol (TKIP) and mandatory 802.1x authentication.

WPA is a software upgrade recommended by the IEEE 802.11i standard body to existing WEP-based Wi-Fi [4] certified hardware while maintaining forward compatibility with the future 802.11i standard. WPA provides WLAN users with data protection while helping to ensure that only authorized users gain access to the network. WPA has addressed all the WEP vulnerabilities and can provide effective protection against both non-targeted and targeted attacks. Implementation of WPA will make it possible for enterprises to protect their campus wireless LANs with scalability without deploying VPN/firewall technology. WPA combines the functionality of 802.1X with TKIP that addresses the vulnerabilities of the static keys used in WEP. A TKIP implement rapid re-keying by generating a new encryption key every 10000 packets and uses a mixing function to cryptographically hash the initialization vectors of data packets with the shared key. TKIP is based on the same RC4 algorithm with 40-bit key used in WEP. The combination of 802.1X authentication, authentication

protocols, dynamic keys and TKIP enhancements is a transitional step that enables enterprises to implement WLANs increased data privacy and integrity protection.

The TKIP process begins with a 128-bit temporal key shared among clients and access points. TKIP combines the temporal key with a 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 data. TKIP provides an automated key mechanism, changing the temporal keys every 10, 000 packets. This offers a dynamic distribution method that significantly enhances the security of the network. TKIP employs a message integrity check (MIC), which adds stronger integrity checking than a simple CRC check to prevent attackers from changing messages after transmission.

Temporal Key Integrity Protocol (TKIP): Having come across the deficiencies found in WEP, the IEEE 802.11TG_i has come out with this short-term solution. TKIP installation will include a firmware upgrade and a driver upgrade. The requirements are defined as;

- 1) Deployed systems are to be software or firmware upgradeable
- 2) The current WEP hardware implementation to remain unchanged and
- 3) Minimize performance degradation imposed by the fixes.
- 4) TKIP is a set of algorithms that adapt the WEP protocol to address the known flaws while meeting these constraints. TKIP wraps WEP in three new elements
- 5) A message integrity code (MIC), called Michael, to defeat forgeries
- 6) A packet sequencing discipline, to defeat replay attacks
- 7) A per-packet key mixing function to prevent FMS (Fluher, Mantin and Shamir) attacks

TKIP mandates fresh keys – never-before-used, unrelated cryptographic keys – to address key reuse. The IEEE 802.1X key management scheme provides fresh keys.

Michael. – A MIC algorithm calculates a keyed function of data at the transmitter, sends the resulting value as a tag with the data to the receiver, where it re-computes the value and compares the compound result with the tag accompanying the data. If the two tags match, the receiver accepts the data as authentic; if not, the receiver rejects the data as a forgery

Michael uses a 64-bit key, and partitions packets into 32-bit blocks. Michael then uses shifts, XORs, and additions to process each 32-bit block into two 32-bit registers that will represent the final output, a 64-bit authentication tag. Michael limits the instruction set to minimize performance impact. The security level of a MIC is measured in bits. If the security level of a MIC is 's' bits, theoretically an attacker can on average construct a forgery in about 2^s+1 packet. To meet its performance goals, Michael was designed to provide only about 20 bits of security. TKIP requires a rekey after detecting a MIC validation error and limits rekeying to once per minute. With this design, the maximum expected number of false positives is about one per year.

Per-packet Key Mixing – Concatenating the base key to the 24-bit WEP IV enables an attacker to recover the WEP encryption key via FMS attacks. To defend against them, TKIP introduces a new per-packet encryption key construction, based on a mixing function. The mixing function takes the base key, transmitter MAC address, and packet sequence number as inputs, and outputs a new per-packet WEP key. To minimize computational requirements, the mixing function is split into two phases.

The first phase uses a nonlinear substitution table, or S-box, to combine the base key, the transmitter MAC address, and the four most significant octets of the packet sequence number to produce an intermediate value. The intermediate value can be cached and used for up to 216 packets. Since it includes the transmitter address, the mixing function produces a different value on each host, even when the same base key is used across hosts.

The second phase mixes the intermediate value with the two least significant octets of the packet sequence number, and produces a per-packet key. It uses a small cipher to diffuse the intermediate value and sequence number octets evenly throughout the per-packet key. The second phase de-correlates the packet sequence number from the per packet key thwarting FMS attacks; it costs about 150 cycles per packet.

TKIP keys – TKIP requires two distinct keys; a 128-bit key, used by the mixing function to produce a per-packet encryption key and a 64-bit key, employed by Michael. TGI has recommended IEEE 802.1X to provide both authentication and key management. IEEE 802.1X does authentication after association then derives a fresh master key and finally distributes this key for subsequent use. The station and access point use the distributed master key to derive the pair of keys needed by TKIP.

