Mitigating GPS Vulnerabilities

Shankar Achanta, Steve T. Watt, and Eric Sagen
Schweitzer Engineering Laboratories, Inc.

Presented at the
Power and Energy Automation Conference
Spokane, Washington
March 10–12, 2015

Original edition released March 2014

Mitigating GPS Vulnerabilities

Shankar Achanta, Steve T. Watt, and Eric Sagen, *Schweitzer Engineering Laboratories, Inc.*

***Abstract*—The Global Positioning System (GPS) is a global navigation satellite system that is ubiquitous in applications such as navigation, construction, and precise time synchronization. This economical broadcast technology, operated by the U.S. Department of Defense, provides time synchronization accuracy to a few tens of nanoseconds. GPS technology has become an integral part of power utility system applications for time synchronization. Over the past several years, threats and vulnerabilities have been identified, such as jamming, solar flares, and spoofing, that can affect the proper operation of power utility protection and control systems.**

This paper gives an overview of commonly used time systems and technologies used to deliver precise time. The paper discusses GPS-based time system vulnerabilities and explains how to design resilient time-distribution systems for power system applications to mitigate these vulnerabilities.

I. Introduction

Precise time has found its use in numerous applications in the recent past, and the technology continues to push the limits for accurate time. Global navigation satellite systems (GNSSs) from different countries are used to accurately determine an exact position anywhere on earth, with a precision as low as 1 millimeter, and exact time, with an accuracy in nanoseconds (10^{-9}). These systems are also used to determine speed and direction of travel, making them very valuable for several applications.

The Global Positioning System (GPS), operated by the United States, is a popular example of a GNSS that has become a technology used in a variety of applications and industries. In this paper, GPS technology is discussed, along with time scales and time-distribution methods for precise time applications, with a brief overview of these applications. This paper also discusses some of the vulnerabilities encountered by GPS technology and concludes with mitigation techniques for these vulnerabilities.

II. Time Scales

Before we discuss GPS technology, we look at various time scales available today.

A. International Atomic Time (TAI)

TAI is an atomic time standard based on a weighted average of time kept by over 200 atomic clocks from about 50 scientific laboratories around the world. Because it uses the average of several atomic clocks, this time is the most accurate time known to mankind.

B. Universal Time (UT)

UT is defined by the rotation of the earth, which is determined today by GPS satellites orbiting the earth. Formerly, this time was derived from astronomical observations. UT1 is a version of UT that corrects for the polar wander of the earth, which is a wander of the rotational axis of the earth. UT and UT1 differ by a few tens of milliseconds.

C. Coordinated Universal Time (UTC)

UTC was introduced to account for the effects of the rotation of the earth on timekeeping. UTC and TAI vary from each other by *m* seconds, where *m* represents leap seconds that could be incremented or decremented either on June 30 or December 31 every year.

$$\mathrm{UTC} = \mathrm{TAI} - (10 + \mathrm{m}) \tag{1}$$

Leap seconds account for a time adjustment based on the slowing down or speeding up of the rotation of the earth. The International Earth Rotation and Reference Systems Service (IERS) publishes the leap second occurrence event six months in advance.

Fig. 1 shows the difference between TAI and UTC time scales since the year 1972. At the time of writing this paper, the difference between TAI and UTC is 35 seconds.

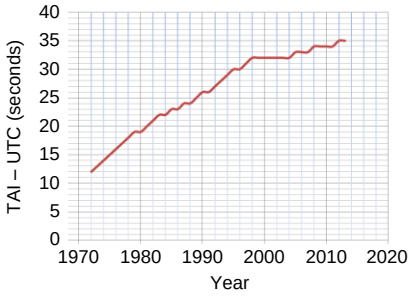

Fig. 1. Time difference between TAI and UTC time scales from 1972 due to leap second insertions.

D. GPS Time

GPS time is synchronized with TAI. The GPS time epoch is midnight UTC on January 6, 1980. No leap seconds are added to the GPS time. Therefore, the difference between UTC and GPS time changes in the increments of seconds each time a leap second is added to the UTC time scale.

$$\text{GPS time} = \text{TAI} - 19 \text{ seconds} \tag{2}$$

E. GPS Week Number

The GPS week number is the week number starting from the epoch time for GPS (January 6, 1980). Weeks are numbered from 0 and count up to 1,023 and then roll over to 0. The rollover cycle for this is 1,024 weeks or 7,168 days, which is approximately 19.6 calendar years. It is important for timekeeping devices that use GPS (such as GPS clocks and receivers) to handle the GPS week number rollover to ensure accurate time reporting.

F. Local Time

Local time is specific to the location and usually has an offset from UTC time. When communicating between geographically separated locations, it is important to use UTC and not local time to avoid confusion in analysis of event time stamps.

Fig. 2 shows the difference in time scales as of December 2013.

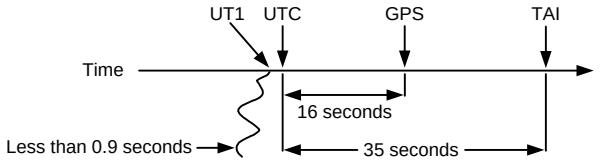

Fig. 2. Difference between UT1, UTC, GPS, and TAI as of December 2013.

Now that we have introduced various time scales, we look at different time-distribution methods and time outputs that are generated from these time scales for commercial and civilian use.

