IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Seamless, Secure Wi-Fi Connectivity for In-Vehicle and V2X communication

Venkata Rao
Senior Solution Architect
KPIT

Abstract: *This white paper explores the concept of Seamless Wi-Fi connectivity in in-vehicle infotainment systems, highlighting its significance in providing an enhanced and uninterrupted connected experience for passengers. It examines the challenges associated with Wi-Fi connectivity in vehicles and proposes strategies and technologies to achieve seamless connectivity. By establishing reliable and high-speed Wi-Fi connections, automotive manufacturers can unlock a range of possibilities for entertainment, information, and productivity within the vehicle, offering a superior user experience and paving the way for future innovations.*

1 Introduction

In recent years, the automotive industry has witnessed a significant transformation with the integration of wireless technologies. Seamless Wi-Fi connectivity has emerged as a critical enabler for delivering a wide range of services, including real-time traffic updates, multimedia streaming, software updates, remote diagnostics, and many more while on the move.

With the rise of connected cars and the internet of things (IoT), drivers and passengers expect to have access to reliable and high-speed Wi-Fi in their vehicles. However, implementing seamless Wi-Fi connectivity for automotive is a challenging task due to various factors such as high-speed mobility, signal interference, physical obstacles, limited bandwidth, network handoffs, security risks, network congestion and network coverage.

One of the main reasons for connectivity issues in cars is the limited range of Wi-Fi signals. The metal body of a car can interfere with Wi-Fi signals, reducing their strength and reliability. In addition, many urban areas have Wi-Fi "dead zones" where there is no Wi-Fi signal available. These dead zones can make it difficult for passengers to maintain a consistent internet connection while on the road.

Seamless Wi-Fi connectivity is crucial for delivering a superior user experience, enable various in-car entertainment and information systems, improve navigation and continuous access to online services. To achieve this, technologies like OpenRoaming and Passpoint have emerged as powerful solutions that ensure effortless connectivity across different Wi-Fi networks.

OpenRoaming is a wireless network roaming standard developed by the Wireless Broadband Alliance (WBA). It allows users to automatically connect to any Wi-Fi network that supports OpenRoaming without the need for additional login credentials.

Passpoint, on the other hand, is a Wi-Fi Alliance standard that allows for seamless and secure authentication and connection to Wi-Fi networks. It uses advanced encryption and authentication protocols to ensure that only authorized users can access the network.

By leveraging OpenRoaming and Passpoint features, IVI systems can provide users with seamless connectivity while on the move. This means that drivers and passengers can stay connected to their favourite services without interruption as they travel from one location to another. For example, as a car moves from a residential area to a business district, the IVI system can automatically switch to a different Wi-Fi network that provides better coverage and bandwidth.

In addition to providing seamless connectivity, OpenRoaming and Passpoint also provide enhanced security. With Passpoint, users can be assured that they are connecting to a secure network that uses advanced encryption and authentication protocols. This reduces the risk of unauthorized access to sensitive information such as personal and financial data.

Overall, by leveraging OpenRoaming and Passpoint features, IVI systems can provide users with a seamless and secure Wi-Fi connectivity experience while on the move.

2 OpenRoaming

OpenRoaming is an industry-wide initiative that aims to simplify Wi-Fi connectivity and enable users to connect automatically and securely to Wi-Fi networks without any manual configuration or authentication. It eliminates the need for users to repeatedly enter usernames and passwords, providing a seamless and frictionless experience. OpenRoaming achieves this with digital certificates and a global federation of identity and service providers.

