INFORMATIVE STUDY AND SOLUTION FOR WIRELESS LOCAL AREA NETWORK (LAN) IN CHINA

Muhammad Waqas Ahmad *,Wang Fei,Wu Zhongdong,Mang Ge
School of electronic and Information Engineering , Lanzhou Jiaotong University, Lanzhou, 730070, China
Email:browneye786b@gmail.com

ABSTRACT: *Main objective of study is to provide information regarding unsecured or poorly secured networks and how to make possible secure wireless communication at the same level and description assist within the scope of this context. We described the emergence of wireless networks with the rise of smart phones and other digital technologies and in the same fashion the security concerns are also increased. We also made recommendations toward a safe wireless network.*

Keywords: WLANs,WNs,Eves dropping,SSID,Wireless

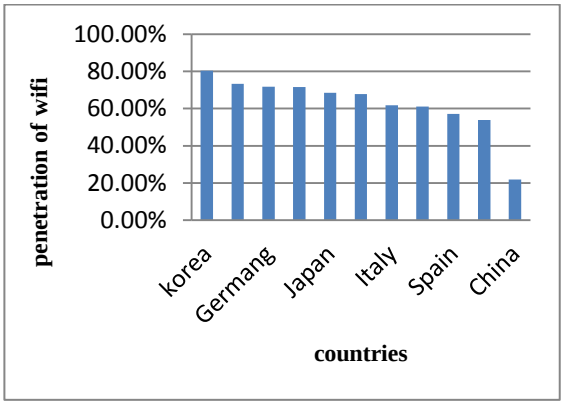
1.0. INTRODUCTION

WNS is the abbreviation of Wireless Network Security, providing much security based advantages and increased accessibility of the information sources, which configuration of the device is informal, closer and low-priced. On the other side, there are a lot of security related issues existing in this context because Wireless communication takes platform side to side the air so the threat of eves dropping is also increased because of the open nature of used medium. In majority cases we think the public Wi-Fi networks especially hotel networks as safe but now there are even more evidences that they are not, nearly 40% of hotels networks are accounted for breaches in china. Whereas risk of interception is greater, as compare optical fiber or wired based communication. Algorithm has significant contribution which radio frequency can be easily encoded with weak algorithm by the hacker. It is already to be noted that the risk possibility associated with various threats to the security system. In the modern society, mostly users have found that Wireless communication is convenient and easy in use than wired communication, in which Wireless Local Area Network (WLAN) devices are flexible and moveable from one place to another place within area connectivity (see Figure.1).Which WLAN permit user to share data within network and compatible devices [1].

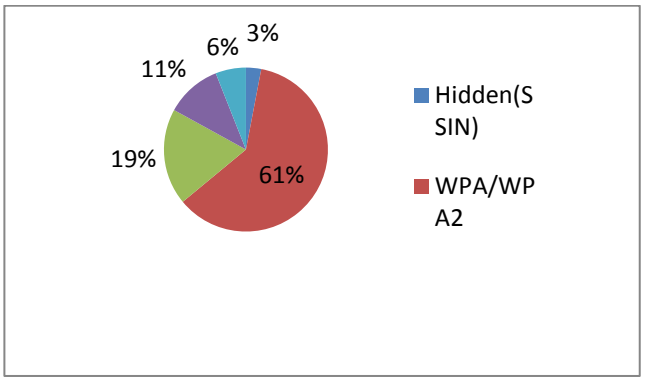
Figure.1 Basic Wireless Components

2.0. Penetration of Wi-Fi

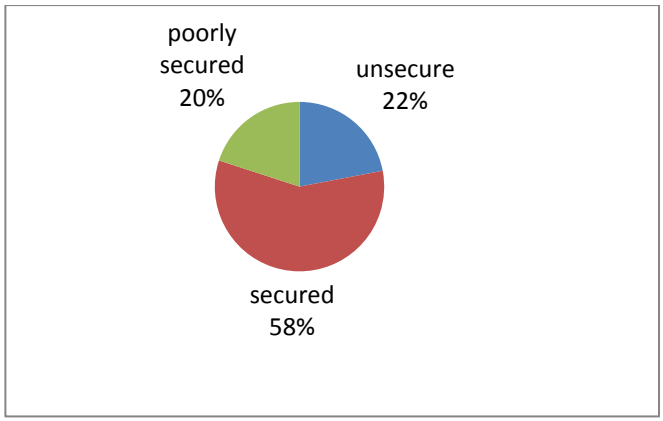
A report published in ministry of communication America in 2011,439 million households were using WNs worldwide which was 25% of overall networks but due to dramatic increase in digital technologies, in 2015 42% of homes are occupied with WNs. In china 110million households are using wireless network but due to its huge number of population it just makes 21.1% of overall population which places him at 15th place among other countries worldwide.



