Overcoming the Challenges of License-Free Radio Communications With Secure Cellular Radios

Anthony Cipriano
Ethos Energy Group

Tom Bartman and Phoebe Loh
Schweitzer Engineering Laboratories, Inc.

Presented at the
60th Annual Minnesota Power Systems Conference
Saint Paul, Minnesota
November 12–14, 2024

Overcoming the Challenges of License-Free Radio Communications With Secure Cellular Radios

Anthony Cipriano, *Ethos Energy Group*
Tom Bartman and Phoebe Loh, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—Radio communications is essential to power system reliability. License-free radio communications is an attractive solution and can be used for protection and control applications in power systems. While license-free radios can be a reliable solution when conditions are suitable, there are limitations that make them unusable for other applications. These limitations include terrain, clear line of sight, interference, multipath errors, and antenna alignment. To overcome these limitations, cellular radios can be used for reliable communications for both point-to-point and point-to-multipoint applications.**

This paper discusses the benefits of secure cellular radios in overcoming the challenges of license-free industrial, scientific, and medical (ISM)-radio bands for protection and control applications. The paper also discusses the application of cellular radio communications for operational technology (OT) networking, supervisory control and data acquisition (SCADA), and data trending where traditional 900 MHz radio communications cannot be reliably deployed.

I. Introduction

Communications is essential for supervisory control and data acquisition (SCADA); remote engineering access; distributed network automation; real-time data collection; fault location, isolation, and service restoration (FLISR); and other critical infrastructure applications. Radios offer a cost-effective and quick way to add communications links. However, providing reliable and dependable communications between two sites can be challenging. License-free radio communications provides an inexpensive and quick deployment solution. Challenges arise with these license-free industrial, scientific, and medical (ISM)-radio bands that often prevent reliable communication. These challenges can range from radio line of sight to multipath errors to distance.

Cellular radio communications is available for overcoming these challenges of license-free radio systems and are becoming extremely cost-effective alternatives. The paper examines the limitations of ISM-band unlicensed radios and examines the use of cellular radios to overcome these challenges. Furthermore, the paper shares the results of a distributed generation application implemented at Ethos Energy Group and highlights the outcomes of an application of secure cellular radios in real-time data collection and remote access.

II. Technical Considerations When Using Unlicensed Radios

Radios offer an affordable and quick solution for establishing communications between sites.

When using ISM-radio bands, several factors must be considered. These factors include network topologies, clear line of sight, and clutter, which can cause multipath errors, interference, and receiver sensitivity. This section will discuss each of these considerations in detail.

A. Radio Line of Sight

Radios that operate in the 900 MHz ISM band are often favored because of affordability and a lack of requiring a license to operate. Despite these advantages, ISM-band radios are constrained to a clear radio line of sight. Radio line of sight is wider than visual line of sight because of the curvature of the Earth's surface. As the communications path extends farther, higher antennas are needed to sustain the line of sight. Radio line of sight is an ellipsoid-shaped zone between the transmitter and receiver, as illustrated in Fig. 1. This area is known as the Fresnel zone. A clear Fresnel zone is critical for maintaining a reliable signal strength.

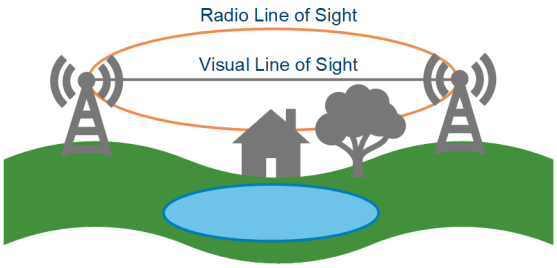

Fig. 1. Radio and Visual Line of Sight

The Fresnel zone is likely the single most important factor for reliable communications. Obstructions within this zone can reflect signals, causing errors or interference. Reflected signals may arrive at the receiving antenna in more than one occurrence and out of phase with the primary intended signal. This results in errors known as multipath errors. Fig. 2 illustrates the diameter of the Fresnel zone and how it is calculated.

