THORCOM

White Paper

Multi-bearer enterprise wireless solutions for mission-critical mobile data systems

Important considerations for implementing a mobile data solution on ESN using a vehicle communications hub with multiple network operators (MNOs), multiple bearers per network, including traffic prioritisation and Quality of Service support.

The emergency service sector has been using mobile data for many years to ensure incidents are attended to quickly, efficiently and safely. The availability of 4G/LTE advanced wireless network services will facilitate much greater use of mobile data applications to improve overall effectiveness and produce better outcomes for the public. Vehicle based users will have access to multiple devices with an expanding range of applications that require reliable and efficient communications provided by a vehicle communications hub.

What are the main requirements of a vehicle communications hub to provide the highest possible levels of availability, resilience, prioritisation, and security to emergency service users?

Avoid bearer switching

Mobile and cellular networks are inherently more unreliable than wired networks. Even networks dedicated to emergency service users will experience message loss caused by signal fading (driving past structures, dips in coverage) and areas of marginal coverage or no coverage at all. The use of multiple wireless providers (bearers) can significantly help address this issue.

Some vehicle routers switch between bearers based on signal strength in an attempt to maintain connectivity but this takes time to assess the bearers and switch over, and operates 'after the fact'. Bearer switching does not address the 'drop outs' that happen in real-time and relies on the application to perform re-transmission attempts, introduces transmission delays and creates the potential for the loss of critical messages.

Bearer switching is also asymmetric because central systems have no knowledge of the radio conditions experienced at the vehicle and cannot know which bearer to switch to when sending critical messages such as 'mobilisation messages' to vehicle resources.

More sophisticated solutions implement parallel bearer operation where critical messages are sent over multiple bearers at the same time, eliminating the need for switching bearers, re-transmissions, delays or message loss. Using parallel bearer operation significantly increases message reliability and system resilience, reduces failed messages and reduces the transmission time for business-critical and mission-critical messages.

Several UK ambulance Trusts already employ multi-bearer parallel operation in their solutions which results in very high message reliability.

Critical messages represent a small fraction of the total messages sent and received by the mobile data solution and can generally be accommodated within the standard data allocations provided by mobile network operators so there is minimal or no increase in airtime costs associated with parallel bearer operation.

Mobile optimised and ‘Bearer Aware’ VPN tunnel

Standard VPN tunnel protocols such as IPSEC may appear a candidate for providing end-to-end IP addressing and security for mobile applications but have a number of drawbacks when used mobile environment with 4G/LTE specific features such as Quality of Service (QoS) and Traffic Prioritisation.

Several UK ambulance Trusts already employ multi-bearer parallel operation in their solutions which deliver very high availability.

Anonymous traffic - IPSEC encapsulates all of its traffic inside a new IP message packet (an IPSEC packet) which is transmitted over air – this effectively anonymises the traffic causing the 4G/LTE cellular system to see only one packet type - meaning that QoS Control Indicator (QCIs) cannot be triggered for any critical traffic because all the traffic looks the same.

Channel bonding and parallel operation - IPSEC is not able to ‘bond’ two or more bearers together to provide multi-bearer parallel operation with critical traffic directed down both bearers and other traffic sent over a single bearer. This means either sending all the VPN traffic at one prioritisation level which might overwhelm the priority bearers, or alternatively sending the VPN traffic down non-prioritised bearers, losing the main advantage of Critical Data Bearer, so neither approach meets the requirement.

Consider a solution that implements an advanced VPN that supports ‘Multi-Bearer Tunnel Protocol’. This will allow traffic classification and mapping of traffic on to 3GPP/LTE Quality of Service Class Identifiers (QCIs) to exploit the traffic prioritisation capabilities of ESN, at same time as directing non-critical messaging over other bonded bearers.

