Wi-Fi 6 환경에서의 IoT 보안 분석

김현호[1], 송종근[1*]
[1]동서대학교 소프트웨어 융합대학

Analysis of IoT Security in Wi-Fi 6

HyunHo Kim[1], JongGun Song[1*]
[1]College of Software Convergence, Dongseo University

Abstract Wi-Fi provides some low-power connection solutions that other Bluetooth cannot provide, and at the same time brings many benefits. First, there is a potentially higher data rate: it can reach 230mbps. Wi-Fi coverage is also wider than competitors, and its operating frequency is also 5GHz, which is much less congested than 2.4GHz. Finally, it also supports IP networks, which is important if you want to send data to the cloud without complexity. The 802.11ac standard of the previous generation still accounts for most shipments (80.9%) and revenue (76.2%). However, there is a limit to accepting IoT devices that will continue to increase significantly in the future. To solve this problem, the new Wi-Fi 6 standard is expected to be the solution (IEEE 802.11ax) which is quickly becoming the main driving force of the wireless local area network (WLAN) market. According to IDC market research analysts, in the first quarter of 2020, independent access points (APs) supported by Wi-Fi 6 accounted for 11.8% of shipments, but 21.8% of revenue. In this paper, we have compared and analyzed the IoT connectivity, QoS, and security requirements of devices using Wi-Fi 6 network.

- Key Words : 802.11ax, IoT, Wi-Fi6, WPA3, Wireless Network, Security

Received 09 February 2021, **Revised 28** March 2021, **Accepted** 30 March 2021

*** Corresponding Author** Jong Gun. Song, College of Software Convergence, Dongseo University, 47, Jurye-ro, Sasang-gu, Busan, Korea.
E-mail: ssongjg@dongseo.ac.kr

Ⅰ. Introduction

According to a report by Cisco [1], the number of Internet users are expected to rise from about 3.9 billion users (about 51 percent of the world's population) in 2018 to 5.3 billion users (66 percent of the world's population) by 2023. As a result, it is estimated that the number of devices connected through IP networks will be more than three times that of the world's population, and 29.3 billion network devices will be connected in 2023, up 18.3billion from 2018. Of the total, Internet of Things (IoT) connectivity's share is expected to increase from 33 percent in 2018 to 50 percent in 2023 for several 14.7 billion.

Given the change in the mobile communication environment as predicted by Cisco, mobile data traffic continues to grow globally, and the main reasons for the increase are the rise and growth of smart devices including IoT, and the increase in video viewership. For devices using this ever-increasing data traffic and IoT and other wireless networks, 802.11ac (Wi-Fi 5) has limitations in quality of service (QoS), such as security. Furthermore. more attention must be given to security for the growing number of IoT devices[2].

As standards such as those related to IoT and security requirements have begun to emerge, research [3, 4] is actively being conducted, and security measures are being prepared to ensure that IoT can be used safely.

In this paper, we compared the technical analysis of IoT connectivity, security, and QoS in Wi-Fi 6 (802.11ax) environment with IoT security requirements and evaluate the stability of IoT devices and suitability of service use in Wi-Fi 6 environment.

Ⅱ. Wi-Fi 6

Currently, Wi-Fi 4 (802.11n) and Wi-Fi 5 (802.11ac) have limitations in creating a pleasant environment in a crowded AP environment. Typically, since high-speed Gigabit Ethernet such as 5G is not fully supported in terms of speed, high-definition streaming (4K, 8K video, etc.), high-definition collaboration, wireless network-only space, and tasks in an environment with multiple access devices such as IoT are difficult to perform pleasantly. Therefore, higher speed and bandwidth are needed to solve these problems. Table 1 shows the specifications comparison of Wi-Fi (4, 5, and 6).

Table 1. Comparison of Wi-Fi 4, Wi-Fi 5, with the Wi-Fi 6 amendment[5]

Parameter	Wi-Fi 4 (802.11n)	Wi-Fi 5 (802.11ac)	Wi-Fi 6 (802.11ax)
Spectrum	2.4GHz and 5GHz	<6 GHz, excluding 2.4GHz	Between 1 and 6GHz
Bandwidth	20 to 40MHz	20 to 160MHz	20 to 160MHz
Modulation	64 QAM	BPSK to 256 QAM	BPSK to 1024 QAM
MIMO	SU	SU and DL-MU	SU and DL-UL-MU
Mechanism to reduce power consumption	NA	NA	TWT
Data rate	300 Mbps	433 Mbps (80MHz, 1 SS) 6933Mbps (160MHz, 8 SS)	600.4Mbps (80MHz, 1SS) 9607.8Mbps (160MHz, 8SS)
Backward compatibility	IEEE 802.11a/b/g	IEEE 802.11a/n	IEEE 802.11a/b/g/n/ac