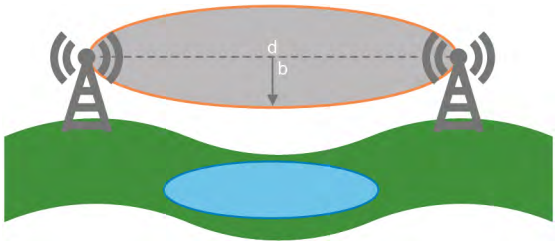

Fig. 2. Fresnel Zone Between Antennas

The maximum width of the Fresnel zone is calculated as follows:

$$b = 17.32\sqrt{d/(4f)}$$

where:

b = radius in meters

d = distance between antennas in kilometers

f = transmitted frequency in GHz

B. Clutter

Clutter is defined as any object that protrudes into the radio line of sight. Clutter can be buildings, trees, water towers, transmission towers, and residential homes. Clutter affects ISM-radio band transmissions by reflecting off of the objects and affecting link reliability. For an acceptable radio link in the ISM band, the Fresnel zone should be at least 60 percent clear of clutter [1]. However, in some real-world scenarios and practical applications, a 60 percent clutter-free zone was found insufficient to secure an acceptable link.

Clutter can evolve over time as vegetation and trees grow or when new buildings are constructed. Clutter can also be difficult to predict over a long link.

C. Multipath Errors

A transmitted radio signal may reach the receiver through multiple paths by way of reflections, as shown in Fig. 3. This may be caused by terrain or atmospheric conditions. Multiple paths lead to interference through unintended phase shifting.

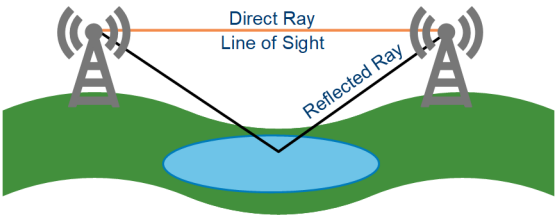

Fig. 3. Multipath Errors Due to a Reflected Radio Signal

Multipath errors also lead to poor signal quality and can be caused by structures or reflections off bodies of water, such as rivers or lakes. For instance, in one application, a body of water was between the transmitting and receiving antennas with a clear line of visual sight. It was thought that a reliable link would be established; however, due to the Fresnel zone, a portion of the signal was reflected and led to multipath errors. These errors were eliminated by slightly raising the antennas.

D. Interference

License-free ISM-radio bands are susceptible to interference from other nearby ISM radios.

The free nature of ISM usage leads to an important consideration regarding radio frequency interference, in that although a reliable, established link may be in operation, nothing prevents someone nearby from operating a new ISM-band link in the future. In one instance of troubleshooting a problem with a intermittent radio link, a nearby 900 MHz antenna was found mounted on a privately owned pole.

E. Receiver Sensitivity

Receiver sensitivity is a specification in the receiving radio and is an important consideration for the reliability of received signals. Think of a crowded room of people with a person on stage in the front of the room. The people in the room are talking, creating considerable noise. Now imagine the person on stage wants to speak to someone in the back of the room, over all those people talking. Receiver sensitivity is comparable to the minimum volume the speaker on stage must speak and still have the person in the back of the room understand what is being said. For a radio, receiver sensitivity is the lowest signal level that the receiver can decode for proper operation. If the received signal strength is below the receiver sensitivity, the radio will not be able to decode the signal. Fade margin is a term to describe the level of signal in excess of the receiver sensitivity for a reliable signal. In good practice, a fade margin of 20 dB is preferred. For example, if the receive sensitivity for a radio is –93 dB, a received signal level of –73 dB is a comfortable fade margin.

