GE
Grid Solutions

Enabling a Secure, Reliable

and High Performing Field Area Network with Cellular Technology

EVOLUTION OF INDUSTRIAL COMMUNICATIONS TECHNOLOGY

imagination at work

Industry White Paper

INTRODUCTION

In the world of electric utilities, privately owned communication networks remain the vehicle of choice for interconnecting assets in the Field Area Network (FAN). Public wireless technologies, such as cellular on the other hand, are not as widely used. By industry estimates (Navigant SGNC 2014), 80% of communication devices shipped to North American utilities in 2016 will fall under the private wireless category, while only 8% will be cellular based.

This, in part, is due to common adoption barriers for cellular among electric utilities, which include misconceptions around the lack of security, reliability and performance. This paper will address those concerns by showcasing how cellular and private wireless technologies compare.

SECURITY

Securing the Field Area Network (FAN)

While the North American Electric Reliability Corporation- Critical Infrastructure Protection (NERC-CIP) security recommendations apply mostly to critical assets in the transmission grid, more utilities in North America have been requesting comparable security mechanisms in their Field Area Networks.

It's common nowadays for utilities to require the encryption of all wireless communication in Field Area Networks, protecting against eavesdropping and theft or manipulation of sensitive data. Advanced encryption mechanisms include the use of certificate management, public key infrastructure (PKI) and key rotation algorithms to guard against compromises associated with static, pre-shared keys.

Centralizing control of network access is of equal importance to securing the grid. It ensures that a single, protected database and source of truth is used to identify users and machines, and to authenticate them on network resources for authorized times, locations and roles. Such access control systems like RADIUS are commonly located in the control center.

Firewalling is another NERC-CIP recommendation that is increasingly used to extend a security perimeter around the FAN. It permits valid types of traffic (e.g., SCADA between specific devices) to flow over specific network paths while blocking unapproved traffic as defined by company policies and grid network operators. Advanced firewalling capabilities such as intrusion detection and prevention (IDS/IPS), enable the monitoring of traffic for suspicious patterns such as those generated by hacking/intrusion attempts. When such patterns are identified, networking devices can either alert the operator or automatically block the intruder.

It is commonly understood that the aforementioned security mechanisms are possible with utility-built and operated private networks; however, public cellular networks do offer comparable capabilities. As an example, standards-based encryption technologies like IPSec VPNs and APNs with key rotation are used to enable an end-to-end encrypted IP tunnel through which data can flow securely between utility assets. Similar to a private network RADIUS, authorization, authentication and accounting services are also offered on cellular networks. Additionally, many cellular carriers offer advanced firewalling and IDS/IPS capabilities as a service to help utilities identify and deny invalid or illegal traffic from entering their domains.

RELIABILITY

Ensuring Reliable Communications for FAN Applications

What makes an electric grid reliable and highly available is a complex intertwining of internal processes, power system design, automation philosophy, and choice of vendors for automation and communications. What makes a wireless communications network reliable enough for FAN applications?

A FAN router is required to survive harsh environments. Standards such as IEEE 1613 and IEC 61850-3 offer the specifications needed to build substation-hardened equipment able to withstand electrostatic discharge (ESD), electromagnetic field (EMF) radiation as well as mechanical vibration commonly encountered in grid applications.

Another component that impacts the overall reliability of a FAN communications network is the choice of radio frequency. Licensed frequencies are protected by law against interference and are thus considered more reliable by default than unlicensed frequencies. The latter can be made to operate reliably, but often at the expense of over-engineering the network albeit with no future protection against interference. The design of the FAN and backhaul networks plays a significant role in ensuring communications reliability. A well designed network is built with enough capacity for current and future applications, has redundant paths, and utilizes Quality of Service (QoS) to ensure traffic prioritization.

Such hallmarks of a reliable network are also found with modern cellular carriers. For the network edge, many communication vendors offer substation-hardened cellular routers that are fit for harsh electrical environments. As for the spectrum, cellular technology operates on licensed spectrum to guarantee protection against interference. The carrier's backbone and core networks are built with redundancy and capacity to reduce and eliminate bottle necks and single points of failures. And while Quality of Service has always been a missing component from public carrier offerings, as recently as Fall 2015, a few Tier 1 carriers in the US started offering minimum committed throughput of 500Kbps-2Mbps for an added fee in order to guarantee operation even during congestion. Finally, a new class of Mobile Virtual Network Operators has been emerging and where the customer is offered a multi-carrier cellular connectivity service to ensure uptimes exceeding 99.99%. They utilize tower infrastructure of existing Tier 1 carriers, and virtualize the backend all while offering the customer a single point of contact for account and device management. This way a customer's router may operate on carrier A's tower until that becomes unavailable or degraded, at which point the MVNO service transparently switches the customer to carrier B's infrastructure in a few seconds.

PERFORMANCE

Application Performance Requirements in the FAN

Applications commonly deployed in the FAN can vary dramatically in their performance requirements. Protection applications such as distributed generation disconnect and fault location, isolation, and service restoration (FLISR) require network latencies of 50-100 msec as an example while SCADA monitoring and control applications tend to be ok with 1 second latency. Refer to Table 1 for an overview of FAN application requirements.

