Network Administration/System Administration (NTU CSIE, Spring 2024) Homework #10

B12902110 呂承諺

May 6, 2024

1 課程內容

(a) 5 GHz Wi-Fi uses frequencies ranging from 5.15 GHz to 5.35 GHz and 5.47 GHz to 5.895 GHz. We choose 5.50 GHz as an average for calculation.

$$\lambda = \frac{c}{f} = \frac{299\,792\,458\,\text{m/s}}{5.50 \times 10^9\,\text{Hz}} = 0.0545\,\text{m} = 54.5\,\text{mm}$$

(b)

$$\frac{P_r}{P_t} = \frac{G_t G_r \lambda^2}{(4\pi d)^2} = \frac{1\,(1)\,(0.0545)^2}{(4\pi\,(1))^2} = 1.88 \times 10^{-5}$$

(c) For a certain wavelength λ, suppose only the distance changes, while all other factors remain the same.

$$P_r = \frac{P_t G_t G_r \lambda^2}{(4\pi d)^2} \propto \frac{1}{d^2}$$

This shows that both 2.4 GHz and 5 GHz signals attenuate by the same factor.

(d) Suppose the wavelength is the only changing factor.

$$P_r = \frac{P_t G_t G_r \lambda^2}{(4\pi d)^2} \propto \lambda^2$$

A 2.4 GHz wave have a longer wavelength than a 5 GHz wave, so 2.4 GHz gets a stronger signal.

(e) Bandwidth refers to the maximum data transfer rate of the connection, while throughput refers to the actual data transfer rate.

References

- Wi-Fi - Wikipedia
- List of WLAN channels - Wikipedia
- Friis transmission equation - Wikipedia
- Lecture slides "Wireless Communications & Networking" by Professor Michael Tsai, page 12
- Bandwidth (signal processing) - Wikipedia
- Bandwidth (computing) - Wikipedia
- Bandwidth & Throughput - 魂系架構 Phil's Workspace
- Network throughput - Wikipedia

2 討論題

(a)

Protocol	Cryptographic algorithm	Algorithm secure	Integrity check	Authentication methods	Possible attacks
WEP	RC4	Weak	CRC-32	64-bit key	Fluhrer, Mantin and Shamir attack
WPA	RC4+TKIP	Weak	Michael	Personal (PSK) Enterprise (802.1X)	NOMORE attack
WPA2	AES-128	Strong	CCMP		Krack attack
WPA3	AES-128 or AES-256	Strong	CCMP	Personal (SAE) Enterprise (802.1X)	FragAttacks

WEP Originally proposed to provide the same level of security as wired networks. Uses the RC4 encryption algorithm, which is insecure today.

WPA Introduces TKIP to patch the flaws in WEP due to RC4. Also adds a Message Integrity Check function named Michael. However, WPA still relies on weaknesses in WEP, making it still vulnerable to attacks.

WPA also adds enterprise mode authentication which authenticates via a 802.1X server.

WPA2 Introduces AES-128 and CCMP to replace RC4, TKIP, and Michael, enhancing security. Though attack methods have been discovered, they can be avoided by firmware updates. The cryptographic algorithms are considered strong according to today's standards.

WPA3 Further enhances security by mandating AES-128 and CCMP as the minimum encryption algorithm in WPA3-Personal, and supporting AES-256 in WPA3-Enterprise. In addition, it replaces PSK in WPA and WPA2 with SAE for more secure key exchange.

References

- Lab 10 Slides
- Wired Equivalent Privacy - Wikipedia
- Wi-Fi Protected Access - Wikipedia
- CCMP (cryptography) - Wikipedia
- FragAttacks: Security flaws in all Wi-Fi devices

(b)

Generation	IEEE 802.11 standard	Radio frequency (GHz)	Theoretical transfer speed (Mbps)	New features
Wi-Fi 5	802.11ac	5	433–6933	• Mandatory 80 MHz and optional 160 MHz channel bandwidth • 256-QAM • Up to 8 MIMO spatial streams • MU-MIMO up to 4 downlink clients
Wi-Fi 6	802.11ax	2.4 and 5	574–9608	• Orthogonal frequency-division multiple access (OFDMA) • 1024-QAM • Both downlink and uplink MU-MIMO
Wi-Fi 6E	802.11ax	6	574–9608	Wi-Fi 6 capabilities in the 6 GHz band

References

- IEEE 802.11ac-2013 - Wikipedia
- Wi-Fi 6 - Wikipedia

(c)

Frequency band (GHz)	Transfer speed	Congestion	Coverage	Ease of blockage
2.4	Slowest	Most	Best	Hardest
5	Faster	More	Better	Easier
6	Fastest	Least	Worst	Easiest

More and more applications nowadays demand higher network throughput and lower latency, which leads to the need of a broader spectrum. The 6 GHz band ranges from 5.925 GHz to 7.125 GHz, providing a wide and contiguous frequency band that supports up to 7 non-overlapping channels, making it suitable for high-throughput applications.

Also, as the number of devices have grown substantially, the 5 GHz may face congestion in populated areas. Therefore we need to open up more frequency bands to minimize congestion.