III. Overcoming These Challenges With Cellular Radio Technology

A cellular network is a group of transmitters, receivers, and radios interfacing with the rest of the carrier equipment. Generally placed on towers or commercial rooftops, these devices, when joined together, create a telecommunications network. This is performed by interlocking regions between towers into cells, hence the name cellular. Cellular networks provide communications over a wide geographical area. Providers of these networks offer the service of using them for a fee. Major cellular internet service providers (ISPs) own the license on spectrums used for this technology, which is why it is required to lease a service through them. These telecommunications networks have become a popular alternative in electric power and industrial uses when the challenges of ISM-band license-free communications cannot be overcome. There are several generations of cellular technology in use today.

A. 3G, 4G, and 5G Technology

Cellular radio technology is based upon the generation or the evolution of the technology. As cellular technology evolved, speeds and bandwidth increased while latency, the measurement of delay, decreased. In an end-to-end latency test, time is measured round-trip, i.e., the time it takes for a device to send a request and then receive the reply.

3G, or third generation, was established in 2001. In addition to voice calls and SMS text messages, internet browsing was possible with 3G. With the development of 3G, speeds of 2 Mbps were possible, which enabled video streaming and email.

4G, or fourth generation, was implemented in 2009 as 4G Long-Term Evolution (LTE). Download speeds were greatly increased to 100 Mbps, which enabled online gaming and high-definition videos.

5G, or fifth generation, was implemented in 2019. 5G is breaking out into three separate directions [2]. The first is enhanced mobile broadband, which is the natural high-speed progression of 4G, the next is massive Internet of Things (IoT), and the last direction is high reliability and low latency.

B. *Cellular Radios for Critical Infrastructure*

Many industrial applications refer to cellular radios as cellular routers. When choosing a cellular solution for industrial and critical infrastructure applications, it is important to take into account the generation of technology used, the solution's suitability for harsh environments, and the security of the data being moved across the network. Support for a stateful firewall, virtual private network (VPN), and media access control (MAC) filtering are critical to the creation of a secure cellular link.

C. *The First Responder Network Authority (FirstNet)*

FirstNet offers highly secure and prioritized network access for essential government services, including electric, gas, water, and sewer utilities. It manages network congestion by providing a dedicated lane of connectivity, ensuring no data throttling occurs anywhere in the U.S. [3]. Some cellular routers are FirstNet-certified, which provides greater reliability for recloser controls, motor-operated switches, capacitor banks, voltage regulators, substation facilities, etc.

A FirstNet-capable device offers several advantages, which exceed those of commercial-band cellular networks for critical communications. The FirstNet network is designed to keep first responders, emergency personnel, and utilities operational during large-scale emergencies. It ensures cybersecurity and resiliency through dedicated core hardware in the cellular provider's data centers, public safety Internet Protocol (IP) ranges, and multiple layers of AES-256 encryption. Additionally, it avoids congestion issues during high cellphone usage in emergencies because it does not compete with commercial traffic.

D. *Latency*

A bench test was conducted using two cellular radios approximately 19 miles apart, as shown in Fig. 4. The test observed the time difference between the binary input status with a time stamp in the relay and the sending of an unsolicited Distributed Network Protocol (DNP3) message to a real-time automation controller, as shown in Table I. This included the processing time of both the real-time automation controller and the relay. The relay and real-time automation controller are time-synchronized and enable logging of the status change.

