White Paper

Seamless secure communications for vehicles and mobile teams

Author
Jon Curnyn

Revision
v1.1

Publish Date
April 2017

CUBIC | vocality

Table of Contents

INTRODUCTION

During the last decade demand for reliable, secure, high bandwidth, communications has grown exponentially. This demand has not been limited to stationary users. Mobile 'on the move' communications quality and availability are a necessity for today's mobile teams of workers and vehicles and for new use cases such as connected highways and autonomous driverless vehicles.

The need for reliable secure communications is shared by many industries and organizations such as emergency/blue light services, public transportation, first responders, oil & gas, mining and the military. Their day to day activity may see them operating in remote areas with limited communications, or in urban areas with high bandwidth but heavily used commercial communications available, and in some cases moving between such areas.

The use cases include mission critical applications through to business applications through to best effort applications. They involve control of machines and devices, and person to person communications needs.

This paper comprises the following sections:

- Provides some use cases and applications for vehicle based communications;
- Provides some use cases and applications for mobile teams;
- Provides information on the wireless communications technologies suitable for use in these cases and applications;
- Outlines the problems with wireless communication in challenging environments which present barriers in achieving reliable communications;
- Outlines the security issues inherent with communications architectures & solutions required to deliver both secure communications and robust and resilient systems which are not vulnerable to cyber security attacks;
- Highlights the Vocality gateway products and software products that can be used achieve seamless reliable secure communications in remote and urban environments for mobile teams and vehicles.

VEHICLE USE CASES AND APPLICATIONS

There are many applications where secure reliable wireless communications are required on vehicles, ranging from current use cases in public transportation to law enforcement and the military. A few such examples are introduced below, in addition to some emerging use cases in the V2X (vehicle-to everything) arena.

Public Transportation

Consider the use case of buses which may operate in both urban and rural areas where ticket vending and validation is required on entry to the vehicle. In certain cases, the vehicle is linked to centralized vending and billing systems requiring always available communications between the vehicle and these centralized systems. In addition, it is advantageous to be able to track the location of the vehicle as it proceeds on its route for both security and updating travelers on any timetable adjustments.

The buses may be fitted with 3G or LTE technology wireless modems which link the vehicle to the centralized systems, but as the vehicle passes through urban areas with no mobile operator coverage called 'notspots' (e.g. behind buildings, in depressions or troughs in the landscape), or pass through rural areas with no coverage at all, the ticketing and asset tracking business applications will fail, and in the case of ticketing, lead to a loss of revenue.

Law Enforcement

Police forces around the globe rely on UHF/VHF radio systems for delivering voice and low rate data communication services. The intention is to replace these systems over time with commercial LTE solutions for increased bandwidth for video and data applications (e.g. image transfer, messaging) in addition to voice.

However, the coverage of these UHF/VHF radio systems, such as TETRA or P25, is far from universal, and LTE as indicated above has 'notspots' and areas of no coverage at all. In addition, at critical times such as terrorist attacks, commercial LTE networks become heavily loaded or in some cases disabled. Therefore, a number of projects are underway to provide complete coverage for law enforcement agencies by operating multiple wireless communications network connections or 'bearers' (operating on different frequencies) to deliver seamless communications which are useable under all circumstances.

These projects combine the following bearers:

- Default to use of UHF/VHF where available;
- Use LTE where the applications require bandwidth and LTE coverage is available;
- Switch to satellite where UHF/VHF and LTE are not available.

Note, the satellite connectivity is enabled by the affordability of next generation High Throughput Satellites (HTS) which deliver services at a price point similar to home broadband.

Military

Consider the use case of a mobile platoon-sized group of soldiers (circa 50 persons) operating in up to ten land-based vehicles in a remote and/or hostile location with the need for voice, video and data (e.g. image transfer) applications between all vehicles. In addition, the group would have communication from the remote location to centralized command.

This solution would typically be delivered through use of Mobile Ad-hoc Network (MANET) technology mounted in each vehicle, and with one or more vehicles also equipped with a satellite communication device. The MANET technology would typically offer line of sight communication up to ranges of low numbers of miles, and may be augmented with a drone if the terrain is particularly prohibitive to line-of-sight communication.

Vehicle-to-Everything V2X

There are a range of new use cases for wireless communication in the areas of connected highways and connected vehicles, and autonomous vehicles, where the applications are operated using technology termed Vehicle-to-Everything, abbreviated to V2X. A sample of such use cases and applications are described below.

For road safety, there are a number of use cases including but not limited to:

- Forward collision warning;
- Lane change warning;
- Emergency brake light warning;
- Emergency vehicle approaching.

For traffic control, there is the 'platooning' use case where vehicles are grouped together electronically to reduce separation through simultaneous acceleration and braking. This application is intended to reduce congestion, decrease journey time in periods of congestion, increase road capacity and reduce vehicle fuel consumption.

The platooning use case is also relevant to the autonomous vehicle use case, where many autonomous vehicles can be platooned. In addition, autonomous vehicles can be controlled remotely from centralized locations.

These above use cases are delivered through use of V2X communication which can include Vehicle-to-Infrastructure (V2I), Vehicle-to-Vehicle (V2V), Vehicle-to-Pedestrian (V2P), Vehicle to Device (V2D) and Vehicle-to-Grid (V2G) communication. These communications are typically slated to be delivered with a version of Wi-Fi, also referred to as Dedicated Short Range Communication (DSRC) which operates in licensed bands where V2X senders dynamically form ad-hoc networks hence obviating the need for any infrastructure. In addition, the currently in development 5G communication system is also being positioned as a solution for V2X applications.

Note, this V2X wireless technology is in addition to any in-vehicle network, and any wide area networking needed for remote control of vehicles (e.g. LTE). The diagram in Figure 1 shows a public transportation example where vehicles participate in local V2X communication and in addition run business applications over wide area networks.

