

## Resist attack on the local area network

**Luay Abdul wahid Shihab**

Department of Branch of Basic Science, College of Nursing, University of Basrah, Basrah,  
IRAQ

Luaay.abdulwahid@uobasrah.edu.iq

**Manhalmohammed basher**

Agricultural technical college , Northern technical university

Manhalbasher@gmail.com

### Abstract

The purpose of the research is to protect the LAN from hackers and to make network security protected. Over the past five years, the number of WLANs including homes, schools, airports, commercial and government offices has increased, creating different types of threats. Events do not stop around the clock and information is pouring down on us like torrent hour by hour. In order to be in the picture and keep up with the new as much as possible we had to stretch the ropes between us and the world around us, but how is it? In order to communicate, technology and security are essential. The axis of communication is networks. Information cannot be exchanged locally or globally.

To make the network secure, you must use a strong security system, starting with a strong encryption system, **installing antivirus software, and updating your firewall.**

**Keywords:** resist , attack , local area network:

### 1.Introduction

Local networks are short-term networks and the size of the network can be in the hospital, home, college or company, so the penetration is through the files involved in the network devices and hacker first identify the main machine in the network usually have a number one name and after determining the device break the secret number.

A Wireless Local Area Network (WLAN) refers to the computer local area network that uses the wireless channel as the transmission medium. 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 , Integrity, authentication [1] .vulnerabilities affect intranet security and credentials in a small enterprise environment. This would help to prove the equivalence of the information security importance on either against external invasions or internal penetrations [2].. The WLAN is widely used in the domains where mobile data processing is required or the layout of physical transmission medium cannot be performed SSID (Service Set Identifier) SSID acts as a WLAN identifier. Thus all devices trying to connect to a particular WLAN must be configured with the same SSID. It is added to the header of each packet sent over the WLAN and verified by the AP. A client device cannot communicate with an AP unless it is configured with the same SSID[3] .

The other advantages for WLAN include cost-effective network setup for hard-to-wire locations such as older buildings and solid-wall structures and reduced cost of ownership-particularly in dynamic environments requiring frequent modifications[4].

Illegal practices have emerged on the Internet, with the function or assistance of a locality or locality as the case may have led to the emergence of a new range of cross-border crimes, other than cybercrime, cybercrime or cybercrime , Beware of showing off your ability to protect your network under protection and that your network is not hackable One doesn't need to have physical access to your wires to get into your LANs now [5] .

## 2. type of attack on network:

1. Virus deployment: Currently the Internet has become more in the spread of viruses that target files and secret accounts of hacked devices where they are deleted or transferred to other devices