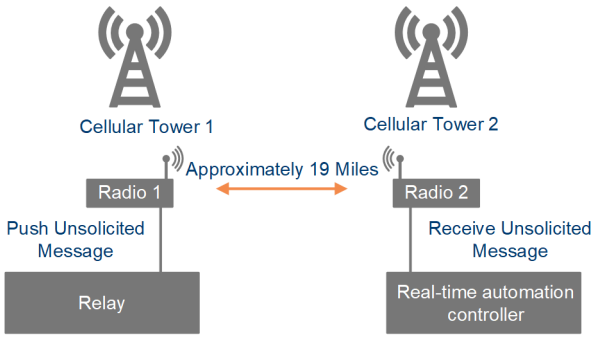

Fig. 4. Test Over a 19-Mile Link

TABLE I
ONE-WAY LATENCY OVER 19-MILE LINK

Message	Radio 1 Relay Sequential Events Recorder (SER)	Radio 2 Automation Controller Sequence of Events (SOE)	Latency
Relay DNP3 LED 1 Asserted	8/8/2024 23:55:29.393	8/8/2024 23:55:29.634	241 ms
Relay DNP3 LED 1 Deasserted	8/8/2024 23:55:51.076	8/8/2024 23:55:51.166	90 ms
Relay DNP3 LED 1 Asserted	8/8/24 23:56:20.216	8/8/2024 23:56:20.978	762 ms
Relay DNP3 LED 1 Deasserted	8/8/24 23:56:36.227	8/8/2024 23:56:36.978	751 ms
Relay DNP3 LED 1 Asserted	8/9/2024 8:01:36.000	8/9/2024 8:01:36.802	802 ms
Relay DNP3 LED 1 Deasserted	8/9/24 8:01:39.461	8/9/2024 8:01:39.562	101 ms
Relay DNP3 LED 1 Asserted	8/9/2024 8:01:45.007	8/9/2024 8:01:45.622	615 ms
Relay DNP3 LED 1 Deasserted	8/9/2024 8:01:47.811	8/9/2024 8:01:48.326	515 ms
Relay DNP3 LED 1 Asserted	8/9/2024 8:01:51.561	8/9/2024 8:01:52.093	532 ms
Relay DNP3 LED 1 Deasserted	8/9/2024 8:01:53.731	8/9/2024 8:01:54.098	367 ms
Relay DNP3 LED 1 Asserted	8/9/2024 8:01:59.169	8/9/2024 8:01:59.606	437 ms
Relay DNP3 LED 1 Deasserted	8/9/2024 8:02:01.152	8/9/2024 8:02:01.602	450 ms
AVERAGE			472 ms

This test demonstrates that the latency varies considerably. At times, the point-to-point latency was 90 ms while at other times, the same test took over 800 ms. This variance is expected when transmitting over a public network. This test also showed that while many challenges of ISM-radio bands were overcome, the cellular radios tested would not be suitable for protection applications.

The same test was conducted with two cellular routers connected to the same cellular tower at close range, as shown in Fig. 5. The latency is shown in Table II.

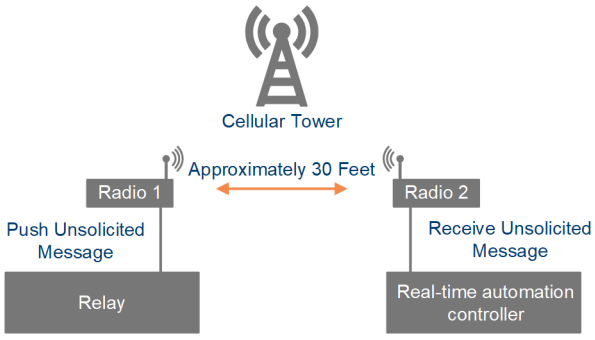

Fig. 5. Test Using Same Cellular Tower

TABLE II
ONE-WAY LATENCY WITH SAME CELLULAR TOWER LOCATION DISTANCE ~10 METERS

Message	Radio 1 Relay SER	Radio 2 Automation Controller SOE	Latency
Relay DNP3 LED 1 Asserted	8/19/2024 10:01:38.934	8/19/2024 10:01:39.325	391 ms
Relay DNP3 LED 1 Deasserted	8/19/2024 10:01:41.326	8/19/2024 10:01:41.829	503 ms
Relay DNP3 LED 1 Asserted	8/19/2024 10:01:43.876	8/19/2024 10:01:44.341	465 ms
Relay DNP3 LED 1 Deasserted	8/19/2024 10:01:46.021	8/19/2024 10:01:46.349	328 ms
Relay DNP3 LED 1 Asserted	8/19/2024 10:01:49.646	8/19/2024 10:01:49.837	191 ms
Relay DNP3 LED 1 Deasserted	8/19/2024 10:01:51.350	8/19/2024 10:01:51.837	487 ms
Relay DNP3 LED 1 Asserted	8/19/2024 10:01:53.596	8/19/2024 10:01:53.849	253 ms
Relay DNP3 LED 1 Deasserted	8/19/2024 10:01:55.142	8/19/2024 10:01:55.409	267 ms
Relay DNP3 LED 1 Asserted	8/19/2024 10:01:59.321	8/19/2024 10:01:59.869	548 ms
Relay DNP3 LED 1 Deasserted	8/19/2024 10:02:00.187	8/19/2024 10:02:00.529	342 ms
Relay DNP3 LED 1 Asserted	8/19/2024 10:02:04.008	8/19/2024 10:02:04.369	361 ms
Relay DNP3 LED 1 Deasserted	8/19/2024 10:02:05.124	8/19/2024 10:02:05.377	253 ms
AVERAGE			366 ms

