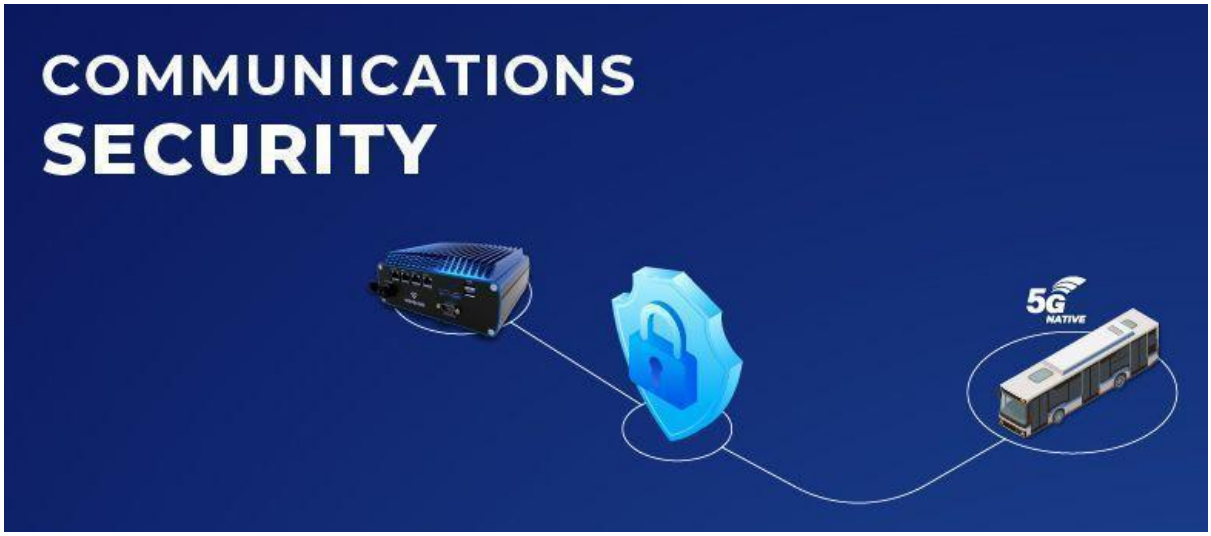
wavecom
Technologies

White Paper

Connected Bus by Wavecom

How can we get secure communications on board buses?



Reliable connectivity is essential for modern bus fleets, as it supports important functions such as real-time fleet management, ticketing systems, passenger information, and on-board security. Security threats that lead to connectivity disruptions can negatively affect operational efficiency, service reliability, and passenger experience. Additionally, security vulnerabilities can expose bus operators to data breaches and potential financial losses.

A resilient connectivity solution must include a wide array of features that extend beyond simple network connectivity. These functionalities provide the security, management and flexibility needed to meet the specific requirements of their deployment environments, while ensuring efficient connectivity.

This White Paper explores the key challenges in achieving secure communications on-board buses against growing threats, using the **Wavecom** **Modular Gateway** in **Connected Bus** solution ecosystem, to mitigate risks while ensuring operational resilience.

Date: 13th February 2025
Version 2.2

Connected Bus by Wavecom
How can we get secure communications on board buses?

Introduction

An IoT Gateway allows us to bring IoT assets together into a single ecosystem, with different communication networks to exchange data seamlessly, whether for instance they use Wi-Fi, 5G or LoRaWAN. However, security is a critical issue in IoT ecosystems because of the amount and sensitivity of data involved.

Figure 1 - Communications Security | Modular Gateway

Hence, it is essential that a resilient connectivity system incorporates a variety of functionalities beyond simply connecting to the network. These functionalities guarantee not only efficient connectivity, but also the security, management and flexibility needed to respond to the specific requirements of the environments in which they are located.

The **Wavecom** **Modular Gateway** is an example of a highly versatile and secure IoT Gateway that functions seamlessly with a wide range of bus on-board assets (Figure 1).

IoT Gateway Security

For **Wavecom**, security is a critical function of IoT Gateways because they handle sensitive data and are often connected to the internet, requiring strong security measures to protect against unauthorized access and data breaches. This includes encryption, authentication and access control mechanisms.

