Detection of tapping via wifi

Baringin Sianipar[1,*], Muhammad Zarlis[2], Benny B Nasution[3]

[1]Student of Computer Science, University of North Sumatra, Medan, Indonesia
[2]Department of Computer Science, University of North Sumatra, Medan, Indonesia
[3]Senior Lecture of Information Technology, Polytechnic Medan

*aniparbaringin87@gmail.com

Abstract. The need for cheap and efficient communication network makes wireless one that is in demand by many users to the need access information from the internet. Because wireless network has become one of the communication tools that have been used by many people who are mobile, but the techniques used to protect the security of user data is not completely secure. The steps performed in this study, the first is to scan the wireless signals in the study site using Wi-Fi Scanner tools designed by the author using Visual Studio 2013. Then do security testing against wireless network, namely through the process Scan MAC (Media Access Control) SSID (Service Set Identifier), Frequency, and encryption used in access point that the existence of bugs can be known.

1. Introduction

The development of communication technology very rapidly with the progress of the infrastructure that supports mainly communication using a wireless network.This is the one why it needs a better security to protect users from eavesdropping attacks. Where wirelesses using electromagnetic radio wave technology to communicate with the media as the transmission medium replacing a cable (wired).

Research ***Ruchir Bhatnagar and Vineet Kumar Birlayear*** **2015** "Security in Wireless Networks"that organizations that use wireless networking standard IEEE 802.11 protocol has not completely safe and still very vulnerable to attacks that cause data as well as information could be intercepted mupun in hacking. And also in Huang Zhikun 2014 study entitled "Design and Implementation of Security Network System" in the conclusion of the study said there was no guarantee of security of all kinds of theft, hacking, and the privacy of network users conceded.

In this case the author is interested in discussing the detection of eavesdropping through Wi-Fi which is focused on the data link layer and the physical layer where the data link layer has close links that cannot be removed from the physical layer to detect tapping in a network so that data, frames the entrance or the exit is not can be read or known by others. So users of wireless networks as a means of communication channels have security guarantees.

2. Literature Review

OSI reference model (Open Systems Interconnection) illustrates how information from a software application on a computer moved across a network medium to a software application in another computer. OSI reference model is conceptually divided into seven (7) layers where each layer has a specific network functions. This model was created by the International Standards Organization (ISO) as a first step toward international standardization of protocols

used in the various layers. Open Systems Interconnection can be interpreted as an open system to communicate with other systems (Stallings).

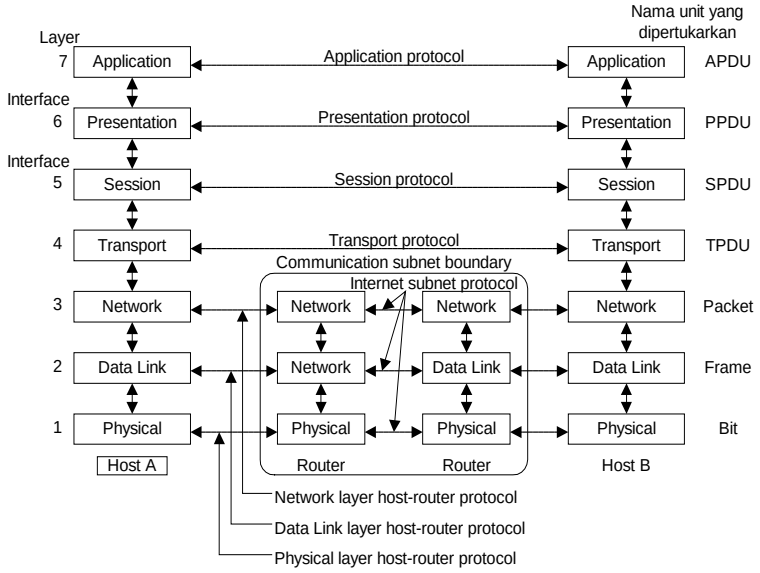


Figure 1. Osi Reference Model

2.1 Wireless LAN

Wireless Local Area Network (WLAN) is a collection of computers that are connected to one another to form a computer network using conditioned media / wave as data traffic lane. The most interesting part of course work units, namely 802.11 units responsible for the wireless LAN. This unit itself is divided again into a unit that is "really work", but now no longer with dots and numbers but with the letters a, b, c so that a unit of 802.11a, 802.11b, 802.11g, and so on , The following table Wi-Fi standard development of the times.

