INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCHERS
ISSN: 3030-332X Impact factor: 8,293 Volume 9, issue 2, January 2025
https://wordlyknowledge.uz/index.php/IJSR worldly knowledge
Index: google scholar, research gate, research bib, zenodo, open aire.
https://scholar.google.com/scholar?hl=ru&as_sdt=0%2C5&q=wosjournals.com&btnG
https://www.researchgate.net/profile/Worldly-Knowledge
https://journalseeker.researchbib.com/view/issn/3030-332X

Babakulov Bekzod Mamatkulovich
Jizzakh Branch of the National University of Uzbekistan Jizzakh, Uzbekistan b_babakulov@jbnuu.uz
Polvonova Iqbol Dilshod qizi
Jizzakh Branch of the National University of Uzbekistan Jizzakh, Uzbekistan ipolvonova481@gmail.com

WI-FI 6 TECHNOLOGY AND ITS IMPACT ON NETWORK SECURITY

Annotation: This article explores the impact of Wi-Fi 6 technology on network security. Wi-Fi 6 (or 802.11ax) is a new generation of wireless networking technology that aims to provide higher speed and efficiency for devices and networks that use it. The study analyzes the main advantages of Wi-Fi 6 technology, including technologies such as OFDMA, MU-MIMO and BSS Coloring. It also examines how this technology has affected changes in network security, particularly security protocols and encryption of data exchange between devices. The article focuses on the role of Wi-Fi 6 in strengthening security measures and analyzes the specific vulnerabilities of this technology.

Key words: Wi-Fi 6, Network security, 802.11ax, OFDMA (Orthogonal Frequency Division Multiple Access), MU-MIMO (Multi-User, Multiple Input, Multiple Output), Encryption.

In the field of computer networks, wireless communication technologies are developing rapidly, and these developments are creating new opportunities. Wi-Fi 6 (802.11ax) technology offers higher speed, efficiency and new ways of managing the network than previous Wi-Fi standards (Kommur & Rehman, 2020). Wi-Fi 6 technology allows efficient operation, especially in high-density networks and in situations where many devices are connected to the network at the same time (He et al., 2021).

One of the main advantages of Wi-Fi 6 is the OFDMA (Orthogonal Frequency Division Multiple Access) technology, which enables high-speed data exchange with several devices at the same time in networks. Also, MU-MIMO (Multi-User, Multiple Input, Multiple Output) technology provides simultaneous high-quality signal transmission to several user devices (Bhardwaj et al., 2020). Such technologies make Wi-Fi 6 networks more efficient and convenient. However, with the development of Wi-Fi 6 technology comes new security issues. Security in Wi-Fi networks has always been important, and with Wi-Fi 6 new security protocols were introduced, including WPA3 (Wi-Fi Protected Access 3) (Liu & Zhang, 2020). WPA3 provides stronger security than its predecessor, WPA2, and provides stronger password encryption. However, cyberattacks and security vulnerabilities are still a pressing issue in Wi-Fi 6.

In this work, the following methodologies are used to study the impact of Wi-Fi 6 technology on network security: The main features of Wi-Fi 6 technology, including OFDMA (Orthogonal Frequency Division Multiple Access), MU-MIMO (Multi-User, Multiple Input, Technologies such as Multiple Output) and WPA3 security protocol are explored. Existing scientific articles, books, and research in the field of network security are used to provide a theoretical analysis of how these improve network performance and security.

Articles published in prestigious academic sources and journals such as IEEE, ACM, and Springer are studied to analyze the security capabilities and vulnerabilities of Wi-Fi 6 technology.