Examining the tests in Table I and Table II, we observed that average latency times were similar. This observation indicates that the distance of the location does not significantly affect latency; instead, it largely depends on the radio network availability.

IV. SECURING RADIO COMMUNICATIONS

Encryption and authentication add confidentiality to communications. One method of securing communications in this way is by using a VPN, and a common practice to establish a VPN is through Internet Protocol Security (IPsec).

IPsec is a standardized framework for securing IP communications for a trusted or untrusted network. IPsec provides confidentiality, integrity, and authentication. Strong encryption algorithms provide confidentiality, while integrity is provided with the use of message validation schemes known as checksums and hashes. A hash is a one-way mathematical function that transforms a string of data into a fixed-length value known as a hash value. This one-way operation means that the input data cannot be recreated from the hash value. Hash values are used as digital fingerprints. By comparing the hash value of a sent message to the hash value of a received message, the receiver can verify that the message was not tampered with.

IPsec builds a secure tunnel of communications between two endpoints, as shown in Fig. 6. The protocol exchanges secret keys between the two endpoints. Once the tunnel is established, the sender and receiver agree on the encryption algorithm to use.

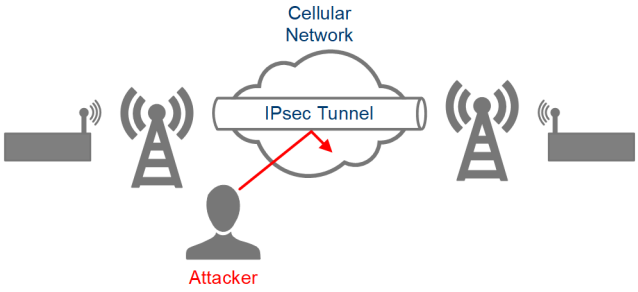

Fig. 6. Wireless Secure Communications Through an IPsec VPN Tunnel

IPsec uses two protocols for data transfers, which are summarized in Fig. 7.

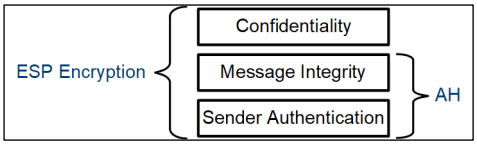

Fig. 7. Encapsulating Security Payload (ESP) and Authentication Header (AH) Work Together

1. AH

   The AH protocol authenticates IP traffic but performs no encryption. The authentication is performed by calculating hashed messages throughout the packet of data.

2. ESP

   The ESP protocol provides confidentiality by encrypting data. In addition to confidentiality, ESP provides authentication, integrity, and anti-replay and can be used with or without the AH protocol. Wrapping SCADA traffic in a protective IPsec stream provides secure communications between gateways to which end devices, such as programmable logic controllers (PLCs) or relays, are connected.

V. REAL-WORLD USE CASE

There are numerous use cases where data are needed for real-time data collection, SCADA systems, and remote engineering access. However, the location of these devices can sometimes pose challenges, which limits data reporting.

One of the use cases at an energy utility is a data logging and monitoring system for their devices located in remote areas of the U.S., as shown in Fig. 8. They would like to view data not only within the U.S. team but also from outside the U.S. team, with the ability to monitor and analyze real-time data.

