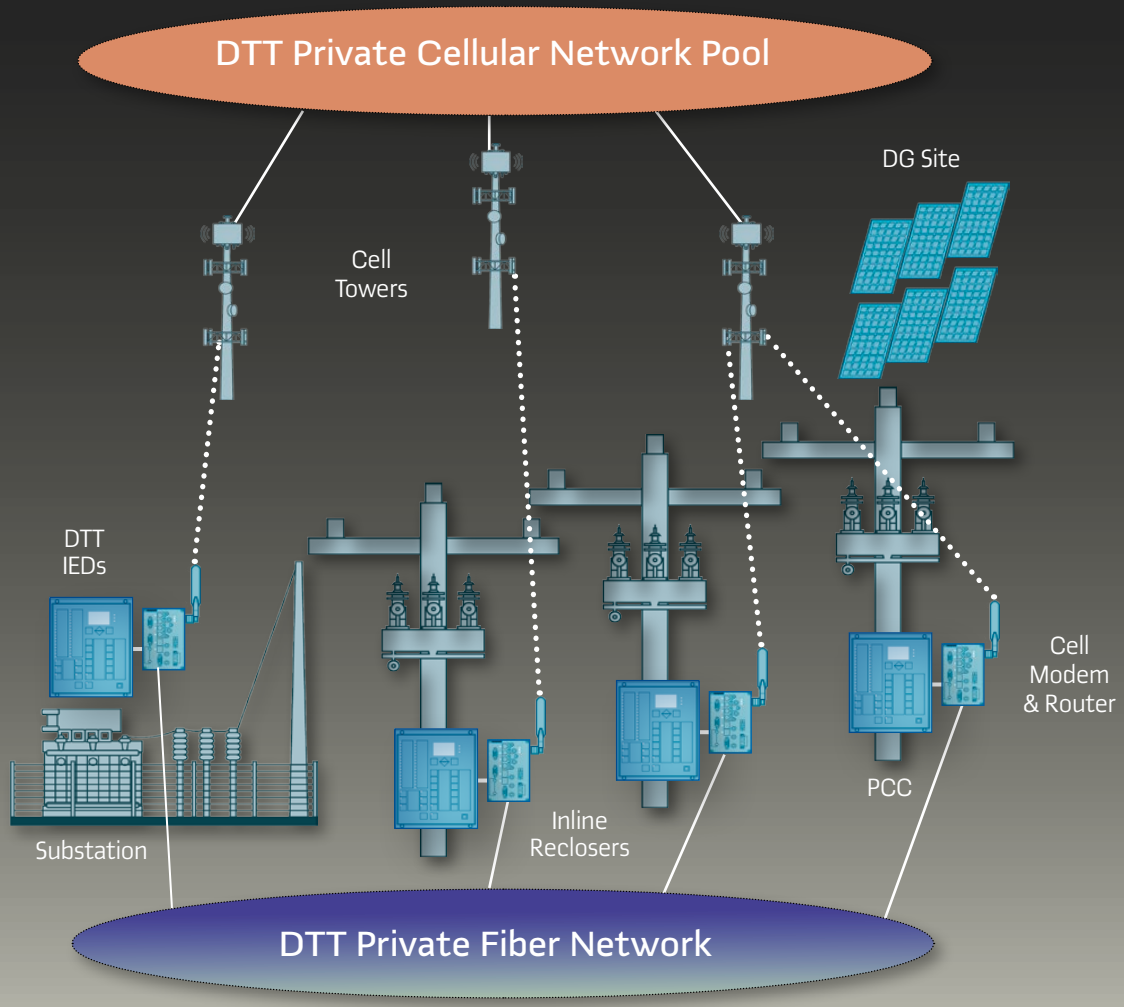
Wireless Communication Systems supporting



Redundant "GOOSE" Communication Systems

by Andre Smit and Suraj Chanda, Siemens Industry, Inc., USA, and
Terry Fix, Dominion Energy Richmond, USA