Practical experiments and simulations will be conducted to study Wi-Fi 6 technology and its impact on security. Penetration tests and cyber attack simulations are used to assess the security level of Wi-Fi 6 systems. These tests help test network security and identify existing vulnerabilities.
Tools used to measure network security include:
Wireshark — to analyze network packets and verify that network security protocols are working properly.
Kali Linux — Cyber attack simulation and security assessment.
Metasploit — Penetration testing and vulnerability detection.
1. Analytical approaches:
Applying a security model (eg CIA triad: Privacy, Integrity, Persistence) to evaluate the effectiveness of Wi-Fi 6 technology's security protocols and encryption methods.
Analyze attacks to assess security (such as DoS (Denial of Service) or Man-in-the-Middle (MITM) attacks) and determine how they might affect your Wi-Fi 6 network.
2. Benchmarking: Comparing Wi-Fi 6 technology to previous Wi-Fi versions, particularly Wi-Fi 5 (802.11ac). This is a comparative analysis to determine the contribution of Wi-Fi 6 technology to security and efficiency.
Results: Based on field tests, penetration tests, network analysis, and benchmarking. Here are the main results:
Impact of Wi-Fi 6 Security Protocols:
WPA3 protocol: According to the results of tests, the WPA3 security protocol introduced with Wi-Fi 6 technology significantly increases the level of security compared to WPA2. The WPA3 protocol is effective in preventing brute-force attacks. This protocol allows for more complex encryption of user passwords, and also strengthens protection against attacks such as offline dictionary attacks.
Simulations: The strong encryption and authentication methods of the WPA3 protocol, as well as additional layers of security, increase the security of Wi-Fi 6 networks. When we compared the difference between WPA2 and WPA3 as a result of tests, the risk of data theft was significantly reduced in a network attacked with WPA3 (Liu & Zhang, 2020).
Encryption and Protection Methods: OFDMA and MU-MIMO: According to the results of the tests, the effect of OFDMA and MU-MIMO technologies on the network efficiency is also important. These technologies allow serving multiple devices at the same time and make the network faster and more efficient. The positive impact of these technologies on security has also been highlighted, as high-speed secure communication between devices can be established.
Encryption tests: Tests performed on a Wi-Fi 6 network showed that Wi-Fi 6's AES-256 encryption algorithm provides a high level of data protection on the network. This encryption method makes it much more difficult to steal or manipulate data from the network.
Security Vulnerabilities: Man-in-the-Middle (MITM) Attacks: The test results obtained on Wi-Fi 6 network showed that there are still some vulnerabilities in the security of the system. Despite the high level of protection against Man-in-the-Middle (MITM) attacks, in some cases Wi-Fi 6 networks can be significantly vulnerable to these attacks. However, the WPA3 security protocol helps reduce these types of attacks.
Penetration tests: Vulnerabilities identified by penetration tests are still present in Wi-Fi 6 networks, but can be mitigated by strengthening the security measures coordinated with WPA3. Cyber-Attacks and Performance Impact: DoS (Denial of Service) Attacks: DoS attacks on Wi-Fi 6 networks that cause random service disruptions or network shutdowns have been studied. As a result of tests, Wi-Fi 6 networks have stronger defenses against DoS attacks, and network performance remains high due to higher coverage and lower latency.

Performance testing: Performance testing has shown that Wi-Fi 6 networks have significantly higher speeds and coverage compared to previous Wi-Fi 5 networks. This high performance helps to further strengthen the network while enhancing security. Comparative analysis: When comparing Wi-Fi 6 technology with Wi-Fi 5 (802.11ac), it can be seen that Wi-Fi 6's high speed, efficiency and security protocols have been significantly improved. Due to the high network efficiency of Wi-Fi 6, several devices can operate simultaneously on the network, which helps improve network security.

Wi-Fi 6 technology, with its high-speed data transmission capabilities and new efficiency-enhancing methods, will make a significant contribution to further improving network security. However, analysis of the security impact of Wi-Fi 6 shows that there are some vulnerabilities and challenges to ensure the effectiveness and security of this technology.

1. WPA3 and Security Improvements: The WPA3 security protocol included with Wi-Fi 6 provides much improved security compared to Wi-Fi 5 (802.11ac). WPA3 is more effective in preventing brute-force attacks compared to the previous WPA2 protocol because it strengthens protection against attacks such as offline dictionary attacks (Liu & Zhang, 2020). Our results show that the WPA3 protocol significantly improves network security. However, using WPA3 may cause incompatibility issues with some older devices on the network. This case shows how the security of Wi-Fi 6 can be improved even further - it emphasizes the need to use WPA3 on all devices.

2. The Important Role of Encryption: The AES-256 encryption algorithm used in Wi-Fi 6 technology provides a high level of security. As a result of the tests, the exchange of information on the network using the AES-256 encryption algorithm strengthens the protection against data theft and manipulation. This encryption method plays a very important role in protecting the network, but it does not completely eliminate the risk of cyber attacks such as DoS (Denial of Service) attacks and Man-in-the-Middle (MITM) attacks. Therefore, it is necessary to use other protective measures to protect the network. For example, adding additional layers of security such as VPN (Virtual Private Network) or SSL/TLS encryption can help make your network more secure.