WiFi as a mobile communications bearer

The solution should allow a WiFi connection to be added to the available communications bearers when a vehicle is at a depot, station or location that has a suitable WiFi access point and network connectivity to the data centre. As well as supporting this ‘WiFi Bearer’, the hub should also provide a separate WiFi Access Point capability to connected mobile devices.

The WiFi bearer may be used in preference to, or in conjunction with, the other mobile network operator bearers. The addition and removal of the WiFi bearer to the communications sub-system should be automatic and transparent, and require no user intervention.

Traffic prioritisation and quality of service

The Emergency Service Network (ESN) will provide fixed connection, known as an ‘APN’. This will incorporate multiple bearers including a Critical Data Bearer for mission critical data use, an Essential Bearer for business-critical application use and a Default Bearer for other applications such as email and web access, etc.

A second cellular service may be used to provide an independent additional bearer, possibly also with traffic prioritisation, and infrastructure WiFi may also be available as a third bearer.

The solution needs to be able to identify traffic types based on the protocol, addresses and port numbers used and map the traffic to the appropriate bearers. This cannot be done by simply encapsulating traffic inside an IPSEC tunnel because IPSEC makes the traffic anonymous - instead the solution should take a two-step process:

1. Identify the application traffic type and map it on to an instance of the multi-bearer tunnel protocol. Several instances of the tunnel run in parallel – one for each category of traffic.
2. Map each tunnel instance to the appropriate bearers using a 4G/LTE Traffic Flow Template which has been configured by the network operator to map tunnel instances to 4G/LTE QCI/ARP values

Modern data encryption

High quality data encryption is required for confidentiality to secure personally identifiable information and protect systems which are part of Critical National Infrastructure.

Standard key negotiation protocols such as Internet Key Exchange (IKE) require ‘stateful key exchange’ which can fail in areas of marginal radio coverage because of the complex handshake processes involved.

Consider solutions that use strong data encryption and modern cipher suites such as AES-256-GCM and that meet or exceed the NCSC/CESG recommendations.

Integration with mobile network operators

Solutions that are integrated with the Mobile Network Operator (MNO) infrastructure via protocols such as Remote Authentication Dial-In User Service (RADIUS) have a range of off-the-shelf benefits that include:

Device and user authentication – meets the requirements of the NCSC/CESG ‘End User Device Security Collection’ (EUD)

IP address assignment – allows device IP address assignment and management from a central database

Presence information – provides real-time presence information, i.e. whether a device is online and active or switched off. Presence information can be maintained separately for each bearer leading to faster routing decisions

Device control – allows a device to be disabled if it is lost or stolen by marking it as out-of-service

Accounting information – provides counts for data transferred in each direction for the duration of the session. This allows measurement of utilisation, traffic analysis and billing functions

Coverage diagnostics – provides network cell tower identification with each access to the network, which can be analysed geographically with utilisation information to determine cellular coverage issues.

Include transition technologies

The roll-out of new 4G/LTE wireless services such as ESN will take time, in particular access to the Critical Bearer at the same geographic coverage standard provided by legacy network services. Look for a vendor that supports legacy network services, such as Airwave TETRA in the UK to allow applications to make continued use of existing network coverage whilst the new service is being rolled out.

Open standard and Flexible Interfaces

Highly reliable parallel-bearer operations are technically complex to deliver and integrate. Proprietary solutions with inherent technical limitations are therefore sometimes evolved to meet the requirement, causing potential integration issues with third party devices and applications that implement conventional IP networking.

Look for a vendor that provides a generic solution which works with all cellular network technologies, WiFi and Satellite Communications bearers (ideally up to a maximum of 16 bearers), and uses standard IP networking (IPv4 and IPv6) to support any standard device, system or application that employs conventional TCP/IP or UDP/IP protocols.

About Thorcom Systems
Thorcom Systems makes mobile workforce management and fleet management solutions. We are a UK technology company with over 20 years’ experience delivering leading edge solutions to business-critical and mission-critical users in the emergency services, public utilities and public transport sectors.

For more information visit
https://thorcom.uk

THORCOM