GNITED MINDS
Journals

*International Journal of Information Technology and Management*

*Vol. IX, Issue No. XIV, November-2015, ISSN 2249-4510*

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

# SECURITY MECHANISMS FOR WIRELESS LOCAL AREA NETWORKS

www.ignited.in

International Journal of Information Technology and Management
Vol. IX, Issue No. XIV, November-2015, ISSN 2249-4510

# Security Mechanisms for Wireless Local Area Networks

**Davinder Pal Singh[1] Dr. Vijay Pal[2]**

[1]Research Scholar, Dept. of Computer Science, OPJS University, Churu, Rajasthan

[2]Associate Professor, Dept. of Computer Science, OPJS University, Churu, Rajasthan

***Abstract - Wireless Virus detection is a challenging research area that is considerably different to and much less understood than, Virus detection in wired networks. The first challenge facing wireless Virus detection systems (WVDSs) is the broadcast nature of the physical (PHY) layer, which makes passive access to the medium a trivial undertaking. Secondly, the limited bandwidth available to wireless physical layer imposes significant efficiency restrictions on Virus detection techniques. Finally, a wireless network typically consists of mobile client stations like laptops and handheld computers which have limited battery life and computing resources, introducing further constraints on the techniques that may be adopted by a WVDS.***

***Keywords - WVDS, PHY, VDS***

- - - - - - - - - - - - - - X - - - - - - - - - - - - - -

## INTRODUCTION

The problem of Virus detection has been studied for several years with early papers on the subject appearing in the late 1970s and early 1980s. While the definition of a Virus varies slightly from paper to paper, definitions such as the following are widely accepted: “any set of actions that attempt to compromise the integrity, confidentiality or availability of a resource”. A Virus detection system then is a system which attempts to detect and in some cases react to Viruses, whether on one system, group of systems, or computer network.

### Wireless Security Initiatives

The wireless LAN (WLAN) industry is the fastest growing networking market, only overcome by limitations to secure it. There has been a widespread adoption of wireless networks in the SOHO user market. Wireless local area networks technology is recognized, accepted and adopted by many organizations worldwide. Many companies and government entities are realizing the competitive advantage of deploying wireless technology in the workplace. Wireless technologies are continually evolving and providing advancements in speed, bandwidth, and security. However, large enterprises have been reluctant to deploy wireless networks due to perceived limitations in wireless security and the risks it poses to the organization. Simply, WLAN’s are a disruptive technology that has many challenges with securing its networks.

### Security Features of Wireless LAN

A message traveling by air can be intercepted without physical access to the wiring of an organization. Any person sitting in the vicinity of a WLAN with a transceiver with a capability to listen/talk can pose a threat.

To make the WLANs reliable the following security goals were considered:

- Confidentiality
- Data Integrity
- Access Control

The following security measures are a part of the 802.11 IEEE protocol:

- Authentication
- Association

Data Confidentiality and Integrity
Authentication and Access Control
Intrusion Detection and Prevention

## Data Confidentiality and Integrity

The protection of data as it moves across the shared medium is the most familiar aspect of WLAN security. Confidentiality is delivered through the use of encryption algorithms used to encode information in a manner that can only be decoded and read by the parties for which it is intended. Going hand-in- hand with encryption are the concepts of data integrity and non-repudiation, which help to prevent hackers from altering data. Non-repudiation is achieved through the use of a hashing algorithm which takes a snapshot of each frame's content before it is encrypted.

Even if a frame were to be decrypted, it would not be possible for a hacker to alter data contained within and fraudulently resend the data, a process known as spoofing. Strong data confidentiality and integrity are especially critical for wireless traffic, as frames can be more easily intercepted and potentially compromised by virtually anyone in vicinity of the network.

## Authentication and Access Control

The mechanisms used to grant authorized users access to the wireless network and the resources residing on the broader enterprise network are just as important as encryption and integrity. Sophisticated implementations also allow for the definition of access control policies that grant different users or groups unique security settings and access to different network resources.

Robust authentication and access control measures are especially vital to WLANs because there is little available in the way of physical separation of unauthorized users from the network. A user can potentially have a laptop outside of the office premises, and without an authentication mechanism to keep them out, they could gain full access to the corporate network.

- **Service Set Identifier (SSID)**

This is the most basic security authentication mechanism for 802.11 networks. The SSID can be used as a shared secret; however, as a security mechanism it is virtually worthless. In reality, the SSID is transmitted unencrypted. An attacker can use passive eavesdropping to discover the SSID, or if she is impatient, she can use an active attack. To actively attack a WLAN using SSID as a shared secret the attacker sends a forged disassociates message to the target and then eavesdrops as the target automatically begins to re-associate with an authentication transaction. This security mechanism is only effective against the most unskilled attacker AP send beacon messages to announce their presence and operating parameters to clients. By turning off the broadcast of this SSID, clients would not be able to automatically identify and associate with the AP, but would instead require pre-knowledge of the SSID. Unfortunately, this mechanism fails as a security feature because although the SSID is no longer broadcast on the beacon, it is still sent out in other network management traffic, which can be sniffed by an attacker.