IEC 61850 Applications

Wireless communication is not a medium used extensively by protection engineers in their protection and control systems designs and applications. The reason is that engineers would only trust a direct wire connection to transmit information for one relay to another. In the 80's Fiber optic was extensively deployed and used for line differential applications on short feeders transmitting phasor data between 2 or 3 relays. Later we also used high-speed high bandwidth Sonnet systems to provide relay to relay communication. For POTT and DTT applications copper lines were used to transmit information for device to device. The installed cost for direct fiber was greatly mitigated when we could get leased telephone lines from Telekom providers.

There was always a common theme in that we only trusted copper or fiber as mediums to transmit data between protection devices. Wireless communication systems were perceived not suitable as we could not trust the systems to provide adequate latency, bandwidth, availability and security. The modernization and digitization of the grid however require us now to move outside the substation fence and communicate to field devices.

WiMAX radio installation on recloser: The deployment of more and more distributed generation increases the need to communicate information between field devices and the substation devices. (Figure 1).

Wireless communication is really the only cost-effective medium to use. Fiber buildouts will definitely help us in the future, but this is not always feasible or immediately available. The IEC 61850 standard has really made a difference for considering the use of wireless communication systems. The GOOSE message is really ideally suited for use on wireless systems. It is a small data packet that can contain digital and analogue information including important quality information.

In this article we will discuss the use of 2 different wireless technologies that were applied in protection and control schemes over the past 8 years.

WiMAX

WiMAX was the first wireless technology we could really use in 2010 to transmit GOOSE messages between protection field devices.

WiMAX is a point to multi point radio Architecture: The system consists of a central base station radio, typically mounted on a tower, and remote subscribers. The field protection / automation controllers are connected to the subscriber radios. This architecture forms a layer two Ethernet network over the radio links. This communication system, much like any standard Ethernet network, supports IEC61850 GOOSE messaging. (Figure 2).

Unlike Wi-Fi, the WiMAX standard calls for Quality of Service to be implemented in WiMAX radios. This is likely the most important feature for using a wireless communication system to communicate protection and control/ automation data between field and substation devices. The quality of service is used to set aside a guaranteed bandwidth and a priority for the transmission of the GOOSE messages. The protection GOOSE messages cannot be impacted by other

by Andre Smit and Suraj Chanda, Siemens Industry, Inc., USA,
and Terry Fix, Dominion Energy Richmond, USA

network traffic. The latency of this channel is the best for each radio link and is predictable.

In Wi-Fi radios tested, all traffic is funneled through the same communication pipe. If you were to increase traffic e.g. download a fault recording file, it could increase the latency of the GOOSE messages. Should Wi-Fi radio systems incorporate quality of service features they can be used for the transmission of GOOSE messages much like WiMAX. The WiMAX provided a consistent latency of 70 ms to get a GOOSE message from one IED to another IED.

Installation - The higher the base stations can be mounted the farther the reach to the subscriber. The minimum height we found was 200 feet to get above the tree lines on the east coast of the US. We could reach 6 to 9 miles from the base station to field devices. We reached distances of up to 15 miles on installations using high gain antennas and base stations mounted at over 300 feet.

On some applications the distance to cover can be too great to reach with a single Base Station to subscriber link. In these instances, we used a hop, back to back subscribers linking to separate base stations. A hop between devices could potentially double the latency and must be considered in the system design.

Although we recommend doing a formal path study we found we could easily use Google Earth to find high ground for towers and create paths to the coordinates of the field equipment. The elevation tool in Google Earth can be used to determine if there are any obstacles in the communication path. We added tree clutter to the highest points to see that we had a good clear communication path from the base station to the subscriber.

Tower assets are very valuable if you consider using WiMAX. We for example used water tower assets where radio towers were available.

We found that it was of utmost importance to first install the base stations on the tower assets and then physically test every link to prove the RF links.