Table 1. Standard 802.11

802.11Protocol Group Parameters

Protocol	Release Date	Bandwidth	Max Speed
802.11	1997	2.4GHz	2Mbps
802.11a	1999	5GHz	54Mbps
802.11b	1999	2.4GHz	11Mbps
802.11g	2003	2.4GHz	54Mbps
802.11n	2009	2.4GHz/5GHz	600Mbps
802.11ac	2011.11 (Draft)	2.4GHz/5GHz	867Mbps
802.11ad	2012.12 (Draft)	60GHz	7000Mbps

Standardization of wireless 802.11 specifies that in order to join the AP network, the host should be allowed to send and receive data via the AP.

2.2 Access Point

An Access Point in Wireless Local Area Network (WLAN) at station network provider that transmits and receives data (which is usually referred to as a transceiver) of a Wireless

Local Area Network (WLAN) on one side and connected to a wired network or the other. Each access point can serve many users in the coverage area of the network, and if people move out of range limit of an Access Point, it is automatically moved to another point. Access Point is responsible for relations between the Wireless Local Area Network (WLAN). Every Access Point can support simultaneously, for many users. Adding extra Access Point is very effective to add a range of Wireless Local Area Network (WLAN).

2.3. Wireless Network Security

At this time the issue of network security becomes very important and noteworthy, networks connected to the Internet basically insecure and always can be exploited by hackers, both Local Area Network (LAN) or Wireless network. At the time the data is sent will pass through some of the terminal to reach the destination means it will give a chance to other users who are not responsible for intercepting or alter the data.

2.3.1. WEP (Wired Equivalency Privacy)

According Sopandi (2010: 126) .WEP (Wired Equivalency Privacy) is the standard used to encryption data sent over the wireless network.

2.3.2. WPA2 (Wi-Fi Protected Access2)

According to Rajab (2010). WPA2 is a new security protocol designed to fix several security vulnerabilities present in the original WPA. WPA2-Personal is one of two variations of WPA2 protocols and suitable for use in a classroom setting or home-based business; WPA2-Enterprise is also an option, although a special authentication server known as RADIUS required on WPA2-Enterprise network to function properly.

2.3.3. WPA2 / PSK (Wi-Fi Protected Access2 / *Pre Shared Key)*

According to Rajab (2010). WPA2-PSK (Wi-Fi Protected Access2 / *Pre Shared Key)*is the latest wireless security, and better than WEP and WPA-PSK, but still able to crack or intercepted but it takes a lot of time. In WPA2-PSK (Wi-Fi Protected Access2 / *Pre Shared Key)*. There are two types of decryption, the Advanced Encryption Standard (AES) and Temporal Key Integrity Protocol (TKIP).

2.3.4. MAC Address Filtering

Medium Access Control (MAC) Filtering is a wireless security system by attaching the MAC address as a key. MAC address or unique identifying address contained in any hardware connected to the network, this address is different from 1 (one) with each other. MAC Address allows devices on the network to communicate between each other.

2.4 Data Link Layer

Data-link layer (data link layer) is a layer second from bottom in the OSI model, which can convert network frames that contain data that is sent into bits of crude to be processed by the physical layer. This layer will transmit data between network devices adjacent to each other in a wide area network (WAN), or between nodes on a segment of a local area network (LAN) of the same. This layer is responsible for making frames, flow control, error control error correction and re-transmission of the frame is considered a failure. The MAC address is also implemented in this layer

3. Draft System

Here is a picture of a system design that will's working to resolve the problem.