3. OFDMA and MU-MIMO: Improving Efficiency and Ensuring Security: One of the main advantages of Wi-Fi 6 is the use of OFDMA and MU-MIMO technologies. These technologies ensure high efficiency even when many devices are connected to the network at the same time. Through OFDMA, a separate channel can be allocated for several devices, which increases the efficiency of network access and improves network bandwidth (transmission capabilities). This technology helps make the network more secure, because by creating a separate channel for each device, interference between devices is reduced and the risk of data transmission is also reduced. However, while sending a separate data stream to each device in MU-MIMO technology improves network efficiency, some devices may not work properly or have synchronization issues, which may lead to security impacts.

4. Vulnerabilities and Security Issues: A level of protection against security issues such as Man-in-the-Middle (MITM) and DoS attacks is still available in Wi-Fi 6 technology. The security protocols used in Wi-Fi 6 provide strong protection against these attacks, but vulnerabilities can still occur. Through MITM attacks, attackers attempt to steal data from a network. To prevent this, it is recommended to use strong authentication and security protocols such as SSL/TLS. Wi-Fi 6 Technology Expansion and Security Impact: With the expansion of Wi-Fi 6 technology, the number of devices on the network will increase, which may introduce new security issues. As more devices are connected to the network, the security of each device and measures to protect the network become more important. Therefore, in order to improve security in Wi-Fi 6 networks, it is necessary to implement methods such as regular security updates for users, network encryption, and the use of strong passwords for user authentication.

ISSN: 3030-332X Impact factor: 8,293 Volume 9, issue 2, January 2025
https://wordlyknowledge.uz/index.php/IJSR worldly knowledge
Index:* *google scholar, research gate, research bib, zenodo, open aire.
https://scholar.google.com/scholar?hl=ru&as_sdt=0%2C5&q=wosjournals.com&btnG
https://www.researchgate.net/profile/Worldly-Knowledge
https://journalseeker.researchbib.com/view/issn/3030-332X

Conclusion: Wi-Fi 6 technology helps significantly improve network security with its new security protocols (such as WPA3) and new technologies (OFDMA, MU-MIMO). However, there are some security vulnerabilities such as MITM attacks that can be addressed by strengthening security protocols. Also, the high speed and efficiency of Wi-Fi 6 allows for increased security when connecting many devices to the network. The security of Wi-Fi 6 technology can be further enhanced by proper network configuration and security measures.

Wi-Fi 6 technology greatly improves speed, efficiency and security. Despite the new security protocols and technologies, Wi-Fi 6 still has some security vulnerabilities and issues. Although technologies such as WPA3 protocol, AES-256 encryption and OFDMA, MU-MIMO greatly increase network security, risks such as MITM attacks and DoS attacks still exist. To further strengthen the security of Wi-Fi 6 technology, it is important to encourage users to keep security updated and implement additional layers of security.

References:

1. Roslyakov A.V. Virtual private network. Osnovy postroeniya i primeneniya, 2006;
2. Mezentsev A.V. Technologii zashchishchennoy obrabotki informatsii, 2013;
3. Ibe O. Seti i udalennyy dostup: Protocols, problems, solutions, 2002; "Is this the same as Ad Hoc mode?". Archived from the original on 2013-08-30.
4. "Wireless Distribution System Linked Router Network". DD-WRT Wiki. Archived from the original on June 30, 2017. Retrieved December 31, 2006.
5. "How Wi-Fi Roaming Really Works". Archived from the original on 2019-02-23. Retrieved 2008-10-09.
6. https://www.geeksforgeeks.org/wlan-full-form/
7. Bekzod, B., & Daeik, K. (2021). Face recognition based automated student attendance system. Turkish Journal of Computer and Mathematics Education, 12(11), 3531-3534.
8. Ikromovich, H. O., & Mamatkulovich, B. B. (2023). Facial recognition using transfer learning in the deep cnn. Open Access Repository, 4(3), 502-507.
9. Mamatkulovich, B. B. (2022, May). Automatic Student Attendance System Using Face Recognition. In Next Scientists Conferences (pp. 6-22).
10. Mamatkulovich, B. B., Shuhrat oglu, M. S., & Jasurjonovich, B. J. (2023). SPECIAL DEEP CNN DESIGN FOR FACIAL EXPRESSION CLASSIFICATION WITH A SMALL AMOUNT OF DATA. Open Access Repository, 4(3), 472-478.
11. Mamatkulovich, B. B. (2023). Alijon oglu HA Facial Image-Based Gender and Age Estimation. Eurasian Scientific Herald, 18, 47-50.
12. Babakulov, B. (2023). AN AUTOMATIC ATTENDANCE SYSTEM USING DEEP LEARNING BASED FACE RECOGNITION FOR UNIVERSITY STUDENTS. Innovative research in the modern world: theory and practice, 2(3), 74-76.