The two signal statistics that must be recorded are the Received Signal Strength Indicator (RSSI) and Carrier to Interference plus Noise Ratio (CINR). RSSI in dBm is an indication of the power level being received by the antenna. Therefore, the less negative the number (close to zero) the stronger the signal. CINR in dB is an indication of the quality of the signal. A higher CINR is desirable in order to adequately distinguish the signal from interference from other antennas or environmental factors. The radio can use higher Quadrature amplitude modulation QAM with lesser interference. We strived to get to QAM 32 to 64 on all protection communication links.

Figure 3 was used to determine adequate RSSI.

If RSSI is - 82dB or more, the link is good. If the RSSI was between -82dB and -86dB the link was tested again with higher gain antenna or height was adjusted or repositioned.

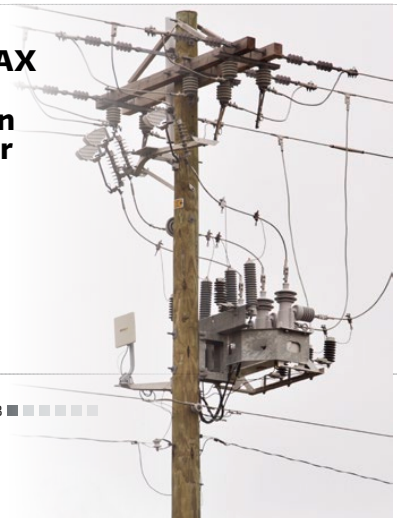
At RSSI - 60dB and higher, the signal is too strong and will cause saturation. The antenna can be adjusted to face away from the base station direction until acceptable signals are measured. In many instances we made use of bucket trucks to physically test the field radio links and establish antenna mounting height and primary switch location.

Testing WiMAX Radio Link: Once we determined the best location for radio link the installation of the field recloser or switch could be finalized. (Figure 4).

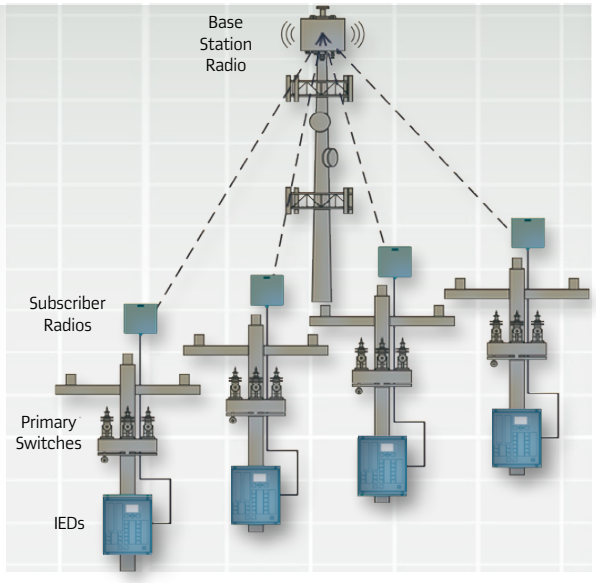
Andre Smit xx xxxxan xxxx xxxxx xxxxxx xxxx xxxxxxx xxx xxxx xxxx engineer for the past 6 years. She pursued her PhD at the University of Western Ontario, Canada and her Masters and Bachelor's degree in Electrical Engineering in India. Palak has proven expertise in Distribution Automation, Power System Protection, & Microgrid Solutions. She is author of more than 25 international journal and conference papers and is also a member of the IEEE Smart Distribution Committee.

Suraj Chanda xxxx xxxxan xxxx xxxxx xxxxxx xxxx xxxxxxx xxx xxxx xxxxtfolio at General Electric (GE). He has 18 years of industrial experience in Power generation, transmission and distribution. In the past decade, he has held various teams in product development and R&D in GE Grid Automation. He received his M.E.Sc. from the University of Western Ontario, Canada. Vijay holds 5 international patents and several journal/conference papers.