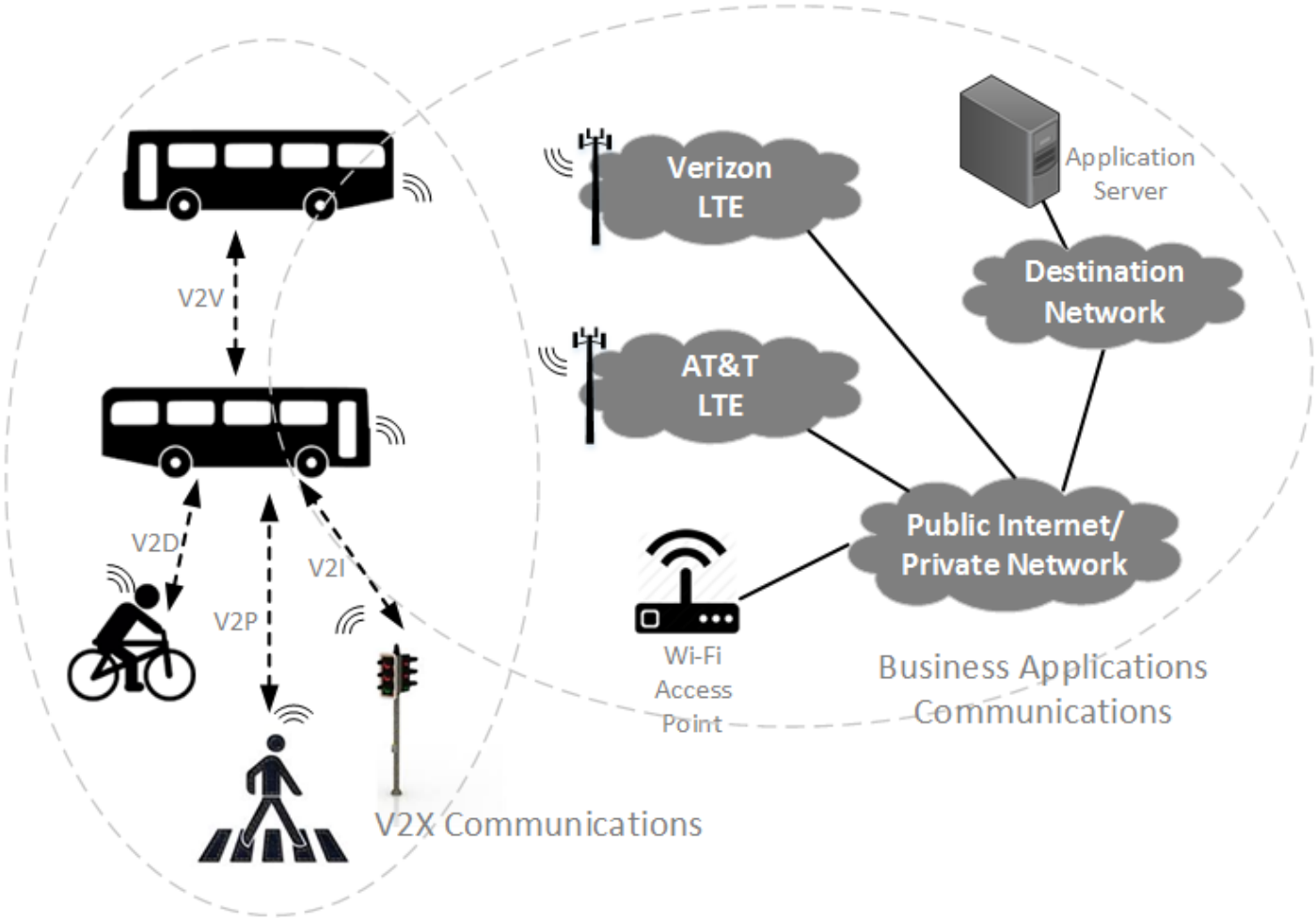

Figure 1 Hybrid V2X and Business Application Communication Use Case

MOBILE TEAMS USE CASES AND APPLICATIONS

First Responders

Consider the case of First Responders who are called out to emergency or disaster relief situations. These personnel will initially assemble in their country of origin (say at a hotel, government or NGO-operated location) whilst equipment and transport is arranged, then use public and/or private transport to reach the relief zone.

Whilst in hotels or, for example, airports the mobile team will need to access public and private infrastructure such as 3G/LTE and Wi-Fi networks. Once at the relief zone they may be required to use satellite communication, as local infrastructure could be non-operational or non-existent.

The applications used by the first responder team will include voice, push-to-talk radio communications, messaging, video and data transfer (e.g. images, reports).

A second example for First Responders is shown in Figure 2 where the emergency services are called to an incident. The vehicles and personnel from each of the emergency services (police, fire, ambulance) proceed to the incident location, during which they may have access to UHF/VHF radio and/or LTE communications.

Upon arrival at the incident location the various vehicles and personnel form a private Mobile Ad-hoc Network for local communication. At first LTE may not be available, due to lack of network coverage or network overloading, so no communication with Command may be possible initially. Later an Incident Control vehicle arrives at the scene with its satellite communication capability allowing communication with Command.

Secure Field Communications

Consider the case of senior government, civil service, diplomatic or military personnel who are required to travel to foreign locations but maintain secure communications with their leaders whilst abroad.

As with the first responders the personnel and their teams may be located in urban areas with national infrastructure available, or be in remote locations where no infrastructure is available. Therefore, the teams need to utilize 3G/LTE networks, connect wirelessly to hotel or public Wi-Fi services, or use satellite or UHF/VHF radio communications, whilst at all times maintaining security.

The security requirement may be provided through use of strong commercial grade encryption (e.g. Public Key Infrastructure or PKI with IPSec protocols which provide confidentiality, authentication, tamper proofing etc.) or through higher grade encryptors, or both.

The applications used by the personnel team will include voice, remote access to information, messaging, and data transfer (e.g. images, reports).