.2. Hacking: Illegal access to computers through some hacking softwar

3. attack on the router

4. Coverage and camouflage by sending fake files by email

The grid is designed as shown in Figure 1

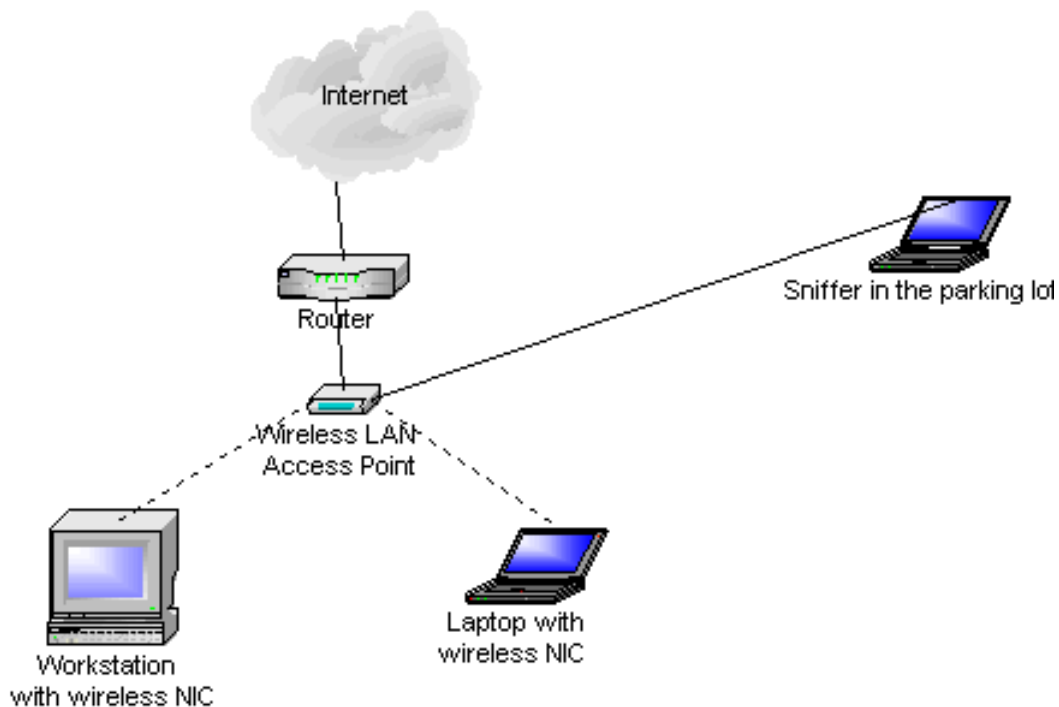


Figure ( 1 )

## 3. Previous studies :

In previous studies in research ( 2 )A sequential attack program has been used that will be easier and more accurate at some points. The attack process includes only three main patterns ( 4 )found that the more secured a network became, the higher the performance impact .

the performance and security issues of IEEE 802.11 wireless LANs with the layered security policy model, It studied the interaction between different security policy layers and their

effects on performance (response time and throughput) of congested and Improvement of throughput for TCP traffic of various stations.

( 5 )Protect the local network using encryption flow and prevent hackers from penetrating the network And how to use the network your local network in order to design and build a good . Through their research (6) when the Internet congestion occurs causing interference by the attacker and takes his role in the attack.

#### **4.WLAN Implementations**

Varies due to organization size and security concerns

Current technology not ideal for large-scale deployment and management

Will discuss a few tricks that can help the process and a few technologies under development to ease enterprise deployments

#### **Defense Against Network Attack:**

**In defending against network attack, there are broadly speaking four sets of available tools :**

- 1. The software and system must be maintained, updated and arranged.**
- 2. theuseoffirewallstostopbadlikeVariousand network exploits, and to detect signs of attack and compromise .**
- 3. Search for attack or intrusion in terms of installing detection software.**
- 4. encryption — protocols such as DDOS and SYN that enable you to protect specific parts of the network against particular attacks.**

#### **research goals :**

- 1.Protect and resist the LAN from attack
- 2.Identify and distinguish the attacker and disable it

#### **5. Basic Configuration**

### **DESIGNING THE PHYSICAL NETWORK**

#### **Rogue Networks**

Network users often set up rogue wireless LANs to simplify their lives

Rarely implement security measures

Network is vulnerable to War Driving and sniffing and you may not even know it

### **DESIGNING THE PHYSICAL NETWORK**

electronic high security because of the strong and difficult to break and therefore the confidentiality of this system depends on the secret key Encryption converts the text flowing to the explicit text of the encrypted beta - beta at the same time. The encryption key is a sequential (serial) binary consisting of a set of zeros and units (1, 0) is called sequential key. Encryption system flowchart includes two parts(Wireless LAN Security and Management).

**1. Algorithm to generate the key sequence . 2. Gate**

1 . Choose two large initial numbers  $p, q$  randomly.

2 Calculate  $p * q = n$

3 Calculate the function of  $Q(n)$ :  $m = Q(n) = (p-1)(q-1)$

4 Select the initial number  $e, m > e > 2$  so that:  $GCD(m, e) = 1, m, e$  can not divide

5 Determine  $d$  so that:  $m \text{ mode then } d = e, (m \text{ mode}) 1 = e * d.$

The numbers  $n, e$  are the declared key (public), and the numbers  $p, q, d, m$  are secret keys, without which the RSA becomes a single path function.

