CONSIDERATIONS WHEN DEPLOYING MULTIPLE DISTRIBUTION AUTOMATION APPLICATIONS ON A SINGLE WIRELESS INFRASTRUCTURE

Maciej Goraj
RuggedCom - Spain
MaciejGoraj@RuggedCom.com

Tony Burge
RuggedCom - USA
TonyBurge@RuggedCom.com

ABSTRACT

This paper describes various wireless communications requirements for multiple distribution automation applications and the available point-to-multipoint or mesh wireless communications technologies available for these applications.

INTRODUCTION

Increased power demands in recent years have put correspondingly increasing pressure on electric utility companies to improve operational efficiencies. Providing immediate access to critical and operational data to field force personnel, improving distribution automation communications, and providing additional security via video surveillance all support efforts to improve operational efficiencies. With multiple technology options, beginning with the decision to use public/carrier infrastructure or invest in private infrastructure, and various application requirements, it is imperative to minimize infrastructure by selecting a wireless technology that provides the data capacity, security, and flexibility to support these applications on a single network infrastructure.

MULTI-APPLICATION REQUIREMENTS

Networks are often driven by one application, but once in place these networks are often required to support many others. In the case of utilities, distribution automation applications provide the most immediate efficiencies; however, other applications, such as video surveillance/monitoring, voice services, and field force automation are desired to provide additional operational efficiencies and grid robustness.

Throughput

Please note, this paper is not written with the intention of providing full capacity modelling (which would be a subject in itself); rather, this paper provides general guidelines of the most critical requirements, of which throughput is one.

Surveillance-quality video throughput requires approximately 2 mb/s using MPEG-4 compression. Lower resolution, lower frame rate video monitoring can be accomplished using as little as 256 kb/s, which still exceeds many wireless communications capacities. Most of this communication is uplink data.

SCADA polling, Volt/VAR control, Fault Detection, Isolation, and Restoration, and Capacitor Bank monitoring applications do not require substantial data—perhaps 10-15 kb/s each. However, when aggregated, the throughput for these mission critical applications can exceed 100 kb/s. Most of the communication for these applications is uplink data.

In certain substation environments, cell phone coverage is poor and a dedicated phone line is impractical or too expensive. Therefore, a Voice over IP (VoIP) line is often required to provide field engineers the ability to communicate with advisers at the back office. A good, toll-quality VoIP connection requires 64 kb/s. This communication equally splits between uplink and downlink.

Finally, operational efficiencies can be extended by providing field personnel with wireless connectivity while performing maintenance—for maintenance work orders, access to agency Intranet for schematics and manuals, and more. This communication can easily require 500 kb/s. This communication is mostly downlink data traffic.

Range

The range of the radio frequency (RF) technology and interference mitigation features implemented contribute directly to coverage. The more coverage provided by a solution, the less amount of infrastructure and capital expenditure is required.

For a wide area wireless broadband solution, range should be measured in kilometres, not meters. Range is determined by occupied channel bandwidth, power allocation, deployed frequency, and features such as Orthogonal Frequency Division Multiplexing (OFDM). There is often a trade off between throughput and coverage, so it is important to find the balance that provides the throughput required for multiple applications while maximizing the range.

Latency

Latency, or response time, for power utility applications is measured in milliseconds for point-to-multipoint wireless communications. Mission-critical distribution automation applications often operate effectively with wireless technologies that support less than 100

millisecond roundtrip response time. Even the most efficient, transparent transceivers support at best 8 to 10 milliseconds, which is why point-to-multipoint RF communication is not used as a primary communication technology for generation and transmission protection and control applications that require a quarter of a cycle, or 4 millisecond response time to protect high valued equipment. (However, point-to-point RF communications may be used as a redundant communications technology for fiber in these protection and control applications.)

A good target for round trip, point-to-multipoint latencies for distribution automation is under 40 milliseconds. This latency metric provides room for retries without adversely affecting distribution automation applications.

Security

Power utility infrastructure is arguably the most important asset to industrialized states, provinces, and nations. Protecting data that monitors and controls this infrastructure is a primary requirement for wireless networks deployed for such purposes. At a high level, data security can be discussed in three categories: Transmission Security, Network Authentication, and Data Segregation.

Transmission Security

Transmission security involves encrypting data at a transceiver prior to sending the message. The receiving transceiver then decrypts the message. This process protects the contents of the message as it is transmitted over the airwaves.

Certain encryption standards, such as RC4, DES and AES have emerged to enhance the integrity of wired and wireless communications.

Network Authentication

While transmission security facilitates the integrity of data as it is be transmitted over the airwaves, network authentication is intended to prevent unauthorized access to the network itself, which is a vital component of network security. It would be disturbing enough to have data "sniffed" over the air; it is even more harmful to have unauthorized access to the network itself. Unauthorized network access can result in denial-of-service, access to sensitive, utility-wide operational data, and manipulation of the data to interfere with the power grid itself.