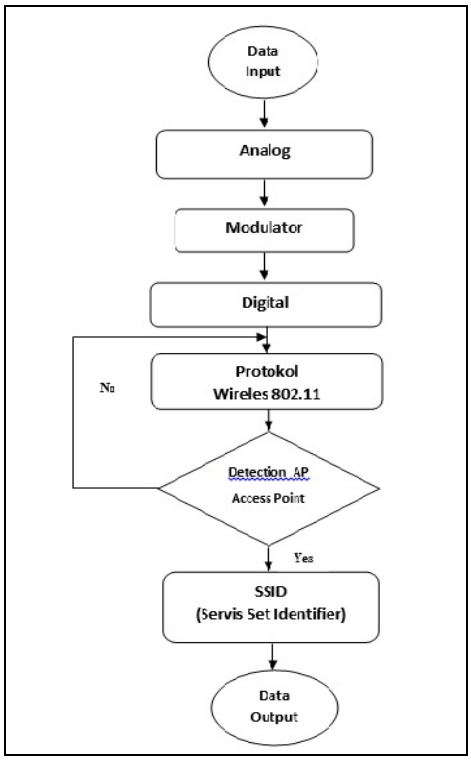


Figure 2. System Design

Based on Figure 2 begins with the initial process of data input a message to be sent, the message using analogue data into digital data will demodulator. Furthermore, the data will be entered into a wireless protocol to detect whether the data is legitimate or not to access the wireless network.

3.1 Mechanisms of Access Point (AP)

a. AP using multiple radio frequencies called channels / channel for communication with the wireless device / mobile station (STA). Access Point broadcasting / broadcast its presence on each channel with wireless transmitting short messages regularly with intervals of 10 x per second (f = 10 Hz). These messages are referred to the beacon / beacon.
b. The device must go into a frequency channel and listen to the beacon. This process is called scanning. The scanning process can be activated / accelerated by sending a request / request.
c. Device wireless station (STA) may find some access Point in large networks and should be decided access Point which are connected by a large selection of SSID, signal strength, roaming, policy protocol (security policy).
d. When the device is ready to connect to access Point, The device will send the authentication request (request) messages.
e. Access Point directly will reply by sending an authentication response (response) message.
f. The device will send an association request message. then connect to access Point and can send messages

4. Experimental Result

4.1 Tapping Mechanism

In conducting wiretaps, attackers usually do various ways to be able to enter a built-in system, one example of which is often used by the attacker to change the mac address, among others, is often called Mac Spoofing. With the following mechanism:

1. Disguise the attacker's presence in the network (Obfuscating network presence).
2. Bypass / break through security to access the device (bypass access control).
3. Imitating (Virtual) duplicate user identities in authentication (impersonate).

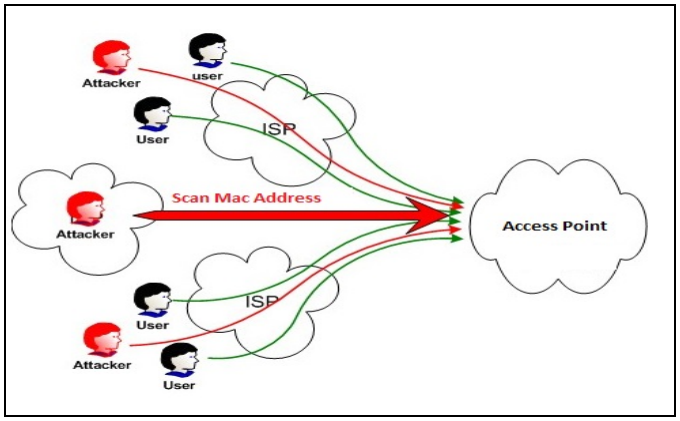
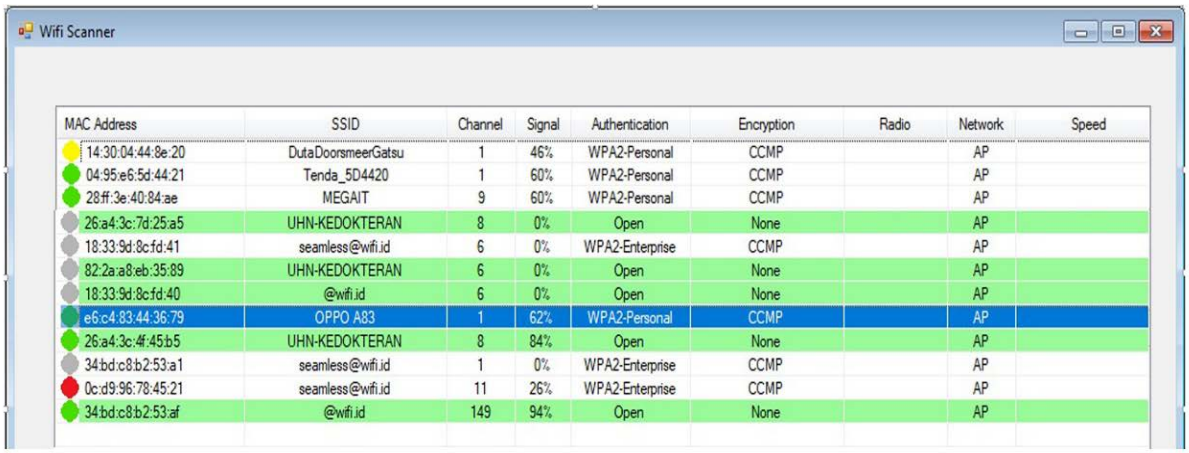