III. Time-Distribution Methods

A. Wide-Area Distribution Methods

1) GNSSs

GNSSs use signal transit times to determine location, velocity, and precise time using GNSS receivers on earth, which receive signals wirelessly from orbiting satellites. There are several GNSSs in service today around the world.

The United States GPS is the best-known GNSS. Others include the Russian GLONASS and, in the near future, the Chinese Compass and European Galileo systems. All of these systems broadcast time signals with carrier frequencies in the range of 1,200 to 1,800 MHz.

2) Ground-Based Radio Stations

Before GNSSs existed, ground-based radio stations such as WWVB and Long Range Navigation (LORAN) were popular for distributing accurate time traceable to UTC. WWVB, located in Colorado in the United States, transmits time information traceable to UTC using a radio carrier at 60 kHz. This time can be decoded by WWVB receivers in North America depending on the proximity of the receivers to the WWVB station. Although WWVB transmits very accurate time signals relative to UTC, the timing accuracy at the receiver is affected by signal propagation delays and the zero-crossing uncertainty of the carrier wave. With digital signal processing techniques and delay compensation, accuracies down to 1 millisecond can be achieved using the WWVB signals [1].

B. Local-Area Distribution Methods

Once we receive time signals from wide-area distribution methods, these signals have to be converted into a format that can be easily processed by the downstream intelligent electronic devices (IEDs). There are several standards that describe the formats that are used to distribute time locally through a network. Popular examples include IRIG-B, Network Time Protocol (NTP), and Precision Time Protocol (PTP) based on IEEE 1588. Each of these distribution methods has its own benefits and tradeoffs, and its usage depends on the level of timing accuracy for applications.

Table I compares the popular local-area time-distribution methods.

TABLE I
LOCAL-AREA TIME-DISTRIBUTION METHODS

Time-Distribution Method	IRIG-B	NTP	PTP (IEEE 1588 and IEEE C37.238)
Physical Layer	Coaxial cable	Ethernet	Ethernet
Model	Master-slave	Client-server	Master-slave
Synchronization Accuracy	~100 ns to 1 µs	~1 to 100 ms	~100 ns to 1 µs
Compensation for Latency	Yes, using cable length as user input	Yes	Yes
Update Interval	Once per second, pulse per second	Minutes	Configurable (typically once per second)
Hardware Requirements	Special hardware required at master and slave	Master only	Support required for high accuracy
Relative Implementation Cost	Medium (IRIG-B cabling)	Low (software)	Medium to high (every device must support PTP for best accuracy)

IV. Oscillators and Cesium Standards

Oscillators are a critical and essential component for any timekeeping device. These components are disciplined or trained by an external time source (e.g., GPS) and keep time at the local instrument or device. The characteristics of these components are critical in achieving accuracy for precise time applications. This section describes some basic concepts for oscillators and cesium standards.

A. Oscillators

Any device that produces time output signals has an oscillator. Every clock is made up of two components. The first component is an oscillating device that counts the length of a second or the time interval that is desired. This oscillates by laws of physics and is referred to as a frequency standard. Examples of this include the classic pendulum that swings with a certain frequency (shown in Fig. 3). The second component of a clock is a device that counts these periodic transitions cumulatively to come up with a count (usually digitized) value that can be used to generate a variety of signals, such as pulses per second.

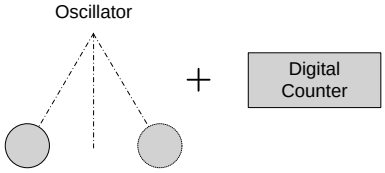

Fig. 3. Illustration of a clock.

In most modern electronics equipment that has active circuitry, there is a crystal oscillator. When certain crystals are subjected to mechanical stress, they produce electric signals across opposite sides of the crystal. Conversely, when an electric potential is applied, these crystals produce mechanical vibration. This is known as the piezoelectric effect. Quartz has excellent mechanical stability and decent immunity to external environmental conditions. When a quartz crystal is connected in a closed-loop electronic circuit, it can be used as a reliable source for frequency and time in electronics [1].

For any frequency device, the number of events per unit of time (e.g., oscillations) is known as frequency.

$$F = 1/T \tag{3}$$

where:

T is the time period or time between the events.

Some of the common characteristics inherent to crystal oscillators are the following:

- Aging is defined as the change in frequency of an oscillator due to internal changes rather than external factors such as temperature and power supply.
- Accuracy is the measured or calculated value of the frequency stability of an oscillator. This defines the quality of the oscillator.
- Drift is the change in frequency with time in an application that uses oscillators. This includes internal factors such as aging and external factors such as temperature and power supply for the oscillator.
- Offset is the difference between the actual and the specified frequency for an oscillator.

B. Cesium Standard

The present official definition of a second is based on a cesium atom. The second is defined as the duration of 9,192,631,770 periods of radiation corresponding to the transition between the two unperturbed states of a cesium atom. The cesium standard is considered the primary frequency standard for its accuracy and long-term stability. This is also known as an atomic clock or atomic standard.

There are other time and frequency standards such as oven controlled crystal oscillators (OCXOs), temperature compensated crystal oscillators (TCXO), and rubidium standards that are used in timekeeping devices, depending on application requirements.

V. Global Positioning System

GPS (shown in Fig. 4) provides a high-accuracy time signal [1].