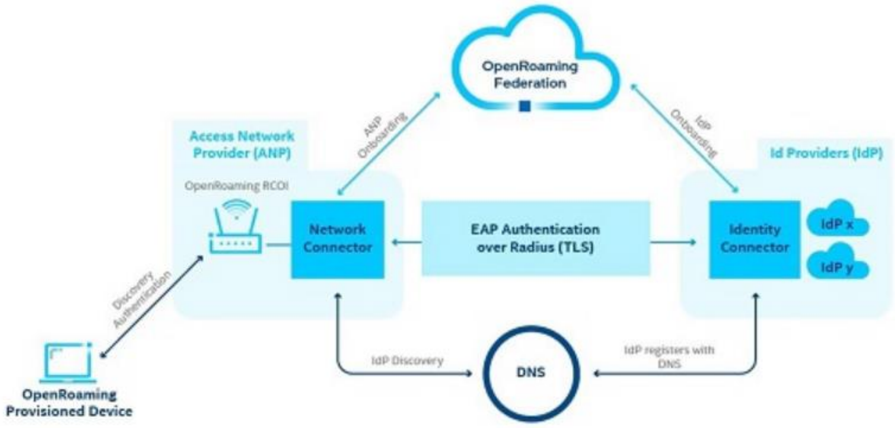
OpenRoaming is a WBA standard and the goal of OpenRoaming is to make it easy for users to access Wi-Fi networks seamlessly and securely, without the need for usernames, passwords, or other forms of authentication.

The way OpenRoaming works is simple. When a user enters a Wi-Fi hotspot, their device sends a request to the hotspot's Access Point (AP). The AP then uses the user's credentials to verify their identity and grant them access to the network.

OpenRoaming is particularly useful for IVI systems because it allows users to connect to Wi-Fi networks automatically, as they move between hotspots, without any interruption in service. This technology is based on a federated identity model that uses digital certificates to authenticate users and devices. By leveraging OpenRoaming, IVI systems can provide passengers with hassle-free Wi-Fi connectivity while traveling and OpenRoaming leverages the Passpoint feature, which is a standard developed by the Wi-Fi Alliance to provide a secure and seamless connection to Wi-Fi networks.

2.1 OpenRoaming Architecture

The OpenRoaming architecture consists of three primary entities: Identity Providers (IdPs), Access Network Providers (ANP)/Network Operators (NOs), and Roaming Consortium Providers (RCPs). IdPs serve as trusted entities that authenticate users, while NOs manage the Wi-Fi networks. RCPs play a crucial role in establishing and maintaining trust relationships between IdPs and ANPs. The OpenRoaming architecture allows users to roam across different Wi-Fi networks seamlessly, without the need for manual intervention.



OpenRoaming can create an easy-to-use, secure, plug-and-play architecture through a cloud-based roaming federation framework that uses PKI and standard legal frameworks. By doing this, Wi-Fi networks and devices remove the barriers to adopting roaming services.

2.2 Key Features and Components

OpenRoaming incorporates several features to ensure seamless connectivity. These include:

Digital Certificates: OpenRoaming utilizes digital certificates to establish trust and enable secure authentication between IdPs, ANPs, and users. These certificates ensure the integrity and confidentiality of the authentication process, reducing the risk of unauthorized access.

Federated Identity: OpenRoaming enables users to leverage their existing identities with trusted IdPs. This eliminates the need for creating separate accounts or credentials for each Wi-Fi network, streamlining the authentication process, and enhancing user convenience.

Roaming Consortium Providers (RCPs): RCPs play a crucial role in the OpenRoaming ecosystem. They facilitate the establishment of trust relationships between IdPs and ANPs by verifying the identity and credentials of participating entities. RCPs ensure that the roaming agreements are respected and provide a centralized platform for managing the federation.

Seamless Network Handover: OpenRoaming enables seamless handover between different Wi-Fi networks. When a user moves from one network coverage area to another, the system automatically maintains the user's connection without any interruption or manual intervention. This ensures continuous connectivity and a smooth user experience throughout the journey.

Dynamic Service Discovery: OpenRoaming allows devices to dynamically discover and connect to available Wi-Fi networks without user intervention. Devices can proactively search for compatible networks and seamlessly transition between them based on signal strength, quality of service, or user preferences.

Global Federation: OpenRoaming aims to create a global federation of Wi-Fi networks, IdPs, and ANPs. This federation enables users to roam across different networks seamlessly, whether they are in their home country or traveling internationally. It promotes interoperability and collaboration among various stakeholders, fostering a unified and scalable ecosystem.

Passpoint Integration: OpenRoaming leverages Passpoint technology to enable automatic and secure authentication. Passpoint-based infrastructure and components, such as Passpoint-enabled devices and APs, are required to achieve seamless connectivity within the OpenRoaming ecosystem.