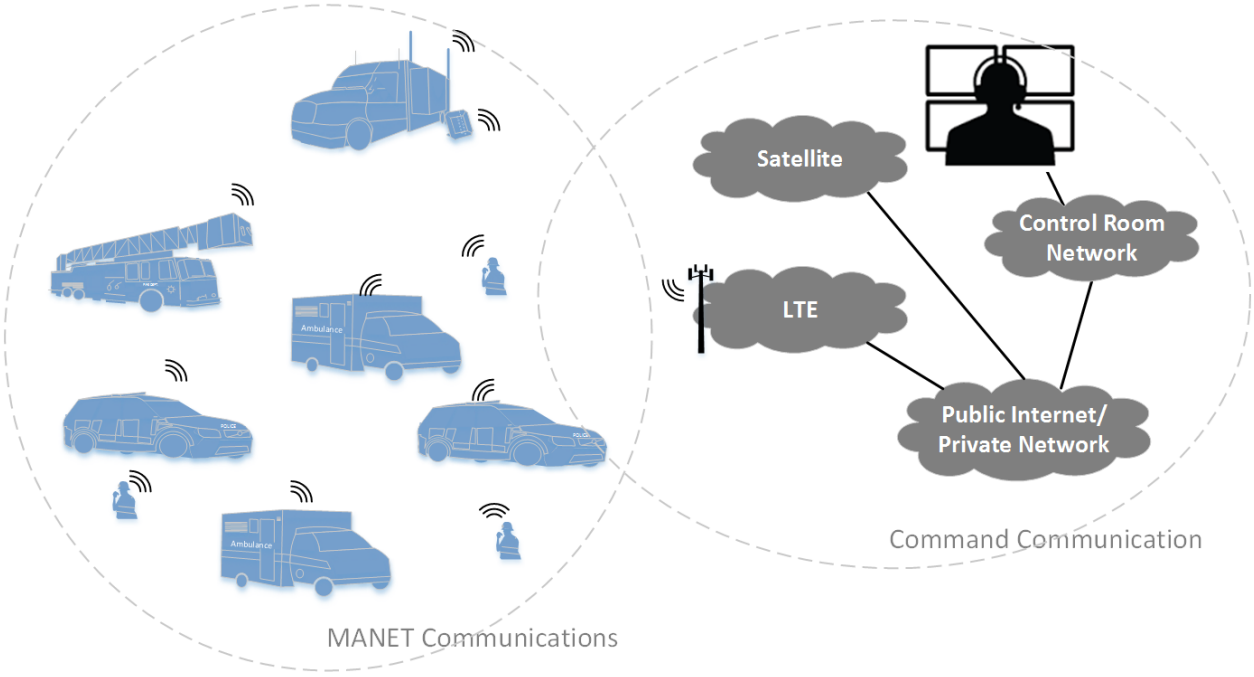

Figure 2 First Responders with Inter-vehicle Communication and connection to Command

WIRELESS COMMUNICATIONS BEARERS

There is a myriad of different technologies available for the delivery of secure reliable communications, each with its advantages and disadvantages.

The mainstream wireless technologies in use today, or being positioned for future adoption, are introduced below along with notable advantages or disadvantages. They are grouped into wide area networks used for long range communication, local or personal area networks used for short range communication, and infrastructure-less technologies used for ad-hoc communication.

Note, wide area network communication generally operates in licensed bands or spectra, hence any new technologies need allocation of spectrum by national governments. Short range technology typically operates in licensed or unlicensed bands.

Wide Area Networks/Long Range Bearers

UMTS/3G: Now ubiquitous across most of the developed world and beyond, UMTS offers global calling and data services through a myriad of different pricing plans and service offerings. The operator networks offer reasonable coverage, and reasonable levels of service, but cannot be relied upon for mission or business critical applications. In times of crisis they frequently become significantly overloaded, or in some cases disabled.

LTE/4G: Successor to UMTS/3G serving the same purposes but offering increased bandwidth, particularly uplink bandwidth, LTE offers the same benefits and drawbacks as UMTS, but currently with less national coverage. Will be onward developed in terms of performance and coverage. Considered as a successor to UHF/VHF radio for emergency services, however many specialist features need to be added to commercial LTE to meet the needs of this community. It is far from certain that LTE will be adopted for mission and business critical applications, and for this reason specialist private LTE networks may be developed and deployed by governments or military (or others who have the necessary licensed spectra) on a permanent or temporary basis, including static or mobile cell towers on drones/UAVs. As such this may lead to hybrid devices/relays which allow users to operate on both commercial and private LTE networks.

UHF/VHF radio: Line of sight communication for voice and low data rate services widely deployed with industry, government and military users. Viewed as very reliable and secure (when needed), but limited capability to deliver the bandwidth increases needed for new applications.

Specialist UHF/VHF radio: Line of sight communication for voice, video and high data rate services limited to specialist markets such as military users. Viewed as very reliable and secure (when needed), but limited availability and high cost.

Satellite: The only solution offering truly global communication. Most operable satellites are used for voice and low data rate applications by specialist markets such as oil & gas, mining, military, broadcast etc. With the advent of next generation High Throughput Satellite technology, significantly higher bandwidth is available at price points similar to fixed line home broadband services, making its adoption more likely.

High Altitude Platforms (HAPS): Viewed as a lower cost alternative to satellites, these communications solutions orbit in the stratosphere with the aim of offering 3G like services to 'off -grid' areas. One example is the 'Google Loon' project, but commercial deployments are yet to become mainstream.

Public Wi-Fi: With the mobile operators looking to supplement their available bandwidth through use of unlicensed Wi-Fi hotspots in public locations, this approach offers significant throughput gains over UMTS/3G and fills coverage holes in both 3G and LTE commercial networks. However, these Wi-Fi networks may be used by large numbers of users and offer no quality of service guarantees.

5G: Planned successor to LTE/4G networks very much in the technology development phase, with the aim of delivering significantly higher throughput in the 10-50Gbits/s range. No firm standards or rollout plans at the current time, this technology is planned for the 2020s.

Low Power WAN for IoT: LPWAN comprises a number of competing technologies aiming to deliver low power wide area networking for low data rate Internet of Things (IoT) (e.g. sensors). The technology is in its infancy but a number of trials and city deployment pilots are in operation (e.g. the LoRaWAN IoT network in Cambridge, U.K.)

Local Area Networks/Short Range Bearers

Wi-Fi: widely adopted wireless LAN technology offering high throughput at very competitive price points. Wi-Fi is deployed mainly for private use within residential and commercial properties offering ranges of 30m-50m, but has increasing adoption for public hotspots and specialist usage such as connections between drones and their base stations due to its operation in the unlicensed ISM (Industrial, Scientific & Medical) bands.

DSRC: Dedicated Short Range Communications or DSRC, sometimes referred to as Wireless Access for Vehicular Environments (WAVE) was specified for use in ad-hoc communication between vehicles and for use between vehicles and vehicle related infrastructure and as such is closely associated to V2X. The technology includes 802.11p (a modified version of Wi-Fi for operation in the licensed 5.9GHz

band), and IEEE1609 standards for security, set-up and management. Note, a number of vehicle management projects described as using DSRC use alternate technology such as infrared, different protocols etc.

Bluetooth: offers a very short range Personal Area Network (PAN) of less than 10m, Bluetooth is a cable replacement technology with widespread adoption in mobile phones and personal computing devices. Released as several variants, the latest Bluetooth Low Energy (BLE) variant may fall between two stools with Wi-Fi offering higher throughput and Zigbee (and similar technologies) offering lower power and lower cost for low data rate applications such as Home Automation.