1 WiMAX radio installation on recloser



2 WiMAX architecture



3 **Scale for determining RSSI**

WiMAX provides an excellent platform for IEC 61850 devices. It is a modern standard supporting Ethernet and it is very easy to establish an Ethernet network between IED's. Each feeder system can be placed on its own unique VLAN. We could, for example, create on one RF link separate data service tunnels for different VLANs and also a separate service tunnel for DNP3 traffic.

We found that reading the IEC 61850 stack from the field devices to a control center HMI Client was problematic. The size of the packets was sometimes too big "Jumbo Packets" and the radios struggled to keep the Ethernet links up with the client and the field devices. We moved to DNP3 and the radios coped better with the smaller better managed DNP packets.

The small ±300 byte GOOSE messages did not present a problem to the radios as long as the maximum time between GOOSE messages was long enough. The radios definitely could not support 10 or even 100 ms between messages. We could stretch the maximum time significantly as we could not detect any packet loss in the WiMAX radio systems.

In a fault event an avalanche of GOOSE will be created. We found that if the automation system operates at high speed we could locate a fault, isolate it and close a tie switch before there was any sign that the radios had trouble to keep up with the delivery of the GOOSE packets. It is very important to consider the number of GOOSE applications required to perform the protection and control functions. For the most part 3 applications per relay will be supported.

Lastly the time between GOOSE massages must be established through exhaustive testing of the protection and control functions making sure the radios will support the system. These tests are best performed in a laboratory environment. There is no easy set of rules on how the GOOSE applications should be configured.

Network Configuration - The GOOSE structure and application settings must be adapted for use in WiMAX. The following parameters of each GOOSE application must be adapted:

- VLAN
- Maximum time
- Minimum time
- VLAN priority

A Virtual LAN (VLAN) is any broadcast domain that is partitioned and isolated in a communication network at the data link layer (OSI layer 2). The Layer II VLAN parameter is the key differentiation feature for an IEC 61850 based GOOSE message. It is crucial to have a unique VLAN assigned to each P&C system. This VLAN assignment avoids any duplicates and/or collisions of Layer II GOOSE messages between devices from two different systems.

WiMAX is likely the best wireless communication system for the transmission of protection and control data. The deployment is however quite difficult especially if tower assets are not readily available. The system must be continuously maintained to ensure availability. We used the GOOSE message quality information to monitor and report communication link failures.

WiMAX provides a private layer two network with adequate security if security features available are used.

In two instances we did find that WiMAX radios were installed by others that interfered with the RF links. Frequencies were changed to overcome the interference. This could have been avoided by proper registration of all assets with the FCC. The new WiMAX registration management system will improve the registration process and management though service registration providers that will eliminate this phenomenon experienced in an unlicensed spectrum.

Cellular Communication

Cellular communication has become a new and important platform that can be leveraged to transport P&C data across a provider's cellular network. This might sound like a foreign concept but is actually nothing new. Many DTT systems today rely on leased telephone

> **The modernization and digitization of the grid require us no to move outside the substation fence.**

The higher the base stations can be mounted the farther the reach to the subscriber.

Terry Fix xxxxan xxxx xxxxx xxxxxx xxxx xxxxxxx xxx xxxx xxxx published two papers with Cirid on the subject of Smart MV Neutral Treatment. He has 10 years' experience in implementing MV smart grid technology including the implementation of an Intelligent MV Line Monitoring Systems. Martin is currently working on LV smart metering implementation.

4 **Testing WiMAX radio link**

by Andre Smit and Suraj Chanda, Siemens Industry, Inc., USA,
and Terry Fix, Dominion Energy Richmond, USA

lines form 3rd party providers. These aging public wired networks are becoming unreliable and cellular networks are a modern reliable alternative.

The major driver to use a cellular system is the ease of deployment. There is no need to find or install tower assets. The cellular providers have already installed extensive tower assets making cellular service widely available, similar to the old copper telephone line networks we use.