Figure 3. Mechanism Wiretapping

4.2 Research Result

This experiment was conducted to identify the presence of Access Point in the form of complete information with the name of the SSID (Service Set Identifier), Mac Address, channel, signal strength, network type and security or safety in use. This was done to facilitate the attack to get a connection with an existing wireless network. Here's a screenshot of the results of Wi-Fi scanner.



MAC Address	SSID	Channel	Signal	Authentication	Encryption	Radio	Network	Speed
14:30:04:44:8e:20	DutaDoorsmeerGatsu	1	46%	WPA2-Personal	CCMP		AP	
04:95:e6:5d:44:21	Tenda_5D4420	1	60%	WPA2-Personal	CCMP		AP	
28:ff:3e:40:84:ae	MEGAIT	9	60%	WPA2-Personal	CCMP		AP	
26:a4:3c:7d:25:a5	UHN-KEDOKTERAN	8	0%	Open	None		AP	
18:33:9d:8c:fd:41	seamless@wifi.id	6	0%	WPA2-Enterprise	CCMP		AP	
82:2a:a8:eb:35:89	UHN-KEDOKTERAN	6	0%	Open	None		AP	
18:33:9d:8c:fd:40	@wifi.id	6	0%	Open	None		AP	
e6:c4:83:44:36:79	OPPO A83	1	62%	WPA2-Personal	CCMP		AP	
26:a4:3c:4f:45:b5	UHN-KEDOKTERAN	8	84%	Open	None		AP	
34:bd:c8:b2:53:a1	seamless@wifi.id	1	0%	WPA2-Enterprise	CCMP		AP	
0c:d9:96:78:45:21	seamless@wifi.id	11	26%	WPA2-Enterprise	CCMP		AP	
34:bd:c8:b2:53:af	@wifi.id	149	94%	Open	None		AP	

Figure 4. Results Detection Wi-Fi Scanner

From Figure 5 it can be seen, the Wi-Fi signal, Mac Address, channel, encryption and signal strength can be seen in real time, and there are four (4) category signal quality ranging from excellent (in green), good (yellow), Fair (red) to very poor (grey).

Quality	Signal strength
Excellent (Green)	> 60 -100%
Good (Yellow)	< 50 - 60%
Fair (Red)	< 10 - 40%
Very Poor (Gray)	< 0 - 10%

Figure 4. Table Quality of Signals

And the picture below we can see that *mac address* can be a major clue attacker to target which will be attacked. So *mac address* can be on the track or on the block. *Mac address* which is already encoded in the above cannot be changed anymore. But many Nic driver permit change *mac address*. For the safety of the network *mac address* can be disguised. This process is called *mac* spoofing. So *mac* spoofing the goal is to change the identity of network devices / change *mac address*, if using existing topology, then that will be visible beside the AP is Mac-Address of the Wireless Client but the AP does not read IP address that can be categorized as an attacker or intruder.