IEEE 802.1X port-based Network Access Control (PNAC) and Extensible Authentication Protocol (EAP) are often implemented in Authentication, Authorization, and Accounting (AAA) servers to provide secure network access. IEEE 802.1X is often implemented under the name RADIUS.

Data Segregation

Within a physical network, administrators may require virtual networks to segregate data such that access to data can be limited to certain functional groups.

IEEE 802.1Q (VLAN Tagging) provides separate virtual networks within a single physical network, which provides administrators the ability to restrict user or application access only to relevant portions of the network.

Other Security Considerations

Other security measures to be considered are intrusion detection features, tamper-evident/tamper-proof fabrication, and facility security.

Prioritization

With multiple applications (or services) running over a single network, it is important that mission-critical data receive priority. Without such a mechanism, VoIP calls or field force network access could hinder fault detection notifications, out-of-tolerance voltage variation corrections, SCADA polling responses, and more.

IEEE 802.1P, Quality of Service (QoS), was defined to provide multiple levels of prioritized service.

Proprietary and Standards-based Protocol Support

The utility grid has been called the oldest, most enduring network in existence. With such a legacy comes the need for supporting legacy protocols that may have been deployed decades ago. A wireless broadband network should natively support many of these protocols to reduce capital expenditure and operational costs.

Key requirements for protocols are physical interfaces and protocol support for active and passive serial support (Modbus, Modbus TCP, DF1, and DNP-3), standards-based Layer 2 messaging (e.g., IEC 61850 GOOSE messaging), and full TCP/IP Ethernet communications.

Uplink Biasing

Commercially-focused wireless communications solutions provide more downlink throughput than uplink—the idea being that for home or commercial use, a person desires to download content such as videos and images in much greater proportion than uploading massive amounts of data to other locations.

The concept of uplink biasing for power utilities is to dedicate more throughput on the uplink (from the substation to the back office). For power utilities a much greater need for throughput is in the uplink. Without a mechanism to support this uplink biasing, an organization may have 2 mb/s to a substation; however, less than 1 mb/s would be available for uplink communications. In short, the throughput on the downlink would be

underutilized while there would be too little throughput for the uplink.

At a minimum, a wireless broadband network for power utilities should support an uplink/downlink duty cycle of 75% uplink and 25% downlink, configurable.

Redundancy

Equipment redundancy with hot- or cold-standby assists in restoring communications when a transceiver fails. This becomes especially important when the locations of these devices are not easily accessible. Equipment provided for a wireless communications network should provide levels of redundancy at the master station/base station/access point and at the remote/subscriber unit to improve network reliability and availability.

Robust Equipment

All the features discussed previously are of little value if the equipment is not rated for a utility or environmentally harsh environment. Extended operational temperature specifications, documented mean-time-between-failure (MTBF) ratings, and utility-specific standards for electro-static discharge compliance provide the basis from which the other features discussed may operate for the long term.

MULTI-APPLICATION OPTIONS

The various wireless technology options discussed will be compared (or contrasted) based on a subset of the requirements discussed previously (interface support, redundancy and robustness are manufacturing-specific, not technology-specific):

- Throughput
- Range
- Latency
- Security
- QoS (Prioritizaton)
- Uplink Biasing
- Ecosystem

The two top levels of wireless technologies are public carrier or private infrastructure. Private infrastructure refers to utility-owned, closed-loop wireless networks.

Public Carrier

Public carrier infrastructure provides pervasive coverage in most populated areas, significant throughput, moderate security, and response times under 100 milliseconds. Public carriers, by virtue of pervasive coverage using approved modems, provide a high level of ecosystem of products from various vendors—from handsets, to cellular modems for Utilities and more. However, the concern remains whether public infrastructure can facilitate guaranteed prioritized service. Many carriers are working on features to support prioritized service—usually with a higher rate of pricing. If a utility is in an area with pervasive public carrier coverage with a guaranteed level of service at a fixed price, this would alleviate the initial capital expenditure of a private infrastructure. This is often not the case. From a business case perspective, public carriers focus on individual consumer-based users that make up the majority of the carriers customer base.

Also of note is broken chain of custody for data in a third party network operations center and the embedded downlink biasing included in the technology (instead of uplink biasing).

In summary, public carriers have evolved to meet many needs of power utilities and require limited capital expenditure. Public carriers provide moderate throughput, pervasive coverage, acceptable latency, and adequate security features. However, the need for additional security, channel availability during emergencies, and the ability to pass significant data in the uplink remain concerns.

