GNSS Time Signal Spoofing Detector for Electrical Substations

David M. Laverty, *Senior Member, IEEE*, Colin Kelsey, John O'Raw

Abstract— **This paper introduces a novel method of GNSS spoofing detection with applications in electrical substations. Time sensitive applications in electricity substations, including Phasor Measurement Units (PMU) and Merging Units (MU), rely on Global Navigation Satellite Signals (GNSS), often GPS, for time transfer. Recently, sophisticated 'spoofing' attacks have become feasible due to the availability of low cost Software Defined Radio (SDR) systems.**

The proposed method uses multiple GNSS receive antennas placed in close proximity at the electricity substation, such that it is not possible for an attacker to target a unique spoofing signal towards each antenna. In a system employing three or more receive antennas, during a spoofing attack two or more of the GNSS receive antennas will return an estimated position in impossible locations. This is sufficient to raise alarm that time sensitive applications should use an alternative time source or holdover clock.

The contributions of this paper include a detailed description of the proposed method, an experimental assessment of GNSS receiver and substation clock position estimation variance to establish the minimum separation required between receive antennas, and a validation of the method by experimentally demonstration. A further benefit of the authors' method is that it may be put into practice immediately using commercial-off-the-shelf (COTS) substation clock equipment.

***Index Terms*— Time Synchronization, GPS, GNSS, Spoofing Attack, Phasor Measurement Unit**

I. Introduction

TIME transfer and time synchronization is an important function in the electrical substation. Phasor Measurement Units (PMU), Merging Units (MU), and various protection relays depend on synchronism with the UTC time base for their operation [1], [2], [3]. These devices synchronize with a substation clock using one of several methods, including Precision Time Protocol (PTP), Network Time Protocol (NTP), IRIG-B or even 1-pulse-per-second (1PPS) over coaxial cable.

The substation clock synchronizes to UTC by means of a time signal, usually from a Global Navigation Satellite System (GNSS). GNSS include the GPS (USA), GLONASS (Russia), BeiDou (China) and Galileo (EU) constellations. Terrestrial signals are sometimes used for a limited subset of applications requiring time transfer, but tend not to provide the precision time available from GNSS that is required in the substation.

The GNSS signals are transmitted by constellations of satellites in medium earth orbit (MEO) with relatively low power, meaning that by the time the signal reaches the Earth's surface the power density is of the order of fW/m^2 (10^{-15} W/m^2). This is said to be equivalent to viewing a 25 W light bulb at a distance of 10,000 miles [4]. The GNSS signal can be blocked or jammed over a large area with a terrestrial transmitter of very low power, essentially saturating the spectrum used by the GNSS signal with noise or an unmodulated carrier. Such devices are known to be used in haulage and courier businesses by drivers intending to interfere with GNSS tracking devices on their vehicles. A famous example of such a device caused interference with Newark Airport's ground based GNSS augmentation systems in 2012 [5]. Such devices would cause substation clocks to lose their lock on GNSS signals. Annually, the Royal Navy's 'Joint Warrior' training exercise leads to blocking of civilian GNSS uses, usually in Scotland [6]. However, the blocking 'attack' is relatively easy to identify due to the complete loss of time and position. In such conditions, applications can failover to stabilized crystal oscillators or atomic clocks until the GNSS signal is restored.

The much more challenging attack to identify is 'spoofing' of the GNSS signal. This is when a terrestrial transmitter is configured to produce a signal which looks like a legitimate signal from a GNSS constellation, but the data has been manipulated to adjust the time or position information interpreted at the target receiver (i.e. the substation clock under attack) [7]. Spoofing can be achieved using a replay attack, in which past data is recorded and replayed, but this too can usually be identified easily in the application. Reflecting the seriousness with which this problem is regarded, the US DOE has funded the US$4.3M 'Tempus' project to find GNSS spoofing mitigation solutions [8].

