International Journal on Perceptive and Cognitive Computing (IJPCC) Vol 10, Issue 2 (2024)
https://doi.org/10.31436/ijpcc.v10i2.488

Next-Generation Hotspot (NGH): Advancing Automatic Roaming and Seamless Wi-Fi Network Logins

Zainab S. Attarbashi[1], Atikah Balqis Binti Basri[1], and Shayma Senan[2]
[1]Department of Computer Science, International Islamic University Malaysia, Gombak, Malaysia.
[2]Electrical and Computer Engineering Department, International Islamic University Malaysia, Gombak, Malaysia.

*Corresponding author Zainab_senan@iium.edu.my

(Received: 20th June 2024; Accepted: 8th July 2024; Published on-line: 30th July 2024)

Abstract— In an increasingly connected world, Wi-Fi hotspots play an important role in ensuring continuous and reliable internet access for users and devices. Next-Generation Hotspot (NGH) technology has been introduced to decrease the possibility of multiple authentications for users because it uses the network providers to exchange the user authentication and it will be the upgraded version of Hotspot 2.0. NGH addresses the growing challenges of Wi-Fi connectivity, such as network congestion, security vulnerabilities, and complex authentication processes. As the demand for wireless access increases, NGH uses advanced features like Passpoint standards and IEEE 802.1x protocols to offer seamless, one-time authentication across multiple networks. This article provides an overview of NGH, focusing on its ability to enhance user experience by simplifying login procedures and improving security. By investigating the limitations and reasons why this NGH technology is being used, as well as security-related topics that concern the user. It also explains the benefits of NGH, this research highlights its potential to revolutionize wireless communication, offering valuable insights for service providers and the network industry to optimize and innovate future Wi-Fi solutions.

Keywords— Next-Generation Hotspot, Passpoint, authentication, seamless WiFi.

I. Introduction

In the era where seamless connectivity is essential, the role of Wi-Fi hotspots has become increasingly critical in maintaining uninterrupted internet access for both users and devices. As the demand for reliable and widespread wireless connectivity continues to increase, Next-Generation Hotspot (NGH) [1] technology became as an important advancement that is building upon the existing Hotspot 2.0. NGH aims to address key challenges associated with Wi-Fi connectivity, such as network congestion, security vulnerabilities, and complex authentication processes.

The evolution of Wi-Fi technology emphasizes its growing importance and capability. From the early days of Wi-Fi 802.11b, which offered basic wireless connectivity, to the advent of Wi-Fi 5 (802.11ac) with its significant improvements in speed and capacity. The latest advancements, such as Wi-Fi 6 (802.11ax) and the emerging Wi-Fi 7 (802.11be), promise even greater enhancements in speed, efficiency, and handling of multiple devices as summarized in table 1.

However, the current technology is challenged by complex logins and limited roaming [2]. These limitations disrupt connectivity and restrict user experience, especially in areas with frequent network handovers. Complex logins require unnecessary input of complex passwords, wasting valuable time and disrupting user flow [1]. Traditional Wi-Fi networks function as isolated entities, requiring manual reconnection and re-authentication when transitioning between hotspots. This disrupts ongoing activities and decreases productivity, creating a disjointed experience.

TABLE I
COMPARISON BETWEEN DIFFERENT WIFI TECHNOLOGIES

Feature	Wi-Fi 4	Wi-Fi 5	Wi-Fi 6	Wi-Fi 7
Standard	802.11n	802.11ac	802.11ax	802.11be
Frequency Bands	2.4 GHz, 5 GHz	5 GHz	2.4 GHz, 5 GHz	2.4 GHz, 5 GHz, 6 GHz
Max Speed	600 Mbps	3.5 Gbps	9.6 Gbps	30 Gbps
Channel Bandwidth	20, 40 MHz	20, 40, 80, 160 MHz	20, 40, 80, 160 MHz	20, 40, 80, 160, 320 MHz
MIMO	Up to 4x4	Up to 8x8	Up to 8x8	Up to 16x16
Latency	Higher	Lower	Lower	Lowest

Next-Generation Hotspot (NGH) addresses these limitations by introducing automatic roaming and seamless logins [3]. This is achieved through innovative technologies like WiFi certified Passpoint, which automatically connects users to authorized networks without manual logins.