Field Area Network Applications	One-way Network Latency Between Controllers	Application Reliability Requirement	Application Bandwidth Requirement Per Node	Security Requirements
AMI	Minutes	Low	Low, 10's of Kbps	High
SCADA Control	1-2 seconds	High	Low, 10's of Kbps	High
SCADA Monitoring	1-2 seconds	Low	Low, 10's of Kbps	Medium
Dynamic Fault Isolation	<100 msec	High	Medium, 100's of Kbps	High
Load Shedding	<100 msec	High	Medium, 100's of Kbps	High
Distributed Generation SCADA Monitoring	1-2 seconds	Low	Low, 10's of Kbps	Medium
Distributed Generation SCADA Control	1-2 seconds	High	Low, 10's of Kbps	High
Distributed Generation Disconnect	< 100 msec	High	Medium, 100's of Kbps	High
MicroGrid Balancing	< 100 msec	High	Medium, 100's of Kbps	High
MicroGrid Monitoring/Dispatch	1-2 seconds	High	Medium, 100's of Kbps	High

Table 1: Automation applications deployed in modern FAN's, along with performance criteria typically associated with them.

Network Performance in the FAN

A well performing private wireless network is required to offer enough capacity for all desired applications at all desired communication times; congestion should be kept at a minimum. Furthermore, the latency of communications between end points must be such that they meet or exceed application requirements. As an example, a fault isolation protection application may require its reclosers to hear one another's transfer trip messaging in less than 100 msec. One factor that impacts latency is capacity planning and the effective throughput available between end points. The higher the throughput the lower the latency tends to be. A clean radio link, a good signal to noise ratio, and little to no interference also positively impact a network's latency.

In well-designed private networks, QoS mechanisms are used to prioritize important applications such as SCADA or GOOSE over others in order to minimize their latency. Traffic shaping, which is another function of QoS can be used to carve a dedicated throughput on a per-application basis, whereby as an example the operator may decide to dedicate 100Kbps for SCADA on a certain uplink while giving 20Kbps for all other applications.

Cellular communications, especially 4G LTE technologies offer compelling performance characteristics nowadays equivalent to - or even exceeding those of - private proprietary networks. A typical LTE link may offer several Mbps of effective throughput between end points, which is plenty of bandwidth to run most, if not all, FAN applications. And while latency on older 3G networks can be relatively high, modern 4G LTE networks offer latencies in the sub 50msec range. Couple that with the new offerings of carrier QoS, the cellular carrier becomes fit for purpose for latency sensitive FAN applications. Table 2 overviews the latency and throughput characteristics of various wireless technologies.

Wireless Technology	Adjacent Nodes Latency	Throughput	Reliability	Range	Topology
Wi-Fi / Proprietary Broadband	< 10 msec	100's of Mbps	Medium	< 1 mile	Point to Multipoint, Mesh
802.15.4 Mesh	100's of msec	100's of Kbps	High	< 0.5 Mile	Mesh
LPWA	seconds	100's of bps	Medium	1-10 miles	Point to Multipoint
WIMAX	< 10 msec	10's of Mbps	Very High	1-10 miles	Point to Multipoint
Licensed Narrowband	100's of msec	10's of Kbps	Very High	5-50 miles	Point to Multipoint
Unlicensed Frequency Hopping	10's of msec	1 to 10's of Mbps	High with Mesh or dual uplinks	< 30 miles	Point to Multipoint
Public Cellular Carriers	50 msec (LTE)	10's of Mbps	High with QoS	1-5 miles	Point to Multipoint

Table 2: Common wireless technologies used in North American FANs, and corresponding basic performance characteristics.

CONCLUSION

Thanks to its massive ecosystem that drives constant innovation, cellular technology characteristics such as security, reliability and performance have in many instances surpassed those of private proprietary wireless networks. Furthermore, the race by Tier 1 carriers to offer QoS and guarantee network throughput help quell the fears of network availability, especially during disasters. Network availability is also elegantly addressed with modern mobile virtual network operators (MVNOs) with their multi-carrier failover connectivity services. And while recurring monthly cellular fees may be a concern for utilities that are not OPEX oriented, newer Industrial Internet of Things (IIoT) automation protocols can dramatically optimize the volume of data exchange between FAN devices. A typical recloser's SCADA monitoring monthly cellular bandwidth of 100 Mbytes a month may be reduced to less than 1 Mbyte per month with over 90% of cost savings.

The ecosystem of cellular technology and carriers evolved dramatically in recent years to offer security, reliability, and performance characteristics that meet the requirements of modern FAN applications. Whether cellular will overtake private wireless technologies in the FAN is to be determined. The arm wrestling between the technologies is ongoing, and the cultural shifts happening within utilities undergoing IT and OT convergence may bring more changes.

For information on GE MDS' Orbit Cellular Solutions, visit:
http://www.gegridsolutions.com/Communications/catalog/MDSOrbit.htm

View and interact with our Interactive MDS Orbit platform explorer online:
http://www.gegridsolutions.com/productexplorers/orbit/default.aspx

GE
2018 Powers Ferry Road
Atlanta, GA 30339
Tel: 1-877-605-6777 (toll free in North America)
678-844-6777 (direct number)

GEGridSolutions.com

imagination at work

GE, the GE monogram and MDS are trademarks of General Electric Company.

GE reserves the right to make changes to specifications of products described at any time without notice and without obligation to notify any person of such changes.

Copyright 2016, General Electric Company.

GEA-31985(E)
English
160928