GPS is one of the most popular and successful GNSSs available today. GPS technology has seen tremendous growth in several business sectors since its inception and has become an essential part of data communications infrastructure across the globe. The free availability of this technology has enabled many applications across a diverse range of industries including aviation, public safety, recreation, telecommunications, transportation, mapping and surveying, finance, and power utilities.

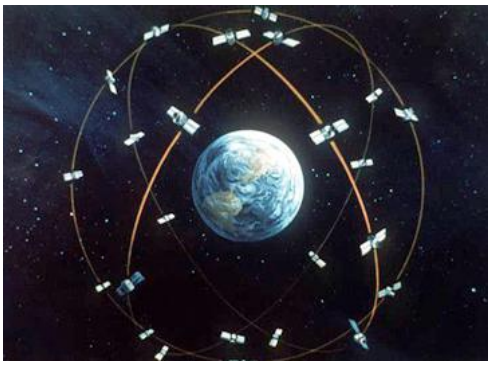

Fig. 4. The Global Positioning System. This image is provided courtesy of the U.S. Department of Defense.

GPS comprises three segments, namely space, control, and the user. Fig. 5 shows how these three segments form the GPS system.

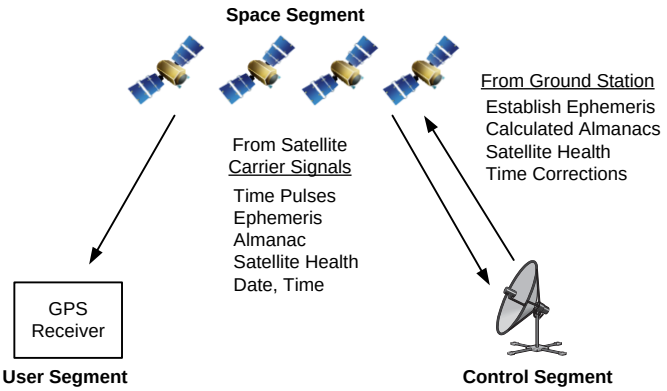

Fig. 5. The three segments of GPS.

A. Space Segment

The space segment consists of a constellation of satellites orbiting the earth that transmit radio signals to users. There are more than 24 satellites available for civilian applications. The satellites orbit in six orbital planes around the earth twice per day at an altitude of about 12,000 miles. These orbital planes are designed in such a way that there are at least six satellites visible on any part of the earth at all times. The GPS satellite constellation is controlled by the U.S. Air Force, which is responsible for periodic maintenance and enhancements.

Each satellite transmits information, known as a navigation message, at the rate of 50 bits per second.

The navigation messages from the satellites are generated using a process called a direct-sequence spread-spectrum (DSSS) technique. DSSS is a technique where an information signal occupying a narrow frequency band is combined with a higher-frequency signal to generate a signal that occupies a wider frequency band. The higher-frequency signal is often a digital signal that is generated in a pseudorandom fashion. The resultant signal that occupies a wider frequency band is transmitted over the communications channel and is decoded by the receiver by combining the received signal with the

same pseudorandom high-frequency signal. Fig. 6, Fig. 7, and Fig. 8 illustrate the DSSS technique.

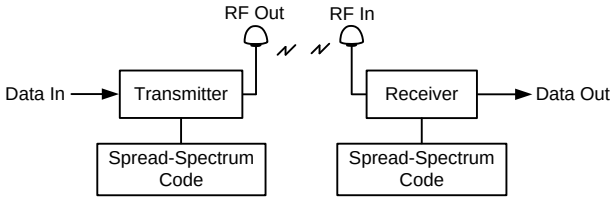

Fig. 6. The DSSS technique.

In Fig. 6, *Data In* is the information at the transmitter, which is combined with the spread-spectrum code. The resultant signal is transmitted via a wireless communications channel. At the receiver end, the same spread-spectrum code is used to retrieve the information sent by the transmitter [2].

This can be explained in the frequency domain, as shown in Fig. 7.

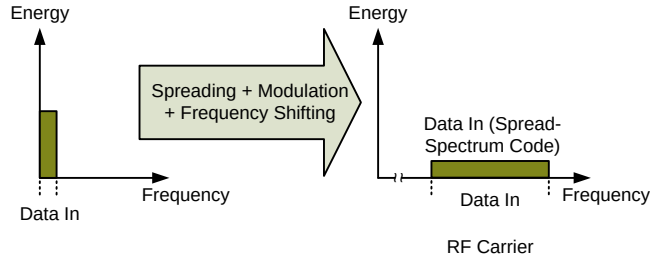

Fig. 7. Signal spreading.

In the transmit block, the incoming data (Data In) go through the spreading and modulation operations and are spread and shifted (for wireless transmission) in frequency. At the receiver end, despreading and demodulation operations are performed to extract the original data, as shown in Fig. 8.

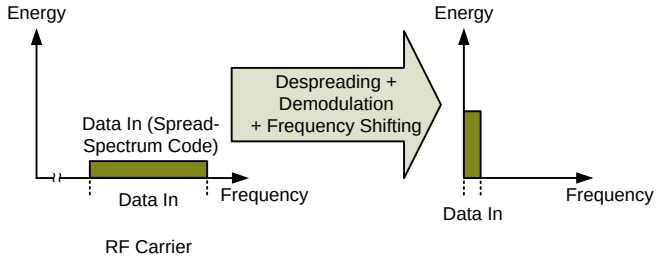

Fig. 8. Signal despreading.