Recently, Software Defined Radio (SDR) transceivers have become available which make possible more sophisticated spoofing attacks [9]. An SDR allows generation of GNSS signals with programmatic control of time and position characteristics [10], allowing an attack to be constructed in which the time signal observed by the substation clock at its surveyed position is gradually adjusted over a long period of time, slowly bringing the substation out of synchronism with

Manuscript submitted: 15th February 2021. This work was supported by the British Council 'TIIWAM', US-Ireland 110 'CREDENCE' and the EPSRC 'CAPRICA' (EP/M002837/1) projects.

David Laverty is with the School of Electronics, Electrical Eng. and Computer Science, Queen's University Belfast, Belfast, BT7 1NN, United Kingdom (e-mail: david.laverty@qub.ac.uk).

Colin Kelsey is with the Nanotechnology and Integrated Bioengineering Centre (NIBEC), School of Engineering, Ulster University, BT37 0QB, Northern Ireland, United Kingdom (c.kelsey@ulster.ac.uk).

John O'Raw is with the Dept. of Computing, Letterkenny Institute of Technology, Port Road, Letterkenny, Rep. of Ireland (john.oraw@lyit.ie).

the rest of the grid [11]. Recently, spoofing attack methodologies have been demonstrated which cannot be detected by existing anti-spoofing methods [12]. This has the potential to destabilize the protection and control systems and lead to loss of customer supply.

This paper describes a method of detecting a spoofing attack which may be employed using conventional substation clocks. The authors' method will distinguish between a legitimate GNSS signal and a terrestrial 'spoofing' attack, and will allow the substation to failover to a backup time source such as an atomic clock until the interference is removed. The authors' method is not vulnerable to recent spoofing methods which can bypass existing anti-spoofing countermeasures [12].

The key benefit of the authors' approach is that it has a high technological readiness level (TRL) and thus it may be deployed immediately using existing substation qualified 'commercial-off-the-shelf' (COTS) equipment. The authors' method exploits changes in position estimation under a spoofing attack when multiple receive antennas are located in close proximity. In contrast, other methods require special antennas and receivers [13] which are not available as qualified substation products. Although not necessary for its operation, the authors' position estimation method can be used in conjunction with other spoofing detection methods, and with good engineering practice such as directional receive antennas, to yield a holistic spoofing detection solution.

The authors have experimentally assessed the position estimation performance characteristics of substation clocks and GNSS chipsets. The GNSS chipsets considered are designed for integration into devices such as substation clocks, providing the time and navigation solution. This work allows the maximum position variance of GNSS receivers to be determined, and thus the minimum antenna separation required in order to operate the proposed position variance spoofing detection method. A key contribution is the finding that the method is feasible even on smaller substations. It is found that existing substations clocks have position variances such that antenna placement may be as little as 14 meters apart. This allows antenna placement on substation control buildings. Modern GNSS chipsets can reduce this requirement to 10 meters or less; although they are not used in the substation clock hardware available to the authors at the time of writing, they indicate the performance expected to be available in future substation clock products.

II. Background on GNSS Timing

Global Navigation Satellite Systems (GNSS) consist of a constellation of satellites in Medium Earth Orbit (MEO) which broadcast time signals derived from atomic clocks in orbit, which are themselves synchronized to atomic clocks at ground stations on Earth. The primary function of the GNSS is to provide position information, in 3D (latitude, longitude and altitude) around the surface of the Earth. Each satellite in the GNSS constellation broadcasts a time signal which is synchronized with the other satellites in the constellation, information about the orbit of the satellite sending the signal called the 'ephemeris', and a table of positional information for all the satellites in the constellation known as the 'almanac'.

A receiver on Earth listening to the signals from several satellites will observe the time signals arriving at different times, as a consequence of the propagation delay from each satellite varying in proportion to the distance between the satellite and the receiver. The receiver uses the differences in signal arrival time, along with the known positions of the satellites, to determine the position of the receiver using the process of trilateration. In doing so, the receiver is solving for four unknowns; its latitude, longitude, altitude, and the clock error. Solving for four unknowns requires the receiver observe at least four satellites [14].