Meshed: One of a number of competing low range, low power, low data rate technologies for use in Home Automation and other applications. Technologies such as Zigbee/802.15.4, Z-Wave and 6LoWPAN can operate in meshed configurations to cover larger areas at low cost and low power usage.

NFC: Near Field Communication is a very low range (circa 10cm) wireless technology for delivering easy-to-use, safe, two-way interactions between devices for applications such as contactless payment.

Infrastructure-less Mobile Ad-hoc Networks

Unlike the long range and short range networking technologies described, the MANETs in use today for secure reliable communication are typically proprietary, offered by specialist vendors with little standardization or public information available, hence no vendor interoperability.

Therefore, the text below provides some information on the types of technology used in these proprietary offerings and the benefits and drawback associated with each.

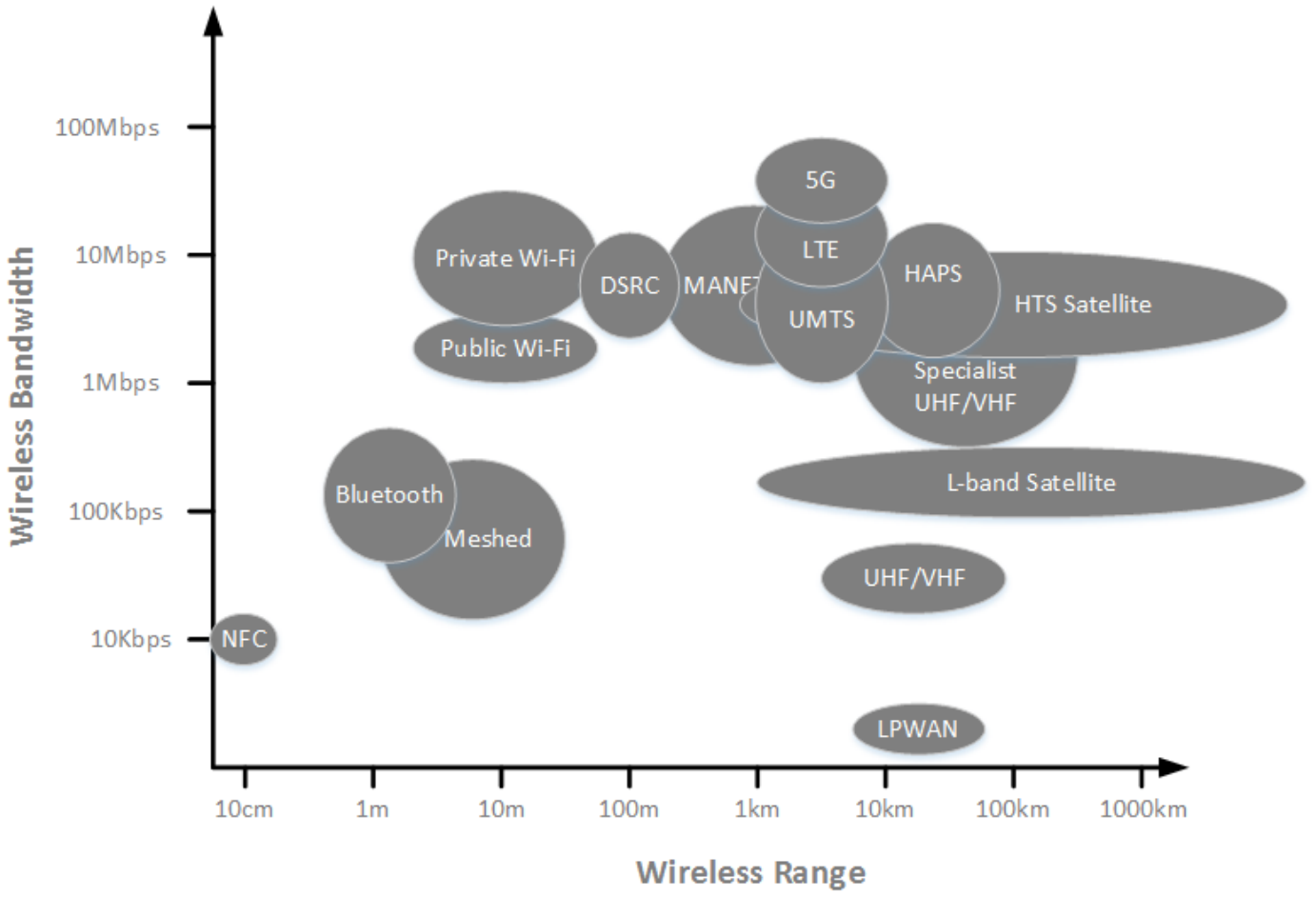

Figure 3 Wireless Bearer Range vs Bandwidth Comparison

MANET Waveform: the wireless physical and link layer technologies deployed in MANETs tend to operate in the frequency spectra between 1.5 and 2.5GHz and deliver throughputs in 10s of Mbits/s and ranges of a small number of kilometres. They should be considered as short or medium range technologies, where higher range is achieved with specialist, high value antennae.

MANET IP Networking: the IP routing protocols which operate MANETs tend to fall into one of three types:

- Proactive types determine the topology of the networks/nodes in advance of sending traffic, and as a result the routing overhead is high, but the initial latency is low;
- Reactive types only determine the network topology when they have traffic to send and as a result the routing overhead is low, but the initial latency is high;
- Hybrid types which combine elements of both pro-active and reactive types.

All types can achieve good operation up to sizes of circa 75 vehicles at speeds of up to 70km/h.

Multiple Bearers

With each of the wireless technologies designed for a specific purpose, it is now common for multiple wireless technologies to be deployed together. For example, as shown in Figure 4 it is advantageous to use both long range and short range bearers for the traffic control and vehicle control use cases (selecting the most available bearer in any location) and long range communication for applications that require it.