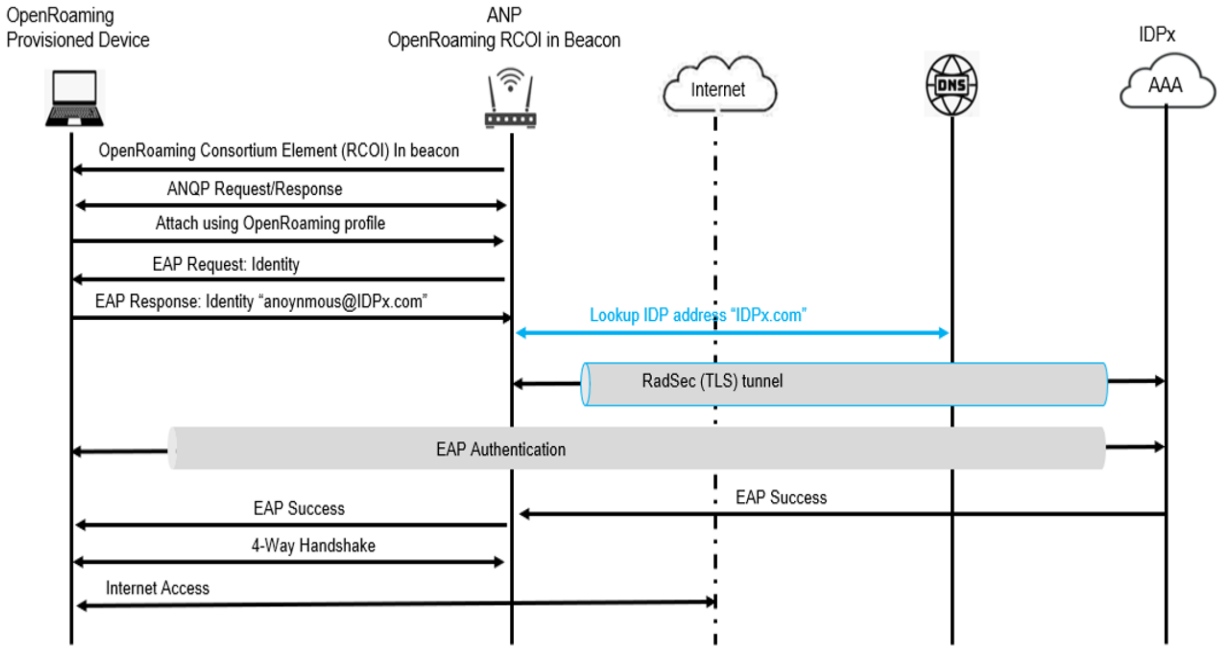
Privacy and Data Protection: OpenRoaming emphasizes user privacy and data protection. It ensures that user credentials and sensitive information are securely transmitted and stored, following industry best practices and encryption standards. OpenRoaming also provides users with control over their personal data and allows them to manage their privacy preferences.

Analytics and Insights: OpenRoaming facilitates the collection of anonymized data about user behaviour, network performance, and roaming patterns. This data can be leveraged to gain insights into user preferences, optimize network infrastructure, and deliver personalized services to enhance the user experience.

These key features and components of OpenRoaming contribute to seamless Wi-Fi connectivity, simplified user authentication, enhanced privacy and security, and efficient network management within IVI systems. By leveraging OpenRoaming, IVI systems can deliver a connected and immersive experience to passengers, enabling them to stay connected, entertained, and productive while on the move.

2.3 OpenRoaming Discovery and Authentication Flow

The way OpenRoaming works is simple. When a user enters a Wi-Fi hotspot, their device sends a request to the hotspot's Access Point (AP). The AP then uses the user's credentials to verify their identity and grant them access to the network.