References

- 2.4 GHz vs. 5 GHz vs. 6 GHz: What's the Difference? - Intel
- 2.4 GHz vs 5 GHz vs 6 GHz WiFi: Which is Right for You?
- What Is Wi-Fi 6E? | PCMag
- Wi-Fi 6E 中的 6G 頻段介紹 - 兩倍頻寬兩倍突破 | TP-Link 台灣地區

(d)

Mode	Suitable scenarios	Reason
Standalone mode	Smaller amount of APs (e.g., home)	• No additional cost for AP controller • Easier setup
Controller mode	Larger amount of APs (e.g., business, school)	• Centralized management, e.g., possible to deploy configuration changes to lots of APs • Scalability: Easier to add new APs

3 問答題

(a) SSID

(1) SSID stands for service set identifier. It is typically the network name that users see.

BSSID stands for basic service set identifier. It is usually the MAC address of the access point.

One extended service set (ESS), identified by an SSID, may consist of one or more access points. Each access point has its own BSSID.

(2) An AP can provide service of several SSIDs simultaneously. Most home APs today can deploy a main SSID and another guest SSID. Another example is using different SSIDs for 2.4 GHz and 5 GHz signals from the same AP.

Different APs can share the same SSID. Just configure the APs to the same SSID. This is exactly how the `csie` Wi-Fi works in the department.

(3) An evil twin is a malicious Wi-Fi AP that mimics a legitimate one, often set up to have the same SSID as a public Wi-Fi and a fake login page. When a device automatically connects to the AP, the attacker can start monitoring the victim's traffic and extract sensitive information.

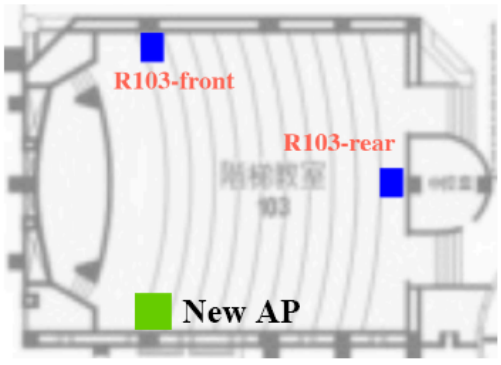
We can prevent the evil twin attack by not connecting to public or insecure Wi-Fi, and by using secure application protocols such as SSH or HTTPS.

(4) The device will often choose the AP with the best signal quality or the first one that it connected to. Standards 802.11k, 802.11v, and 802.11r facilitate transition between basic service sets.

References

- Service set (802.11 network) - Wikipedia
- Evil twin (wireless networks) - Wikipedia
- What is an Evil Twin Attack? Evil Twin Wi-Fi Explained
- Fast Roaming with 802.11k, 802.11v, and 802.11r - Windows drivers | Microsoft Learn

(b) I would place the new AP at the front-left of the classroom, as its the farthest to both existing APs.



4 實作題

The answers below are based on Windows 10.

(a) **Steps**

(1) If this is the first time connecting to the Wi-Fi, we need to create a profile in XML format. Here we use a WPA3-Personal profile as an example.

```xml
<?xml version="1.0"?>
<WLANProfile xmlns="http://www.microsoft.com/networking/WLAN/profile/v1">
  <name>Ultramarine</name>
  <SSIDConfig>
    <SSID>
      <name>Ultramarine</name>
    </SSID>
  </SSIDConfig>
  <connectionType>ESS</connectionType>
  <connectionMode>auto</connectionMode>
  <MSM>
    <security>
      <authEncryption>
        <authentication>WPA3SAE</authentication>
        <encryption>AES</encryption>
        <useOneX>false</useOneX>
      </authEncryption>
      <sharedKey>
        <keyType>passPhrase</keyType>
        <protected>false</protected>
        <keyMaterial>MY_PASSPHRASE</keyMaterial>
      </sharedKey>
    </security>
  </MSM>
</WLANProfile>
```

Then we add it to the system.

```
netsh wlan add profile filename=Ultramarine.xml
```

(2) Connect to the Wi-Fi with the following command.

```
netsh wlan connect name=Ultramarine
```

Result

```
C:\Users\user>netsh wlan connect name=Ultramarine
Connection request was completed successfully.

C:\Users\user>ping 1.1.1.1

Pinging 1.1.1.1 with 32 bytes of data:
Reply from 1.1.1.1: bytes=32 time=33ms TTL=56
Reply from 1.1.1.1: bytes=32 time=247ms TTL=56
Reply from 1.1.1.1: bytes=32 time=126ms TTL=56
Reply from 1.1.1.1: bytes=32 time=129ms TTL=56

Ping statistics for 1.1.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 33ms, Maximum = 247ms, Average = 133ms
```

References

- How to connect to a Wi-Fi network on Windows 10 | Windows Central
- How to connect to a wifi in powershell knowing the SSID and password? - Stack Overflow
- WPA2-Personal profile sample - Win32 apps | Microsoft Learn

(b) `csie` and `csie-5g` both use WPA2-Enterprise, type PEAP. This can be seen under network properties in Windows' settings.