Wi-Fi 6 is significantly higher in reliability, bandwidth, capacity, and functionality than Wi-Fi 5. Therefore, it is suitable for communication environments such as high-definition streaming and IoT environments where many devices are connected, and volume of data is high. In addition, in some cases, security is maintained by using separate encryption modules for each device, but many current wireless environments security use WPA2 security settings. However, since security in the case of WPA2 can eventually be cracked, wireless security in the IoT environment can be secured by using the new WPA3 rather than WPA2, to prevent cracking, eavesdropping and intrusion. Among Wi-Fi 6 technologies, Target Wake Time (TWT) is a technology for low-power devices, and the battery time of low-power devices can be expected to increase with IoT.

Wi-Fi 6 is backward compatible with all standards of 802.11a/b/g/n/ac, the introduction of 1024 QAM has increased the maximum transmission speed by 25% compared to the existing Wi-Fi 5, and regarding MIMO, the addition of uplink-MIMO to the existing Wi-Fi 5 MIMO has also reduced the probability of collision.

In Wi-Fi 6, new technologies and the new security standard WPA3 (Wi-Fi Protected Access3), were introduced to address Quality of Experience (QoE), Co-Channel Interference (CCI) and Overlapping Basic (OBSS) interference. Furthermore, the maximum transmission speed of Wi-Fi 6 supports 10Gbps, and the speed of 1Gbps can be implemented with wider coverage and lower latency.

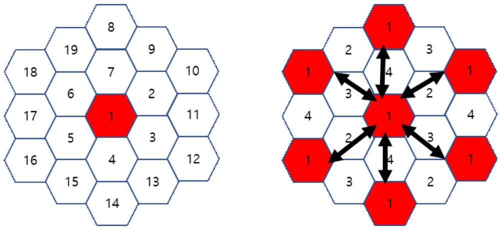

Fig. 1. Low Frequency Reuse (Left) and Increased Frequency Reuse (Right) [6]

In general, more wireless access to the AP or interference from the channel will result in lower transmission speeds and increased delay speeds. The resulting example shows that the Low Frequency Reuse to the left is free from interference when reusing a low-band (20Mhz) frequency channel as in Figure 1, and the Increased Frequency Reuse to the right shows an example of the state of interference when reusing a high-band (80Mhz) frequency channel.

2.1 WPA3

WPA3 is a new security standard that was created 14 years after WPA2 was used as the standard in 2004 and has a vulnerability to the cracking of existing traffic, one of the major problems with WPA2 security. WPA3 reinforces these areas to provide a more secure wireless network environment, and a key technology called SAE (Simultaneal Authentication of Equals) can be introduced to prevent cracking. Other major improvements in WPA3 were classified into password-based mode, open network encryption, simple connection protocols, and management frame protection [7].

The changes in WPA3 can be divided into three main categories. The first is encryption level and supports two modes. For encryption there is Enterprise and Personal mode, and the big difference between the two modes is that the encryption level for Enterprise mode is 192-bit and Personal mode is 128-bit. The second is that it has simplified the setting of security options for IoT devices.

Finally, the third point is that WPA3 supports individual encryption, making it difficult for devices to access each other's data even if they are connected to the network.

2.2 OFDMA

While traditional OFDM (Orthogonal Frequency Division Multiple) delivered only one line per client, OFDMA (Orthogonal Frequency Division Multiple Access) has significantly improved its ability to share with all clients while efficiently using multiple lines. Figure 2 below illustrates OFDM and OFDMA, and while the traditional method (OFDM) has a somewhat reduced communication environment due to inter-AP interference with limited frequencies in several APs, the interference phenomenon in OFDMA is significantly reduced, lowering the chances of communication degradation [8].

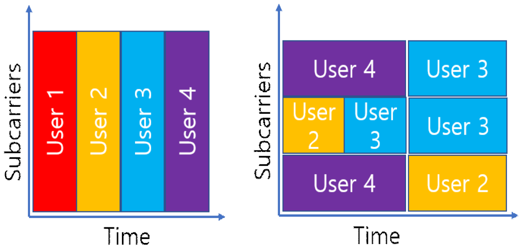

Fig. 2. OFDM(Left) and OFDMA(Right)

2.3 WPA3

Multiple Input & Multiple Output (MIMO), a multi-access (multi-user, multi-entry and output) technology, was introduced for the first time in Wi-Fi 4 (802.11n), and Multi-User Multiple Input & Multiple Output (MU-MIMO) was introduced for Wi-Fi 5 (802.11ac).

