Securely Augmenting Private Wireless Systems with Cellular Connectivity

A Machfu Case Study

John Geiger & Chinmay Shete, Machfu

MACHFU

Cellular based Industrial Internet-of-Things (IIoT) solutions are often labelled as lacking the availability to meet the needs of mission critical industrial use cases.

However, as cost effective and ubiquitous LTE cellular communication come of age many secondary use cases are appearing where joint deployment of private and cellular radios on grid assets can augment traditional use cases providing additional bandwidth for deployed systems, increasing their efficiency and productivity and reduce operational costs.

The Fault location, Isolation and Service restoration (FLISR) use cases involve isolating line faults by reconfiguring feeder switches and reclosers in real time and often drives the need for private wireless systems. Today 75% of North American grid connectivity uses private wireless connectivity with only 14% of connections using cellular systems.

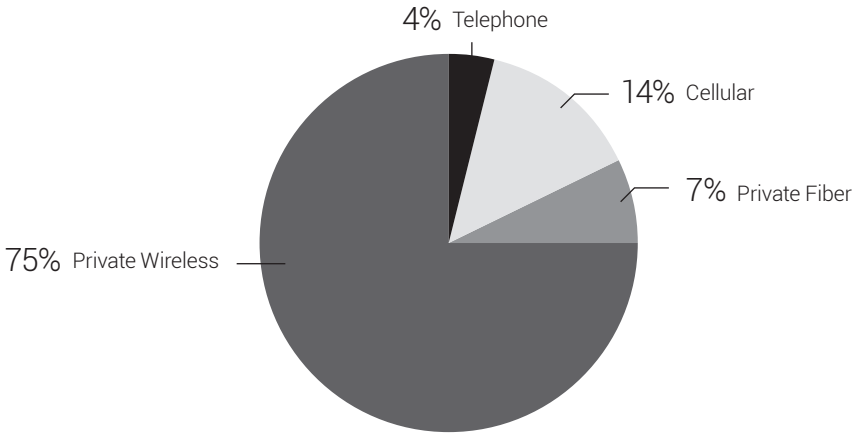

Figure 1: Machfu Gateway serving as an intelligent device to connect different pieces of equipment and sensors to the cloud.

Recently the US Department of Energy published a paper "Distribution Automation Results from the $2.2 Billion Smart Grid Investment Grant (SGIG) between 2010-2013. The paper lists 5 major findings that can achieve substantial grid impacts and benefits. Four out of the five findings benefit greatly from an augmented cellular communication strategy.

1. **FLISR was a key driver and found to result in fewer and shorter outages, lower outage costs, reduced equipment failure, and fewer inconveniences for consumers.** As discussed, this use case is often used to derive specification that require using private wireless to meet availability and latency requirements.
2. **Improved distribution system resilience to extreme weather events by automatically limiting the extent of major outages and improving operator ability to diagnose and repair damaged equipment.** This use case is well suited to cellular augmentation. During emergencies, additional cellular bandwidth is extremely beneficial to diagnose and reconfigure systems. While using cellular alone may not be viewed as meeting overall availability requirements, augmenting private technologies with cellular would only increase availability and greatly improve the system bandwidth.
3. **More effective equipment monitoring and preventive maintenance that reduces operating costs, enables more efficient use of capital assets, reduces the likelihood of equipment failures, and leads to fewer outages.** Private wireless systems lack the capacity to monitor and carry unsolicited back ground traffic. Low cost IIoT cellular services are an ideal method to augment critical private wireless systems enabling connections to low bandwidth monitoring devices.
4. **More efficient use of repair crews and truck rolls that reduces operating costs, enables faster service restoration, and lowers environmental emissions. Cellular services can be used to augment private system giving repair crews**

visibility to access, configure and monitor the health and state of equipment on the grid. The bandwidth of the private systems are limited and lack the capacity to service the high bandwidth of typical web based applications used by the mobile work force. Cellular technologies easily meet the needs of the use case.

5. **Improved grid integration of selected distributed energy resources (DER) such as thermal storage for commercial and municipal buildings.** As DER continues to become more ubiquitous throughout the grid, traditional private wireless solution can't scale to meet the need. Cellular service today connects billions of devices and is more than adequate to meet the availability needs and scale of the DER use case.

Recent advances in 4G LTE cellular are enabling private systems to be augmented with cellular based gateways to expand where Distribution Automation can add value in Grid operations. Machfu worked is working to augment licensed radio solutions. The gateway provides LTE connectivity that can be used in conjunction with private radios. Features of the gateway include:

- Multi-Zone (LAN, WAN , VPN) firewall that can be configured precisely to allow only the smallest set of data flows required to meet the functional requirements. Examples of such data flows are SCADA traffic (including unsolicited events) between remote SCADA backend and grid devices connected to the gateway, gateway management traffic from a network operations center etc.
- Secure bidirectional communication between remote SCADA backend and grid devices using SSL or IPsec/L2TP VPN solutions. The remote SCADA backend equipment and the devices connected to the Machfu gateway can be assigned IP addresses in the private subnet ranges (e.g. 192.168.x.y, 10.x.y.z). The VPN server can then route traffic between these subnets to essentially create a private virtual network across the internet.
- An alternate secure but VPN-less approach is also possible by using public static IP addressing on the cellular interfaces of the Machfu gateways, coupled with the configuration of various NAT firewall rules (DNAT, SNAT and MASQUERADE).
- Support for both Wi-Fi client and access point modes (even simultaneously if desired). The access point mode is used to allow on site crews access to devices through the gateway for configuration etc. Corporate AAA based WiFi security support is also available.
- Support for commonly used communication (utilities) protocols such as DNP3 and Modbus in order to create virtual/ software representations of grid devices on the Machfu gateway. This is a powerful feature and allows for example, a new non-DNP3 grid device to be emulated on the gateway as a DNP3 device and be controlled via the same existing SCADA DNP3 backend. For DNP3 based grid devices, the gateway can simply pass SCADA DNP3 traffic through (subjected to firewall restrictions) and/or create a virtual representation in order to perform edge analytics.
- Support for HTTPS, MQTT, CoAP and other connectors to use various cloud services offered by AWS and Azure. For different use cases, if desired, various metrics/data can be sent to the cloud platforms for storage, analytics etc.

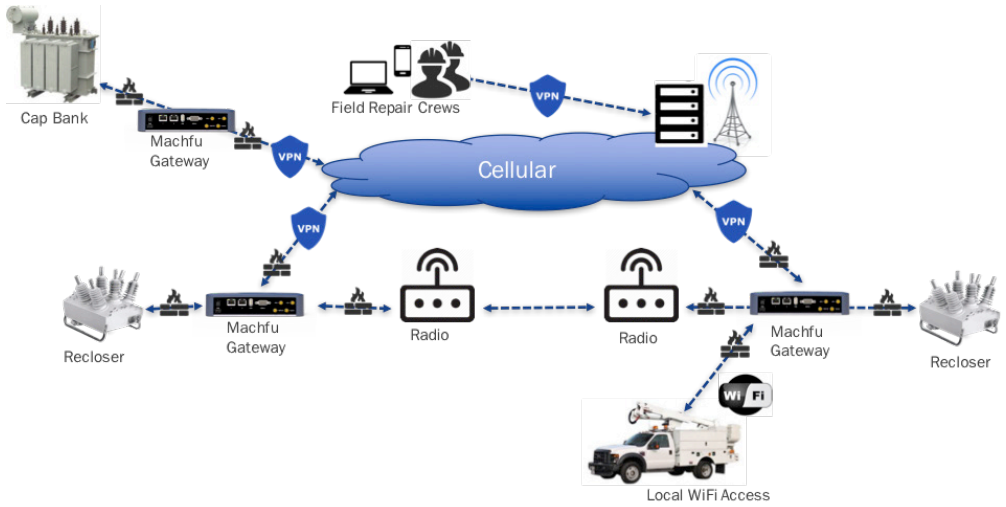

Figure 2: Securely augmenting private wireless networks with cellular capability.

The resulting system provides superior network availability, higher system bandwidth to manage outages and weather-related events, remote access by field personal reducing site visits lowering maintenance costs and improving safety.

The Machfu IoT Edge Gateway provide many features that simplify the development of "Edge Applications" by reducing the time to create and integrate them reducing development time from months or years to weeks or even days. Consequently, enterprise applications are able to access edge data and gain insights from diverse sources. The positive implications of edge applications drive business results across the enterprise. The Machfu platform, designed from ground up to enable rapid development of industrial IoT applications has features that include:

- Client/Server RESTful architecture simplifying application development
- Well-defined Java APIs for accessing, configuring and operating edge devices abstracting developers from the internal implementation details of the edge device.
- Application developers can solely focus on developing web-based applications
- Embedded industrial protocol support for DNP3, Modbus etc. simplifying integration with existing field devices
- Easy to deploy and self-provisioning capabilities minimizing training needed for installation

Authors:

John Geiger

VP of Business Development, Machfu

John has 20 years of experience and subject-matter expertise in developing innovative solutions for Utility, Oil & Gas, Water/Waste Water, Traffic, Rail, Heavy Industrial and Commercial markets. He is credited multiple patents associated with the application of communication technologies in the industrial scape and actively participates in the SGIP and IEEE802. Previous positions include Wireless Center of Excellence Leader for GE Digital Energy and VP of Engineering for MDS.

Chinmay Shete

Machfu

Chinmay Shete is the Director of Embedded Systems at Machfu and the resident guru on Linux, Android and other embedded operating systems. He has 15 years of experience delivering secure IoT solutions in Smart Grid, water distribution and building automation. He is an expert in multiple programming and scripting languages, network stacks and Android App development. Chinmay has a Masters in EE from the University of Southern California.

Reference

https://energy.gov/sites/prod/files/2016/11/f34/Distribution%20Automation%20Summary%20Report_09-29-16.pdf

MACHFU

Germantown Innovation Center
20271 Goldenrod Lane, Suite 2004
Germantown, MD 20876

301-540-5372
info@machfu.com
www.machfu.com