**Research on Wireless Network Security Model**

**Submitted By:**

**Group 14**

**Saad, MD. Tahsin Hasan**

**ID: 17-35171-2**

**Bepari, Masum**

**ID: 18-36780-1**

**Nazmul Hasan**

**ID: 1837377-1**

**Supervised By:**

**DR. Afroza Nahar**

**Associate Professor**

**Department of Science Faculty of Engineering**

**American International University – Bangladesh**

**Table of Contents**

**RESEARCH ON WIRELESS SECURITY MODEL**

**1. INTRODUCTION ----------------------------------------------------------------------------------------3**

**1.1 Importance of the Proposed Research -------------------------------------------4**

**1.2 Problem Statement-----------------------------------------------------------------------4**

**2. RESEARCH QUESTIONS -----------------------------------------------------------------4**

**2.1 Limitation-----------------------------------------------------------------------------------5**

**2.2 Research Objective ---------------------------------------------------------------------5**

**3. METHODOLOGY -----------------------------------------------------------------------------5**

# 3.1 Securing Your Wireless Networks---------------------------------------------------5

**3.2 Security Protocols for Wireless Networks----------------------------------------7**

**3.3 Access Control---------------------------------------------------------------------------- 8**

**3.4 Analysis---------------------------------------------------------------------------------------9**

**3.5 Cost Timing----------------------------------------------------------------------------------9**

**3.6 Result------------------------------------------------------------------------------------------9**

**4 WORK SCHEDULE-----------------------------------------------------------------------------9**

**1. Introduction**

In economic life, industrial production, services, and other social relationships networks have become common structural elements. Wireless networks are a popular solution for homes, businesses, and telecommunications networks. A wireless network refers to a computer network that makes use of wireless connections between nodes in the network. The internet has evolved significantly compared to when it first became popular in homes and businesses decades ago. With more and more mobile devices available, the majority of connections are made wirelessly. Wireless computer networks are playing a major role in modern communications. Laptop computers, cell phones, and embedded systems in common appliances and automobiles may be connected to form an ad hoc network or to a fixed network infrastructure such as the Internet through wireless access points. Wireless access points have been installed in office buildings, homes, airports, hotels, highway service stations, and other facilities, providing people with unprecedented conveniences and flexibilities to exchange information and enjoy online entertainment. People today, for example, can connect their laptop computers to the Internet while sitting in their own backyards or while waiting for flights in the airports. Wireless computer networks have started a new revolution in the information industry. Contract to the rapid development of wireless network applications, the network security is the bottleneck of wireless network. The wireless network has no physical connection node at all which is different with wired network. The data transferred in completely open environment, anybody can get the communication content by some specific tools in the coverage of wireless network. The attacker can pretend to be a valid identity and then access to wireless network to attack and theft information. Wireless network is more dangerous than wired network for its open policy. Therefore, it’s important and necessary to research on the security model on wireless network.

**1.1 Importance of The Proposed Research**

Wireless Network Security system is easy to be installed and can access the internet smoothly. Moreover the system gets a well-structured and advance security system implemented it on. Devices and confidential information are kept safe and secure. There is less loophole and weakness that the security system gets vulnerable to be penetrated and attacked.

The proposed research will help the corporation or organization to make a safe and sound security system for their devices, information and documents from any kind of cyber threats and attacks.

**1.2 Problem Statement**

Studies shows that, the structures of wireless network security models are mostly implemented on massive system stored with important information, private documents and data which need to be much secure. These models are developing and upgrading day by day with an unbreakable protection and less loophole. But the criminals also developing their tools more strong to penetrate the protection. The new developers doesn’t think the way like a cyber-attacker thinks. That’s why there’s always been a weakness and vulnerabilities of the security system.

**2. Research Questions**

From the problem statement, there are following question arises:

1. How the security system need to be build more advance?
2. Which initiatives will make its infrastructure more strong and unbreakable?
3. What features could be added to an updated version so that the security system becomes more easy and user friendly?
4. Which facts should be concentrated on regarding the protection of the system?

**2.1 Limitations**

The new developers follows the corny methods of developing a security system. But this is not enough. To beat a cyber-attack the developers need to think how the attackers strategies to hit. They should get clear idea about every possible ways of attack so that they can build the security system more powerful and unbreakable. But unfortunately, most of the developers doesn’t keeps this in mind and doesn’t have any clear idea about the strategies of attacks. But it is a matter of hope that they are learning and getting more efficient day by day to develop a strong wireless network security model.

**2.2 Research Objective**

On the basis of the research questions mentioned above, some objectives needed to be set up for the wireless network security model

1. Identify the loophole of the security system.
2. Determination of strongest protection.
3. Upgrade the features of the models
4. Seek the vulnerabilities
5. Make the security more efficient

**3. Methodology**

We are developing a programmable security processor platform to enable secure data and multi-media communications in wireless handsets. The objective is to enable secure communications at data rates. Below are some important wireless network security issues.