There are several advantages of using DSSS communication, including resistance to interference and jamming. One other important benefit is the coexistence of simultaneous transmitters sharing the same frequency band and communicating with multiple receivers. Although all the transmitters use the same frequency band and transmit signals simultaneously, the receivers can receive and recover signals from each of the transmitters using the spread-spectrum codes. GPS satellites in the space segment use the same DSSS technique as they transmit the satellite signals to earth using unique spread-spectrum codes (also known as pseudorandom number [PRN] codes) for each satellite. A simplified satellite block diagram is shown in Fig. 9 [3].

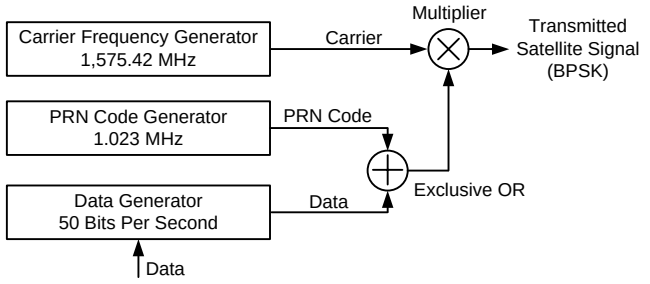

Fig. 9. Simplified satellite block diagram.

Each satellite has four extremely stable atomic clocks. These clocks are used to generate the radio frequency (RF) of 1,575.42 MHz (also known as an L1 signal) and a time signal for the PRN sequence generator at 1.023 MHz and a 50 Hz signal for data. The data at 50 bits per second are combined (via an exclusive OR operation) with the PRN (unique for each satellite) spreading code at 1.023 MHz. The resultant signal at 1.023 MHz is modulated using the carrier frequency of 1,575.42 MHz for wireless transmissions. The modulation format used is bi-phase shift keying (BPSK), where the signal changes phase by 180 degrees every time the data transition from 0 to 1 or from 1 to 0.

B. Control Segment

The control segment consists of a master control station located in Colorado and several ground control stations that communicate with the satellites. The control segment does the following:

- Provides orbital data of all the satellites (almanac) to each satellite.
- Time-corrects for the onboard satellite time.
- Observes and predicts the behavior of clocks in the satellites.
- Observes the orbital movement of the satellites, and calculates the orbital data for each satellite (ephemeris).
- Communicates information such as satellite health and clock errors.

C. User Segment

The user segment comprises devices and technologies that receive the GPS signals and use them for various applications. GPS receivers need to receive valid GPS signals from at least three GPS satellites to determine the latitude, longitude, and altitude of a position and receive signals from an additional GPS satellite to determine time. Commercially available GPS receivers often have 12 channel receivers, meaning that the receiver can simultaneously track up to 12 GPS satellites. GPS receivers have the same PRN codes programmed in them that match the codes in the GPS constellation of satellites. The receivers use these codes to recover the received signal and synchronize their local clocks to the clocks on the GPS satellites. This gives each GPS receiver the capability to generate a time reference with the same accuracy as the atomic clocks used inside each GPS satellite.

There is another frequency band for GPS signals, known as an L2 signal, that operates with a carrier frequency of 1,227.6 MHz. The L2 carrier signals are simultaneously transmitted with the L1 signals from the GPS satellites with special encryption. The encryption for the L2 GPS signals is introduced in the PRN code for these signals. The L2 GPS signals are used for United States military applications for precise positioning and timing. The receivers that can decrypt L2 signals must be authorized by the U.S. Department of Defense, and these receivers are protected from GPS spoofing.

Due to the vast proliferation of GPS technology, there are commercially available GPS receivers for a very low cost. These receivers are civilian receivers that track and decode L1 signals from GPS and cannot decrypt L2 signals. These devices are often used in combination with application-specific designs to create an end product that solves a customer problem. Also, there are specialized GPS receivers available for precise timing applications that use GPS satellite information to produce time signals as accurate as 100 nanoseconds to UTC. Fig. 10 and Fig. 11 show the timing performance of typical GPS receivers available today [4]. Receiver B, shown in Fig. 11, has a tighter control (less variation in the timing accuracy) than the timing performance of Receiver A (shown in Fig. 10).

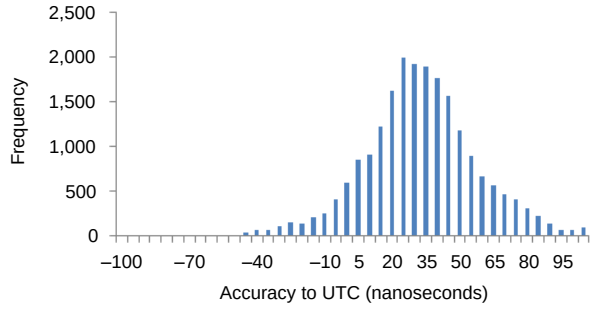

Fig. 10. Timing performance of Receiver A.

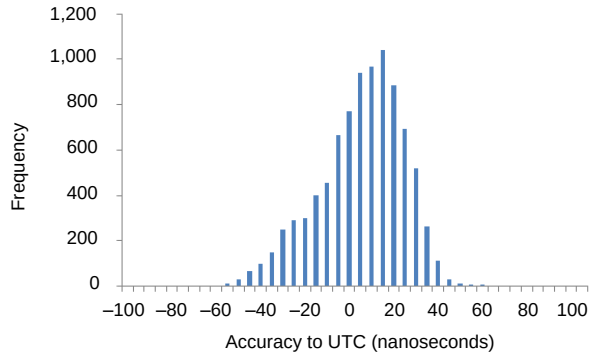

Fig. 11. Timing performance of Receiver B.