The big difference is that there are up to four channels for MU-MIMO in Wi-Fi 5, but up to eight for Wi-Fi 6, which can double the speed. Figure 3 below shows a comparison between Single User-MIMO and MU-MIMO. In Single User-MIMO, multiple terminals cannot be processed simultaneously upon request, but MU-MIMO can respond to requests from multiple terminals at the same time to ensure a pleasant network environment[9].

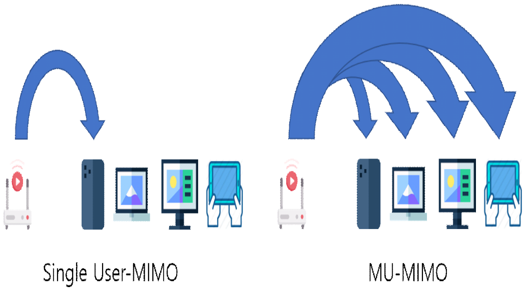

Fig. 3. Single User-MIMO and MU-MIMO

2.4 TWT(Target Wake Time)

TWT is a new technology that has emerged in Wi-Fi 6 and aims to improve the power efficiency of devices. These technologies are currently very useful in devices that utilize wireless networks such as smartphones and laptop IoT (Internet of Things) devices. The use of TWT-enabled devices allows lower power in communication than before, thus reducing unnecessary waste of power, resulting in increased battery-use time [10].

Ⅲ. IoT Security Requirements

IoT has various elements. Among them, the core elements can be classified into six categories: IoT network, cloud, user, attacker, service, and platform. Security requirements also differ for each element [11]. Table 2 below shows the six key elements of the IoT summarizing each of them.

Table 2. Explanation of six key elments in IoT

No.	Security List	Explanation
1	IoT Network	As there are no significant differences in IoT networks from existing networks, attention should be paid to issues related to the security of existing networks.
2	Cloud	Generally, most IoT devices have low power and low specifications. In other words, there is a limit to storing data, so there is a need to protect data on IoT devices by utilizing cloud backup.
3	User	The user is the most vulnerable element in terms of IoT security. The reason for this is that the security system will inevitably become vulnerable from neglect from those such as users and system managers. Therefore, they must undergo security training and conduct security inspections from time to time.
4	Attacker	No matter how well the user follows security checks and rules, attacks by attackers can cripple security. Because most IoT devices have limited resources, there is a limit to applying general security, leaving no choice but to apply a lower level of security.
5	Service	For service, the server and user provide services to each other based on trust. For a first-time user to use the service, the server must obtain consent for various uses of personal information, and the server that receives the consent provides the service to the user. If this trust is used by attackers for malicious purposes, serious problems can arise.
6	Platform	Because there are limited resources to increase the security level of IoT devices, each IoT device can selectively choose security depending on its performance. This can provide optimal security and services.

In addition to the items described in Table 1, there are many other items that require security requirements, but in order to reduce these risks, it is necessary to pay more attention to management and security checks by each security list (user, service provider, etc.) than to expect higher security levels due to the development of lightweight and IoT-related security technologies.

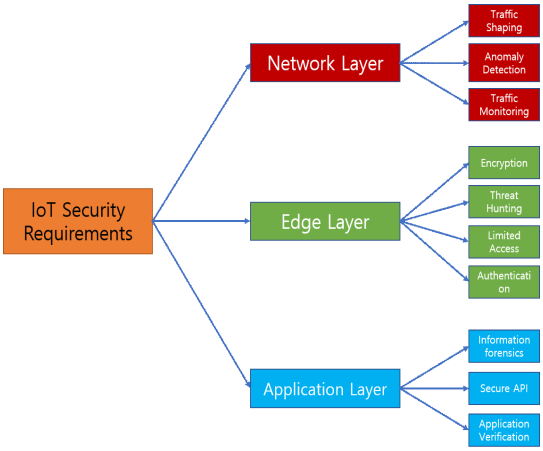

Fig. 4. IoT Security Requirments(3 Layer)[12]

Figure 4 lists IoT security requirements by 3 layers (Network, Edge, Application). There are three layers, and vulnerabilities exist in each. First, there is insufficient physical security, inadequate authentication, and energy in the Network Layer. In the Edge Layer, there are improper encryption and opening ports that are not used or needed, and finally in the Application Layer, there are inadequate patch management, weak programming, and insufficient auditing mechanisms. Table 3 lists the vulnerabilities and security requirements for each layer.