OpenRoaming Provisioned Device
ANP OpenRoaming RCOI in Beacon
Internet
DNS
IDPx
AAA
OpenRoaming Consortium Element (RCOI) In beacon
ANQP Request/Response
Attach using OpenRoaming profile
EAP Request: Identity
EAP Response: Identity "anoynmous@IDPx.com"
Lookup IDP address "IDPx.com"
RadSec (TLS) tunnel
EAP Authentication
EAP Success
EAP Success
4-Way Handshake
Internet Access

2.4 OpenRoaming Security

OpenRoaming leverages secure authentication protocols such as RadSec, EAP-Transport Layer Security (EAP-TLS), EAP-Tunnel TLS (EAP-TTLS), or EAP-Authentication and Key Agreement (AKA). All authentication traffic is TLS encrypted. OpenRoaming networks are secure networks and leverage Wi-Fi Protected Access (WPA)2-Enterprise or WPA3 over-the-air encryption, and as such offer enterprise-grade protection, unlike current open wireless guest networks.

3 Pass point (Hotspot 2.0)

Passpoint, also known as Hotspot 2.0, is a Wi-Fi standard developed by the Wi-Fi Alliance that enhances Wi-Fi connectivity and provides seamless and secure access to Wi-Fi networks. Passpoint simplifies the authentication and connection process, enabling devices to automatically connect to Wi-Fi networks without the need for manual configuration or user intervention.

Passpoint allow users to roam between wireless networks as they move around a campus or city by constantly switching to stronger, closer networks to avoid service disruptions. It is typically used when transitioning from cellular data to Wi-Fi, a process that relies less on the former.

Mobile devices typically come configured for Passpoint support. There are several large service providers with interoperability agreements, allowing their customers to roam on partner networks, thereby expanding the range of Wi-Fi networks they have access to and reducing the number of devices the cell towers are required to support.

Hotspot 2.0, also known as Wi-Fi Certified Passpoint, is a standard for public-access Wi-Fi that enables seamless roaming among Wi-Fi networks and between Wi-Fi and cellular networks. It is based on the IEEE 802.11u standard for interworking with external networks.

To provide seamless Wi-Fi connectivity for IVI systems, vehicle manufacturers and service providers can integrate OpenRoaming and Passpoint technologies into their systems. This would allow IVI systems to automatically connect to Wi-Fi networks as the vehicle moves between different locations without requiring any manual intervention from the user.

For example, a vehicle with an IVI system that supports OpenRoaming and Passpoint could automatically connect to a Wi-Fi network at a coffee shop, and then seamlessly transition to another network as the vehicle drives away from the coffee shop and towards another location with Wi-Fi coverage.

Overall, OpenRoaming and Passpoint are powerful features that can help provide seamless and secure Wi-Fi connectivity for in-vehicle infotainment systems, enhancing the user experience and making it easier to stay connected while on the go.

3.1 Passpoint Protocol and Infrastructure

Passpoint relies on the IEEE 802.11u standard to enable seamless connectivity. It introduces the concept of "Passpoint profiles" that define the network's identity, security, and connection parameters. Passpoint-enabled Wi-Fi networks broadcast these profiles, allowing nearby devices to discover and connect to them automatically.

Passpoint employs the Extensible Authentication Protocol (EAP) for secure authentication. It supports various EAP methods, including EAP-TLS, EAP-TTLS, and EAP-SIM, providing flexibility for different authentication mechanisms based on network policies and user credentials.

To support Passpoint, network operators must deploy a Passpoint-enabled infrastructure. This includes:

Access Points (APs): Passpoint-enabled APs broadcast Passpoint profiles, allowing devices to discover and connect seamlessly. APs must support 802.11u and be integrated with the necessary authentication and security mechanisms.

Authentication Servers: Passpoint relies on authentication servers to validate user credentials and perform secure authentication. These servers communicate with devices using the EAP framework and validate the user's identity.

Online Sign-Up Servers: In cases where users need to sign up or register for Wi-Fi services, online sign-up servers facilitate the creation of user accounts and manage the authentication process.

Configuration and Policy Servers: These servers store and distribute Passpoint profiles to APs. They also define network policies, including quality of service (QoS) parameters and access control rules.

3.2 Enhanced Authentication and Encryption

Passpoint enhances the authentication and encryption mechanisms used in Wi-Fi networks. It improves security and privacy while ensuring a seamless connection experience.

Key elements of Passpoint authentication and encryption features include:

Secure Credential Provisioning: Passpoint enables the secure delivery of user credentials to devices through digital certificates or secure SIM card-based mechanisms. This eliminates the need for users to manually enter authentication information, enhancing convenience and reducing the risk of credential theft.

