DragonWave
www.dragonwaveinc.com

ABOVE GROUND LEVEL agl

Microwave Radio for Wireless Public Safety

Bernard Prkic

Article

August 20, 2015

Wireless public safety networks are in a flux, driven by emerging user requirements and expectations, such as bidirectional video streaming and real-time uploading and downloading of high-resolution pictures. These new, high-data-rate requirements are beyond the capabilities of the legacy — mostly time-division, multiple-access-based — data backhaul architectures that support the majority of today's wireless public safety networks.

At the same time, traditional values of public safety networks must be upheld. If remote and sparsely populated areas are to gain service, then service latency has to remain low and service availability needs to be high. In addition, the networks have to be both resilient against attacks or natural disasters and meet the highest standards in terms of network integrity and data confidentiality.

The following information explains why the third generation of rugged, all-outdoor, ultrahigh-capacity packet microwave radios can be the ideal backhaul engine for wireless public safety networks.

Important Attributes for Microwave Radio Backhaul

- Rapid deployment capability
- Acceptable total cost of ownership
- High service availability on the order of 99.995 to 99.999 percent
- Low link latency: 0.1 milliseconds to 1 millisecond per link
- High link bandwidth: up to 200 megabits per second per wireless base station site

- Support for frequency and phase synchronization in cases where a time-division duplex or 4.5 G-based technology is used for the radio access
- Network resilience, no single point of failure in any vital part of the network
- A high degree of network integrity and data confidentiality

Public Safety Networks

Microwave radio technology has found its way into public safety networks, providing data backhaul services for wireless applications such as TETRA, which is Terrestrial Trunked Radio, a professional mobile radio and two-way transceiver specification designed with government agencies and emergency services in mind.

Rapid deployment capability and an acceptable total cost of ownership are clearly important attributes for any backhaul technology supporting a wireless public safety network. But more is needed, especially for next-generation broadband wireless public safety networks. Additional important requirements that are desired by microwave radio backhaul include high service availability on the order of 99.995 to 99.999 percent, low link latency of 0.1 milliseconds to 1 millisecond per link and a high link bandwidth up to 200 megabits per second per wireless base station site. Other important requirements are support for frequency and phase synchronization in cases where a time-division duplex (TDD) or 4.5 G-based technology is used for the radio access, network resilience such that there is no single point of failure in any vital part of the network, and there is a high degree of network integrity and data confidentiality.

Wireless Networks in Flux

Public safety teams have been equipped with digital photo and video cameras and portable or vehicle-based data terminals for remote database access and for command and control purposes. There is a latent need for public safety applications to support live high-definition video streaming and instantaneous uploading of photos and film. Unfortunately, wireless access and backhaul technologies deployed in most of today's wireless public safety networks are still based upon time-division multiplexing (TDM) technologies developed more than 15 years ago, and are therefore incapable of providing a veritable broadband service. Examples of TDM technologies in use are plesiochronous digital hierarchy (PDH) and synchronous digital hierarchy (SDH)/synchronous optical networking (SONET).

In some markets, this discrepancy between user needs and network capabilities is being addressed by a hybrid network model. The key voice service and narrowband messaging services are kept on the private, dependable and full-coverage wireless public safety network. Meanwhile, broadband data capability is provided by third-party public land mobile broadband networks.

Although this hybrid solution may appeal to the instincts of the procurement community, it has serious shortcomings and can therefore only be regarded as a mediocre stopgap solution. The main reason is that public wireless networks have not been engineered — mostly because of competitive cost pressures — to be as resilient and secure as dedicated, public-safety wireless networks.

Examples of weaknesses of public broadband networks that render them to be a suboptimal choice for public safety applications include a lack of battery backup systems or the use of a short-term battery backup, the existence of single points of failure almost everywhere in the access part of the network, and the use of frequency bands that are generally higher than the bands used by wireless public safety networks and therefore provide less in-building coverage. Sites used by public broadband wireless networks are more readily accessible and therefore are more easily compromised or sabotaged than the secure sites purpose-built for a public wireless safety network.