Thus TKIP works as a front end to WEP and it applies the per-packet key mixing function and WEP encryption to packet fragments, but the Michael MIC function applies to whole packets. The interrelationships of the TKIP components are to enhance its security. TKIP uses RC4 to encrypt the MIC as in fig.4, which decreases the information about the MIC key visible to an attacker. An attack that changes the packet sequence number also changes the per-packet encryption key, making it likely that both WEP ICV and TKIP MIC will decrypt incorrectly. Michael and its countermeasures make attacks that alter encrypted data computationally infeasible. Since the MPDU is protected from random bit-errors by both the IEEE 802.11 Frame Check Sequence (FCS) and by the WEP ICV, a valid FCS and ICV but invalid MIC implies the packet is most likely a forgery. Since the MIC protects the source and destination addresses from change, packets can no longer be redirected to unauthorized destinations or the source spoofed.

Counter-Mode-CBC-MAC Protocol (CCMP) - The Advanced Encryption System (AES) is the main encryption algorithm to be used in this CCMP solution by IEEE 802.11i. The main features are;

- 1) Use a single key to provide confidentiality and integrity to reduce key management overhead and minimize the time spent computing AES key schedules.
- 2) Provide integrity protection for the plaintext packet

header, as well as integrity and confidentiality of the packet payload.

- 3) Allow pre-computation to reduce latency. Since packets can be lost, the receiver may perform pre-computation for a packet that never arrives. However, the sender's efforts are rarely discarded
- 4) Support pipelining to increase throughput.
- 5) Small implementation size, to keep costs reasonable
- 6) Small overhead for each packet
- 7) Avoid modes that are encumbered by patents.

CCM was designed to meet all these criteria. CCM uses counter mode for encryption and the Cipher Block Chaining Message Authentication Code (CBC-MAC) for integrity protection. These algorithms employ only the encryption primitive at both the sender and the receiver. CCM uses the same key for both confidentiality and integrity. This pitfall is being removed by CCM by guaranteeing that the space for the counter mode never overlaps with that used by the CBC-MAC initialization vector. That is, if an advanced encryption algorithm behaves like a pseudo-random permutation, then the output of the cipher operating on each of these two spaces will be independent.

Like TKIP, CCMP employs a 48-bit IV, ensuring the lifetime of the AES key is longer than any possible association. Thus, key management can be confined to the beginning of an association and ignored for its lifetime. CCMP uses a 48-bit IV as a sequence number to provide replay detection.

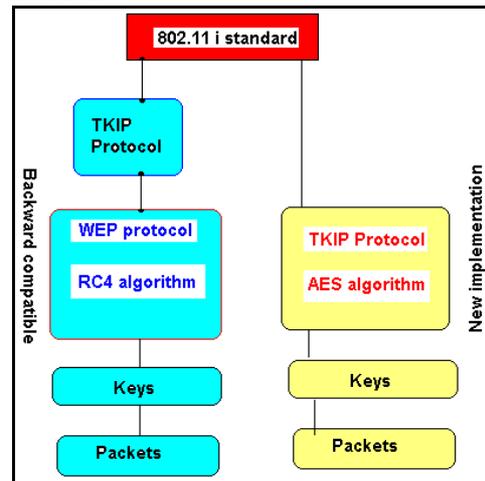


Fig. 4. TKIP protocol with WEP protocol

AES in CCMP removes the need for per-packet keys and hence there is no per-packet key derivation function. CCMP uses the same AES key and associated AES key schedule to provide confidentiality and integrity protection for the entire packets in an association. The CCM MIC length is adjustable between two octets and sixteen octets. CCMP uses an 8-octet MIC, which is stronger than Michael. But unlike TKIP and WEP, the encrypted ICV is no longer required. TKIP provides integrity protection over the whole MSDU and confidentiality over MSDU, leading to implementation complexity. Since CCM provides both services, it is obvious that it provides confidentiality and integrity protection over the same data structure though CCMP has to provide the protection for the entire packet header to defend against fragmentation sort of attacks.

V. OTHER EFFECTIVE WIRELESS LAN SECURITY SOLUTIONS

A. Virtual Private Network (VPN) over WEP-enabled WLAN

A VPN enables users on a public or un-trusted network such as the Internet or a WEP-based Wireless LAN to establish a secure connection to a private network. The VPN protects the wireless LAN by creating a tunnel that shields data from unauthorized access. VPNs enable a high level of trust through the use of proven industry-standard security mechanisms, including IPsec that employs strong algorithms such as Triple data encryption standard to encrypt data with other algorithms for authentication of data packets. IPsec also uses digital certificates to validate public keys. When used over a wireless LAN, the VPN gateway handles authentication, encapsulation and encryption. The combination of an IPsec-based VPN and 802.11 with WEP provides a practical and scalable solution for the protection of mission-critical data transmitted over a wireless LAN.