The Wi-Fi Certified Passpoint Program, commonly referred to as 'Passpoint' (or 'Hotspot 2.0') [4], was developed to address the limitations in seamless interworking between WiFi networks and mobile cellular networks, as well as among Wi-Fi hotspots themselves. Prior to Passpoint, Wi-Fi technology struggled with smooth transitions between networks and hotspots, creating a fragmented user experience. The Passpoint initiative aims to integrate Wi-Fi networks as a seamless extension of service provider networks, enabling users to transition effortlessly from one hotspot to another, like the seamless handovers experienced in cellular networks. Passpoint technology facilitates all control-plane functions required for automated and uninterrupted connectivity to Wi-Fi hotspots. Through Passpoint, service providers can utilize advanced Wi-Fi systems to offload traffic and offer high-bandwidth services, while subscribers benefit from reduced frustration and enhanced performance compared to traditional Wi-Fi hotspots. NGH also utilizes the latest security standards like WPA3 to secure data. Figure 1 compares traditional hotspots and NGH across different categories such as authentication, security, and user experience.

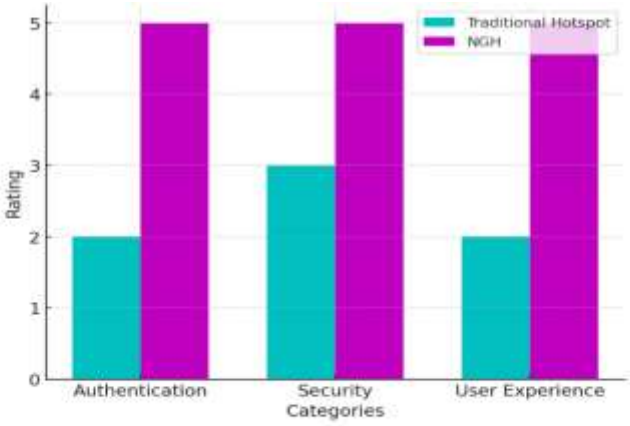

Fig 1. Comparison between traditional hotspot vs. NGH

In NGH, Passpoints can detect nearby Wi-Fi networks and immediately connect to the one for which the user has authorization. The second key benefit of Passpoint is enhanced security. Passpoint networks provide a higher level of security than standard Wi-Fi networks since they require the use of the enterprise-grade WPA2 security protocol for wi-fi access. The third advantage that Passpoint provides is seamless roaming across multiple WiFi networks of the same organization or partner networks without the requirement to maintain the SSID name consistent throughout the networks. It also eliminates the need for MAC addresses for visitor recognition and authentication, making it a future-proof solution for MAC randomization threats [5]. Users will register once for the NGH and download a secure password profile to their device via a variety of out-of-band mechanisms. When users return to or visit any of the brand's or partner's locations, they will be immediately connected to Wi-Fi via a safe and encrypted connection.

NGH outperforms the previous ones when it comes to issues such as efficiency and reliability during congestion or overloads as figure 2 showing the multiple steps involved in the traditional authentication process versus the one-time authentication process of NGH.

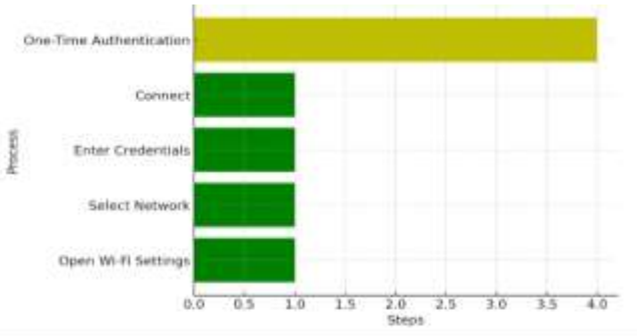

Fig 2. Steps for traditional authentication process

Another key development is beamforming. Unlike conventional signals that are broadcast in the general direction, beamforming allows an individual hotspot to direct the signals to each device connected to it. Narrow-based signal transmission is very reliable, fast, and can be extended far enough for longer distances. Also, Orthogonal Frequency Division Multiple Access (OFDMA) which allows dividing the available frequencies into small sub-channels for use by separate devices. They improve spectrum usability, reduce latency, and increase performance generally within congested areas.

II. Related Works

The development and deployment of Hotspot 2.0, also and Next-Generation Hotspot (NGH) technologies made significant advancements in enhancing Wi-Fi connectivity and user experience. These technologies aim to address longstanding challenges associated with seamless network access, user authentication, and efficient integration with cellular networks. As the demand for reliable and continuous wireless access increases, recent research has focused on evaluating the performance, security, and overall impact of these technologies on modern Wi-Fi networks. Table 2 provides a summary of recent studies related to Passpoint and NGH technologies, highlighting key findings and areas of focus. This overview includes performance evaluations, security considerations, and the impact of these technologies on both service providers and end-users.