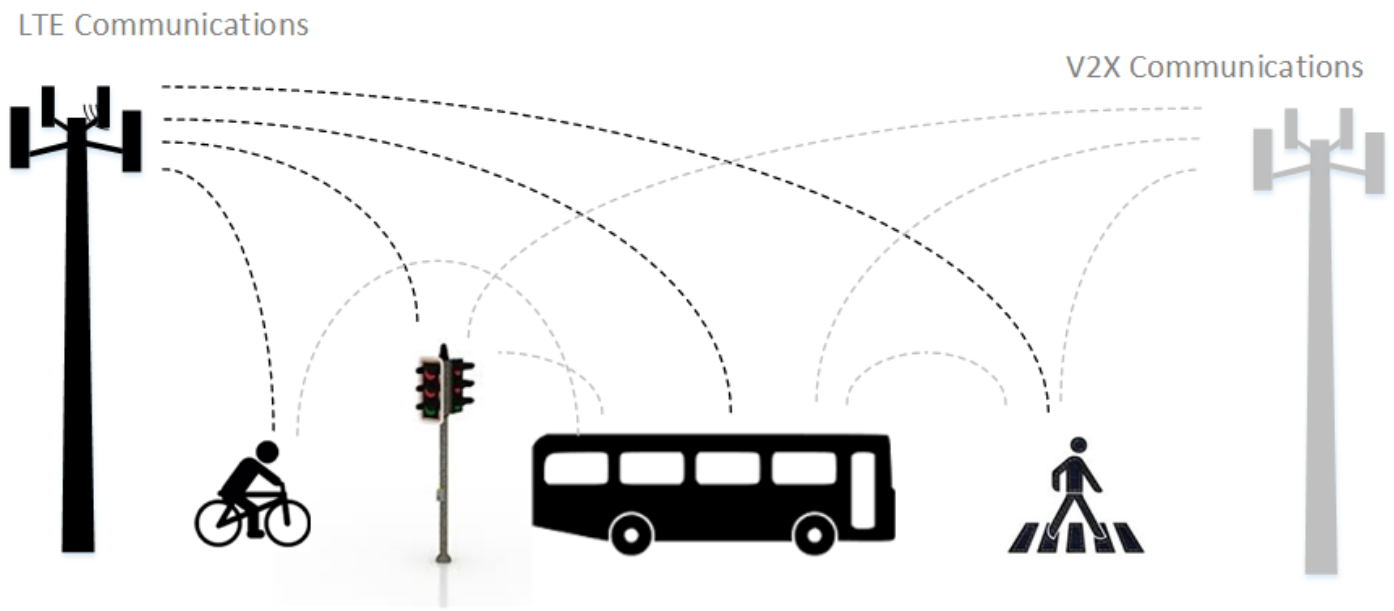

Figure 4 Multiple Bearers in Heterogeneous Wireless Communication Environments

OPERATION IN CHALLENGING ENVIRONMENTS

Introduction

In ideal conditions static wireless links and wireless networks can be as reliable as wired networks, but when users or vehicles become mobile the communication can vary in available bandwidth or suffer from intermittent connectivity to the network. In such circumstances the applications that operate over the wireless network (e.g. image transfer, voice calls) can become unreliable or simply fail to operate at all, with the applications' behavior under such conditions frequently exacerbating the situation.

The causes for variable bandwidth and intermittent connectivity are down to a number of factors such as network loading, user prioritization, terrain, range between devices, obstacles in the path between devices, use within buildings/vehicles which adversely affect radio wave propagation, and any interference (either intentional or unintentional).

The effects of such circumstances will vary from mild bandwidth reduction to complete connectivity failure. However, to mitigate these circumstances there is a toolbox of techniques and approaches which can be deployed to significantly improve application performance and reliability over wireless networks and in summary these comprise:

- Ensure applications operate effectively over bearers by masking the wireless nature of the bearer or making the applications 'wireless aware';
- Optimize, accelerate and compress application traffic to make best use of available bearer(s) bandwidth;
- Automatically select the most appropriate bearer(s) to use at any instant in time for application traffic;
- Add extra resources and capacity if necessary and where practical and cost effective.

Some specific examples of these techniques and approaches are listed below:

- Use of high gain intelligent antennae which adapt with location and position;
- Optimization of application traffic to reduce bandwidth by ensuring redundant or duplicated information is not sent over the network;
- Accelerating applications by masking them from network conditions they are unable to handle (e.g. very high latency, packet loss) through use of gateways;
- Masking bearer unreliability from applications through use of applications gateways which handle the transient nature of the wireless bearer whilst being always available to the native application (sometimes referred to as 'spoofing');
- Making applications natively resilient to the variable and unreliable nature of wireless communications (e.g. judicious selection and configuration of transport protocol parameters);
- Intelligent use, control and management of multiple wireless bearers for selecting the most appropriate bearer available at any instant in time for ensuring highest performance, lowest cost or best range;
- Intelligent use, control and management of multiple wireless bearer on different frequencies to mitigate interference or jamming;
- Addition of extra network capacity at selected locations (e.g. where an LTE or UMTS network has no coverage, deploy a Wi-Fi hotspot or booster box) linked to the mobile network (significantly lower cost than additional cell towers);
- Addition of aerial resources such as UAVs to fill areas of poor coverage;
- Addition of wireless relays to address any specific range or coverage issues.

Multiple Bearers

With the prevalence of many wireless technologies for many different purposes it is common for a mobile team or vehicle to be in a location where multiple wireless bearers are available, or move between locations where different wireless bearers exist. In addition, in locations where ample bandwidth is available, it is may be advantageous to combine or bond multiple radio links (operating on different frequencies) together for increased accessible bandwidth, or to operate radios on multiple operator networks simultaneously so as to always have the optimal wireless access, and switch to a new bearer before fully losing coverage.

In these cases, to ensure optimal use of these bearers the gateway should be able to detect the presence of available bearers at any instant, then use each bearer effectively to ensure optimal performance for each application. This is achieved through definition of a multi-bearer policy which defines how each bearer is detected, how it is controlled and operated and how each traffic type is sent over each bearer. Thereafter the multi-bearer gateway would operate automatically without user intervention to maintain seamless connectivity.

As with single bearer solutions, if applications are not designed to operate over unreliable networks it is important to mask the underlying bearer changes to ensure applications continue unaffected.

The benefits of this multi-bearer approach are:

- Can provide extra bandwidth where multiple homogeneous and/or heterogeneous bearers exist through bonding bearers together;
- Extends coverage by defaulting to wide area bearers when local area bearers become unavailable;
- Where multiple mobile operator networks exist, simultaneously connect to each to ensure the optimal wireless access is being used, and optimize access through intelligent bearer switching and predictive bearer switching to reduce downtime;
- Controls costs by selecting lowest cost bearer where appropriate;
- Deliver Quality of Service by selecting the best bearer for each traffic type;
- Mask or diminish bearer connectivity delays;
- Can report locations of no coverage for additional capacity planning.