In case of calamities, public broadband networks — ironically especially those parts located in the disaster area — will tend to overload or will be forced offline because of a power outage or structural damage to sites or the backhaul network. Avoiding this problem has historically been one of the key rationales behind pouring significant amounts of money into dedicated, purpose-built wireless public safety networks.

Public broadband networks use a mix of owned infrastructure and leased infrastructure for data backhauling. Data security and confidentiality are therefore not warranted. And the public broadband network is more exposed to the Internet and therefore is more prone to malicious intrusion and attack than a largely stand-alone public safety network.

There's a genuine need to evolve the broadband data capabilities of public wireless safety networks to the level of current 4G LTE networks and beyond. In order to support such an evolution, microwave backhaul has to evolve too.

Traffic Type	Throughput w/o BAC	Throughput w BAC
Web traffic (Top 100 sites, HTTP and HTTPS)	242.5 Mbps	622.6 Mbps
XLS and email traffic mix	242.5 Mbps	606 Mbps
MP4 video traffic	242.5 Mbps	355 Mbps
Mixed traffic (Web, video and ftp)	242.5 Mbps	505 Mbps

Table 1. An example of how throughput in a 28-megahertz-wide channel can be increased by applying bulk compression.

The Ideal Backhaul Engine

The third generation of rugged, all-outdoor, ultrahigh-capacity packet microwave radio is the ideal backhaul engine for next-generation broadband wireless public safety networks.

First, all payload generated by a broadband wireless network is by default packet-based. There's no need for circuit emulation or deployment of hybrid systems. High-capacity Gigabit Ethernet (GE) or even 10 Gigabit Ethernet (10GE) interfaces substitute a large number of narrowband, legacy PDH and SDH/SONET interfaces.

Second, no shelters at all are needed for backhaul equipment. Third-generation packet microwave radios are rugged, all-outdoor systems with four GE interfaces, plus a potent multigigabit Ethernet switch (14+ Gbps) in a single, integrated system. It disposes of traditional split-mount system indoor units and cell-site routers, freeing up space and budgets.

Third, they provide high baseline spectral efficiency, in the order of 8 bps/Hz using 2048 QAM or 4096 QAM modulation. Spectral efficiency can be doubled to 16 bps/Hz by deploying 2x2 line-of-sight (LoS) MIMO (multiple-input, multiple-output) communications or 2+0 cross-polarization interference cancellation (XPIC). MIMO communication is a radio frequency scheme where multiple transmitters and receivers (with a minimum of two) are used at each end of a link to increase the link spectral efficiency of a single (polarization) radio channel by up to 100 percent, or to increase link budget by up to 9 dB (in a 2x2 MIMO case). XPIC is a radio frequency interference cancellation scheme enabling the

use of a single radio channel in two spatially orthogonal polarizations in order to double link throughput and, in a way, spectral efficiency.

Beyond that, there's the possibility of boosting spectral efficiency to >32 bps/Hz by deploying wire-speed bulk data compression. Spectral efficiency reduces operational expenditure by paring down channel size and spectrum lease cost or provides for additional traffic capability. Table 1 shows an example of increased throughput in a 28-megahertz-wide channel that results from bulk compression.

Ultrahigh-capacity packet microwave radios support a large channel size. It helps to use large channels where high throughputs are required for trunking purposes. Third-generation all-outdoor packet microwave radios support 100 (ANSI) and 112 (ETSI) megahertz-wide channels. In case even more capacity is required, multicarrier microwave radio variants are available as a cost-effective alternative to discrete 2+0 and 4x4 MIMO configurations.