# 3.1 Securing Your Wireless Network

Today’s home network may include a wide range of wireless devices, from computers and phones, to IP Cameras, smart TVs and connected appliances. Taking basic steps to secure your home network will help protect your devices – and your information – from compromise.

* [**Understand How a Wireless Network Works**](https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network#understand)
* [**Use Encryption on Your Wireless Network**](https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network#use)
* [**Limit Access to Your Network**](https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network#limit)
* [**Secure Your Router**](https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network#secure)
* [**Protect Your Network during Mobile Access**](https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network#assume)

**Understand How a Wireless Network Works**

Going wireless generally requires connecting an internet "access point" – like a cable or DSL modem – to a wireless router, which sends a signal through the air, sometimes as far as several hundred feet. Any device within range can pull the signal from the air and access the internet.

Unless you take certain precautions, anyone nearby can use your network. That means your neighbors – or any hacker nearby – could "piggyback" on your network or access information on your device. If an unauthorized person uses your network to commit crime or send spam, the activity could be traced back to your account.

## Use Encryption on Your Wireless Network

Once you go wireless, you should encrypt the information you send over your wireless network, so that nearby attackers can’t eavesdrop on these communications. Encryption scrambles the information you send into a code so that it’s not accessible to others. Using encryption is the most effective way to secure your network from intruders.

Two main types of encryption are available for this purpose: Wi-Fi Protected Access (WPA) and Wired Equivalent Privacy (WEP). Your computer, router, and other equipment must use the same encryption. WPA2 is strongest; use it if you have a choice. It should protect you against most hackers. Some older routers use only WEP encryption, which likely won’t protect you from some common hacking programs. Consider buying a new router with WPA2 capability.

Wireless routers often come with the encryption feature turned off. You must turn it on. The directions that come with your router should explain how. If they don't, check the company’s website.

## Limit Access to Your Network

**Allow only specific devices to access your wireless network:** Every device that is able to communicate with a network is assigned a unique Media Access Control (MAC) address. Wireless routers usually have a mechanism to allow only devices with particular MAC addresses to access to the network. Some hackers have mimicked MAC addresses, so don't rely on this step alone.

## Secure Your Router

## It’s also important to protect your network from attacks over the internet by keeping your router secure. Your router directs traffic between your local network and the internet. So, it’s your first line of defense for guarding against such attacks. If you don’t take steps to secure your router, strangers could gain access to sensitive personal or financial information on your device. Strangers also could seize control of your router, to direct you to fraudulent websites.

**Change the name of your router from the default:** The name of your router (often called the service set identifier or SSID) is likely to be a standard, default ID assigned by the manufacturer. Change the name to something unique that only you know.

**Change your router's pre-set password(s):** The manufacturer of your wireless router probably assigned it a standard default password that allows you to set up and operate the router, as its “administrator.” Hackers know these default passwords, so change it to something only you know.  The same goes for any default “user” passwords. Use long and complex passwords – think at least 12 characters, with a mix of numbers, symbols, and upper and lower case letters. Visit the company’s website to learn how to change the password.

**Turn off any “Remote Management” features:** Some routers offer an option to allow remote access to your router’s controls, such as to enable the manufacturer to provide technical support.  Never leave this feature enabled. Hackers can use them to get into your home network.

**Log out as Administrator:** Once you’ve set up your router, log out as administrator, to lessen the risk that someone can piggyback on your session to gain control of your device.

**Keep your router up-to-date:** To be secure and effective, the software that comes with your router needs occasional updates. Before you set up a new router and periodically thereafter, visit the manufacturer’s website to see if there’s a new version of the software available for download. To make sure you hear about the latest version, register your router with the manufacturer and sign up to get updates.

**And when you secure your router, don’t forget to secure your computer too:** Use the same basic computer security practices that you would for any computer connected to the internet. For example, use protections like antivirus, antispyware, and a firewall -- and keep these protections up-to-date.

## Protect Your Network during Mobile Access

Apps now allow you to access your home network from a mobile device. Before you do, be sure that some security features are in place.

**Use a strong password** **on any app that accesses your network:** Log out of the app when you’re not using it.  That way, no one else can access the app if your phone is lost or stolen.

**Password protect your phone or other mobile device:** Even if your app has a strong password, it’s best to protect your device with one, too.

## 3.2 Security Protocols for Wireless Networks

There are three main types of wireless security protocols, and there are differences. Choosing the right level of encryption should be the first thing you do when you’re setting up a wireless network. Before you make a decision, you need to be familiar with the different security protocols

**Wired Equivalent Privacy (WEP):**

Wired Equivalent Privacy (WEP) is a security protocol, specified in the IEEE Wireless Fidelity (Wi-Fi) standard, 802.11b, that is designed to provide a wireless local area network (WLAN) with a level of security and privacy comparable to what is usually expected of a wired LAN. A wired local area network (LAN) is generally protected by physical security mechanisms (controlled access to a building, for example) that are effective for a controlled physical environment, but may be ineffective for WLANs because radio waves are not necessarily bound by the walls containing the network. WEP seeks to establish similar protection to that offered by the wired network's physical security measures by encrypting data transmitted over the WLAN. Data encryption protects the vulnerable wireless link between clients and access points; once this measure has been taken, other typical LAN security mechanisms such as password protection, end-to-end encryption, virtual private networks (VPNs), and authentication can be put in place to ensure privacy.