TABLE III
SUMMARY OF RELATED WORKS

Ref.	Title	Key Findings
[6]	Analysis of multiple access methods of modern Wi-Fi networks	Provides a comparative analysis of various access methods in contemporary Wi-Fi networks and their effectiveness.
[7]	Automatic Roaming Consortium Discovery and Routing for Inter-federation Wireless LAN Roaming System	Investigates automatic discovery and routing methods for inter-federation roaming in wireless LANs.
[8]	DVB-NGH: The Next Generation of Digital Broadcast Services to Handheld Devices	Discusses advancements in DVB-NGH for digital broadcasting to handheld devices and its implications for wireless communication.
[9]	Wi-Fi 7: The Next Frontier in Wireless Connectivity	Describes new features in Wi-Fi 7, including Multi-Link Operation (MLO), and their impact on performance.
[10]	DOLOS: Tricking the Wi-Fi APs with Incorrect User Locations	Wi-Fi user location privacy by creating ambiguity in location estimates, significantly degrading the accuracy of state-of-the-art localization systems without compromising Wi-Fi communication performance.
[11]	Challenges and Opportunities of 5G Network: A Review of Research and Development	Explores the potential benefits and challenges of integrating Passpoint with 5G technology.
[12]	A Review of Wi-Fi 6 : The Revolution of6th Generation Wi-Fi Technology	Reviews key enhancements in Wi-Fi 6, including efficiency and high-speed capabilities.

III. ADVANTAGES OF NEXT-GENERATION HOTSPOT

NGHs provide significant advantages over traditional Wi-Fi networks by automating the roaming and login processes. These advantages can be divided into three categories:

A. Improved User Experience

- *Seamless Connectivity:* Users can move between access points with uninterrupted connectivity, eliminating the need to manually search, select, and enter passwords for each network. This improves the overall user experience significantly, especially in dynamic environments such as airports, train stations, and shopping malls.
- *Reduced Frustration:* Manual password entry on mobile devices can be time-consuming. Automatic logins minimize the problem by allowing users to connect to Wi-Fi networks quickly and easily.
- *Increased Efficiency:* Automatic roaming saves users time by eliminating the need to reconnect to a new network each time they move. This improves overall efficiency and productivity, especially for mobile users.

B. Enhanced Security

- *Reduced Risk of Password Theft:* Manually entered passwords on public Wi-Fi networks are vulnerable to interception and theft. Next-Generation Hotspots (NGHs) utilize secure protocols for credential transmission, thereby mitigating the risk of unauthorized access and password breaches [14].
- *Enhanced Network Security:* NGHs can implement more stringent security measures and authentication methods, such as WPA2/WPA3 enterprise security, which offer superior protection against cyberattacks compared to traditional open Wi-Fi networks [11].
- *Centralized Credential Management:* With NGHs, user credentials are managed centrally through automatic logins. This approach simplifies the process of updating and revoking access, thereby strengthening overall network security.

C. Network Management Optimization

- *Decreased Administrative Burden: The elimination of manual configuration and troubleshooting tasks reduce the workload on IT personnel, thereby enhancing the efficiency of network management [12].*
- *Enhanced Network Performance:* *NGHs can dynamically allocate resources and prioritize user traffic based on location and usage patterns. This optimization improves overall network performance and ensures a stable, high-quality connection for all users.*

IV. IMPLEMENTATION ISSUES

Next-generation hotspots (NGH) may have replaced the current Hotspot 2.0, which implements Hotspot 2.0 into a real network. Users seem to favor WiFi over hotspots due to the coverage area, and taking over the mobile network will strain the users' mobile phones. Even with such advancements in the network, there are some weaknesses and limitations where the system is not immune to any threats and attacks from outside of the network due to the behavior of the hotspot:

A. Cost of Implementation

The usage of hotspots is widespread across the technology world as every service provider has expanded to provide wide coverage to public places. For the user to experience full coverage of the Next-Generation Hotspot, service providers need to lay out plans for implementing the Next-Generation Hotspot (NGH), which would definitely be costly due to the high demand from the users [13]. Due to the technological advancement of the Next-Generation Hotspot (NGH), they cost more due to the use of a wireless 5G network.

The other reason for it to cost more than the current network is maintenance, where every service provider will offer users higher speed and network efficiency than before, which logically will cost more to upgrade to better performance with the help of network technical experts.

B. *Speed of Connectivity*

In general, hotspot connectivity is depending upon the strength of the wireless network signal within the coverage area provided by the service provider. Consequently, regions with suboptimal signal reception, regardless of the network, may experience slower connection speeds.