Private Infrastructure

One new concept to this paper is introduced at this point: deployed frequency. Frequency is not a feature necessarily, because each technology may be deployed within various frequency bands. As a general rule of thumb, and all things being equal (such as power and occupied channel bandwidth), the lower in the RF electromagnetic spectrum a technology is deployed, the better the propagation and building penetration characteristics. For most wireless data communications, the range of point-to-multipoint frequencies available are 140 MHz to 5.8 GHz.

Narrowband

Often deployed in frequencies from 140 MHz to 900 MHz, a narrowband solution provides excellent RF propagation characteristics. Added to this is the very narrow channel size (hence the term narrowband) allotted by regulatory agencies (ETSI, IC, FCC, etc.). The channel size allocated is usually limited to 25 kHz and often down to 6.25 kHz. While this narrow channel with high power allocations and operating in the lower portion of the RF electromagnetic spectrum provides excellent range, throughput is significantly limited. Even with evolving technologies, the most anticipated throughput for a narrowband solution is 1 to 2 bits per Hertz, or up to 50 kb/s. Even with excellent range, throughput is sufficient only for the most essential communications.

Since narrowband licenses are protected by regulatory agencies, the transceiver does not need to compete for channel usage, which provides very deterministic and low latency communications. With such low throughput, the ability to support higher level security and prioritized services are also limited, because these features require

overhead (or throughput) to operate. Most narrowband options known to the authors are proprietary; therefore, the ecosystem of products available is limited to a single manufacturer.

Narrowband communications provide the best coverage of any private network option, which significantly limits the infrastructure and capital investment required. This comes at the expense of advanced security and the ability to support multiple applications.

Mesh Wi/Fi
Broadband mesh technology is most often deployed in unlicensed bands with some deployed in designated bands for public safety or other entities. This technology is often based on IEEE 802.11 standards to some degree, which means that throughput is very high, but range is significantly limited. Broadband mesh technology provides high levels of security and adequate QoS.

For a wide area network deployment, the limitation of range results in a high level of required infrastructure. Even though mesh technology facilitates node-to-node relaying or hopping, this comes at a cost: reduced throughput and increased latency at each node. Some manufacturers overcome this limitation by providing a multi-radio solution in a single box. This multi-radio solution becomes more expensive with the same limitation of range (even though throughput and latency are improved). Each manufacturer implements different mesh algorithms, so the ecosystem of products is usually limited to a single vendor.

Broadband mesh technologies provide very high throughput, sufficient security, and QoS to support multiple applications; however, the amount of infrastructure required often makes this technology significantly higher to deploy than other technologies.

Proprietary Broadband
This category refers to proprietary RF designs or modifications of standards, such as 802.11, that improve range in an attempt to balance throughput and coverage.

Proprietary broadband solutions have been successfully deployed for over a decade for power utilities. These solutions provide good throughput balanced with good range and acceptable latencies. Most of the proprietary broadband solutions are deployed in unlicensed or lightly licensed bands, which puts additional responsibilities on manufacturers to includes interference mitigation features (listed later in this paper) to facilitate deterministic communications.

Since these solutions are based on proprietary technology, the ecosystem of solutions is limited to a specific vendor for a specific implementation. Also, QoS is often implemented to a minimum level.

Proprietary broadband solutions are field-proven; however, the proprietary nature locks a utility to a specific vendor and the throughput is, at most, adequate to support multiple services.

Broadband over Standards
Wireless broadband based on fully interoperable standards provides the benefits of high throughput, adequate range, high security, and often full implementation of QoS. Broadband over standards, such as IEEE 802.16e, is deployed in licensed, lightly licensed, and unlicensed bands, so there is flexibility of deployment in areas where regulatory allocation of certain frequencies is limited.

Since this category is based on standards, the ecosystem of solutions available is larger and not limited to a single vendor per implementation (providing that appropriate interoperability testing and certification have occurred). In certain geographical regions, bandwidth is limited to such a degree that deploying these wider-band solutions (e.g., channel sizes of 3.5 Mhz) is not feasible.

If frequencies are available, this category provides high throughput with highly secure, prioritized service and moderate coverage.

CONCLUSION

As we look for opportunities to improve the efficiency of existing power generation, wireless communications technologies to support these efficiencies becomes a critical component. Communications technologies must provide more accurate and available communications that permit the power utility to respond more quickly and accurately to real time power situations. Obtaining information from sensors, reclosers, relays, and other in-field devices and the ability to make decisions and send them back to distribution automation devices is paramount.

What if a separate network was required for each application: fiber for video surveillance. Broadband for field force automation and VoIP applications. Deterministic, low latency communications for SCADA and recloser, Volt/VAR, and relay control? The infrastructure and operations costs would be very high. The amount of infrastructure can be reduced by selecting a solution that supports the specific needs of multiple applications. Each technology has its merits; the goal is to align the requirements as closely as possible with the features of the technology to maximize throughput and coverage, minimize latency, and provide secure, prioritized communications.