B. Key Distribution Method

In order to overcome the current practice of manually setting the group key in every station of a wireless LAN, here comes a simple key management scheme.

- 1) Every user U_1, U_2, \dots, U_n to participate in a WLAN is assigned an individual key K_{U_i} to be used for distributing the group keys to them. These individual keys are stored in a central key management server (KMS) that has to be secured appropriately. As individual key of a user also needs to be available at the terminal of the user (for example, a laptop or any other mobile devices), it either has to be stored on the terminal, or to be computed on the fly.
- 2) The central KMS regularly generates a new group key K_{group} and distributed it to i) all mobile stations by using specific broadcast messages, which are sent without encrypting them in the MAC layer, ii) all access points by setting the appropriate MIB-variable via the simple network management protocol (SNMP) and
- 3) The broadcasted key distribution frames contain a name identifying the key management domain (e.g. the name of the key management server), the sequence number p of the group key $K_{group:p}$ currently in use, the sequence number q of the group key $K_{group:q}$ distributed in this key frame (these two numbers are used for fast setup and detection of a new group key), two numbers r and s defining the range of user-ids for which the group key is distributed in this key management frame, an integrity check value over the common part of the key management frame which is generated using the group key $K_{group:q}$ and for every user i in the range $[r, s]$, a tuple $(I, E(K_{U_i}, K_{group:q}))$.

When a user switches on his mobile phone, the key management process (KMP) is started. After receiving the first key distribution frame, KMP asks the user to type in his passphrase for the key management domain with the name specified in the receive frame. Using the passphrase the KMP computes the user's key K_{U_i} for this key management

domain either by decrypting the appropriate entry in the key-file, or by directly mapping the passphrase to the key, e.g. computing a cryptographic hash value of the passphrase.

From local configuration information the KMP reads the identity i of the user in this key management domain, looks for the appropriate entry in the key distribution frame, and then decrypts the group key. After obtaining the group key $K_{group:q}$, KMP computes the integrity check value and compares it to the value included in the key management frame. If both values match, the key management frame is assumed to be authentic. For computation of the integrity check value the authors have proposed to use the cryptographic hash function SHA-1 in the HMAC construction.

C. Firewall

has the ability to restrict network traffic through a gateway according to a set of rules. Typically located at a gateway or access point, it controls the flow of traffic, preventing inside and outside users from accessing data and services as defined by the system administrator. Superior firewalls employ stateful packet inspection, rather than just packet filtering technology. WLANs can be isolated from the wired network with a firewall.

VI. WLAN SECURITY COMPONENTS

IEEE 802.1X provides network login capabilities between PCs and the edge-networking infrastructure. It offers an architectural framework for implementing various authenticating schemes. 802.1X does not provide encryption as WEP, 3DES, AES or any other cipher. 802.1X focus on authentication and key management and it can be used in conjunction with a cipher. 802.1X is not a single authentication method and it utilizes EAP as its authentication framework and hence any 802.1X-enabled switches and access points can support a wide variety of authentication methods. It supports open standards for authentication, authorization, and accounting including RADIUS and LDAP, so it works with existing infrastructure for managing remote and mobile users. Using an authentication protocol such as EAP-TLS, LEAP, or EAP-TTLS, 802.1X provides port-based access control and mutual authentication between clients and access points via an authentication server.

RADIUS (Remote Authentication Dial-in User Service): For authentication to work, the user's transmission must go through a wireless LAN access point to reach the back-end server performing the authentication. The wireless client contacts the access point, which in turn communicates with the RADIUS server on the enterprise LAN. The RADIUS server then verifies the client's credentials to determine whether the device is authorized to connect to the LAN. If the RADIUS server accepts the client device, the server sends data, including security keys, to the access point to enable a secure connection with the client.