The clock error assumes the receiver does not know what time it is, certainly not with sufficient precision to determine accurate position. Once the equations for the four unknowns are solved, the receiver knows its location and also an estimate of the time-of-day, corrected to Coordinated Universal Time (UTC), with a precision of the order of nanoseconds. Calculating the uncertainty in the timing information is a complex matter, with several metrics available including 'Horizontal Dilution of Precision' [15] which must account for various effects including atmospheric, multipath and ephemeris error sources. The signals travel at 'c' (3 x 10^8 m/s), and so travel ~30 cm in 1 ns. If a receiver is reporting location accuracy of <5 m, as is quite common, then the timing error is of the order of 17 ns or better.

The GNSS clock (receiver) provides time information to substation equipment by means of modulated or unmodulated serial time codes (e.g. IRIG-B), Precision Time Protocol (PTP) over Ethernet, or at the most fundamental level by means of a TTL pulse train at a rate of 1-pulse-per-second (1PPS). A properly configured system will have adjustments made for the cable length to the GNSS antenna on the exterior of the substation, and individual apparatus will have compensation for their distance from the GNSS clock, Fig. 1. The velocity factor of the cable needs to be determined, although the approximation of 0.7c is usually a reasonable estimate.

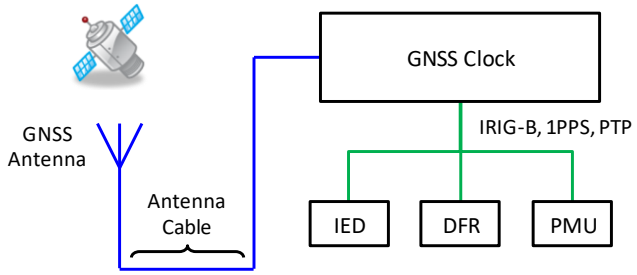

Fig. 1 Overview of Substation Time Distribution

A. *Effect of Time Error in Substations*

In modern substations, protection and control systems are dependent on continuous point-on-wave (CPOW) sampled value (SV) measurements of voltages and currents from buses and lines. The SVs are measured by merging units, which are synchronized to the substation clock. Errors in the substation clock's time-keeping manifest as phase errors when compared

with measurements taken at other substations.

The problem is perhaps most apparent when considering the Phasor Measurement Unit (PMU). It has been demonstrated that time synchronization vulnerabilities exist in PMU based systems [2], [3]. At nominal frequency, the periods of 50 Hz and 60 Hz power systems are 20 ms and 16.7 ms respectively. On a 60 Hz system, a time error of just 26.5 μs yields a phase error of 0.01 radian, the limit for Total Vector Error (TVE) in [16], whilst 46.3 μs represents a phase angle error of 1° (55.5 μs at 50 Hz). If an attacker were to interfere with the time signal arriving at a substation, it would be possible to cause protection systems based on phase angle to act on false information. Consequently circuits would be opened and customer supply would be lost, and in serious coordinated attacks the stability of the whole electricity grid would be compromised leading to widespread disruption.

III. GNSS Jamming and Spoofing

GNSS signals arrive at the surface of the Earth with a power density of the order of 10^{-15} W/m^2, and operate at frequencies in the range 1.1 to 1.6 GHz. Consequently, it is relatively trivial to construct a small portable transmitter which can overwhelm this portion of the spectrum with either a strong carrier or noise, blocking the GNSS receiver from detecting the genuine signals and rendering it incapable of determining location or time. Such devices are known as 'GPS jammers' and, although usually illegal, are easily obtainable via several online marketplaces. They are known to be used in haulage and marine environments to circumvent regulations, for example to obfuscate the hours a vehicle has been driven [17], [18]. In the EU, the 'Strike3' project has conducted long term monitoring to assess the frequency and threat of GNSS outages [19]. The study shows that in a city centre location, 100s of outages per week were observed.

GNSS jamming is relatively easy to detect because the receiver will indicate that no lock is available, and can be configured to cease reporting position and time information. This forces a timing application to failover to a local oscillator to maintain time until the time signal is restored, a process known as 'holdover'. Generally, applications will be designed to be tolerant of loss of time signal, and thus 'fail safely'. It would need to be anticipated that an antenna fault or similar could occur.