VI. Applications of Precise Time in Power Systems

Electric power utilities require precise time for the efficient delivery and control of power transmission and distribution networks. Power utilities rely on GPS-synchronized clocks to synchronize devices in substations, control centers, and distribution feeder circuits. Having precise time available across the entire power grid enables utilities to better monitor and control power systems with faster response times to effectively manage disturbances and ultimately prevent system-wide blackouts.

The following subsections discuss some of the power utility applications for precise time.

A. Disturbance Recording

When power system faults occur, it is important to align the data recorded by several IEDs for post-event analysis that includes finding the root cause that triggered the fault as well as assessing the severity and duration of the fault. Usually an accuracy of 1 millisecond is adequate for this type of characterization. Time synchronization was missing during the North American Northeast blackout of 2003, and it took several months for the utility engineers to time-align event reports and determine the root cause for the blackout. Accurate time-tagged records greatly simplify the task for basic outage analysis, as well as for large-scale disturbance and blackout analysis. The most recent North American Electric Reliability Corporation (NERC) proposal requires that events be time-tagged within one-quarter cycle (approximately 4 milliseconds at 60 Hz) accuracy [5].

Although this accuracy requirement seems to be very easy to achieve given that the accuracies of the GPS receiver-based clocks are in the nanosecond range, all the error terms must be considered, including the rise time of the time signal inputs and the sampling frequency for the IEDs using the time signals.

B. Sequential Events Recorder (SER) Reports

An SER report provides a chronological list of state changes that the IED went through during its operation. These states could be closing or opening a teleprotection contact output, alarms, or logic status on internal logic elements. Reviewing these events can be very useful for troubleshooting the operation of the IED and monitoring the status changes. A typical requirement for time-synchronization accuracy for this application is 1 millisecond.

Digital relays and event recorders produce SER or sequence of events (SOE) reports that provide a chronological list of when monitored devices changed state. Changes of state may be opening or closing, asserting or deasserting, turning on or turning off, and so on. Device monitor points can include circuit breaker status contacts, protective relay and teleprotection contact outputs, and, in modern IEDs, logical statuses on internal logic elements.

C. Power System Fault Location

Traveling wave fault location uses the time of arrival for traveling waves (TWs) that are generated when faults occur on transmission lines. The TWs travel toward either end of the transmission line and reach the end at different times based on where the fault occurred. In order to accurately locate the faults using the TW, it is important to have a precise time reference at each end of the line and exchange this information

between the two ends via a reliable communications channel. Because the TW travels at the speed of light, small errors in time synchronization could lead to large errors in determining the fault location. For example, a 2-microsecond error can create an uncertainty of 600 meters in fault location. Fortunately, there are several time-distribution techniques, including GPS, that provide submicrosecond accuracies.

There are digital communications devices designed for critical infrastructure that distribute time over a wide-area network (WAN) independent of GPS. Terrestrial time-distribution techniques can also be used for this and have an advantage over GPS in that they are less susceptible to spoofing or jamming. Fig. 12 shows a typical example of a traveling wave fault location system that has two relays that exchange time-of-arrival information via a 64 kbps channel using a multiplexer. Although GPS receivers are shown at each of the relays in Fig. 12, terrestrial time-distribution techniques can also be used for accurate time synchronization [6].

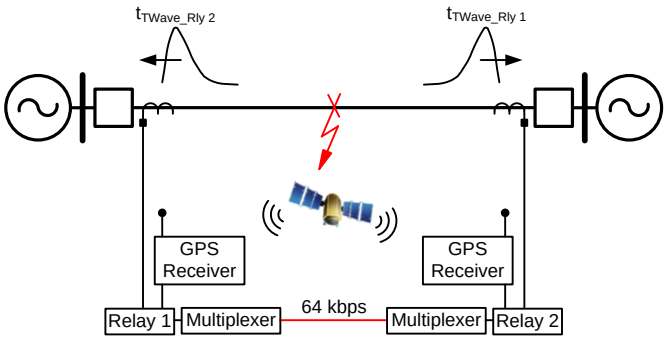

Fig. 12. Traveling wave fault location system.

D. IEEE C37.118.1-2011 Synchrophasor Measurements for Power Systems

Synchrophasors consist of analog and digital quantities from various power system apparatus with an associated precise time stamp. These quantities are collected and time-aligned from various IEDs in the power system. A common time reference for all these data collected over a wide area has traditionally been used for post-event analysis. Recently, new technologies have allowed synchrophasors to be processed in real time, which opened up several applications such as real-time wide-area protection and control, metering data, and sampled measured values.

One of the key requirements for synchrophasors is the precise time synchronization of the devices that are sampling the analog and digital quantities across the power system. IEEE C37.118.1 for synchrophasors defines this requirement to be less than 1 microsecond. Note that a time error of 1 microsecond corresponds to a phase error of 0.022 degrees for a 60 Hz system and 0.018 degrees for a 50 Hz system. The synchrophasor standard calls for a total vector error (TVE) of less than 1 percent. This corresponds to a maximum time error of ±26 microseconds for a 60 Hz system and ±31 microseconds for a 50 Hz system. However, the TVE is a summation of errors from time synchronization, instrumentation conversion, and phasor measurement processing errors. This accuracy of less than 1 microsecond can be achieved with time sources such as GPS and distribution methods such as IRIG-B or PTP.