- **MAC Address Access Control List (ACL)**

Some vendors implement a MAC Address (i.e., Ethernet address) filter or ACL to prevent unauthorized access to an AP. MAC addresses of authorized clients are entered and stored in a list internal to the AP, and only clients with MAC addresses matching this list are allowed access to the AP (alternately, certain MAC addresses may be blocked instead).

This is similarly ineffective as a security measure because all traffic sent over the network contains the MAC address in the unencrypted header. Therefore, by capturing just a single packet and examining its header, an attacker can determine a legitimate MAC address and program his device with this address.

Further, the process of manually maintaining a list of all permitted MAC addresses is time consuming and error-prone making it only practical for small and fairly Static network

## Authentication Mechanisms

802.11 specify two authentication mechanisms:

1. Open system authentication

2. Shared key authentication

### 1. Open system authentication

The open system provides identification only and is essentially a "null" authentication. A client requesting access to an AP simply sends its MAC address to the AP, and the AP replies with an authentication verification message: any client who requests authentication with this algorithm will be authenticated. This mode of authentication is implemented where ease-of-use is the primary concern or when security is not an issue for a network administrator. It is important to note that open system authentication is the default setting in many 802.11 WLAN devices.

The 802.11 standard allows for use of WEP encryption even with open system authentication. In this case, both devices must share a WEP key, but unlike the “shared key authentication” described in the next section, the key is not used for authentication, only for encryption. In this mode, a client is authenticated using open system authentication and then both ends immediately begin WEP-encrypted communications. This mode is actually considered somewhat more secure than shared key authentication because key-related information is not exchanged over the air.

Authentication Request
WS
AP

**2. Shared system authentication**

Shared key authentication is a feature of the original 802.11 standard and can only be used if the legacy wireless security features of the device are enabled. It does not apply when WPA or WPA2/802.11i is in use, where a similar but somewhat stronger “pre-shared key” scheme is available.

In this mode, the secret shared key is manually distributed and configured on all participating stations. The shared key authentication process follows a challenge-response scheme where the encryption/decryption is performed using WEP’s RC4 pseudo-random number generator (PRNG) to validate the challenge-response. After a “success” message is received, the link is considered authenticated.

The shared key authentication method was intended to provide a greater degree of security compared to the open system authentication; however, weaknesses in the WEP encryption used in the challenge-response scheme can allow the key to be easily recovered if this exchange is intercepted by an attacker. As well, it must be noted again, that this authentication only confirms the identity of the hardware not that of the user.

802.11 do not specify any key management processes or a mechanism, therefore ensuring the security of shared keys is the responsibility of the user. As with any passphrase-based system, strong passphrases should be chosen to minimize the possibility of password guessing, and should be changed regularly.

**802.1X Authentication**

Both the WPA and the WPA2/IEEE 802.11i amendment specify the mandatory use of another standard, IEEE 802.1X, for network authentication. 802.1X is an ethernet standard (IEEE 802.1 family; it is not wireless LAN specific) that provides a framework for authentication, on top of which various methods (such as passwords, smart cards, certificates, etc) can be used to verify identity. 802.1X works at the MAC layer to restrict network access to authorized entities.

On a typical network, there may be many ports available through which a supplicant may authenticate for service. The authentication server is the entity that verifies the identity of the supplicant that was submitted to the authenticator, and directs the authenticator to allow access if the verification was successful.

**Data Confidentiality and WEP/WPA/802.11i/WPA2**

The IEEE 802.11 core standard specifies an optional data confidentiality mechanism using the WEP protocol. It is intended to provide protection for a WLAN from casual unauthorized eavesdropping and to ensure data integrity. Since its release, the WEP protocol has been proven to exhibit many weaknesses, resulting in the development of stronger security and data confidentiality measures. As documented earlier, IEEE 802.11 working group was formed to tackle this task.

Due to the long process, the Wi-Fi Alliance released an interim standard known as Wi-Fi Protected Access (WPA) which was based on an early draft of the eventual 802.11i standard content. Because the two improved security standards turned out to be largely compatible, 802.11i was also adopted by the Wi-Fi Alliance and came to be known as Wi-Fi Protected Access version 2 (WPA2). Although WEP/WPA/WPA2 is strictly optional within the 802.11 standard, they are requirements for Wi-Fi™ compliance certification.