**Wi-Fi Protected Access (WPA):**

WPA or Wi-Fi Protected Access, is a Wi-Fi security standard that's intended to replace the older WEP, or Wired Equivalent Privacy. WEP was supposed to keep Wi-Fi networks secure but turned out to be very easy to break, so it's been deprecated in favor of WPA. WPA is very common; almost all Wi-Fi equipment made in the last decade supports it.

WPA makes using Wi-Fi networks more secure than leaving them unencrypted. With unencrypted Wi-Fi networks, it's possible for someone using a program called a packet sniffer to see the data coming across the network. This can include all of the web pages you're viewing, the email messages you're sending, even passwords and credit card numbers. Using encryption keeps all of this confidential information private by scrambling the plain text data, so that it looks like gibberish to an attacker.

**Wi-Fi Protected Access 2 (WPA2):**

Short for ***W***i-Fi ***P***rotected ***A***ccess ***2***, WPA2 is the security method added to WPA for wireless networks that provides stronger data protection and network access control. It provides enterprise and consumer Wi-Fi users with a high level of assurance that only authorized users can access their wireless networks. Based on the IEEE 802.11i standard, WPA2 provides government grade security by implementing the National Institute of Standards and Technology (NIST) FIPS 140-2 compliant AES encryption algorithm and 802.1x-based authentication. There are two versions of WPA2: WPA2-Personal, and WPA2-Enterprise. WPA2-Personal protects unauthorized network access by utilizing a set-up password. WPA2-Enterprise verifies network users through a server. WPA2 is backward compatible with WPA.

**3.3 Access Control**

1) Closed Network Access Control: Closed Network is a proprietary access control mechanism. With this mechanism, a network manager can use either an open or a closed network. In an open network, anyone is permitted to join the network. In a closed network, only those clients with knowledge of the network name, or SSID, can join. In essence, the network name acts as a shared secret.

2) Access Control Lists: Another mechanism used by vendors (but not defined in the standard) to provide security is the use of access control lists based on the Ethernet MAC address of the client. Each access point can limit the clients of the network to those using a listed MAC address. If a client’s MAC address is listed, then they are permitted access to the network. If the address is not listed, then access to the network is prevented.

**3.4 Analysis**

Wireless network security is easy to be installed and low cost. Also it is very easy to bring and access to the internet through wireless network. Implementing a wireless network security to any system makes sure the highest security and mobility of it. The PDR, PPDR and APPDRR models could be implemented on the systems of any corporation according to their managements and needs. Big systems need PDR (Protection, Detection, and Response) model, and gradually the medium and massive systems need PPDR (Polley, Protection, detection, and Response) and APPDRR (Analysis, Polley, Protection, Detection and Response) model.

**3.5 Cost Timing**

This research could be very much cost efficient. Although, according to the discussion above, this research need no cost until it is been implemented.

**3.6 Result**

The security model need to be dynamic as the wireless network security. The model keeps the wireless network security in basic level and also can adjust the model itself according to the network system working status. Also it needs to keep the wireless network working even under attack. So the discussed models could be applied and implemented on the system so that the network be secured and can deal with any penetration and attack.

**4 Work schedule**

|  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** |
| **Proposal Writing** |  |  |  |  |  |  |  |  |  |  |  |  |
| **Data Collection** |  |  |  |  |  |  |  |  |  |  |  |  |
| **Analysis** |  |  |  |  |  |  |  |  |  |  |  |  |
| **Report / First** |  |  |  |  |  |  |  |  |  |  |  |  |
| **Report / Final** |  |  |  |  |  |  |  |  |  |  |  |  |
| **Typing** |  |  |  |  |  |  |  |  |  |  |  |  |

**REFERENCES**

1. [**https://www.fortinet.com/resources/cyberglossary/wireless-network**](https://www.fortinet.com/resources/cyberglossary/wireless-network)
2. [**https://en.wikipedia.org/wiki/Wireless\_network**](https://en.wikipedia.org/wiki/Wireless_network)
3. [**https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network**](https://www.consumer.ftc.gov/articles/0013-securing-your-wireless-network)
4. [**https://blog.rsisecurity.com/what-are-the-different-security-protocols-for-wireless-networks/**](https://blog.rsisecurity.com/what-are-the-different-security-protocols-for-wireless-networks/)
5. [**https://searchsecurity.techtarget.com/definition/Wired-Equivalent-Privacy**](https://searchsecurity.techtarget.com/definition/Wired-Equivalent-Privacy)
6. [**https://searchnetworking.techtarget.com/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2**](https://searchnetworking.techtarget.com/feature/Wireless-encryption-basics-Understanding-WEP-WPA-and-WPA2)