E. Sampled Measured Values

Process bus involves the exchange of high-speed, real-time instantaneous voltage and current measurements using an Ethernet network. It is based on IEC 61850-9-2 and related international standards. Process bus technology promises to seamlessly deliver smart instrument transformer measurements to a wide variety of protection and control devices located on the same network. Because process bus inputs are sampled at high rates (typically 4 to 16 kHz) with independent digitizers distributed throughout the substation, time synchronization becomes critical for all applications that require data from multiple locations (e.g., bus differential protection).

Because the precise time synchronization of process bus measurements is as important as the measurement values themselves, a mechanism must be implemented to deal with system startup, network component failures, maintenance-related shutdown, and other events that can affect data delivery and time synchronization. Similar to synchrophasors, the timing accuracy for sampled measured values is less than 1 microsecond.

VII. GPS Vulnerabilities

GPS relies on communication from satellites 12,000 miles from the earth and has a received signal power of –127.5 dBm, or 178 • 10^{-18} watts. Considering these facts, GPS is remarkably reliable, but it does have some vulnerabilities. There are several types worth considering.

A. Solar Flares

One vulnerability is atmospheric interference, primarily caused by solar flares. Solar flares are the sudden brightening on the surface of the sun due to a large release of energy (up to 6 • 10^{25} joules). X-rays and ultraviolet (UV) radiation emitted by solar flares can affect the ionosphere, which is a layer 53 to 370 miles above the earth. Large solar flares that can impact the GPS signal occur randomly but average out to one to two times per year. They tend to concentrate at the end of each 11-year solar cycle. Solar flares can last anywhere from a few seconds to an hour and can temporarily prevent a GPS receiver from receiving a signal.

B. GPS Jamming

GPS receivers can also be blocked by jamming, which is noise in the 1.57542 GHz frequency range used for civilian GPS. GPS jamming devices are illegal in the United States, but can be purchased internationally for under $100. If a GPS jamming device is near a GPS receiver, it prevents the receiver from maintaining a GPS lock.

C. Antenna Failures

Antenna failures are one of the largest contributors to system failures in GPS time systems. Any clock that uses a GPS signal requires a GPS antenna that needs to be installed outdoors for best reception. This means that the antennas selected for these critical time systems need to be weatherproof and must be able to withstand harsh environmental conditions. In areas prone to lightning, clock systems often experience antenna damage due to lightning strikes. While it is important to pick the right antenna for reliable operation of the clock systems, there are solutions such as redundant clock systems available today to mitigate these types of failures.

D. Multipath Errors

Multipath errors can also prevent a GPS receiver from having accurate GPS information. Multipath errors come from a GPS clock receiving a signal that has been reflected off of an object such as a building or mountain. Because of the extra delay of the reflected signal, the GPS information will be inaccurate. Most GPS receivers are sophisticated enough to ignore multipath signals if they receive a direct path signal because they use the earliest arriving signal. But if the direct path of a GPS antenna is blocked, the device is susceptible to a multipath error.

E. GPS Spoofing

Because GPS signals for civilian use are not encrypted, it is feasible for an attacker to mimic, manipulate, and replay an L1 GPS signal. Spoofing is when an attacker intentionally generates signals that closely mimic GPS signals and transmits them at a slightly higher power. When this is done, a civilian GPS receiver may lock on to the spoofed signal and be susceptible to intentional shifts in the GPS timing and positioning information created by the attacker.

With solar flares or jamming, a GPS clock senses the loss of the GPS signal and typically switches to a holdover time source. With multipath errors, a GPS clock does not know it is receiving a reflected signal, so it may continue to operate with slightly delayed timing information. Also with multipath errors, because the direct path is blocked, there may be an indication by the clock of a loss of the GPS signal.

Spoofing seems to be the most significant vulnerability to consider. When spoofed, a GPS clock continues to operate, assuming a good GPS signal. However, this signal could be manipulated significantly, causing incorrect time information for event information. It is important to consider all types of GPS vulnerabilities and mitigate the associated risk based on the application for precise time and its criticality.

VIII. Mitigation Techniques

In the following subsections, we discuss some approaches and ideas for mitigating the GPS vulnerabilities.

A. Redundant GPS Clocks With Time Distribution

This approach uses multiple GPS clocks with each receiver separated by some distance. Each GPS clock receives GPS signals simultaneously and produces time outputs independently from each other. These time signals are compared using a system that monitors the health of these signals. Examples include monitoring a loss of signal for IRIG-B outputs from multiple clocks or monitoring the time quality bits in an IRIG-B time code. When there is an antenna failure due to factors such as lightning strikes, GPS timing can still be maintained using the clock reference from an alternative GPS receiver. There are low-cost IRIG-B selection systems available today that reliably select the best IRIG-B source based on the time quality or loss-of-time signals. These systems also provide additional features such as delay compensation so that the accuracy of the time outputs is preserved as the signal traverses through several devices before it reaches downstream IEDs. This approach mitigates GPS jamming and spoofing if the GPS clocks shown in Fig. 13 are separated geographically by sufficient distance.