Table 3. IoT Security vulnerabilities and requirement (3 Layers)

Vulnerability	Security requirement	Architecture Layer
Deficient Physical Security	Limited Access	Edge Layer
Insufficient energy harvesting	Threat Hunting	Edge Layer
Inadequate authentication	MAF Authentication	Edge Layer
Improper encryption	Traffic Monitoring, Encrypt the payload	Network Layer
Unnecessary open ports	Traffic Monitoring, Anomaly Detection, Traffic Shaping Secure API	Network Layer
Weak programming practices	Application Verification	Application Layer
Insufficient audit mechanism	Application Layer	Application Layer
Improper patch management	Information forensics	Application Layer

Ⅳ. IoT Analysis in Wi-Fi 6

Based on the contents of chapters 2 and 3, this chapter compares and analyzes the level of guarantee in the security level of IoT devices in Wi-Fi 6 environments. Comparative analysis will determine whether safe service can be guaranteed when using IoT devices based on the main technologies of Wi-Fi 6 and security requirements and vulnerabilities of IoT devices.

First, the IoT Network can raise security levels due to WPA 3. Vulnerabilities of this such as inappropriate passwords and unnecessary open ports can be controlled to some extent through monitoring by users and administrators, but with the application of the encryption algorithm in WPA3, a higher level of security can be applied. In the Edge Layer, vulnerabilities are related to physical security, inadequate authentication, and insufficient energy. In this regard, WPA3 and TWT can be used to apply high-quality cryptographic algorithms and low-power technologies to compensate for the vulnerability. Vulnerabilities in the Application Layer include program design vulnerabilities, audit mechanisms and improper patches. These issues should be supplemented by appropriate patches as soon as vulnerabilities are discovered. Table 4 below lists such content.

Table 4. IoT Wi-Fi 6 meets the security requirements of IoT

Vulnerability	Security requirement	Wi-Fi 6, IoT Technology
Deficient Physical Security	Limited Access	WPA3
Improper encryption	Traffic Monitoring, Encrypt the payload	WPA3
Inadequate authentication	MAF Authentication	WPA3
Insufficient energy harvesting	Threat Hunting	TWT
Unnecessary open ports	Traffic Monitoring, Anomaly Detection, Traffic Shaping Secure API	Monitoring, WPA3, MU-MIMO
Weak programming practices	Application Verification	IoT S/W, Firmware
Insufficient audit mechanism	Application Layer	IoT S/W, Firmware
Improper patch management	Information forensics	IoT S/W, Firmware

As shown above in Table 4, it can be confirmed that Wi-Fi 6 meets the security requirements of IoT. Additionally, some items are expected to improve further through firmware updates for each IoT device.

Security considerations in locations such as apartments, skyscrapers, schools, and public places where wireless networks are heavily used were like those in Table 4. For service and usability, multiple terminals should be stable and not have degradation when connected to the Access Point (AP) simultaneously, and the operating range of IoT hardware and battery performance must be guaranteed especially in wide areas such as urban areas.

To Analyze these considerations, it can be said that Wi-Fi 6 is an optimized wireless network environment for IoT.

Ⅴ. Conclusions

In 2023, 66 percent of the world's population will be using the Internet, with about 3.6 devices owned per person. As a result, 14.7 billion IoT connections are expected. As such, QoS, security, and connectivity are important as the number of users continues to increase and the number of terminals and IoT devices owned per capita increases. With the appearance of Wi-Fi 6, devices with limited resources such as IoT provide a higher level of security and service and are known to be suitable for maintaining service quality as they can respond to numerous connections. This known content will be technically analyzed to analyze the security and service of IoT devices on Wi-Fi 6. Before analyzing the security of IoT devices in the Wi-Fi6 network, the introduction of new technology (WPA3, MU-MIMO, OFDMA, TWT) of Wi-Fi 6 and IoT security requirements (IoT Network, Cloud, User, etc.) were compared, and an analysis was conducted on the evaluation of Wi-Fi 6 technology related to security requirements being applied. According to the analysis, IoT devices are optimized in Wi-Fi 6 networks as they meet the technological and security requirements. The connectivity and security of IoT devices in Wi-Fi 6 networks are superior to those of previous wireless networks, and they also meet security requirements. It was suitable for the IoT network environment because it was able to respond to numerous connections with wide bandwidth and higher security level and can minimize interception of channels.