Optimization, Acceleration, Compression, Caching

Where wireless bandwidth is limited or unreliable it is advantageous to control the nature and type of application traffic sent over a wireless link. The use of application level gateways allows the following techniques to be applied to application traffic. Note, the gateways are plug 'n' play and require no configuration and are transparent to the application, and for best results require a pair of gateways to be in operation in the path of the traffic:

- Optimization: analysis of application traffic to find recurring fields or patterns in traffic then send the pattern only once over the network, with a lightweight method for restoring the original data at the peer gateway to ensure lossless transmission;
- Compression of packet headers and content to reduce the size of the content being sent over the network, with decompression taking place at the peer gateway;
- Acceleration: with a knowledge of an application level protocol the gateway can operate the application protocol in a tailored fashion over the wireless link with a peer gateway to deliver performance levels not achievable by the native application (e.g. faster downloads, superior resilience to packet loss);
- Caching: removing duplicate requests for information by locally storing or caching the response from the first request for a piece of information. This can be performed on numerous applications and protocols (e.g. web traffic, DNS requests) resulting in reduced bandwidth and improved responsiveness;
- Filtering: removal of unnecessary, erroneous or unsolicited traffic from being sent over a link;
- Transcoding: changing traffic from mis-configured or sub-optimal devices to use less bandwidth hungry encoding;
- Buffering/timeout management: where an application is not real-time or responses can be delayed in time, then simply providing buffering capacity and local protocol operation in the application level gateway can ensure continued operation of an application level protocol during transient wireless bearer unreliability.

SECURE COMMUNICATIONS AND CYBER SECURITY

Overview

The requirement for secure communication has existed for many decades and many existing standards (e.g. the suite of IPSec protocols) fulfill the need for trust, privacy/secrecy and tamper proofing for remote communications. However, with the desire to control vehicles on tomorrow's highways there is now an equally important need for strong cyber security measures for mobile teams and vehicles to prevent malicious attacks which could result in fraud, non-operation or at worst hi-jacking of devices or vehicles for terrorist or criminal purposes.

With multiple applications running over potentially multiple wireless bearers, the need for an overall security architecture is paramount; very frequently security weaknesses and vulnerabilities come about not through weakness in core encryption or authentication algorithms but through weaknesses in key management or more mundane issues such as oversights in failures to apply security patches for vulnerabilities on all nodes on a network.

Therefore, any security architecture must deliver strong defenses and be practical to operate and manage, and any implementation should undergo appropriate industry certification or accreditation programs such as the US Department of Transportation initiative on the next generation of certification services in support of the Connected Vehicle Pilot Deployment Program.

The sections below are not intended to provide deep technical detail on security architectures but to introduce the major elements that need to be considered for any overall security architecture operating in multi-bearer environments and highlight technology components which may form part of any overall architecture.

Link, Access Network, Network-to-Network & Application Security

The security landscape in wireless communication involves elements at multiple layers of the OSI stack and at different points in the network architecture; these are introduced below and are typically used to deliver authentication, integrity checking and encryption:

- Wireless Access/Link: where traffic passes across a wireless link authentication and encryption may be applied to the traffic as it passes over the air. An example of such link encryption is the Wi-Fi Pre-Shared key (PSK) mode operated on residential home routers & devices. Note, once the traffic egresses the wireless link to pass onto its destination it is no longer secure. Also, for ease of access many public Wi-Fi access points do not operate link layer security and users are expected to operate higher layer security if needed;
- Access Network specific: consider an LTE network run by a mobile operator. The elements that connect to that network (e.g. the phone or UE) and operate within that network (e.g. Mobile Management Entity) will operate their own security for the benefits of the network and for network users. Once traffic leaves the mobile network (e.g. to connect to an Internet based host) the traffic is no longer protected;
- Network to Network: where traffic passes across many separate networks (e.g. a wireless access link, a private wired network, the Internet and onto a destination network) then industry standard IPSec protocols can protect the traffic;
- End-to-end: where applications operate their own security (e.g. by opening a Transport Layer Security connection) then the content generated by the application is protected over the entire path to the destination locations, or end-to-end.

Cyber-security Protection

The stated goals of security for communication are to provide message confidentiality, message integrity, delivery to intended recipients only and protection against 'fake' or replayed messages. However, as the world becomes more connected, security must also protect against attempts by malicious persons or organizations to attack infrastructure and devices themselves typically through electronic or 'cyber' means.

With the advent of connected vehicles and autonomous vehicles the results of any successful cyber attack become very significant indeed with threats to loss of life or serious personal injury in addition to criminal matters such as vehicle theft. In addition, there could be significant physical damage, and hence financial penalty and cost, to vehicles and/or property and these factors will demand clear and absolute liability for the organizations operating such solutions and their suppliers and partners.

The cyber security threats are many and can be grouped into:

- Physical attacks where a vehicle, device or component is tampered with, or stolen then corrupted, before being maliciously used on a network;
- Network attacks over wireless interfaces where malicious activity such as hacking, Denial Service of Attacks and jamming are used to inhibit, incapacitate or hi-jack a vehicle or device;

- Connected Service attacks where cloud based or centralized services can be compromised leading to many vehicles or devices becoming inhibited, incapacitated or hi-jacked.
- Social Engineering attacks on the persons involved in installing, provisioning, operating, maintaining and retiring such solutions;
- Criminal attacks including bribery of staff, blackmail of staff, theft of equipment or information by staff.

The pessimists view of the security of IoT devices or vehicles is that there are only two types, 'those which have been hacked, and those which have yet to be hacked'. However, there are many protections being deployed in current generation cyber security aware gateways, which form part of an overall security architecture. Although these architectures can never be perfect across all devices at all times, if properly maintained and operated, these architectures will deliver secure solutions which minimize successful attacks and limit their effects to acceptable levels. These protections include but are not limited to:

- Secure provisioning and management of device credentials;
- Ability to revoke or invalidate device credentials if/when a device becomes compromised, to prevent its use on a network;
- A secure mechanism to completely upgrade the security functionality of device over-the-air (OTA) to ensure it can be upgraded to handle future threats over a lifetime of decades;
- Ability to securely roll-out patches OTA to close off security vulnerabilities as they occur;
- Operating firewalls (either logical or actual) on network interfaces;
- Operating Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) on network interfaces;
- Behavior analysis of the typical activity of a device or system for determining out of the ordinary or anomalous behavior;
- Physical tamper-proofing of devices to prevent corruption or replacement with malicious components;