Today cellular providers offer private networks to companies. These private networks provide a system where only the company's devices are connected to a network.

Cellular private network: These private networks are not connected to the Internet. No unsolicited traffic from the internet will get onto such a network. A utility can create private networks for different applications: AMI network for all meters, a Direct Transfer Trip network for DTT devices, a POTT network for protection devices, a FLISR network for automation devices to name a few. (Figure 5).

These networks can easily be leveraged to transport GOOSE messages between protection devices. VLAN based L2TPV3 tunnels are configured between modems to communicate the IEC61850 "GOOSE" messages. The tunnel configuration settings include:

- VLAN number
- Session parameters
- Local and remote ports
- Local and remote static IP addresses

Security

L2TPV3 Tunnels with IPSec Encryption: The GOOSE PDU (Protocol Data Unit) doesn't include an IP header in order to avoid additional latency caused during processing of the TCP/IP layer. This was done specifically to ensure extremely efficient data processing in the embedded devices such as protection and control relays. Therefore "GOOSE" messages cannot propagate over layer 3 networks without being tunneled. (A tunneling protocol encapsulates another protocol's data and transmits them over an unsupported network through a tunnel. At the other end of the tunnel the data is then decapsulated before it goes out). The Layer 2 Tunneling Protocol (L2TPV3) is used to transmit specific VLAN tagged GOOSE messages over the cellular network. Internet Protocol Security (IPsec) is used for securing tunnel communication by authenticating and encrypting all the tunnel data.

WiMAX is likely the best wireless communication system for the transmission of protection and control data.

Typically, the same GOOSE message is retransmitted with varying and increasing re-transmission intervals until a change occurs in any GOOSE dataset element. L2TPV3 supports this retransmission ensuring the GOOSE message with a given status number is delivered at the tunnel end.

IPsec is one of the key security features implemented in the cellular modem to provide immunity to cyber-attacks. IPsec is configured to encrypt/decrypt any data entering/leaving the tunnels respectively form the modems. IPsec features include:

- Data encryption
- Modems verify pre-shared keys

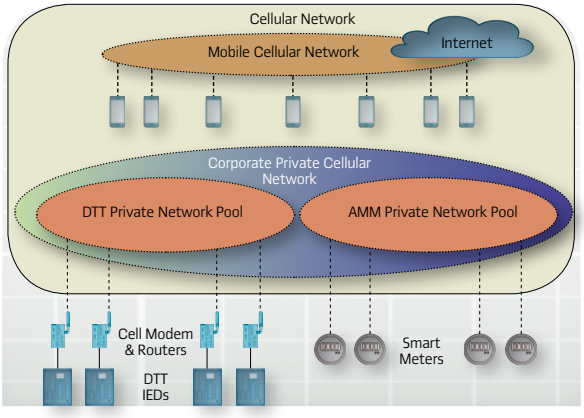
DTT network architecture: As shown in Figure 5, the entire DTT system is part of a cellular private network pool. All the cellular modems and automation controllers are part of a unique IP subnet which has layer 3 isolation from other networks. The network parameters for the devices within the private network are managed as follows:

Cellular Modem

- IP Addressing
  - Static IP Addresses – Assigned for SIM cards in the plan. Modems learn these static IPs upon successful connection to the network
  - LAN IP Addresses – Assigned based on the network addressing for the automation controllers
  - Management IP Address – Local addresses assigned in a subnet completely isolated from Static and LAN addresses
- VLAN addressing and Port Setup
  - LAN port which is connected to the controller is configured as VLAN edge port
  - Management port is on default VLAN and other ports are disabled for security
- Automation Controller
  - IP Addresses assigned on a subnet different from cellular subnet and management subnet
  - Unique VLAN assigned for each DTT system which is different from other automation systems to separate IEC61850 based GOOSE messages

The deployment of more and more distributed generation increases the need to communicate information between field devices and the substation devices.