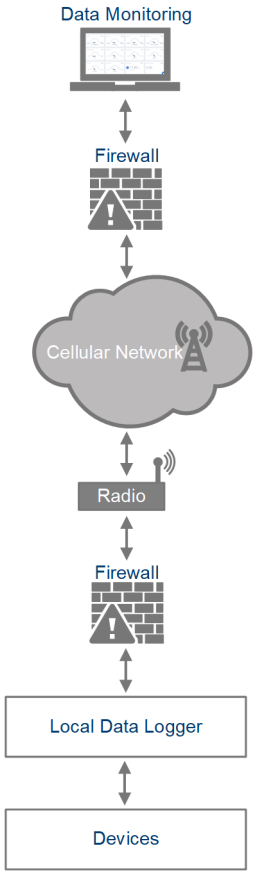

Fig. 8. SCADA Application Using Cellular Communications

Due to the significant distance between the station devices and the data monitoring system, radios are used to send the monitoring data via cellular signals. The user can view data remotely in real time without going to the station to collect or export data. Fig. 9 shows the data monitored in the local U.S. corporate location and outside the U.S. corporate location.

Fig. 9. Data View at a Utility Monitoring Graphical User Interface

VI. Conclusion

When properly deployed, radio communications provides secure and dependable communications. Low-cost license-free ISM-band radios can be deployed quickly for a dependable radio link in many applications. Several factors, however, present challenges to achieving a dependable radio link. The paper examines the challenges of license-free ISM-band radios and presents an alternative through cellular radio communications. The paper also highlights the application of SCADA communications over cellular radios and monitoring real-time data.

VII. References

[1] T. Bartman, B. Rowland, and L. Rogers, "Expanding Protection and Control Communications Networks With Wireless Radio Links," *2019 IEEE Rural Electric Power Conference (REPC)*, Bloomington, MN, pp. 39–45.

[2] K. Mallinson, "The Path to 5G: As Much Evolution As Revolution," 3GPP, May 2016. Available: www.3gpp.org/news-events/3gpp-news/5g-wiseharbour.

[3] FirstNet, "FirstNet Benefits," April 2020. Available: www.firstnet.com/content/dam/firstnet/white-papers/FN_SIM_Benefits.pdf.

VIII. Biographies

Anthony Cipriano received his BS in marine engineering from Maine Maritime Academy in 2016. Since 2017, he has held several positions with EthosEnergy, for the last five years he has held the role of instrumentation, controls, and electrical technician. In this role, he operates, maintains, installs, and troubleshoots various systems and equipment throughout the facility. This includes, but is not limited to, the following equipment: instrumentation, control systems, cybersecurity, SCADA, IT/OT, computers and servers, networking, electrical systems, and associated protection and control devices. During a brief time outside of EthosEnergy, he worked as a chief engineer aboard various harbor tugs ranging from 2,500–6,500 hp.

Tom Bartman joined Schweitzer Engineering Laboratories, Inc. (SEL) in 2006 as an engineering technician for industrial system products. He is now an application specialist in communications, Sales and Customer Service. Prior to joining SEL, he served in the U.S. Navy as an electronics technician with an emphasis on avionics and secure communications. After leaving the Navy, he worked for Harris Inc., as an electronics engineer in the Broadcast Communications division. He has a degree in applied computer science, is a member of International Information System Security Certification Consortium $(ISC)^2$, and obtained his Certified Information Systems Security Professional (CISSP) certification in 2013. Tom holds a patent for validation of arc-flash protection and a patent for a network gateway.

Phoebe Loh received her BS in electrical engineering from Drexel University in 2015 and MS in information systems engineering and management from Harrisburg University of Science and Technology in 2020. Since 2017, she has worked at Schweitzer Engineering Laboratories, Inc. (SEL) as an automation application engineer in Sales and Customer Service, supporting various customers on SEL technologies and products. Prior to working at SEL, she had two years of industrial control system (ICS) experience in different industrial segments.