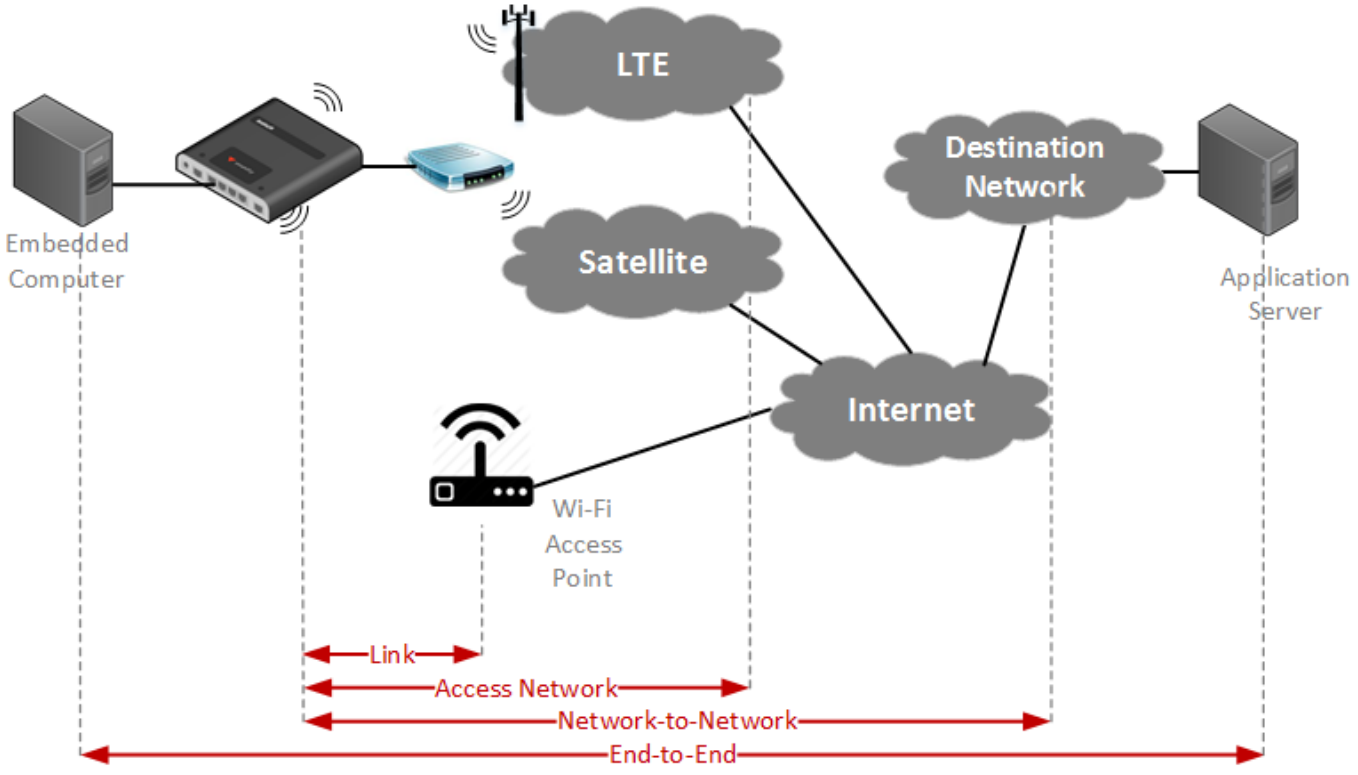

Figure 5 Security Points in a Multi-bearer Network Scenario

- Protection of programmable components (FPGAs, FLASH drives) to prevent re-programing devices with malicious code;
- Hardening against Denial of Service/Distributed Denial of Service (DoS/DDoS) attacks such that devices can survive the duration of the attack and begin normal operation thereafter;
- Real-time processing of wireless messages, where necessary through Hardware Security Modules, to ensure real-time responses and hardening against DoS/DDoS attacks;
- Use of hardware acceleration in security processing to support longer key lengths to protect against brute force key cracking;
- Formulation of, enforcement of and mandatory participation in industry and government certification and accreditation schemes.

Security with multiple bearers

Where multiple wireless bearers are in operation on a device, then each wireless bearer is likely to operate with a different IP address, and in some cases the IP address will be assigned by a network (e.g. LTE), may change over time and may be re-written by any address translation entities operating in the network, hence traffic passing to/from a mobile team or vehicle may arrive at a destination with any IP address. Therefore, as opposed to authentication based on IP address as is commonly used in static networks, identity based authentication must be operated to support mobile devices connecting with IP addresses unknown to the destination.

When a gateway does operate multiple bearers, then the gateway must automatically start the security context associated with each new bearer to ensure continued security. Note, this automated binding of security and bearer is not standard behavior in networking solutions (compare with a Windows PC switching between a Wi-Fi and an LTE interface which would not re-start a VPN but would require the user to re-initiate the VPN tunnel).

Certificate Provisioning & Management

The adoption of Public Key Infrastructure (or PKI) in many commercial grade security architectures is due to the strength of the technology with PKI offering scalability, very strong security and centralized management.

These benefits point to PKI and its use of X.509 certificates being a core of any security architecture, however certificate provisioning, management and protection is not a trivial task.

Therefore, a number of commercial and technical activities are in progress to automate this task including:

- The establishment of publicly available Security Credential Management Services (SCMS) for manufacturers to install devices and vehicles with a trusted certificate (the Enrollment Certificate) during the manufacturing and test cycle;
- The use of these SCMS for providing a block of Pseudonym Certificates to a device which can be for used over a number of years, where each may be valid for a short period (e.g. 1 week) and a number may be used in parallel;
- The use of multiple Pseudonym Certificates during short periods, which are then discarded at the end of the short period, to prevent the tracking of devices;
- A Certificate Revocation List (CRL) issued to a device by a SCMS CRL Signer which allows the device to check the validity of a certificate in use at any instant in time;
- A device shall use the Pseudonym Certificates when participating in V2X communications with other devices, whereby the first device shall use its Pseudonym Certificate to sign a message which presents the holder's permissions but not its identity, send the signed message to the second device(s), and the second device(s) shall use its CRL to confirm if the sender's certificate is valid;
- The Enrollment over Secure Transport standard (RFC7030) from the IETF for use with SCMS for automated provisioning of X.509 certificates;
- Periodic updates to Certificate Revocation Lists (CRLs);
- The Online Certificate Status Protocol (OCSP) for determining the revocation status of certificate as an alternative to CRLs.