5 Cellular private network



Penetration Testing: A penetration test on a GOOSE based DTT application using a RX1400 cellular modem is used to verify the security of the link.

The results showed that the private cellular network and IPsec tunnel network is largely resilient against adversarial attack. The cellular modem's cyber security features were validated and demonstrated it can withstand the majority of threats.

The DTT system design incorporates an innovative communication approach. The DTT system is designed to use Fiber Optic network communication with redundant Cellular communication. The DTT controller will accept the two separate sets of DTT GOOSE signals from the two communication systems. The DTT sending devices will send separate DTT GOOSE over the two communication networks. The controller at the PCC will react on the first DTT GOOSE received from either communication networks.

Redundant GOOSE Communication Systems: A communication failure at any point of the DTT system on either communication system will have little or no effect on the system. This system can be deployed in different combinations of Cellular + Fiber, Cellular + WiMAX or Cellular + Cellular from different providers. The digital wireless cellular system proved to be more reliable than the existing copper leased line networks on a pilot project deployed in the US. (see the Figure on page 46).

Recloser with Polarized Directional Antenna: In the near term it is possible to improve the existing DTT system reliability and selectivity by the deployment of the new GOOSE based system over cellular, and improve the system's reliability and speed with the deployment of fiber in the longer term. (Figure 6).

A communication based DTT system is definitely the desired and more conservative protection approach to ensure that a DG site will be disconnected if the connected feeder system experiences an abnormality that requires maintenance or repair.

The Cellular System Deployment - The ease of deployment of a cellular system in the field is a major differentiator. The communication system's site availability can easily be verified using a cellular phone. A person can physically drive to each location and check if he can exchange data on his smart phone. An LTE signal is preferable. If signals are weak the signals can be verified using a DTT cellular modem/router with a directional antenna. We built a simulation test DTT system consisting of a PCC controller and modem located in a laboratory and a mobile substation DTT unit with modem that can send DTT signals to the PCC unit in the lab over a private cellular network.

Mobile DTT Test System: With this method the entire DTT communication system could be verified in minutes at each location. In a pilot the user verified cellular communication to 22 sites in two days over a two-state geographic area using this method.

table 1 Published latency comparisons

Verizon	Latency (ms)
eHRPD	145.5686
EVDO	137.6714
LTE	85.144

Cellular DTT Installation at Solar Site

The Cellular System Performance - Latency can be defined as the time it takes for a source to send a packet of data to a receiver. It is typically measured in milliseconds. Lowering the peer to peer latency results in better network performance. (Figure 7). There are 2 latencies to consider:

- *Cellular Modem - Modem Latency:* In the cellular terms, this is also referred as User Plane (U-Plane) Latency. (LTE for UMTS) U-Plane latency is defined as one-way transmit time between a packet being available at the IP layer in one modem and the availability of this packet at the IP layer in the other modem. U-Plane latency is relevant for the performance of many applications
- *Controller - Controller Latency:* This latency is one-way transmit time of a packet from source controller to destination controller. This latency includes cellular latency, tunneling and encryption latency (at both the modems)

Since the LTE deployment a few years ago, LTE networks promised the user plane latency to be approximately 1/2 of corresponding latency in existing 3G technologies. This provides a direct service advantage for highly immersive and time critical applications like FLISR, and DTT. The published latency comparison of Verizon on different networks is as shown in Table 1. From the field test results, the end to end controller latency between 120 ms to 300 ms.

This is dependent on number of subscribers connected to the cell tower, number of resources allocated to each cell server and other factors. With the advent of 5G and Verizon upgrading their network to support LTE, the cellular latencies are expected to significantly reduce in the future. ■

Cellular communication has become a new and important platform that can be leveraged to transport P&C data across a provider's cellular network.

6 Recloser with polarized directional antenna

7 Cellular DTT installation at solar site