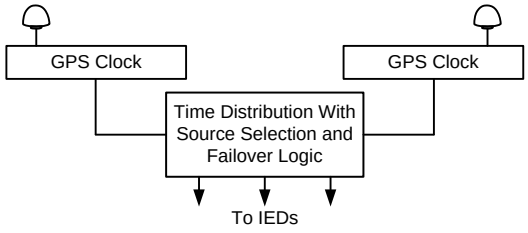

Fig. 13. Time-distribution device with source selection.

B. Redundant Time Sources With Source Selection

As we discussed previously, GPS time systems are traceable to UTC and provide accurate time with accuracies in the order of tens of nanoseconds. There are several time-distribution formats available for use, including IRIG-B, NTP, and PTP. A simple scheme involves time signals from multiple sources that are compared with each other to eliminate the outlier. Fig. 14 shows an example of a device that receives time signals from GPS, IRIG-B, PTP, and NTP.

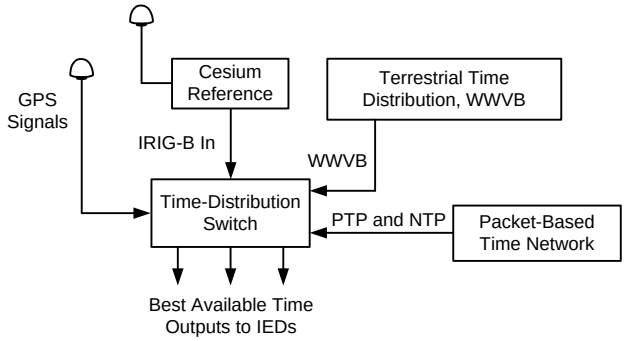

Fig. 14. Time-distribution switch.

The time-distribution switch shown in Fig. 14 receives time signals from a variety of sources, all traceable to the UTC time scale. This device also has the ability to receive GPS signals. The inputs to this switch must be carefully selected so that they have the greatest diversity. The time-distribution switch compares all the incoming time inputs by monitoring several attributes of the time signals using weighting schemes and averaging techniques to determine the best time. It provides this best time to the downstream IEDs. The algorithms to implement the weighting schemes and averaging are beyond the scope of this paper.

This method not only mitigates local GPS disruptions due to antenna failures, jamming, and spoofing, but also provides lossless time signal availability to the downstream IEDs in the event of these failures.

C. Time Distribution Over WANs

Synchronous optical network (SONET) systems are time-division multiplexing (TDM) systems that use frequency synchronization across the entire network for the transport of communications with a high data rate. Some SONET multiplexers are also capable of using the frequency synchronization of the network to distribute time across the network and generate a local time reference such as IRIG-B at each node. SONET multiplexers can make use of multiple GPS clocks or timing references at several nodes. Depending on the size of the network, each timing reference can be separated across a large geographical area. These SONET systems are designed and configured so that each node has its own local time (from a local GPS antenna, for example) and time signals from the two adjacent nodes. The node selects the best available time based on comparing at least three available time signals. This mitigates several GPS vulnerabilities, including antenna failures at a single node or GPS jamming or spoofing at a single node. This SONET-based time distribution provides a strong layer of security against a malicious GPS attack. The nodes distribute the best time based on all the time inputs they receive to the downstream devices. Fig. 15 shows a typical SONET communications ring network.

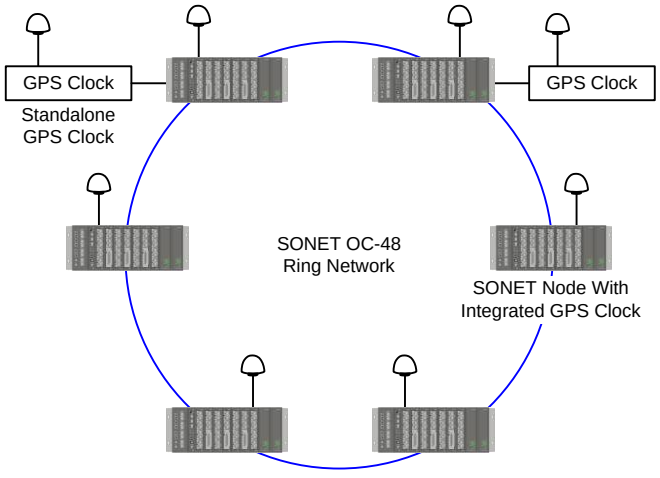

Fig. 15. Typical SONET ring network.

In the event of complete GPS failure due to events such as solar flares, a high-accuracy local oscillator can enable the SONET network to maintain a relative time accuracy of less than 1 microsecond and generate local time references for downstream IEDs. The diagram in Fig. 15 shows that some SONET nodes can be configured to have a built-in GPS clock or obtain time from a separate standalone GPS clock. The advantage of using standalone GPS clocks is that they come with options such as cesium-based oscillators that have a very high holdover accuracy in the event of GPS signal loss [7].

D. Cesium Reference and Local Oscillator Characterization

When GPS clocks receive GPS signals using the GPS receivers embedded in them, the GPS receiver produces a timing pulse that is very accurate (tens of nanoseconds) to UTC. The local oscillators in these GPS clocks (e.g., TCXO and OCXO) are trained by these GPS time signals. These oscillators combined with some logic produce time output signals such as IRIG-B, NTP, or PTP.

When the GPS signals start to drift due to loss of satellite signals or signal manipulation, one approach to minimize the drift is to use the local oscillator characterization to detect the drift in GPS signals. As the local oscillator behavior can be characterized and understood, the aging, accuracy, drift, and offset of these oscillators can be used to see if the signals from the GPS are being compromised.