It is much more challenging to detect GNSS 'spoofing'. This is the process by which an attacker will transmit a terrestrial signal which has been modulated to appear as though it is a genuine GNSS signal arriving from the constellation of satellites. The receiver is unable to differentiate the 'spoofed' signal it is receiving from a genuine signal, and will report time and position information based on the 'spoofed' signal.

GNSS spoofing can operate in a number of ways. In a playback attack, genuine GNSS signals are recorded and then retransmitted at a later time. When retransmitted, the receiver believes the time to be the time at which the original recording was made. This method is easily detectable on a receiver that is in continuous operation, as one could detect a step backwards in the indicated time – an impossibility.

Alternatively, the attacker can calculate the GNSS signals based on an arbitrary position and time, and modulate the transmitter accordingly. This may be limited to the present almanac information held in the receiver, or in a long term attack a new almanac can be transmitted making it possible to spoof any position and time desired.

Until recently, the equipment required for a spoofing attack cost of the order of several thousand dollars and was in the form of large laboratory bench top devices. In the past year, low cost pocket sized software defined radios (SDR) have been demonstrated to be capable of GNSS spoofing, operating from 'credit card sized' computers such as the Raspberry Pi [9]. This has troublesome implications in terms of an attacker being able to deploy a small battery powered spoofing tool which would be difficult to find. Indeed, many such devices could be deployed across a wide area to create a coordinated attack.

IV. Spoofing Mitigation Approaches

Mitigating against a spoofing attack requires that the receiver determines that the received signal is not a genuine signal from the GNSS constellation. This is not a trivial task given that the spoofed signal is intentionally designed to appear as though it is a genuine signal. There are three main approaches that may be used [20]:

- Cryptographic methods
- Distortion detection
- Direction of arrival sensing

The cryptographic methods provide a means of authenticating the genuine GNSS signals by means of encrypting the signals broadcast by the constellation. Although methods like this are used for military services, and the Galileo Commercial Authentication Service [21], there are challenges regarding keeping widely distributed keys secret and playback attacks remain a risk. Methods to verify signals by second channels are possible [20] but require a change to present GNSS designs.

Distortion detection works by identifying a discontinuity in the received signal at the moment that the spoofing attack commences, for example a step change in the received signal's amplitude or phase angle. Distortion detection requires modified baseband hardware, and is only successful if it detects the beginning of an attack. It is possible for the detector to miss the start of the attack, and it will not subsequently be able to determine spoofing whilst the attack is in progress.

Direction of arrival sensing works by using multiple antennas to determine the direction from which the received signal is arriving [22]. In normal operation, many GNSS signals should be arriving from a high elevation, i.e. overhead. Genuine GNSS signals will be arriving from multiple directions; that is one signal from each satellite in view. If the signals are arriving from the same direction, this indicates a single source of transmission and thus a spoofing attack. It would be impossible for all the GNSS satellites to be in the same point in space. If the signals originate from a single point, this is a clear indication of a spoofing attack; if arriving from

the horizon, it indicates the attacker is on the ground as opposed to airborne. Indeed directional antennas could be configured to attenuate signals of terrestrial origin, however the low power density of GNSS signals means this is easily overcome with a higher terrestrial transmit power.

Direction of arrival sensing appears to have the most potential of the methods described. The method described in [20] was demonstrated to operate successfully on a yacht. This design uses two antennas, and can determine the bearing of the attacker and, by Doppler shift, if the attacker and target are moving toward or away from each other. Whilst highly effective, this method requires sophisticated radio hardware to analyze the differential carrier phase between two antennas which are spaced close together, circa 20 cm apart. Whilst such a method would be useful in an electricity substation environment, removing the constraint of having the antennas close together makes the authors' alternative approach possible.