Simultaneous Authentication of Equals (SAE): Passpoint supports the SAE algorithm, also known as Dragonfly Key Exchange. SAE provides robust protection against password-based attacks, improving the security of Wi-Fi network connections.

Transport Layer Security (TLS): Passpoint utilizes TLS for secure communication between devices and authentication servers. TLS ensures the confidentiality and integrity of data exchanged during the authentication process, preventing unauthorized access and eavesdropping.

Encryption and Key Management: Passpoint employs advanced encryption standards, such as WPA2-Enterprise or WPA3-Enterprise, to encrypt data transmitted over the Wi-Fi network. Additionally, it manages the distribution and renewal of encryption keys to ensure continuous secure communication.

By leveraging Passpoint in IVI systems, Seamless Wi-Fi connectivity can be achieved, providing passengers with automatic and secure access to Wi-Fi networks without the need for manual intervention. Passpoint simplifies the authentication process, enhances network **security, and enables uninterrupted connectivity** during roaming or network transitions, contributing to an enhanced user experience in IVI systems.

4 Benefits of OpenRoaming and Passpoint in IVI Systems

IVI systems require seamless Wi-Fi connectivity to provide users with access to a range of features and services. However, traditional Wi-Fi authentication methods can be time-consuming and cumbersome, which can result in a poor user experience.

Integrating OpenRoaming and Passpoint features into In-Vehicle Infotainment (IVI) systems offers several significant benefits for both passengers and automotive manufacturers. These benefits include:

4.1 Seamless Connectivity and Handover

OpenRoaming and Passpoint enable seamless connectivity by automating the authentication and connection process. With these features, IVI systems can seamlessly connect to Wi-Fi networks without user intervention, eliminating the need for manual configuration or repeated authentication. Passengers can enjoy uninterrupted access to online services, such as streaming media, navigation updates, real-time information, remote vehicle diagnostics & maintenance and app downloads & updates throughout their journey. Furthermore, as passengers move between different network coverage areas, the system can seamlessly transition the connection, ensuring a continuous and stable network experience.

Modern in-vehicle infotainment (IVI) systems are now highly sophisticated systems that form the heart of modern vehicles, keeping drivers and passengers informed, entertained on the road, and enabling V2X communication for safety and security.

4.2 Enhanced Security and Privacy

OpenRoaming and Passpoint enhance security and privacy in IVI systems by implementing robust authentication and encryption mechanisms. Passpoint’s support for EAP methods and its use of secure credential provisioning and Transport Layer Security (TLS) ensure that user credentials are protected and communications between the IVI system and Wi-Fi networks are secure. OpenRoaming's use of digital certificates and trust frameworks provides an additional layer of security, establishing trust between entities involved in the roaming process. These features help prevent unauthorized access to the IVI system and protect sensitive user data, ensuring a safer and more secure Wi-Fi experience.

4.3 Simplified User Experience

OpenRoaming and Passpoint significantly simplify the user experience within IVI systems. Passengers no longer need to manually search for and connect to Wi-Fi networks or repeatedly enter authentication credentials. The seamless connectivity provided by OpenRoaming and Passpoint ensures that passengers are automatically connected to trusted Wi-Fi networks, eliminating the hassle of network selection and authentication. This simplified user experience enhances convenience, saves time, and improves user satisfaction. Additionally, the use of federated identities in OpenRoaming allows users to leverage their existing credentials, providing a familiar and seamless authentication experience across different networks.

4.4 Increased Productivity and Entertainment Options

Seamless Wi-Fi connectivity powered by OpenRoaming and Passpoint enhance productivity and entertainment options for passengers in IVI systems. With continuous and reliable internet access, passengers can leverage various online services and applications, such as email, messaging, video conferencing, and cloud-based productivity tools. They can also enjoy uninterrupted streaming of media content, including music, videos, and podcasts. These connectivity benefits enhance the overall in-vehicle experience, enabling passengers to stay productive, entertained, and connected to their digital lives while on the move.

