# WI-FI Security by using Proxy server

**Promila[1], Dr.R.S.Chhillar[2]**
[1, 2] Department of Computer Science and Application, M. D. U. Rohtak, India

**Abstract:**
With the whole world going mobile, data security remains the biggest challenge. Critical data (Business and Safety related) is lying on storage medium on a computer which is connected to hundreds of thousands of computers via internet. Wi-Fi uses a radio frequency to transmit data. Any user with a transceiver can connect to the network, if not properly secured. Use of the mobile networking is on rise and 60% of these are unsecured, risk of external threat is very high. A structured thread by an experienced hacker with malicious intent can get hold of user account and use it to access mission critical data. Thus it is of utmost importance to secure a Wi-Fi network. Stringent security policies must be followed. Multiple lever of security shall be put in place.

**Keywords:** AES, DAIR, MAC, Proxy server, TKIP, WEP, WPA.

## 1. Introduction:

**WI-FI:-**

WI-FI stands for "Wireless Fidelity". Wi-Fi refers to wireless networking technology that allows computers and other devices to communicate over a wireless signal. Wi-Fi is a term for certain types of wireless local area network (WLAN) that use specifications in the 802.11 family. The term Wi-Fi was created by an organization called the Wi-Fi Alliance, which oversees tests that certify product interoperability. A product that passes the alliance tests is given the label "Wi-Fi certified" (a registered trademark).

Originally, Wi-Fi certification was applicable only to products using the 802.11b standard. Today, Wi-Fi can apply to products that use any 802.11 standard. The 802.11 specifications are part of an evolving set of wireless network standards known as the 802.11 family. The particular specification under which a Wi-Fi network operates is called the "flavor" of the network. Wi-Fi has gained acceptance in many businesses, agencies, schools, and homes as an alternative to a wired LAN. Many airports, hotels, and fast-food facilities offer public access to Wi-Fi networks.

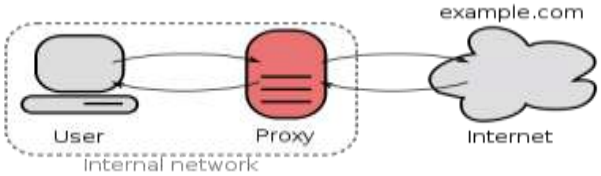

"Figure1. Wi-fi logo"

**Proxy server:-**

A proxy server acts as an intermediary between websites and web browsers. Web browsers are configured to use a proxy server instead of accessing websites directly on the internet. A proxy server acts as a middleman between two networks. One network is typically the public Internet, the other is often a group of client computers sharing a single Internet connection. The primary remaining uses of a proxy server are to protect the privacy of systems behind the server, and to speed up Internet access through caching. However since the proxy can be configured not just to direct data ,but to change it en route,there are many potential uses. A proxy server caches frequently accessed data. If a web browser requests cached data, the proxy server can retrieve it quickly instead of making another request across the Internet, which is slower. A network can be configured so that the only way to reach the Internet is through a proxy server that allows only authorized users who have an account.

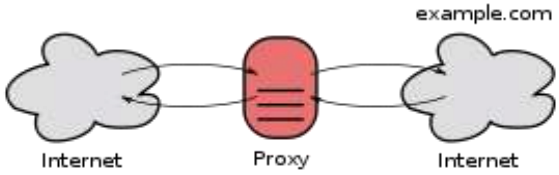
Types of proxy server:-

1. **Forward proxy**: -A forward proxy takes request from an internal network and forwarding them to the Internet.



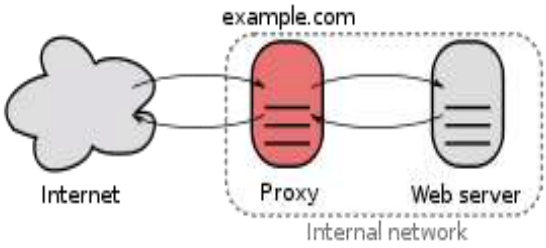

"Figure2. Forward proxy "

1. **Open proxy**: - An open proxy forwards request from and to anywhere on the Internet.




"Figure3. Open proxy "

2. **Reverse proxy**:-A reverse proxy taking request from the Internet and forwards them to servers in an internal network. Those making requests connect to the proxy and may not be aware of the internal network.




"Figure4. Reverse proxy "

## 2. Related Work

**10 tips of WI-FI security:-**These tips are given by Chad Perrin in 2007

1. Use a strong password.
2. Don't broadcast your SSID:- Serious security crackers who know what they are doing will not be deterred by a hidden SSID — the "name" you give your wireless network
3. Use good wireless encryption.
4. Use another layer of encryption when possible.
5. Restrict access by MAC access.
6. Shut down the network when it is not being used.
7. Shut down your wireless network interface, too.
8. Monitor your network for intruders.
9. Cover the bases:- Make sure you have some kind of good firewall running.
10. Don't waste your time on ineffective security measures [7].