As the Next-Generation Hotspot (NGH) technology becomes widely adopted, it is anticipated to achieve a level of integration similar to established network standards such as 4G and 5G. Currently, 5G provides the highest data rates and increased network capacity; however, once NGH reaches global normalization, managing the growing number of users and devices on the same network standards may present challenges. Technical expertise indicates that electronic devices in proximity to network equipment can contribute to connectivity issues, as interference from radio signal noise can degrade NGH performance [14].

C. *Device Compatibility*

Although the recent use of 5G networks has enhanced connectivity speeds and efficiency, Wi-Fi connections remain competitive in terms of performance. However, the transition to 5G presents compatibility challenges, as not all devices support this new standard. The new mobile phones manufactured subsequently are compatible with 5G, while older models are not, resulting in network compatibility issues.

Outdated software and devices can make additional challenges for the implementation of Next-Generation Hotspot (NGH) technology. To ensure seamless integration and functionality, both user devices and hotspot networks must be capable of updating to support NGH. This ensures that users can access the network effectively, similar to other users with updated equipment.

V. SECURITY CHALLENGES ON NEXT- GENERATION HOTSPOT (NGH)

There are some security challenges associated with implementing NGH, including vulnerabilities in authentication processes, data protection issues, and the potential for misuse:

A. *Vulnerabilities in Authentication Processes*

One of the main security challenges in NGH systems is ensuring robust authentication mechanisms. NGH technology relies on advanced authentication protocols, such as Passpoint, to enable seamless connectivity. While these protocols are designed to enhance user convenience by minimizing manual logins, they also introduce potential vulnerabilities.

For example, the automated authentication process can be vulnerable to man-in-the-middle (MitM) attacks if the initial certificate exchange or credential verification is compromised. Attackers could exploit weaknesses in the handshake or certificate validation processes to gain unauthorized access to the network. Moreover, if the credentials are intercepted or stolen, unauthorized users could potentially access sensitive information or exploit network resources [15].

B. *Data Protection and Privacy Concerns*

Data protection and user privacy represent significant concerns in NGH systems. NGH technology enables seamless connectivity by exchanging user credentials and session information between networks. While this facilitates a user-friendly experience, it also raises issues regarding the protection of sensitive data.

The transmission of user credentials and session data across multiple networks can expose this information to interception or unauthorized access if encryption protocols are not adequately implemented. Furthermore, the centralization of user data for seamless authentication increases the risk of data breaches, where attackers could potentially access large volumes of user information from a single compromised database [16].

C. *Potential for Misuse and Exploitation*

The widespread adoption of NGH technology could also lead to potential misuse and exploitation. As NGH systems streamline network access, they unintentionally create opportunities for malicious actors to exploit network resources. For example, attackers could exploit vulnerabilities in the NGH infrastructure to launch denial-of-service (DoS) attacks or disrupt network services.

Additionally, the seamless nature of NGH connectivity could facilitate unauthorized access to restricted or sensitive areas within a network. Without adequate security measures, attackers could leverage the ubiquitous connectivity to bypass security controls or gain unauthorized access to protected resources [15].

D. *Challenges in Securing Roaming and Interoperability*

NGH technology supports interoperability and seamless roaming across different network operators. However, this very capability caused security challenges. Ensuring secure communication and data integrity between different network domains requires robust interoperability protocols and encryption standards. The lack of standardization or inconsistent implementation across networks can create vulnerabilities that attackers might exploit.

VI. MITIGATION STRATEGIES

Addressing these security challenges requires a multi-faceted approach:

A. Enhanced Authentication Protocols: Implementing stronger authentication protocols and encryption standards can mitigate the risk of unauthorized access and data interception. Regular updates and security patches are essential to address vulnerabilities in authentication mechanisms.

B. Robust Data Encryption: Ensuring end-to-end encryption for data transmissions and user credentials can protect against interception and unauthorized access. Encryption standards should be regularly reviewed and updated to address emerging threats.

C. Network Monitoring and Intrusion Detection: Deploying comprehensive network monitoring and intrusion detection systems can help identify and respond to suspicious activities or security breaches in real time.

D. Standardization and Collaboration: Developing and adhering to standardized security protocols across different network operators and NGH systems can enhance interoperability and reduce security vulnerabilities. Collaboration among industry stakeholders is crucial to establishing and enforcing these standards.