6 Encryption is calculated using the declared key as follows

) .....  $1n \text{ mode}) C = M$

7 Decoding is done using the secret key as follows

(.....  $2 n \text{ mode}) M = C$

The explicit text is divided into blocks and equal sizes  $m$ . Each block is individually encoded so this system belongs to the cryptographic systems after converting them into numbers belonging to  $0, n-1$  [using the equation above where  $c$  belongs to  $0, n-1$ ] Use one type of encoding such as ASCII encoding.

$P = 47 \ \& \ q = 59$

$N = p * q = 47 * 59 = 2773$

$M = \phi(n) = (p-1)(q-1) = 46 * 58 = 2668$

$D = e^{-1} \text{ mod } m \ e = 17$

)  $2667^{-1} \text{ mod } 2668 = 157$

The message is divided into 2-digit blocks and the alphabetical sequence is followed to encode the character as follows

Blank = 00 A = 01 B = 02 C = 03 ..... Z = 26

The message will symbolize:

$M = 0715 \ 1504 \ 0013 \ 1518 \ 1409 \ 1407 \ 0001 \ 1209$ -----

$M = 0715$

$C = M^e \text{ (mod } n) = (0715)^{17} \text{ mod } 2773 = 1462$

**RESULTS AND DISCUSSION:**

[1] In the first research discussed the security challenges and how to attack the LAN and the challenges are man's attack in the middle and 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. [4] In this paper, and found that the more secured a network became, the higher the performance impact. Investigating the performance and security issues of IEEE 802.11 LANs with the layered security policy model. It studied the interaction between different security policy layers and their effects on performance (response time and throughput) of congested. In this paper [5] Protect the local network using encryption flow and prevent hackers from penetrating the network And how to use the network your local network in order to design and build a good network. The results of this research made the network protected You must use a strong security system.

---

Through the system in this paper ( 6 ) , the expected attack was reduced and the attack was reduced and resisted through the encryption program, the virus program, the firewall and the change of the key word constantly to reduce the problems of the Internet ,Through search (6).

### **CONCLUSION:**

Wireless LANs very useful and convenient, but current security state not ideal for sensitive environments.

Growing use and popularity require increased focus on security.

You must know the attacker's thinking.

### **ACKNOWLEDGEMENTS:**

This work depends on practical research and has been working in the laboratory of the Faculty of Nursing at the University of Basrah.

### **Refrence :**

- 1.PROF. RATHNAKAR, DR. VITYANATHAN, DR. PETHUR RAJ,Wireless LAN Security – Challenges and Solutions,International Journal of Computer and Electrical Engineering, Vol. 1, No. 3, August 2009.
- 2.Cheng Hu ,Intranet Security Overlooked Importance,29 Nov 2013,
- 3.YasirZahur and T. Andrew Yang,WIRELESS LAN SECURITY AND LABORATORY DESIGNS,JCSC 19, 3 (January 2004).
- 4.Debabrata Nayak<sup>1</sup>, Deepak B. Phatak<sup>1</sup>, Ashutosh Saxena<sup>2</sup>,Evaluation of Security Architecture for Wireless Local Area Networks by Indexed Based Policy Method: A Novel Approach,International Journal of Network Security, Vol.7, No.1, PP.1–14, July 2008.
- 5.Luaay Abdul WahedShihab,Wireless LAN Security and Management,International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249 – 8958, Volume-2, Issue-1, October 2012.
6. LuaayAbdulwahedShihab , THE MECHANISM OF CONGESTION BETWEEN THE SERVER AND CLIENTS IN A LOCAL AREA NETWORK SOLUTIONS ,International Journal of Civil Engineering, Construction and Estate Management, Vol.3, No.3, pp.63-68, August 2015.