Novel methods have been presented in literature. In [23], multilateration is shown using simulated data to allow the location of a spoofed GNSS signal source to be estimated. Using specialized hardware, in [24] the satellite signal processing front end is exploited to analyze correlation of local clock candidates/replicas. Likewise, special hardware is used in [25] to examine clock drift in the satellite baseband of a spoofed signal.

A comprehensive review of GNSS spoofing vulnerabilities and countermeasures is presented in [26], [27]. Of the mitigation techniques surveyed, a common aspect is the need for specialist hardware and novel signal processing techniques. These are not available to implement in the electrical utility sector. In contrast, the new method presented in this paper can be implemented using conventional substation clocks.

V. Description of New Detector

The authors' detector works primarily by exploiting the sensitivity of GNSS receivers. By placing multiple receive antennas in close proximity, a spoofing attack on one antenna will be received by the adjacent antennas. If the spoofing attack has been tailored for the position of any one antenna, the other antennas will report an invalid location.

The method may be implemented using conventional substation clocks and feeding their position estimations to a substation computer for comparison. The bill of materials for this method is of the order of US$3,000 for each clock and antenna, and another US$3,000 for the computer, yielding a total cost approximately US$12,000. Compared to using a single clock with no spoofing detection mechanism, the marginal cost is US$9,000. It should be noted that the additional substation clocks, suitably configured, will improve the reliability of the time solution in the substation against general equipment failures and malfunctions. Additionally, direction of arrival can be determined using the output of the substation clocks and the substation computer, as described in Section VI.

Fig. 2 shows the implementation of the authors' detector in a substation which is an arbitrary '*a*' meters long by '*b*' meters wide. Three GNSS antennas have been located about the substation perimeter. Each antenna is connected to a separate GNSS substation clock. Each clock separately determines its position (latitude, longitude), the time of day (date and time to nearest second) and a 1PPS pulse indicating the transition of the UTC second as determined by the clock. The clocks are housed in an equipment bay in the substation building, for the purposes of this exercise it is assumed that the clocks are immediately adjacent to each other in the same equipment rack but this is not a necessity. Although the clocks are housed immediately adjacent to each other, the signals that they are processing are the GNSS signals incident on that individual clock's antenna. Thus each clock will determine the position of the antenna to which it is connected. In order that the time pulses from the clocks are coherent, each clock is configured to compensate for the antenna cable propagation delay. Antenna cable lengths are '*x*', '*y*', '*z*' meters, indicated in Fig. 2.

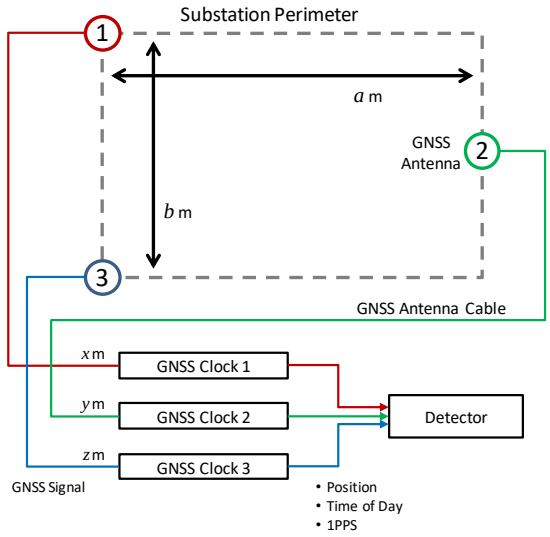

Fig. 2 The authors' detector using three antennas and three substation clocks. The detector receives the output of the clocks, position, time of day, and 1PPS, and determines anomalies. The detector may be implemented on a substation computer, and the clocks co-located in the same rack if desired.

A. Spoofing Detection by Position Estimation

In normal operation, each clock's GNSS receiver estimates the position of the antenna it is connected to by trilateration. Given a clear view of the sky, a GNSS receiver will usually estimate latitude and longitude with better than 5 meters uncertainty (this is validated in Section VII). Allowing that the substation dimensions, '*a*' and '*b*' are an order of magnitude larger (~50 m), there will be a very clear separation between the antenna positions with no possibility of overlapping estimates. The detector, observing the reported positions, will determine what the normal positions of the antennas are, Fig. 3(a).