In this approach, the local oscillator counts the number of counts (based on the frequency of the oscillator) between each period of the time pulses produced by the GPS receiver. By accumulating this count over a long term, any GPS time signal manipulations are detected.

The thresholds for detecting these manipulations are dependent on the technology of the oscillators used in these devices. Algorithms to implement this are beyond the scope of this paper.

E. Multiconstellation GNSS Receivers

Apart from GPS, there are several other GNSSs that are being deployed to provide information such as location, time, and velocity for use in various applications. These include the Russian GLONASS and, in the future, the Chinese Compass and European Galileo systems. There are receivers available today that can simultaneously track these GNSSs and independently extract time signals. One approach is to compare time signals received by several receivers tracking different GNSSs. This approach validates time signals provided by one GNSS with another. As these systems have diversity in carrier frequency, signal coding, and so on, this comparison provides an additional layer of security against vulnerabilities such as jamming and spoofing.

IX. Conclusion

GNSSs have been providing reliable and high-accuracy time for several decades. GPS is the most popular of all the GNSSs available today and has seen some threats recently from intentional jamming and spoofing. Also, this system can experience interference due to natural causes such as solar flares and antenna system failures due to lightning. As applications such as synchrophasors, sampled measured values, and traveling wave fault location rely on GPS, it is very important to understand and address these vulnerabilities. This paper describes the technology behind GPS operation and provides several methods to mitigate the vulnerabilities to achieve a higher degree of reliability for time-critical applications in power systems. Table II summarizes the vulnerabilities and the mitigation techniques.

TABLE II
SUMMARY OF MITIGATION TECHNIQUES

Vulnerability	Effect	Mitigation (as explained in Section VIII)
Solar flares	Signal loss	Holdover oscillator (Subsection D), redundant time sources with source selection (Subsection B)
GPS jamming	Signal loss	Holdover oscillator (Subsection D), redundant time sources with source selection (Subsection B)
Antenna failures	Signal loss	Clock redundancy (Subsection A), holdover oscillator (Subsection D), redundant time sources with source selection (Subsection B)
Multipath effects	Signal manipulation	Redundant time sources with source selection (Subsection B), multiconstellation signal verification (Subsection E), local oscillator characterization (Subsection D)
GPS spoofing	Signal manipulation	Redundant time sources with source selection (Subsection B), multiconstellation signal verification (Subsection E), local oscillator characterization (Subsection D), time distribution over WANs (Subsection C)

X. References

[1] E. O. Schweitzer, III, D. Whitehead, S. Achanta, and V. Skendzic, "Implementing Robust Time Solutions for Modern Power Systems," proceedings of the 14th Annual Western Power Delivery Automation Conference, Spokane, WA, March 2012.

[2] S. Achanta, B. MacLeod, E. Sagen, and H. Loehner, "Apply Radios to Improve the Operation of Electrical Protection," proceedings of the 37th Annual Western Protective Relay Conference, Spokane, WA, October 2010.

[3] Maxim Integrated, "An Introduction to Spread-Spectrum Communications," February 2003. Available: http://www.maxim-ic.com.

[4] Global Positioning System Standard Position Service Performance Standard, October 2001. Available: http://www.navcen.uscg.gov/pdf/gps/geninfo/2001SPSPerformanceStandardFINAL.pdf.

[5] North American Electric Reliability Council, "Technical Analysis of the August 14, 2003, Blackout: What Happened, Why, and What Did We Learn?" July 2004. Available: http://www.nerc.com.

[6] S. Marx, B. Johnson, A. Guzmán, V. Skendzic, and M. Mynam, "Traveling Wave Fault Location in Protective Relays: Design, Testing, and Results," proceedings of the 16th Annual Georgia Tech Fault and Disturbance Analysis Conference, Atlanta, GA, May 2013.

[7] K. Fodero, C. Huntley, and D. Whitehead, "Secure, Wide-Area Time Synchronization," proceedings of the 12th Annual Western Power Delivery Automation Conference, Spokane, WA, April 2010.

XI. Biographies

Shankar V. Achanta received his M.S. in electrical engineering from Arizona State University in 2002. He joined Schweitzer Engineering Laboratories, Inc. (SEL) in 2002 as a hardware engineer, developing electronics for communications devices, data acquisition circuits, and switch mode power supplies. Shankar received a patent for a self-calibrating time code generator while working at SEL, and he is an inventor on several patents that are pending in the field of precise timing and wireless communication. He currently holds the position of research and development manager for the precise time and wireless communications group at SEL.

Steve T. Watt received his B.S. in mechanical engineering from Virginia Polytechnic Institute and State University. He worked in the information technology industry for over 20 years at Hewlett Packard before joining Schweitzer Engineering Laboratories, Inc. (SEL) in 2012. Steve is currently the product manager for precision time products in the time and communications group at SEL.

Eric Sagen received his B.S. in electrical engineering from Washington State University in 1997. He joined General Electric in Pennsylvania as a product engineer. In 1999, Eric was employed by Schweitzer Engineering Laboratories, Inc. as a distribution product engineer. Shortly after, he was promoted to lead distribution product engineer. Eric transferred to the time and communications group in 2006 and is currently a lead product engineer. He is certified in Washington as an Engineer in Training (EIT).