Graph.1 Penetration of wifi network



Graph.2 overall stats of Wifi networks



Graph.3 overall stats of business Wifi networks

After observing more then 2000 networks it is disclosed that a large proportion of wireless networks are either unsecured or poorly secured and this ratio is alarminly high among business networks.

3.0. Technology & Security

Wireless communication is based on radio transmission, throughout without physical connection. The Wireless systems are included in different WLANs, such as personal networks and devices considered to be as Wireless clients. Wireless technology evolves; advance Wireless clients are being developed to provide updated features and functions. In modern society, smart phones are also providing multiple services, such as email, text messaging, web access and voice recognition services, whereas latest smart phones incorporate PDA, Wi-Fi and GPS capabilities. The communication without mobility restrictions within the network coverage is the requirement of modern society, in which new developments are presenting new security risks.

Whereas, these security steps can be taken to secure network include:

- Maintain a complete acknowledgement of network topology.
- Keep record and label fielded Wireless devices.
- Frequently create backups data.
- Implements periodically and randomly security related test of the network.
- Frequently analysis network efficiency reports.
- Monitor new changes and apply patches.
- Monitor and/or up-to-date new threats and vulnerability

4.0. Wireless LAN Structure

To complete the security requirements there is a lot of stuff required to do in this context. Where, a Wireless access point established a Wireless link with a fixed point. Herein, the first requirement is the confidential communication between Wireless Access point and Wireless Clients. However, most Wireless communication started over a fixed network so protection requirements are restricted to the Wireless link. Basic structure in the Wireless LAN is known as BSS and the BSS is the abbreviation of Basic Service Set, which network consist of Wireless access Point and Wireless Clients and in order to form of BSS, Wireless access point broadcasting its SSID (Service Set Identifier) to permit Wireless clients to join the network (see Figure.2) [2-4].

In order to secure communication, authentication and protection should be provided to achieve data confidentially, which authentication encryption should be used. This is a service requirements to establish a secret key between the Wireless Clients and the network. If in case Wireless LAN did not have AP device and all the Wireless clients were communicating directly with each other [5,6]. This Wireless LAN structure is known as Independent BSS (IBSS), see Figure.3.

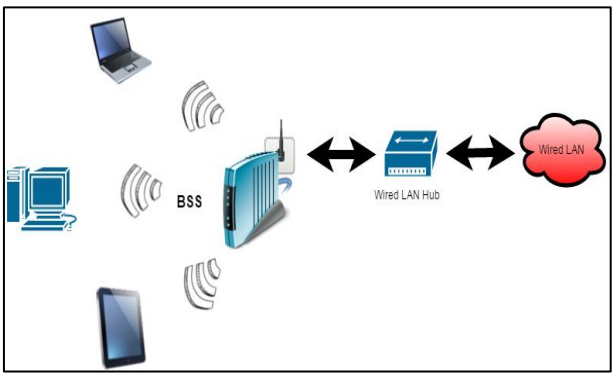


Figure.2 Basic Wireless LAN Structure

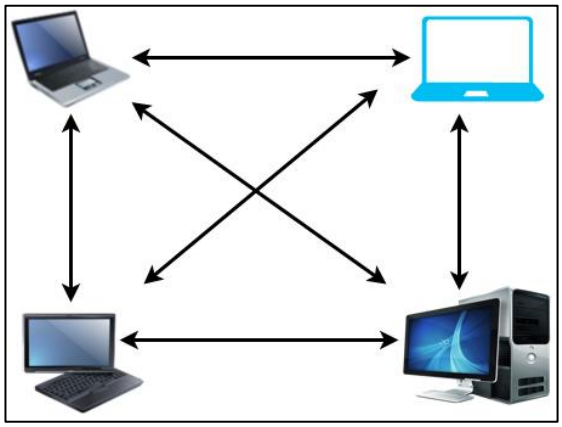


Figure.3 Wireless LAN IBSS Structure

5.0. Common Security Attacks

Basically there have some common security attacks in Wired and Wireless networks, but transmission by Wireless network makes it easy for everyone to attack within the coverage of network, in case if network is not secured. The range of transmission without physical assistance started over 300feet to half mile. Herein, main consideration is focused to on the most common attacks and the security threats are listed below, included:

- Traffic Analysis
- Passive Eavesdropping
- Active Eavesdropping
- Unauthorized Access
- Man-in-the-middle Attacks
- Session High-Jacking
- Replay Attacks
- Rouge AP
- DoS Attacks

There are different other threats makes harder for standard regulators to resolve security related issues without sacrificing network speed. Therefore, it's very important to keep in touch with new challenges in this context.

6.0. 802.11 Standard& Authentication

Wireless media is not easy to secure as compared with wired media, just because of its broadcast nature [7] and this challenge encourage to makes creating a secured protocol. Some Wireless clients such as mobile units are also using Wireless security protocols in many other aspects. Presently, Wireless LAN security achieves to go through the steps of WLAN security by implementing 802.11 security protocols.

The 802.11 is the IEEE standard, was defined in 1997. Basically this standard consists of different three layers (see Figure.4). In the beginning, the standard version supported only 2Mbps bandwidth but with the passive of time motivated developing teams updated standard version that supported 54 Mbps bandwidth. To fulfill the requirements of physical layer, the designers consider the necessity of physical layer that can simultaneously supported more than one signal technique and interface. It is also to be noted that physical layer responsible to providing interface frames with upper MAC layer and supports functionality needs to allow reliable transmission to upper layers, whereas LLC is providing address and data link control.

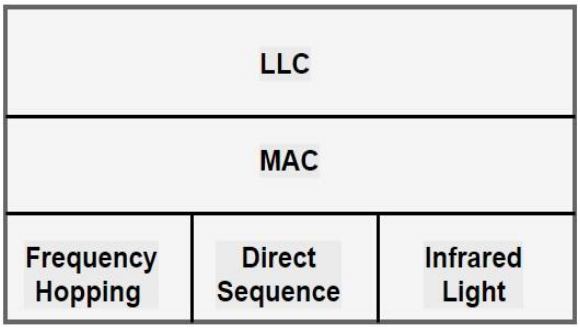


Figure.4Basic Layers (802.11)

To permit Wireless clients to access the network, are required two steps:

1. The first one is required authentication from AP (Wireless-Access Point), and
2. Then getting associated.

Basically there are further 2 types of authentication are used [8].

i. Shared Key Authentication
ii. Open Key Authentication

The WEP (Wired Equivalent Privacy) Standard version developed to use with 802.11, and both are authentication modes. Whenever, any Wireless client wants to be connected with AP. The first client needs to send a request and when AP receive an any new client request then AP sends back a challenge packet to client in clear form of text (unencrypted). The client then encrypts its WEP key and sends back to AP. In which AP efforts decrypt the message by its WEP key. This decryption is defined for the security purpose, if this process succeeded that means the new user or client is an authenticated user or client (see Figure.5), otherwise the user request to access the network is denied.

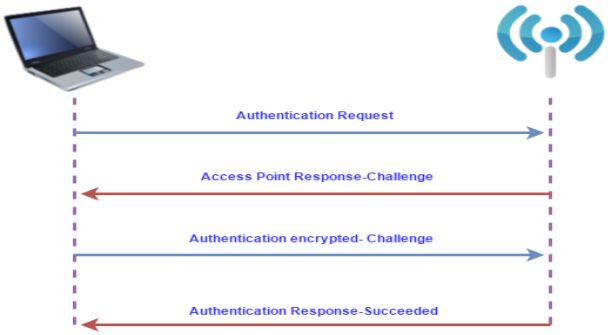


Figure.5Shared Key-Authentication

On the other side, open key authentication not contained any challenge or response message exchange but the user always needs to get authentication. While, open key authentication doesn't dealing any type of authentication but it's more secure. It's possible behind to use open key authentication that it is completely secure and doesn't expose the WEP key to traffic sniffers.