VII. CONCLUSION

In conclusion, Next-Generation Hotspot is a significant advancement in Wi-Fi technology. While there are challenges, collaborative efforts among network providers, technology developers, and users will drive NGH adoption and optimization. Continuous research and development are critical to addressing security concerns and ensuring NGH's long-term success.

Despite these challenges, the potential benefits of NGH outweigh the disadvantages. Both users and network operators benefit from the seamless user experience, enhanced security features, and dynamic resource allocation capabilities. Additionally, NGH-enabled new applications such as AR/VR experiences and remote healthcare have the potential to revolutionize many aspects of our lives.

ACKNOWLEDGMENT

The authors hereby acknowledge the review support offered by the IJPCC reviewers who took their time to study the manuscript and find it acceptable for publishing.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest

REFERENCES

[1] E. Yanmaz, "Next Generation Hotspot (NGH) – A Wi-Fi Roaming Solution," International Journal of Advanced Computer Science and Applications, vol. 13, no. 5, pp. 123-132, 2022.

[2] P. Morgado, L. Santos, and J. Pereira, "Next Generation Hotspot: A Review of the Technology and its Future," IEEE Access, vol. 11, pp. 36485-36502, 2023.

[3] Y.-H. Chiu, C.-C. Wang, and C.-F. Lin, "Performance evaluation of Wi-Fi roaming in Next-Generation Hotspot (NGH) with multi-operator environment," Journal of Network and Computer Applications, vol. 228, p. 104413, 2023.

[4] S. Hoteit, S. Secci, G. Pujolle, A. Wolisz, C. Ziemlicki, and Z. Smoreda, "Mobile data traffic offloading over Passpoint hotspots," Computer Networks, vol. 84, pp. 76-93, 2015.

[5] S. Gupta, M. K. Mishra, and S. Srivastava, "A survey on next-generation hotspot (NGH): A step towards seamless and ubiquitous Wi-Fi experience," Computer Networks, vol. 193, p. 108132, 2021.

[6] Zh. Ismagulova and E. Seidulla, "Analysis of multiple access methods of modern Wi-Fi networks," Q A Iasaýı atyndaǵy Halyqaralyq qazaq-túrik ýnıversıtetiniń habarlary (fızıka matematıka ınformatıka serııasy), vol. 24, pp. 116-128, 2023.

[7] K. Irie and H. Goto, "Automatic Roaming Consortium Discovery and Routing for Inter-federation Wireless LAN Roaming System," Journal of Information Processing, vol. 28, pp. 378-386, 2020.

[8] D. Gomez-Barquero, C. Douillard, P. Moss, and V. Mignone, "DVB-NGH: The Next Generation of Digital Broadcast Services to Handheld Devices," IEEE Transactions on Broadcasting, vol. 60, pp. 246-257, 2014.

[9] A. S. George, A. S. H. George, and T. Baskar, "Wi-Fi 7: The Next Frontier in Wireless Connectivity," Partners Universal International Innovation Journal (PUIIJ), vol. 01, no. 04, pp. 133–145, 2023.

[10] J. Deposada, "Exploring hotspot 2.0 - Fon: The global WIFI Network," Fon, May 28, 2018.

[11] N. Sahu and R. Sahu, "Challenges and Opportunities of 5G Network: A Review of Research and Development," American Journal of Electrical and Computer Engineering, vol. 8, pp. 11-20, 2024.

[12] S. George and A. S. George, "A Review of Wi-Fi 6 : The Revolution of 6th Generation Wi-Fi Technology," Research Inventy: International Journal of Engineering and Science, vol. 10, no. 09, pp. 56–65, 2020.

[13] K. Poularakis, G. Iosifidis, and L. Tassiulas, "Joint Deployment and Pricing of Next-Generation WiFi Networks," IEEE Transactions on Communications, vol. PP, pp. 1-1, 2019.

[14] A. H. Khoula, N. Shah, and A. N. S. Shankarappa, "Smartphone's hotspot security issues and challenges," in 2016 11th International Conference for Internet Technology and Secured Transactions (ICITST), 2016, doi: 10.1109/icitst.2016.7856680.

[15] L. Suárez-Plasencia, C. M. Legón, J. Herrera, R. Socorro, O. Rojas, and G. Sosa Gómez, "Weak PassPoint Passwords Detected by the Perimeter of Delaunay Triangles," Security and Communication Networks, vol. 2022, pp. 1-14, 2022.

[16] J. Herrera, C. M. Legón, L. Suárez-Plasencia, R. Luis, O. Rojas, and G. Sosa Gómez, "Test for Detection of Weak Graphic Passwords in Passpoint Based on the Mean Distance between Points," Symmetry, vol. 13, 2021.