4.5 Promotes Automotive Industry Collaboration

OpenRoaming and Passpoint foster collaboration among stakeholders in the automotive industry. By adhering to common standards and frameworks, automotive manufacturers, Wi-Fi network operators, and identity providers can create a unified and interoperable ecosystem. This collaboration simplifies the integration and deployment of Wi-Fi connectivity features in IVI systems, reducing development costs and ensuring a consistent user experience across different vehicles and networks. The industry-wide adoption of OpenRoaming and Passpoint benefits all parties involved, enabling seamless connectivity for users, and facilitating innovation and market growth for automotive manufacturers and service providers.

In summary, incorporating OpenRoaming and Passpoint features in IVI systems enables Seamless Wi-Fi connectivity, simplifies the user experience, enhances security, and expands network coverage. It can also provide passengers with access to emergency services, such as roadside assistance or medical help, in the event of an emergency. These advancements contribute to an improved in-vehicle experience, enabling passengers to leverage the full potential of Wi-Fi connectivity while on the move.

5 Challenges and Limitations

The primary challenge in providing Seamless Wi-Fi connectivity in IVI systems is ensuring that the connection remains stable and reliable throughout the journey. Unlike other devices, IVI systems are constantly on the move, making it difficult to maintain a stable connection. Additionally, the presence of other wireless devices, such as smartphones and tablets, can cause network congestion, interference, low bandwidth and degrade the Wi-Fi signal quality. This can result in slow data transfer rates, packet loss, disconnection, and poor streaming quality, leading to a suboptimal user experience.

While OpenRoaming and Passpoint offer significant benefits for Seamless Wi-Fi Connectivity in In-Vehicle Infotainment (IVI) systems, there are also several challenges and limitations that need to be considered during implementation. These challenges include:

5.1 Infrastructure Fragmentation

The deployment of Passpoint-enabled Wi-Fi networks and the adoption of OpenRoaming may vary across regions and network operators. This fragmentation can pose challenges for seamless connectivity, as Passpoint profiles may not be universally available or compatible with all IVI systems. Automotive manufacturers may need to ensure compatibility with multiple Passpoint profiles and establish agreements with different network operators to provide consistent and seamless connectivity across various regions.

5.2 Security Concerns

While Passpoint enhances security by implementing robust authentication and encryption mechanisms, there is always a risk of security vulnerabilities. Automotive manufacturers must stay vigilant and ensure that the implemented security measures are up to date, following industry best practices and protocols. Regular security audits and updates are necessary to address any emerging threats and vulnerabilities in the Wi-Fi connectivity infrastructure.

5.3 User Privacy and Data Protection

Collecting and processing user data for authentication and connectivity purposes raises privacy concerns. Automotive manufacturers must comply with privacy regulations and establish clear policies regarding the collection, storage, and use of user data. Obtaining user consent and providing transparency regarding data handling practices are essential to maintain user trust and protect user privacy throughout the Wi-Fi connectivity process.

5.4 Roaming Complexity and Agreements

OpenRoaming aims to create a global federation of Wi-Fi networks, which involves establishing roaming agreements between network operators and identity providers. Negotiating and managing these agreements can be complex and time-consuming. Automotive manufacturers must collaborate with network operators and identity providers to ensure seamless roaming capabilities and address any legal, technical, or business challenges associated with roaming agreements.

5.5 User Experience and Network Transitions

While OpenRoaming and Passpoint aim to provide seamless connectivity and network handover, challenges may arise during network transitions. Switching between Wi-Fi networks may result in brief interruptions or latency issues, impacting the user experience. Automotive manufacturers must optimize the handover process to minimize disruptions and ensure smooth transitions between different networks to provide passengers with a seamless connectivity experience.

5.6 Limited Coverage and Network Availability

The availability and coverage of Passpoint-enabled Wi-Fi networks may vary across regions, especially in remote areas or during long-distance travel. In areas with limited coverage, passengers may experience gaps in connectivity or rely on alternative connectivity options, such as cellular networks. Automotive manufacturers must consider network availability and integrate fallback mechanisms to ensure continuous connectivity and a consistent user experience in areas with limited Passpoint coverage.