**Wired Equivalent Privacy (WEP) Protocol**

WEP employs the RC4 PRNG algorithm by RSA data security, Inc. RC4 is a stream cipher algorithm developed in 1987 by Ronald Rivest. The RC4 algorithm uses a variable sized symmetric key independent of the plaintext to produce the cipher text.

**WEP Operation Theory**

The RC4 stream cipher operates by expanding a secret key and a public 24-bit initialization vector (IV) concatenated to a pre-shared key (generally, the same key used for the authentication stage) into an arbitrarily long key stream of pseudo-random bits. Encryption is achieved by performing an exclusive OR (XOR) operation between the key stream and the plaintext to produce the cipher text. Decryption is done by generating the identical key stream based on the IV and secret key and XORing it with the cipher text to produce the plaintext. Details of the WEP operation can be found in the IEEE 802.11 standard.

Many 802.11b vendors produce products that support 40-bit and 104-bit WEP. Some vendors refer to the 40-bit version as "64-bit WEP" and the 104-bit variant as "128-bit WEP". This discrepancy comes from the fact that although the 40-bit secret key and 24-bit IV are concatenated to make up 64-bits, the 24-bit IV is sent in the clear, thereby reducing the effectiveness to only 40 bits.

### Wi-Fi Protected Access (WPA)

The Wi-Fi Protected Access (WPA) system was created by the Wi-Fi Alliance in an attempt to address the security vulnerabilities in WEP. WPA was an intermediate measure to take the place of WEP while the official 802.11i standards were being developed. WPA was in fact based on an early draft of the 802.11i standard, with key frame information elements intentionally changed to avoid the possibility of conflicts between WPA and the eventual 802.11i release.

The goals of WPA were largely the same as for WEP; improved security was the main objective, but the new scheme had to be supported on the existing hardware base. To do this, RC4 was retained as the data stream cipher due to its low processing requirements, but "wrapped" to cover the insecurities of WEP.

Several major improvements were made in WPA to improve security. A full 128-bit secret key and a larger 48-bit initialization vector (IV) was used- separate individual keys are used in each direction as well as for integrity validation and a new key scheduling process known as the Temporal Key Integrity Protocol (TKIP) was added.

### IEEE 802.11i/Wi-Fi Protected Access version 2 (WPA2)

The official IEEE-endorsed security improvement standard 802.11i was not ratified until 2004 and being backward compatible with the interim WPA standard, came to be known also as WPA2. As of 2006, all commercial products that wish to be Wi-Fi certified must support WPA2 security measures.

WPA2 continues to support the simple pre-shared key (PSK) mode of operation which can complicate key management and distribution issues if there is even a moderate population of wireless users. As with WPA, 802.1X extensible authentication protocol (EAP) is supported; however the Wi-Fi Alliance now requires validation for a wider range of 802.1X EAP methods under WPA2 in its certification program.

### VDS - Virus Detection System

Virus detection system is the process of monitoring the events occurring in a computer system or network and analyzing them for signs of possible incidents, which are violations or imminent threats of violation of computer security policies, acceptable use policies, or standard security practices. Virus prevention is the process of performing Virus detection and attempting to stop detected possible incidents.

## CONCLUSION

All the work in this paper is based on the IEEE 802.11 infrastructure WLAN. The research is specially focused on to study different security problems or flaws in wireless networks and to detect some of these attacks using Virus detection techniques. It is known that wireless networks are prone to more attacks than wired networks because there is no need of any physical access to wireless networks. The sole focus of this thesis is on Virus detection techniques for wireless local area networks (WLAN). The work presented in this thesis is not based on statistical or mathematical modeling; this work is on the basis of Network Simulator 2 (NS2).

## REFERENCES

A. Lazarevic, V. Kumar, and J. Srivastava (2005). Virus detection: a survey, managing cyber threats: issues, approaches, and challenges. *Springer Verlag*, page 330.

Denning E. D. (1987). An Virus detection model. *IEEE Transactions on Software Engineering*, pages 222–32, 1987.

J. M. Estevez-Tapiador, P. Garcia-Teodoro, and J. E. Diaz-Verdejo (2004). Anomaly detection methods in wired networks: a survey and taxonomy. In *Computer Networks*, pages 1569–84.

P Kabiri and A. A. Ghorbani (2005). Research in Virus detection and response – a survey. *International Journal of Network Security*.

P. Garcia-Teodoro, J. E. Diaz-Verdejo, G. Macia-Fernandez, and E. Vazquez (2009). Anomaly-based network Virus detection: Techniques, systems and challenges. *Computers & Security*, pages 18–28.

V. Barnett and T. Lewis (1994). *Outliers in statistical data*. Wiley.