The security of IoT Gateways is maintained through the adoption of key methods, which ensure that they remain as secure as the entire network.

- **Use only authenticated IoT Gateways -** Robust authentication mechanisms help verify the identity of IoT assets and prevent unauthorized access, fortifying the overall security of the IoT ecosystem.
- **Before rolling out, assess the security -** After installing an IoT Gateway, perform a security assessment to ensure it meets security requirements.
- **Update Firmware | Software -** Regularly updating and securing the firmware and software of IoT Gateways is critical in maintaining a robust defence against threats. Outdated or unpatched software can be exploited by hackers to gain unauthorized access or execute malicious activities.
- **Check access to the IoT Gateway on a regular basis -** Monitor and regularly update the access list, including User Accounts and IoT assets, to minimize IoT Gateway risk. Revoke permissions from anyone or any asset that no longer needs access or is suspicious.
- **Include IoT Gateways when auditing security -** Include IoT Gateways in regular assessments and audits.
- **Different networks for IoT Gateways and IoT assets -** Ideally, a separate network should be used for IoT assets and IoT Gateways to segment the traffic.

Connected Bus Solution

The **Wavecom Technologies** **Connected Bus** solution has been developed with the specific needs of bus operators in mind, with the aim of significantly improving their business efficiency and profitability in a modular and evolving way.

Figure 2 - Connected Bus Solution | 5G and Wi-Fi 6/6E

Mainly, it comprises a **Modular Gateway** (5G Native) installed on board vehicle, which is Cloud Managed by the **Wavecom IoT Manager/Multi-Tenant Platform** (5G WAN Manager | SD-WAN), through a GUI-based dashboard showing real-time status and performance metrics, as depicted in Figure 2.

The **Connected Bus** solution features a set of functionalities that promote communication security without compromising system performance.

Modular Gateway

The **Wavecom** **Modular Gateway** is a modular platform that offers a range of technologies, including 5G and Wi-Fi, with the ability to support multiple MNOs (Mobile Network Operators) simultaneously. This provides redundancy or capacity balancing and bandwidth complementarity.

It supports two eSIM 5G modems, providing redundancy by using up to 7 SIM Card profiles from different MNOs. The antenna connected to the **Modular Gateway** and mounted on the roof of the bus picks up the signal switching between 5G cells at the nearest BTS (Base Transceiver Station) along the bus route or at bus stops, as shown in Figure 2.

Inside the bus, passengers connect to the Wi-Fi network via **Modular Gateway**, which provides two separated Wi-Fi 6/6E Access Points engineered for seamless evolution to the next generation of wireless technology. Wi-Fi 6/6E provides a more reliable and secure performance since it uses WPA3 authentication.

In addition to being 5G native and currently supporting independent Wi-Fi 6/6E modules for local communications, the **Modular Gateway** is characterised by a high degree of modularity and evolvability.

As the **Modular Gateway** in **Wavecom Technologies** **Connected Bus** solution is an aggregator of services and applications (as depicted in the Figure 3), it is crucial to ensure the security of its communications.