In this paper, the standard wireless network Wi-Fi (4,5 and 6) was analyzed and among them, the new technology of Wi-Fi 6 was compared and analyzed to see if it is suitable for IoT security requirements.

Although there are few issues in using Wi-Fi 4 and Wi-Fi 5 yet, many aspects such as channel interception, security, and connectivity will make it difficult to use in the future. In contrast, Wi-Fi 6 is optimized for IoT and multiple wireless network access, and through this, it is suitable for solving problems in security, connectivity, and interference. In addition, as responses to IoT security requirements have been sufficiently met, it is believed that the introduction of Wi-Fi 6 will enable a comfortable and secure wireless network for devices that require wireless networks, such as smart devices and IoT.

ACKNOWLEDGMENTS

This work was supported by the Dongseo University Research Fund of 2020. (DSU-20200018)

REFERENCES

[1] Cisco Annual Internet Report(2018-2023) (Rep.). (n.d.).

[2] Kang. B. W., Kim. S. H. (2018). A Development of Non-Invasive Body Monitoring IoT Sensor for Smart Silver Healthcare. The Korea Institute of Converence Signal Processing Quarterly, 19(1), 28-34.

[3] DeepTechHub. (n.d.). Welcome to the IoT Security Foundation. Retrieved from http://www.iotsecurityfoundation.org/

[4] Commission, I. -. (n.d.). International. Retrieved from http://www.iec.ch/

[5] RF Wireless World. (n.d.). Retrieved from https://www.rfwireless-world.com/Terminology/What-is-BSS-Coloring-in-WLAN-802-11ax.html

[6] Nam, J., Lee, J., Kwon, S., & Choi, H. (2019). Comparative Analysis on Security Protocols of WPA3 Standard for Secure Wireless LAN Environments. The Journal of Korean Institute of Communications and Information Sciences, 44(10), 1878-1887. doi:10.7840/kics.2019.44.10.1878

[7] KIM, D. S. (2018, November). Feasibility Analysis of IEEE 802.11 ax in Industrial IoT. Proceedings of Symposium of the Korean Institute of communications and Information Sciences. (pp.24-25).

[8] Farouk, N., El-Mahdy, A., & Elbakly, A. (2019, September). Two-Way DF Relaying for OFDMA System. In 2019 Signal Processing: Algorithms, Architectures, Arrangements, and Applications (SPA) (pp. 121-125). IEEE.

[9] Lee, K. H. (2019). Using OFDMA for MU-MIMO User Selection in 802.11 ax-Based Wi-Fi Networks. IEEE Access, 7, 186041-186055.

[10] Chen, Q., Weng, Z., & Chen, G. (2019). A Target Wake Time Scheduling Scheme for Uplink Multiuser Transmission in IEEE 802.11 ax-Based Next Generation WLANs. IEEE Access, 7, 158207-158222.

[11] HaddadPajouh, H., Dehghantanha, A., Parizi, R. M., Aledhari, M., & Karimipour, H. (2019). A survey on internet of things security: Requirements, challenges, and solutions. Internet of Things, 100129.

[12] Oh, S. R., & Kim, Y. G. (2017, February). Security requirements analysis for the IoT. In 2017 International Conference on Platform Technology and Service (PlatCon) (pp. 1-6). IEEE.

저자 소개

김 현 호 (HyunHo Kim)

2013년 2월 : 동서대학교 정보네트워크공학(공학사)
2015년 2월 : 동서대학교 유비쿼터스 IT(공학석사)
2020년 2월 : 동서대학교 유비쿼터스 IT(공학박사)
2020년 3월~현재 : 동서대학교 소프트웨어융합대학 초빙교수
관심분야 : 사물인터넷, 디지털포렌식, 무선보안, 네트워크 보안, 디지털신호처리

송 종 근 (JongGun Song)

2009년 2월 : 동서대학교 정보네트워크(공학사)
2011년 2월 : 동서대학교 유비쿼터스 IT과(공학석사)
2015년 8월 : 동서대학교 유비쿼터스 IT과(공학박사)
2020년 3월~현재 : 동서대학교 소프트웨어융합대학 조교수
관심분야 : 정보보안, 빅데이터 보안, 백신탐지기법, 해킹 및 방어