In the spoofing attack, the transmitter sends a signal modulated to appear as though it is a legitimate GNSS signal arriving at one of the GPS antennas. In Fig. 3(b), the attacker has chosen to calculate the 'spoofed' GNSS signal based on the position of antenna 1. The signal from the terrestrial transmitter arrives at antenna 1 and has the desired effect. However, the signal additionally arrives at antennas 2 and 3, causing their

receivers to also estimate their position at the location of antenna 1. The detector receives the position information reported by each clock, and will compare against a record of the known antenna positions. Since the positions reported by Clock 2 and 3 are the same as Clock 1, this cannot be reasonably attributed to random error. Rather, it is concluded that there is a GNSS spoofing attack in progress. The spoofing detection method works in a similar manner should the attacker use the position of antenna 2 or 3.

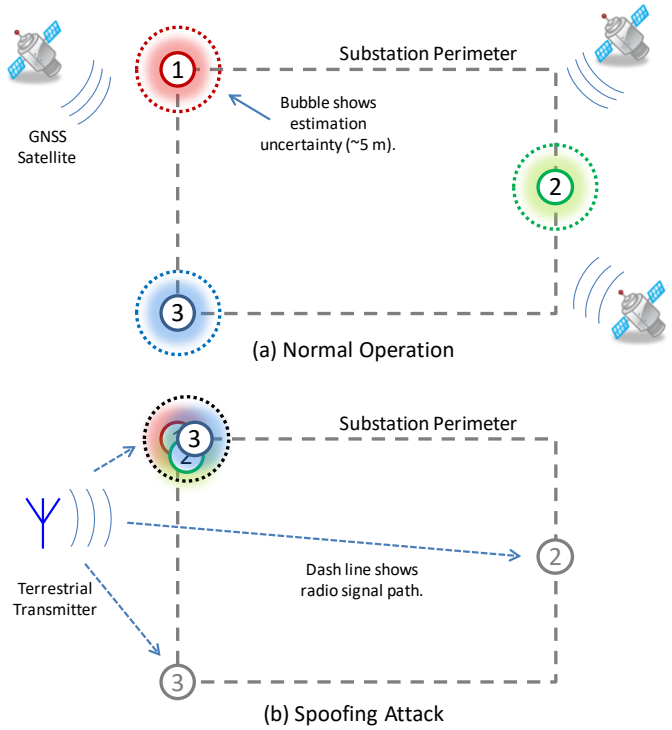

Fig. 3 Behavior of position estimation under (a) normal operation, and (b) spoofing attack. In (a) the receiver determines the position of the antenna using legitimate GNSS signals. In (b) the attacker spoofs the position of antenna 1. Receivers 2 and 3 are deceived into estimating their position at 1.

B. Spoofing Bearing Estimation by Loss of 1PPS Coherence

Although the discrepancy in the position information will be sufficient to determine that a spoofing attack is in progress, it is possible to go a step further and determine the bearing from which the attack originates, assuming that it originates on the same horizontal plane as the substation; i.e. it is a terrestrial attack. This may be achieved by consideration of the 1PPS impulses from the clocks.

In normal operation, the 1PPS from the clocks will be coherent; that is they will pulse at the same instant in time, Fig. 4(a). Although some jitter would be expected, this is of the order of nanoseconds.

Consider the spoofing attack from Fig. 3(b) in which the receivers all determine their positions to be at antenna 1. The receivers will calculate their time-of-day and 1PPS outputs based on their understanding that they are receiving GNSS signals at position 1, yet the radio signal has in fact travelled different distances from the transmitter to each receive antenna. Consequently, the propagation delay to each antenna is different and thus the 1PPS will remain at the same frequency but with slight phase shifts relative to the other clocks, Fig. 4(b). Section VI describes how the bearing and range of the attacker is calculated.