	MAC Address	Client ID	Server	Active Address	Active MAC Addre...	Active Host Name	Expires After	Status
D	C0:87:EB:1B:E7:17	1:c0:87:eb:1b:e7:...	DHCP-WIFI-LT-1234	10.10.8.10	C0:87:EB:1B:E7:17	android-f1839f9e5f48783b	23:26:27	bound
D	90:32:4B:5E:7B:4D	1:90:32:4b:5e:7b:...	DHCP-WIFI-LT-1234	10.10.8.11	90:32:4B:5E:7B:4D	LAPTOP-U3H9G731	02:59:51	bound
D	0C:A8:A7:57:54:48	1:c:a8:a7:57:54:48	DHCP-WIFI-LT-1234	10.10.8.12	0C:A8:A7:57:54:48	Galaxy-Tab-A-2016-with-S-Pen	02:02:52	bound
D	20:EE:28:85:8E:0C	1:20:ee:28:85:8e:c	DHCP-WIFI-LT-1234	10.10.8.13	20:EE:28:85:8E:0C	iPhone	23:34:05	bound
D	0C:A8:A7:33:29:1A	1:c:a8:a7:33:29:1a	DHCP-WIFI-LT-1234	10.10.8.14	0C:A8:A7:33:29:1A	Galaxy-A6	22:58:22	bound
D	4C:49:E3:B5:98:03	1:4c:49:e3:b5:98:3	DHCP-WIFI-LT-1234	10.10.8.15	4C:49:E3:B5:98:03	Redmi4X-Redmi	02:02:56	bound
D	7C:F9:0E:18:90:84	1:7c:f9:e:18:90:84	DHCP-WIFI-LT-1234	10.10.8.16	7C:F9:0E:18:90:84	android-34bfd780661c53d9	02:02:44	bound
D	30:CB:F8:5A:89:43	1:30:cb:f8:5a:89:43	DHCP-WIFI-LT-1234	10.10.8.17	30:CB:F8:5A:89:43	android-a04adfcc19e07106	23:19:02	bound
D	B4:CB:57:71:D4:79	1:b4:cb:57:71:d4:...	DHCP-WIFI-LT-1234	10.10.8.18	B4:CB:57:71:D4:79	OPPO-F9	02:03:39	bound
D	EC:D0:9F:94:DB:23	1:ec:d0:9f:94:db:23	DHCP-WIFI-LT-1234	10.10.8.19	EC:D0:9F:94:DB:23	Redmi4A-hanfil123	02:06:35	bound
D	40:E2:30:70:A0:BE	1:40:e2:30:70:a0:...	DHCP-WIFI-LT-1234	10.10.8.20	40:E2:30:70:A0:BE	ASUS	04:58:36	bound
D	34:E9:11:4A:94:9B		DHCP-WIFI-LT-1234		34:E9:11:4A:94:9B	vivo-1724	Attacker	
D	20:3C:AE:83:37:24	1:20:3c:ae:83:37:...	DHCP-WIFI-LT-1234	10.10.8.22	20:3C:AE:83:37:24	iPhone	03:10:55	bound
D	00:17:C4:1B:6E:1C	1:0:17:c4:1b:6e:1c	DHCP-WIFI-LT-1234	10.10.8.24	00:17:C4:1B:6E:1C	acer-PC	04:03:14	bound
D	54:40:AD:91:F0:3F	1:54:40:ad:91:f0:3f	DHCP-WIFI-LT-1234	10.10.8.25	54:40:AD:91:F0:3F	Galaxy-Tab-S2	02:02:23	bound
D	30:CB:F8:E0:8E:F1	1:30:cb:f8:e0:8e:f1	DHCP-WIFI-LT-1234	10.10.8.27	30:CB:F8:E0:8E:F1	Galaxy-J7-2016	03:38:27	bound
D	20:F7:7C:01:96:8B		DHCP-WIFI-LT-1234	10.10.8.28	20:F7:7C:01:96:8B	vivo-1808	02:00:31	bound
D	3C:A0:67:C5:88:69	1:3c:a0:67:c5:88:...	DHCP-WIFI-LT-1234	10.10.8.29	3C:A0:67:C5:88:69	hp_pc	02:58:01	bound
D	34:E9:11:0E:58:CB		DHCP-WIFI-LT-1234	10.10.8.30	34:E9:11:0E:58:CB	vivo-1718	02:58:27	bound
D	D0:53:49:13:12:88	1:d0:53:49:13:12:...	DHCP-WIFI-LT-1234	10.10.8.32	D0:53:49:13:12:88	ASUS-PC	03:06:28	bound
D	94:D0:29:48:1B:E1	1:94:d0:29:48:1b:...	DHCP-WIFI-LT-1234	10.10.8.33	94:D0:29:48:1B:E1	android-ff972b690475fdd6	02:00:21	bound
D	34:E9:11:19:6F:55		DHCP-WIFI-LT-1234	10.10.8.34	34:E9:11:19:6F:55	vivo-1727	03:20:08	bound
D	9C:A5:C0:06:45:58		DHCP-WIFI-LT-1234	10.10.8.35	9C:A5:C0:06:45:58	vivo_V3	05:00:51	bound
D	34:E9:11:2B:44:A1		DHCP-WIFI-LT-1234	10.10.8.36	34:E9:11:2B:44:A1	vivo-1727	02:00:09	bound
D	6C:C7:EC:50:9D:03	1:6c:c7:ec:50:9d:3	DHCP-WIFI-LT-1234	10.10.8.37	6C:C7:EC:50:9D:03	Galaxy-Note9	04:56:12	bound
D	28:31:66:7D:31:DD		DHCP-WIFI-LT-1234	10.10.8.38	28:31:66:7D:31:DD	vivo-1817	04:44:33	bound
D	F0:6D:78:80:D0:47		DHCP-WIFI-LT-1234	10.10.8.39	F0:6D:78:80:D0:47	android-ae25c3c7debdbc69	02:04:55	bound
D	38:B1:DB:DA:DA:...	1:38:b1:db:da:da:...	DHCP-WIFI-LT-1234	10.10.8.41	38:B1:DB:DA:DA:...	LEnOVo-PC	03:50:37	bound
D	20:5E:F7:80:7D:18	1:20:5e:f7:80:7d:18	DHCP-WIFI-LT-1234	10.10.8.42	20:5E:F7:80:7D:18	Galaxy-J7-Prime	03:38:00	bound
D	EC:D0:9F:BE:E0:...	1:ec:d0:9f:be:e0:df	DHCP-WIFI-LT-1234	10.10.8.43	EC:D0:9F:BE:E0:...	Redmi4A-Redmi	02:00:25	bound
D	B4:CB:57:7D:46:97	1:b4:cb:57:7d:46:...	DHCP-WIFI-LT-1234	10.10.8.44	B4:CB:57:7D:46:97	OPPO-F9	21:35:24	bound
D	D0:4F:7E:90:B8:6A	1:d0:4f:7e:90:b8:6a	DHCP-WIFI-LT-1234	10.10.8.45	D0:4F:7E:90:B8:6A	Ony-Thasya	03:55:13	bound
D	30:52:CB:BC:5F:80	1:30:52:cb:bc:5f:80	DHCP-WIFI-LT-1234	10.10.8.46	30:52:CB:BC:5F:80	DESKTOP-LNJ3NUQ	04:18:20	bound
D	0C:98:38:B6:77:87	1:c:98:38:b6:77:87	DHCP-WIFI-LT-1234	10.10.8.47	0C:98:38:B6:77:87	RedmiNote5-Redmi	23:45:50	bound
D	48:88:CA:69:F9:7C		DHCP-WIFI-LT-1234	10.10.8.48	48:88:CA:69:F9:7C	android-164322fcc42928bb	23:32:37	bound