**Enhancing the Security of Corporate WI-FI Networks Using DAIR:-**DAIR stands for *Dense Array of Inexpensive Radios.* DAIR systems are designed for building wireless network management applications that benefit from RF (radio frequency). The DAIR approach is unique in that it builds on the following two important observations. First, in most enterprise environments one finds plenty of desktop machines. The machines are generally stationary and are connected to wall power. They have good wired connectivity, spare CPU cycles, free disk space, and high-speed USB ports. Second, inexpensive USB-based wireless adapters are readily available and their prices continue to fall, by attaching USB-based wireless adapters to desktop machines, and dedicating the adapters to the task of monitoring the wireless network, we create a low-cost monitoring infrastructure that is then used to manage the security of the network [4].

There are many methos available for the wi-fi security, many encryption schemes such as EAP,TKIP, AES, WEP, WPA, WPA2 etc and many security tips are develeped.

**AES**:- Advanced Encryption Standard is gaining acceptance as appropriate replacement for RC4 algorithm 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.

**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 [5].

**WEP**: - The industry's solution: WEP (Wired Equivalent Privacy) [3], [5], [8], [9], [10]

- Share a single cryptographic key among all devices
- Encrypt all packets sent over the air, using the shared key
- Use a checksum to prevent injection of spoofed packets [6].

Some devices support the various versions of WEP-

- WEP-64-bit key (sometimes called WEP-40)
- WEP 128-bit key (sometimes called WEP-104)
- WEP 256-bit key.

**WAP:-** WAP stands for Wi-Fi Protected Access [3], [5], [8], [9], [10]. This standard was developed to replace WEP. Wi-Fi devices typically support multiple variations of WPA technology. Traditional WPA, also known as WPA-Personal and sometimes also called WPA-PSK (for pre-shared key), is designed for home networking while another version, WPA-Enterprise, is designed for corporate networks.

WAP2 is an improved version of Wi-Fi Protected Access supported by all newer Wi-Fi equipment. Like WPA, WPA2 also exists in Personal/PSK and Enterprise forms [8].

**Evolution of wi-fi security:-** Wi-Fi technology has evolved quickly to adapt to changing market and technological conditions. Global adoption of WPA and WPA2 advanced security mechanisms has further strengthened trust and reliance on Wi-Fi CERTIFIED equipment worldwide [3].

| Date | Milestone |
|---|---|
| September 1997 | IEEE 802.11 standard ratified, including WEP |
| April 2000 | Wi-Fi CERTIFIED program launched, with support for WEP |
| May 2001 | IEEE 802.11i task group created |
| April 2003 | WPA introduced with:<br>•IEEE 802.1X<br>authentication<br>•Temporal Key Integrity Protocol (TKIP) encryption<br>•Support for EAP-Transport Layer Security (EAP-TLS) |
| September 2003 | WPA mandatory for all Wi-Fi CERTIFIED equipment |
| June 2004 | IEEE 802.11i amendment ratified |
| September 2004 | WPA2 introduced with:<br>• IEEE 802.1X authentication<br>• AES encryption<br>• Support for EAP-TLS |
| April 2005 | Support for four additional EAP-Tunnelled TLS Microsoft Challenge Handshake Authentication Protocol Version 2 (EAP-TTLS/MSCHAPv2)<br>•Protected EAP Version 0 (PEAPv0)/EAP MSCHAPv2<br>•Protected EAP Version 1 (PEAPv1)/EAP Generic Token Card (EAP-GTC)<br>•EAP-Subscriber Identity Module (EAP-SIM) |
| March 2006 | WPA2 mandatory for all Wi-Fi CERTIFIED equipment |
| January 2007 | Wi-Fi Protected Setup program launched |
| November 2007 | IEEE 802.11w task group created |
| May 2009 | Support for EAP-AKA and EAP-FAST added |
| January 2012 | Support for Protected Management Frames added to WPA2 |

" Table 1.showing wi-fi security timelines[3]