VOCALITY SOLUTIONS

Vocality has been a supplier of critical communication products for over 20 years with customers on seven continents. Our products are in use with government, military, law enforcement and blue light services, oil & gas, maritime, broadcast and transport customers, in fact with anyone who needs reliable, real-time secure communications in challenging environments.

The Vocality product families address differing user requirements and are designed with a number of common themes:

- Low Size, Weight and Power (SWAP) hardware consuming as little as 3W and smaller than 10cm x 10cm;
- Rich set of network and device interfaces including but not limited to Ethernet, Wi-Fi, UMTS, LTE, serial ports, four wire, analogue phone, PBXs, E1/T1 and ISDN;
- Intelligent applications, capabilities and functionality for operation of secure communications protocols in challenging environments;
- Easy to use, intuitive, plug 'n' play user interfaces incorporating industry APIs for operation in private, public and cloud centric environments.

The Vocality product families are listed in the table below.

Family	Overview	
OPUS	A set of software applications for operation on COTS, virtualized, 3rd party and Vocality platforms including optimization, security, multi-bearer, routing, voice, radio dispatch and other applications.	
BASICS	A family of very low SWAP connectivity products for critical communications supporting phones, radios, computers and other devices. Available in boxed and integrator versions.	
PRO	Rackmount equipment designed for maximum capacity, compatibility and flexibility which is often used as a centralized communications hub.	
ELITE	Created to fulfill the most demanding of requirements when it comes to connectivity and security.	

Vocality Gateway Products

Vocality products are frequently deployed as remote gateways and two examples are expanded upon below.

The OPUS RoIP product operates a number of OPUS Software application modules on a small form factor SWAP radio gateway platform allowing remote computers and radio users to securely communicate to centralized resources over a number of wide area networks such as satellite, 3G/4G or private networks.

Figure 6 OPUS RoIP

The industry leading SWAP design device is available as a boxed product or as a PC104-compatible form factor for integration into vehicles or other housings.

The OPUS application modules include OPUS Multi-bearer for intelligent simultaneous operation of multiple WAN links, OPUS Enhance for ensuring these WAN links are used efficiently and OPUS Secure for strong scalable security over these WAN links.

The ELITE Fusion product is the ideal product for first responders who need to securely communicate with their HQ whilst traveling or on active deployments to remote or urban locations. The product is small enough to carry in hand luggage comprising a Red Enclave and a Black Enclave which can be physically separated for TEMPEST compatibility, between which a 3rd party encryptor can be deployed allowing a remote 'Red' level security network to be operated.

The Red Enclave supports a rich set of device interfaces allowing connection of radios, phones, computers and other IP devices. The traffic to from these devices is efficiently combined and passed to a 3rd party encryptor, before entering the Black Enclave.

The Black Enclave integrates Wi-Fi, 3G, 4G and Ethernet WAN interfaces allowing traffic to be securely tunneled back to HQ through national infrastructure networks, public or private networks. The easy to use touchscreen allows travelers to connect to and use these public networks without the need for a 'Black' level security network laptop.

The ELITE Fusion operates a number of OPUS Software application modules which also allows standalone secure communication (without the need for a 3rd party encryptor), optimization of traffic sent over WAN links and controlled policy based use of available WAN links to provide seamless communication.

Figure 7 ELITE Fusion

Vocality Software Products

The OPUS Suite of software applications are designed to provide intelligent IP networking applications for operation on COTS, virtualized, 3rd party and Vocality platforms. The support for this wide range of platforms means additional hardware need not be deployed to address IP networking solutions, saving on deploying multiple hardware devices, and/or obviating the need for expensive re-accreditation and re-certification programs. The OPUS applications include:

- **OPUS Enhance:** for efficient operation of traffic over low bandwidth or unreliable wireless communication links such as satellite, Wi-Fi or UMTS. The modules provide optimization for bandwidth reduction, acceleration for increased application performance (e.g. download speeds), caching for the removal of duplicate transfers and unwanted traffic filtering;

- **OPUS Secure:** for strong scalable commercial grade security based on IPSec protocols and Public Key Infrastructure this module provides easy to set up interoperable VPN tunnels based on device identity allowing mobile workers to connect from any location in the world. The security is tightly coupled with the OPUS Multi-bearer module allowing security to be automatically provided across multiple simultaneous bearers without the need for user intervention;

- **OPUS Multi-bearer:** policy based control of multiple WAN bearers for seamless connectivity between remote devices and centralized resources ensuring maximum coverage and optimal choice of bearer for each traffic type for each user;

- **OPUS Dispatch:** a rich graphics drag and drop utility to allow creation, edit and management of radio Talk Groups allowing radio users to be added or removed from these radio Talk Groups through single graphic operations which automatically perform complex device configuration without the need for user configuration. OPUS Dispatch can run on gateway devices, standalone COTS or virtualized platforms or in the cloud.

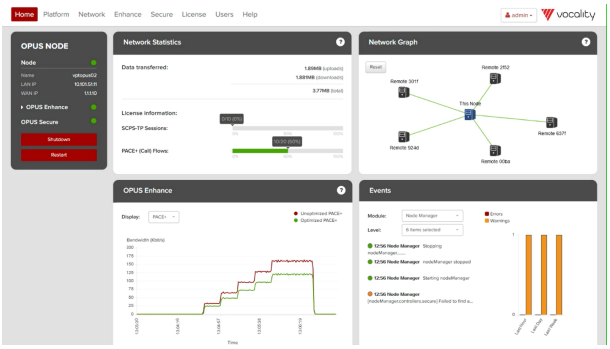

Figure 8 OPUS Node GUI Homepage

ADDITIONAL INFORMATION

You may also want to read the datasheets and setup guides for Vocality products, which are available through the Vocality Support portal.

If you need more information about how we can help solve your communication challenges, please contact your Vocality representative.

About White Papers: White Papers are discussion starters or supplementary information written by Vocality technical experts. Should you have queries which are not answered by our current documentation, your local Vocality support team would be happy to hear from you. E-mail **support@vocality.com**.

Cubic Mission Solutions
Lydling Barn, Lydling Farm, Puttenham Lane
Shackleford, Surrey GU8 6AP United Kingdom
Tel +44 1483 813 130 Fax +44 1483 813 131
E-mail: sales@vocality.com
www.vocality.com

Cubic Mission Solutions
21580 Beaumeade Circle, Suite 230
Ashburn VA 20147 United States
Tel (703) 787 9133 Fax (703) 787 9136
E-mail: sales-usa@vocality.com
follow us on twitter @vocality