5.7 Compliance and Standardization

OpenRoaming and Passpoint rely on adherence to industry standards and specifications. However, ensuring compliance and standardization across different devices, networks, and software versions can be a challenge. Automotive manufacturers must ensure compatibility and compliance with the latest standards and work closely with network equipment providers, software developers, and other stakeholders to address any interoperability issues and achieve a seamless and standardized implementation.

By acknowledging and addressing these challenges and limitations, automotive manufacturers can overcome potential hurdles and provide a robust and reliable Wi-Fi connectivity experience in IVI systems, enhancing the overall user experience for passengers. Collaboration with network operators, identity providers, and industry organizations is crucial to driving the adoption of OpenRoaming and Passpoint standards and addressing challenges collectively.

6 2307072_196095_570_578 pFuture Developments

As technology continues to advance, the integration of OpenRoaming and Passpoint features in In-Vehicle Infotainment (IVI) systems is expected to evolve and improve. Here are some potential future directions:

6.1 Cellular Integration

As 5G networks become more prevalent, future IVI systems can leverage the capabilities of 5G connectivity alongside Wi-Fi networks. This integration can enhance the overall connectivity experience by providing faster speeds, lower latency, and improved network reliability even in areas where Wi-Fi signals are weak or non-existent. Additionally, cellular connectivity can help offload some of the data traffic from the Wi-Fi network, reducing congestion and improving performance. OpenRoaming and Passpoint can be extended to seamlessly transition between 5G and Wi-Fi networks, ensuring uninterrupted connectivity throughout the journey.

6.2 Enhanced Security Measures

With the increasing importance of cybersecurity, future implementations of OpenRoaming and Passpoint may incorporate additional security measures. This can include stronger authentication methods, advanced encryption protocols, and enhanced network monitoring and intrusion detection systems. The goal is to continually improve the security and privacy aspects of IVI systems to protect users' data and ensure a secure connectivity experience.

6.3 Intelligent Network Selection

Future IVI systems can incorporate intelligent algorithms to automatically select the most optimal network based on factors such as network performance, signal strength, and bandwidth availability. This intelligence can dynamically switch between available networks, including Wi-Fi, 5G, or other emerging connectivity technologies, to provide the best possible connectivity experience for passengers.

6.4 Integration with Smart Infrastructure

As smart infrastructure deployments, such as smart cities, progress, IVI systems can integrate with these infrastructure systems. This integration can enable seamless connectivity with smart infrastructure networks, such as intelligent transportation systems or connected roadside units, so called V2X communication, providing passengers with enhanced services and real-time information during their journey.

6.5 Collaboration and Standardization

Collaboration among automotive manufacturers, network operators, identity providers, and other stakeholders will continue to be crucial for driving the adoption and standardization of OpenRoaming and Passpoint. Future efforts should focus on streamlining the integration process, establishing common frameworks, and expanding the global network of Passpoint-enabled Wi-Fi networks to ensure seamless connectivity for IVI systems worldwide.

7 Conclusion

The integration of OpenRoaming and Passpoint features in In-Vehicle Infotainment (IVI) systems presents significant opportunities for enhancing Wi-Fi connectivity and providing a seamless user experience for passengers. By automating the authentication and connection process, OpenRoaming and Passpoint enable passengers to effortlessly connect to Wi-Fi networks, ensuring uninterrupted access to online services and entertainment options during their journey and to enable “One Global Wi-Fi Network” with simple, seamless, and secure connections to public Wi-Fi networks all around the world.

The benefits of OpenRoaming and Passpoint in IVI systems extend beyond convenience. They offer enhanced security, simplified user experience, increased productivity, and collaboration opportunities within the automotive industry. However, challenges such as infrastructure fragmentation, security concerns, and privacy considerations need to be addressed during implementation.

With ongoing advancements in technology, future directions for OpenRoaming and Passpoint in IVI systems involve integrating with 5G networks, implementing enhanced security measures, enabling intelligent network selection, integrating with smart infrastructure, and promoting collaboration and standardization efforts.

By addressing these challenges and embracing future opportunities, automotive manufacturers can create IVI systems that provide seamless, secure Wi-Fi connectivity, enhance the overall in-vehicle experience, and pave the way for the future of connected vehicles for smart transportation.