Topological redundancy: Full support for equipment and topological redundancy leads to link availability in excess of 99.999 percent and to network resiliency on the macro level. Equipment redundancy means that every link can be configured with no single point of equipment failure. Topological redundancy is implemented by building a network topology that can maintain connectivity between key network points A and B through different physical data paths. If one path is cut, one or more alternative paths exist. Third-generation all-outdoor microwave radio equipment supports this through the implementation of redundancy protocols like Rapid Spanning Tree Protocol (RSTP) and Multiple Spanning Tree Protocol (MSTP), protecting against multiple simultaneous failures yet relatively slowly — (200 to 2,000 milliseconds) or G.8031 (Ethernet Linear Protection) and G.8032 (Ethernet Ring Protection) — while protecting against a single failure yet very fast (< 50 milliseconds). Figure 1 shows a network topology that mitigates the risk of the failure of a single link or site.

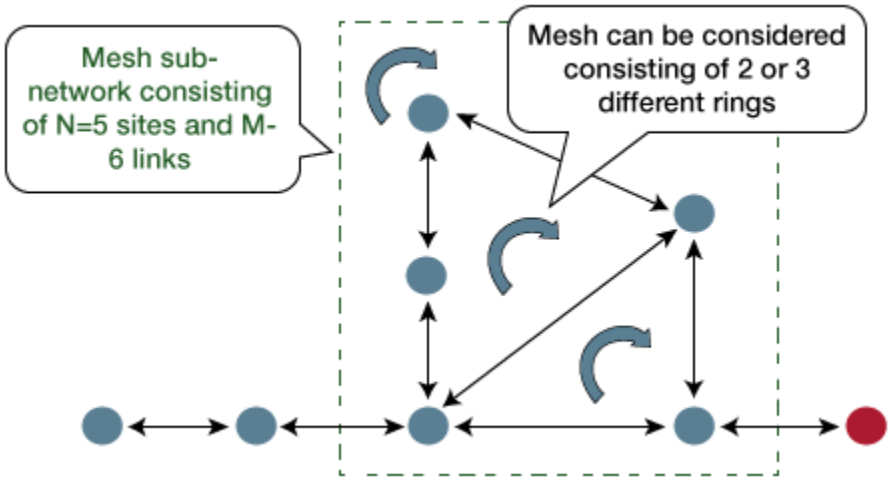

Figure 1. The network inside the green dotted box can be protected topologically. A single link failure will not affect any site; a single site failure won't affect any other site.

Low latency: Microwave radio links featuring high spectral efficiency and capacity provide for lower link latency than less efficient, slower links. Third-generation all-outdoor packet microwave systems can have latencies as low as 0.1 milliseconds. Mobile broadband system-inherent latency is on the order of 10 to 15 milliseconds one way, end to end, and the contribution of third-generation microwave systems to the overall latency is limited. Full system performance is warranted when using such microwave links for backhaul.

Comprehensive synchronization support: Third-generation all-outdoor packet microwave systems support frequency synchronization though Synchronous Ethernet and frequency and phase synchronization. This is achieved by treating IEEE1588v2 synchronization packets with the highest priority in their queueing system and minimizing jitter by means of packet cut-through for highest-priority packets. In addition, phase synchronization accuracy is improved by means of a Transparent Clock, an algorithm compensating for microwave link-induced jitter and latency. Phase synchronization is required for synchronizing TDD-based wireless access technologies and for advanced 4.5G features requiring phase lock of the wireless air interface across the entire network.

Strong support of network integrity and data confidentiality: Third-generation all-outdoor packet microwave systems support SNMPv3 for full encryption of the management plane for the microwave

system. They also support centralized remote access dial-in user service (RADIUS) and terminal access controller access-control system plus (TACACS+) user authentication. On top of this, all of the payload transiting the air interface can be AES256 encrypted.

Conclusion

Wireless public safety networks are evolving toward supporting mobile broadband services, while maintaining the high service availability and data security standards of today's voice-centric networks.

Third-generation rugged, all-outdoor, ultrahigh-capacity packet microwave radio is ideally suited as the main backhaul engine for a broadband wireless public safety network because of its modest total cost of ownership and excellent technical attributes tailored toward supporting 4G and 4.5G wireless access networks.

View this Article Online

http://bit.ly/1JtHN7A