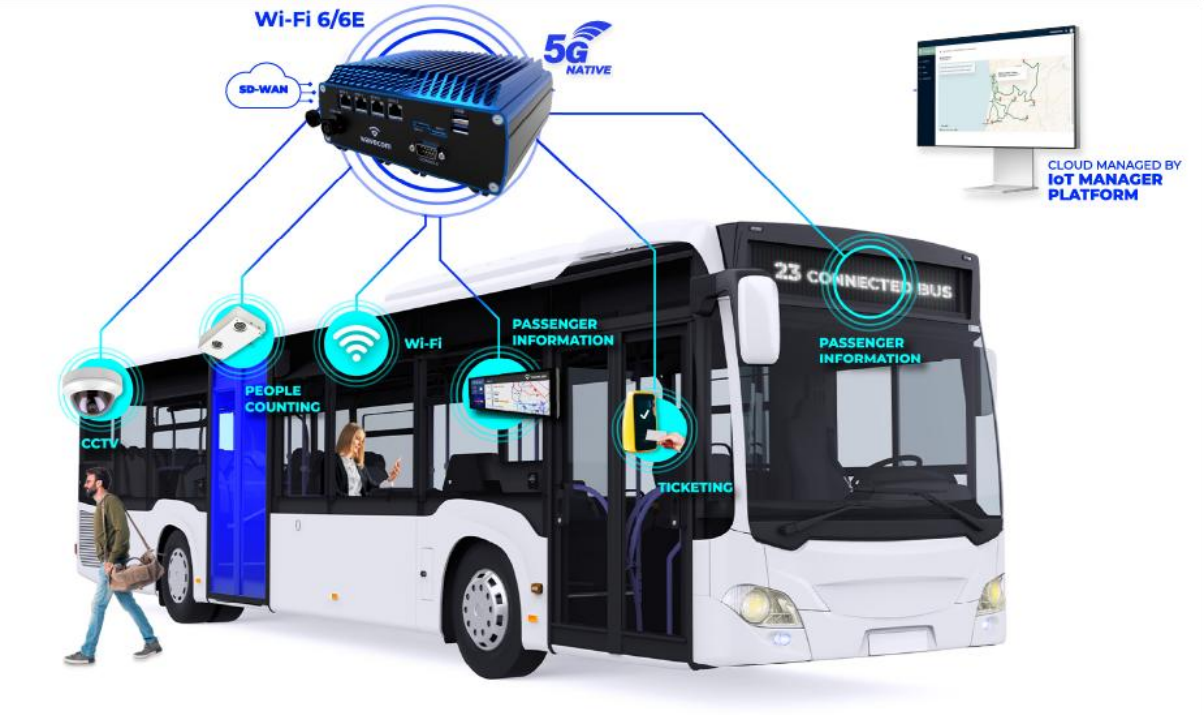


Figure 3 - Modular Gateway | Services and applications' aggregator

In terms of security, the **Modular Gateway** enables (Figure 4):

- Physical communication over Ethernet ports only with authorized devices by validating the MAC address of the device **Modular Gateway** is communicating with.
- Local virtual segregation of Ethernet ports into distinct IP networks, ensuring complete isolation, that prevents any communication between them.

- Prioritization of traffic on cellular output according to specific requirements. Furthermore, it is possible to prioritize traffic on the various Ethernet ports according to the type of traffic.
- Separation of critical and non-critical traffic by modem, since it is possible to have critical traffic that communicates only via a specific modem and non-critical traffic that communicates via a second modem.
- Communication with the various applications under VPN (Virtual Private Networks). It is possible to set up different VPNs for different infrastructures for each of the applications, thus ensuring greater security in the public communications environment and increasing security even further.
- Wi-Fi that allows different configurations and integration with RADIUS server, ensuring minimum security conditions for access.
- Centralized management is always supported by a secure and authenticated connection.
- Local management in the **Modular Gateway**, restricted and limited, to minimize attacks and misuse.