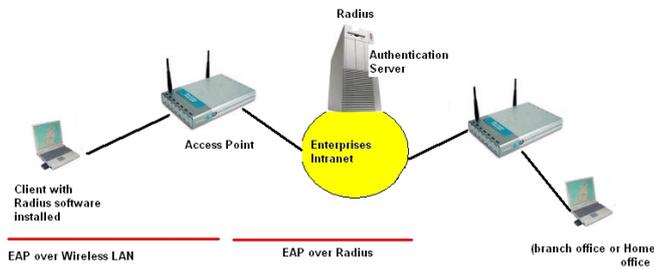


Fig. 5. EAP link to WLAN through AP

EAP (Extensible Authentication Protocol) is a framework for providing centralized authentication and dynamic key distribution. The wireless access point and the RADIUS server communicate using EAP, a point-to-point protocol that supports multiple authentication methods such as token cards, Kerberos, one-time passwords, certificates, public key authentication, and smart cards. When used with 802.1x, it provides an end-to-end authentication – a wireless client that associates with an AP cannot gain access to the network until the user performs a network login. In wireless communications using EAP, a user requests connection to a WLAN through an AP, which then requests the identity of the user and transmits that identity to an authentication server, such as RADIUS as in fig.5. The server asks the AP for proof of identity; the AP obtains it from the user and then sends back to the server to complete the authentication.

EAP performs mutual authentication, where each side is required to prove its identity to the other using its certificate and private key. When both client and server authenticate each other, the result is stronger security.

VII. CONCLUSION

In the current generation of tether-less networks that transmit data over unlicensed radio frequencies has already demonstrated its effectiveness in a host of vertical markets, including health care, retail, manufacturing, logistics, warehousing and academia. Now as it find ways into more general business settings and, increasingly, into publicly accessible implementations, WLAN is definitely poised for a boom. Wireless technology changes the network paradigm of the wired user going to where the data is, to the data going to the user. As such, wireless can support a variety of business critical applications that cannot be effectively met with conventional, wired connections. For day-to-day applications, wireless can provide convenient network access to improve worker productivity. Network designs will, of course, continue to be affected by the development of new technologies and user demands.

The next wave of wireless LANs is likely to be driven by mobility. 802.11 provide link-layer mobility. Users can move transparently within an IP subnet with no effect on their applications or connection. The mobile user can call the data up anywhere at any time. Due to the vulnerability of the wireless channel users may not feel comfortable of using or accessing their and applications and files by wireless Internet.

Network security is gaining attention as more number of enterprises are switching to WLANs having felt the need for stronger, faster, and efficient authentication, authorization, Integration and non- repudiation processes to keep the

corporate information from excessively or impertinently inquisitive people. An effective and efficient security solution may enhance the utilization of pervasive and ubiquitous computing systems for information on demand and all kinds of applications.

REFERENCES

- [1] David; Security of the WEP algorithm; March 4, 2005; <http://www.isaac.cs.berkeley.edu/isaac/wepfaq.Html>
- [2] BORISOV, N., GOLDBERG, I., AND WAGNER, D. Intercepting mobile communications: The insecurity of 802.11, MOBICOM 2001, 2001.
- [3] Fluhrer S., Mantin I., Shamir I., Weaknesses in the key scheduling algorithm of RC4, SAC.2001, 2001.
- [4] Geier, Jim; 802.11 WEP: Concepts and Vulnerability; March 4, 2005; <http://www.wifiplanet.com/tutorials/article.php/1368661>
- [5] Mister and Tavares. Cryptanalysis of RC4-like ciphers. In SAC: Annual International Workshop on Selected Areas in Cryptography. LNCS, 1998. nussen, Meier, Preneel, Rijmen, and Verdoolaege. Analysis methods for (alleged) RC4. In ASIACRYPT: Advances in Cryptology { ASIACRYPT: International Conference on the Theory and Application of Cryptology. LNCS, Springer-Verlag, 1998.
- [6] Prasithsangaree P., Krishnamurthi P., Analysis of Energy Consumption of RC4 and AES Algorithms in Wireless LANs, Global Telecommns. Conf., Globecom.03, Dec. 2003.
- [7] RIVEST, R., RSA Security response to weaknesses in key scheduling algorithm of RC4, <http://www.rsasecurity.com/rsalabs/technotes/wep.html>, 2001.
- [8] IEEE Std 802.11-1997. Wireless LAN Medium Access Control (MAC) And Physical Layer (PHY) Specifications, 18 Nov. 1997.



Dr. V. Vaithiyathan, is a Professor and HOD of the Department of Computer Science and Engineering at SASTRA University Tanjavur India.

Prof. Rathnakar Acharya Graduate in Electrical an Electronic Engg. from Mysore University and Post Graduate in Technology and Management. Having 19 years, of experience in teaching/ research. Presently perusing research (PhD) in QoS issues in WLAN.



Dr. Pethur Raj Chelliah, PhD from Anna University, India, worked as a research associate at the Dept. of Computer Science and Automation at IISc. Bangalore and then Postdoctoral research at Japan (Nagaya Institute of Technology Kyoto University and University of Tsukuba) currently working as senior consultant (SOA Evangelist) at Wipro Technologies Bangalore