7.0. Apply the Concept of Defense-in-Depth Approach

This approach has been widely applied in the secure designing of the wired networks and similarly, this approach applied in the secure designing of the Wireless networks. There are different types of (multiple) security layers and to secure network these layers are significantly contributing to reduce the risk level in Wireless networks. In case, any attacker try to breaches one measure then the additional measure and/or takes place to recover and protect the network. It's really important to understand that separation of Wired and Wireless networks segments are using strong device and authentication system. Network application for filtering based on different protocols and addresses, and detection system in Wireless and Wired networks can be applied to build multiple layers for defense.

8.0. Avoid Excessive Coverage &Secure-AP

Proper placement of Wireless access point has significant contribution to avoid excessive coverage, which radio frequency power transmission controls the propagation of radio frequency signal and coverage of Wireless network by AP. Whereas, Secure Wireless-AP is the more important part in network security, which security has overall effects on the network. To make secure AP is the first step in Wireless network security and the following some recommendations helpful to deal hardening-APs:

- To change configuration default setting;
- To change encryption Keys weekly/daily bases;
- To make sure that access point has strong and exceptional admin password, and change it Weekly/daily bases;
- Disable insecure and irrelevant protocols on AP;
- Configure relevant management associated protocols;
- Active- logging features; and
- Enable threshold parameters
- Define minimum (limit) Client-to-Client Communication through AP
- Develop high- Security Configuration Standards for AP

9.0. Secure Network-Recommendations

Recently, the new vulnerabilities issues are identified and exploited for 802.11 (standard), in which planning, management and implementation should be done carefully of secure network [9], and these following steps are, included:

- Establish dedicated Wireless LAN security best management policies
- Design the best practices for network security
- Logically separate, if the more than one networks are existing
- Enable VPN access (Only)
- Avoid and delete unnecessary protocols
- Protect Wireless Clients.

10.0. Wi-Fi-Protected Access

Wi-Fi is a brand that particularly has been alliance with 802.11 products, which Wi-Fi Protected Access (WPA) is giving protection to Wireless clients. Basically, WPA defines TKIP, which derives keys by mixing a base key with the transmitter's MAC address. It is to be noted that initially vector is varied with that key to generate for each packet keys. WPA also consists of Message Integrity Check (MIC) to protect data forgery. 802.1X is updated version with high security standard. Small level enterprises need to use WPA with 802.1X for key delivery and refresh. Which WEP applied for certify WPA firmware for upcoming upgrades.

11.0. Summary

WNS for WLAN is providing much security based advantages and increased accessibility of the information sources, which configuration of the device is informal, closer and low priced and minimize the attend risk. Establishment of polices for WLAN, has significant contribution to secure network with best practices and in order to secure communication, authentication and protection should be provided confidentially. This is a service requirements is to establish a secret key between AP and Clients. Whereas Wi-Fi is a brand that particularly has been alliance with 802.11 products which Wi-Fi Protected Access (WPA) is giving protection to Wireless clients.

REFERENCES

[1]. [Choi], Min-kyu, et al. "Wireless network security: Vulnerabilities, threats and countermeasures." International journal of Multimedia and Ubiquitous Engineering 3.3 (2008).

[2]. Al Tamimi, Abdel-Karim R. "Security in Wireless Data Networks: A Survey Paper."

[3]. [Earle2005] "Wireless Security Handbook,".Auerbach Publications 2005

[4]. Idris, Noor Aida, and MohamadNizamKassim. "Wireless Local Area Network (LAN) Security Guideline." (2010). [Welch2003] "Wireless security threat taxonomy," Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society 18-20 June 2003 Page(s):76 - 83

[5]. [Chandra2005]," BULLETPROOF WIRELESS SECURITY : GSM, UMTS, 802.11, and Ad Hoc Security (Communications Engineering) ,". Newnes 2005

[6]. [Imai2006]," Wireless Communications Security ,". Artech House Publishers 2006

[7]. [Arbaugh2003] "Wireless security is different,". Computer Volume 36, Issue 8, Aug. 2003 Page(s):99 – 101

[8]. [Earle2005] "Wireless Security Handbook,".Auerbach Publications 2005
[9]. [Wireless80211] "802.11 Wireless LAN Policy.