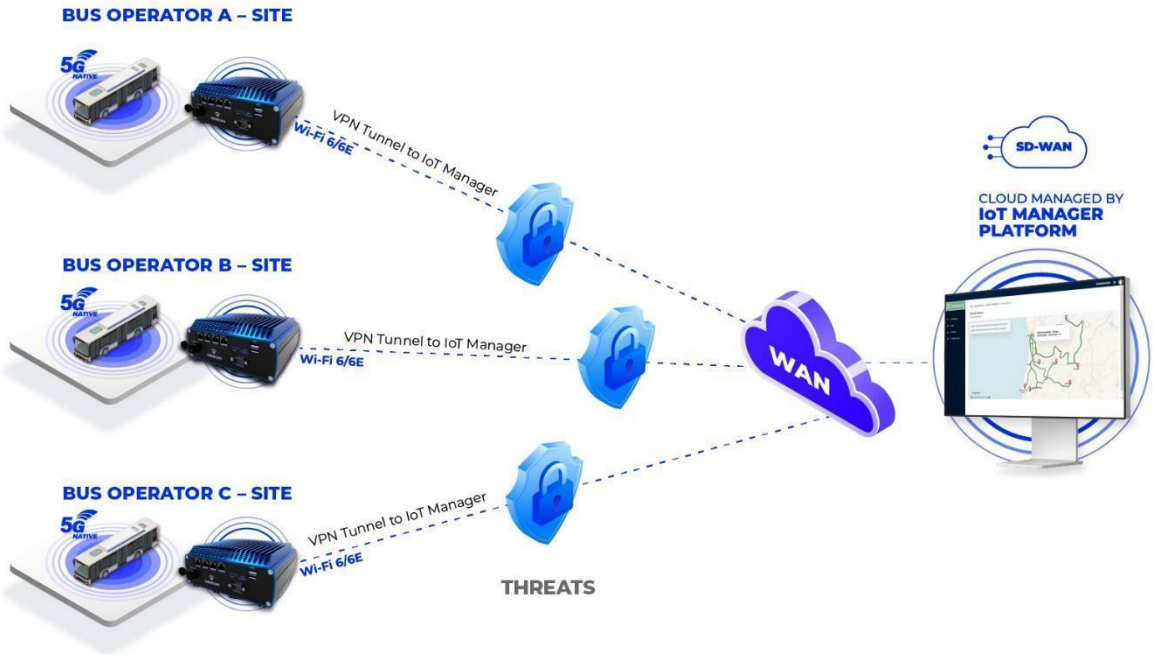


Figure 4 - Communications Security

Furthermore, **Wavecom Technologies' Modular Gateways** can integrate third-party active security applications and security providers that run on their embedded system.

These security applications analyse, prevent and report possible threats in memory or in local data, including communications in transit.

IoT Manager/Multi-Tenant Platform

The **Wavecom** **IoT Manager /Multi-Tenant Platform** (5G WAN Manager | SD-WAN) (Figure 5) is a central software responsible for monitoring and managing all **Modular Gateways** centrally in a Cloud. It adheres to robust security standards, with comprehensive and active analysis conducted throughout the development and service operation.

All communications generated by the platform are designed to be secure.

Figure 5 - IoT Manager /Multi-Tenant Platform

This multi-tenant, high-availability central software is distinguished by its robust security features, including the capacity to define granular, explicit user authorization for data and functions. Furthermore, all operations are subject to internal auditing.

This guarantees from the outset that the data for each domain/group is only accessible in the corresponding domain.

It also allows user accounts to be synchronized using standard protocols (e.g., **Oauth 2.0** or **SAML**) with external identity provided.

It should be noted that **Wavecom** **Modular Gateways** establish secure communications with the **Wavecom** **IoT Manager /Multi-Tenant Platform**, the central software, thus guaranteeing security in every communication from each **Modular Gateway**. In terms of reliability and resilience issues, tunnel protocols (SD-WAN), security policies and other mechanisms are used to prevent possible attacks on the network.

Conclusion

In short, the **Wavecom Technologies** **Connected Bus** solution includes **authentication and access control**, **advanced firewalls** for intrusion detection and prevention, **encryption of data** in communications and files, and **continuous monitoring** to identify suspicious activity in real time.

In addition, **network segregation**, **centralized management** and **well-defined security policies** ensure efficient management and thorough control of the applications that access the networks.

It should also be noted that **Wavecom Technologies** is certified to **ISO/IEC 27001** (the international standard and benchmark for information security management), underlining its focus on data protection and related processes.

Acronyms

4G	Fourth Generation Mobile Network
5G	Fifth Generation Mobile Network
AP	Access Point
API	Application Programming Interface
APC	Automatic Passenger Counting
AVMS	Audio Visual Media Services
BTS	Base Transceiver Stations
CAD – AVL	Computer-Aided Dispatch / Automatic Vehicle Location
CEN	European Committee for Standardization
DPI	Dynamic Passenger Information
FMS	Fleet Management System
GUI	Graphical User Interface
IP	Internet Protocol
LTE	Long Term Evolution
MNO	Mobile Network Operator
SAML	Security Assertion Markup Language
SD-WAN	Software Defined – Wide Area Network
SIM	Subscriber Identity Module
VPN	Virtual Private Network
WPA3	Wi-Fi Protected Access 3
WWAN	Wireless Wide Area Network
ZTP	Zero Touch Provisioning

Contacts

For more information about **Wavecom** **Connected Bus**, feel free to contact us.

Phone: +351 234 919 190
Web: https://www.wavecom.com
e-Mail: wavecom@wavecom.com