Figure 6. Attack Detection Results

Figure 6 above is the result of research in which the attacker infiltrated its way into the system without IP (internet protocol) address that is registered. And predictable user that logs are part of the intruder.

5. Conclusion

Based on the results of this research then there are some things that can be used as a conclusion that:

1. Potential burglary more vulnerable wireless LAN / bigger than any cable network (wired)

LAN, as wireless radio waves can be everywhere, cannot be regulated, sensitive to noise, beacons, and interference.

2. *Wi-Fi Scanner* an effective application for WLAN network security, and needs further development to provide security for the network use admin or client.

References

[1] Andyarunner (2013). *Definition and Objectives Multiplexing*.

[2] Forouzan, B. (2007). *Data Communications and Networking*. United States: McGraw-Hill.

[3] Hasal, Fred (1996). *Data Communication, Computer Network and Open Systems*.

[4] Jiang, P., Xia, H., He, Z. & Wang, Z. 2009 . *Design of a Water Environment Monitoring System Based on Wireless Sensor Networks*, Sensors, 9 (8), 6411-6434.

[5] Mischa Schwartz (2005) *Mobile Wireless Communication*.

[6] Nasution. B. B (2009) *Strategy to Increase Security in Transactions Wireless Culture in Society*.

[7] Narvaez, L., Perez, J., Garcia, C., and Chi, V. *Designing WLANs for VoIP* vol.7 7, July 2007.

[8] Ruchir Bhatnagar & Vineet Kumar Birla (2015) *A Literature Review Of Security In Wireless*

[9] Stallings, W. (1985) *Local Network*, MacmilLAN Publishing Company.

[10] Stallings, William, (1994) *Data and Computer Communications*, Prentice Hall.

[11] Tanenbaum, A., David, J., & Wetherall. (2011). *Computer Network*. United States: Pearson Education. Inc.