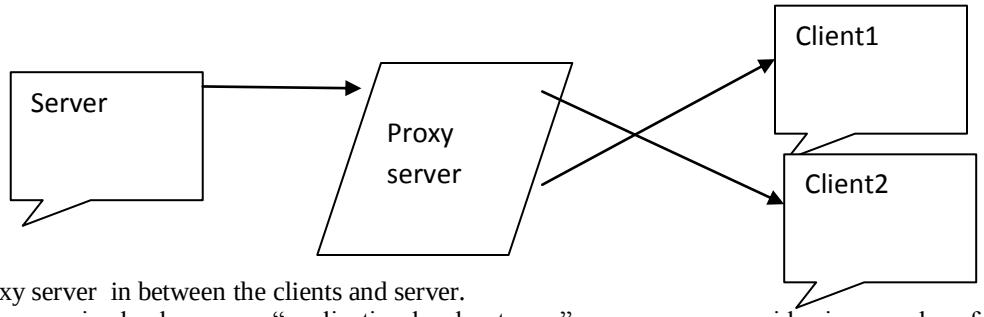
## 3. Proposed work:

Wired networks are more secure than wireless network. Wireless networks can be an effective way to extend network access. Wired networks gain some privacy from their switches and routers and the buildings that enclose them. On a wireless network everyone can 'hear' everyone else, even in public spaces outside the building, so there are problems of privacy of communications, accountability for use and availability of service. WI-FI technology gaining the more and more popularity now days, hence the security issues related to this technology is also needed in excess.

**Protocol stack:** - The protocol stack for WLANs was designed such that existing applications can use them with minor modifications. The three layers are same to other networks:-application, transport and network layers are same. Proxy server works on upper three layers but mostly on the application layer.

| |
|---|
| Application Layer |
| Transport Layer |
| Network Layer |
| MAC/Data-link Layer |
| Physical Layer |

Proxy server plays very important role in LAN network , in the same way if we add the proxy server to WLAN than in the same way with the help of proxy server can protect the WLAN network also .




Proxy server in between the clients and server.

Proxy server is also known as “application level gateway”.proxy server provides increased performance and security. In the proxy server the data enters through one port and is forwarded to another port or the rest of the network. Basically proxy server plays the two important role:-

1. **Performance impovement:-**Proxy servers saves the requests for a certain time period. Hence the performance increases dramatically for a group of users.for example if a person p request for a web page ,after some time another person q requests the same site than the proxy server returns the same web page for person q that it already fetched for the person p,instead of forwarding the request to the server. Hence the time will be saved .
2. **Filteration:-**Proxy severs can also povides the facility of the filtering. Porxy server povides the content filtering application i.e. they control the content that may be relayed either in one direction or in the both directions.Proxy server can filter the requests.for example in school or in colleges certain web sites are blocked or we can not open some web sites this can also be done with the help of the proxy servers.

   Proxy server also provides the facility of caching. Proxy server can retrives the content saved form the previous request made either by the same person or by the different persons.proxy servers keeps the local copies of the frquently requested requests. Proxy server also provides the user authentication facility also.

   All users have there unique user name and password,these user name and password are saved in the proxy server ,if the user name or password do not match than that person can not access the network. This matching of user name and password is done by the proxy server in LAN in same way we can assign each user a unique user name and password so that any other person do not access the network so that the security will be increased.Proxy server plays important role in impoving LAN security and performance.

We can use proxy sever only in a limited area like in college departments or within a compony having limited users where security is the main issue. We can not use them with a large users access because in large users access it in not possible to give such a large amount of user names and passwords. we can use with in a limited users access only.

Hence if the proxy server is successfully added to the WI-FI network it improve the performance as well as the security in this network also.

## 4. Conclusion:

WI-FI networks are growing day by day. The new challenges or we can say the security risks are also increases day to day. We can impove the performance as well as the security with the help of proxy server ,if it is implemented successfully.we can secure the WI-Fi network upto 5-10% with the help of the proxy server.

**References:**


1. www.wikipedia.com
2. www.webopedia.com
3. The State of Wi-Fi® Security Wi-Fi CERTIFIED™ WPA2TM Delivers Advanced Security to Homes, Enterprises and Mobile Devices by Wi-Fi Alliance.
4. Enhancing the Security of Corporate Wi-Fi Networks Using DAIR by Paramvir Bahl*y*, Ranveer Chandra*y*, Jitendra Padhye*y*, Lenin Ravindranath*y* Manpreet Singh*z*, Alec Wolman*y*, Brian Zill*yy* Microsoft Research, Cornell University.
5. Wireless lan security today and tomorrow by *Sangram Goyal* and *Dr. S. A. Vetha Manickam* Center for Information and Network Security Pune University.
6. Wireless security ppt by David Wagner.
7. Ten WI-FI security tips given by Chad Perrin.
8. Introduction to Wi-Fi Network Security By Bradley Mitchell .
9. Sara Nasre Wireless Lan Security Research Paper IT 6823 Information Security Instructor: Dr. Andy Ju An Wang Spring 2004.
10. WI-FI security –WEP, WPA and WPA2 by Guillaume Lehembre.


.

.