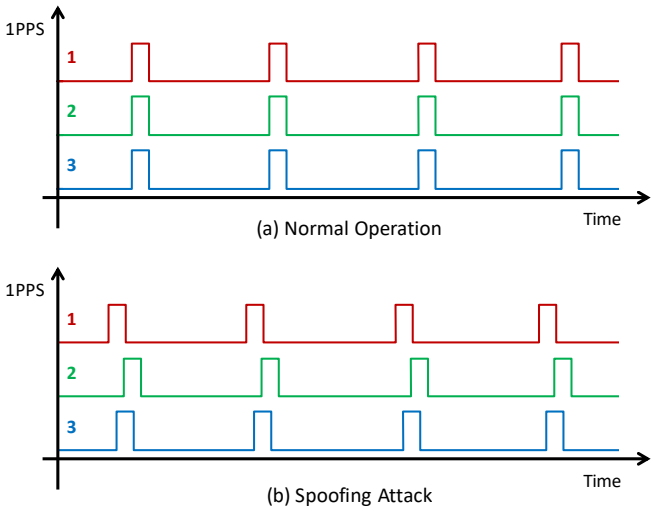

Fig. 4 Behavior of 1PPS outputs (a) during normal operation and (b) during a spoofing attack. The 1PPS are no longer coherent when under attack.

Hypothetically, it is possible for the attacker to generate unique spoofing signals for each GNSS receive antenna. There are many challenges with this. If the attacker used a highly directional antenna and took control of one antenna, then the timing information from the other antennas is in disagreement. This is true even if two antennas are subject to individual spoofing signals. If there is any disagreement in the time pulses, the recommendation is to failover to a holdover clock. The likelihood of such a coordinated attack is considered low. If the attacker is any reasonable distance from the substation, even directional spoofing signals will spread and be picked up by many receive antennas. In order to individually attack three antennas, the attacker will need multiple synchronized transmit locations about the substation perimeter. Physical security considerations should be applied to mitigate this.

The vulnerabilities discussed above are mitigated by having the receive antennas as close together as possible. Instead of positioning them at the substation perimeter, they may be positioned within the perimeter or perhaps on the control building. An assessment of the minimum viable receive antenna placement is conducted in Section VII.

The authors' method can operate with a greater number of receive antennas and substation clocks if so desired. With each new receive antenna, the challenge of targeting a unique spoofing signal increases, but so do the costs of the whole system. While two antennas and clocks are sufficient for spoofing detection, the third antenna adds confidence that a spoofing detection is not an equipment error and enables determination of the attackers' position.

VI. Direction and Range of the Attacker

It is possible to determine the direction and range of the attacker by calculation based on the propagation delay times of the attacker's signal between the several GNSS antennas placed

around the substation. Various multilateration techniques may be applied, for example [23]. Such methods allow the attackers 3D position to be determine, provided sufficient receive antennas are available. Assuming the attacker is terrestrial, and thus coplanar with the receive antennas, a simplified approach is possible. This section derives the formulae for determining the attacker's transmitter position using only three arbitrarily placed GNSS antennas, Fig. 5. It is necessary to solve for bearing, range, and time.

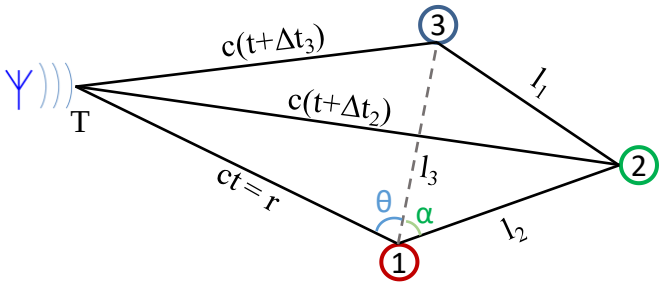

Fig. 5 Signal paths from the attacker's transmitter 'T' to three arbitrarily placed receive antennas, '1', '2', and '3'.

Starting by remembering the Cosine Rule:

$$a^2 = b^2 + c^2 - 2bc\cos A$$

And the Cosine Sum Identity:

$$\cos(x+y) = \cos x \cos y - \sin x \sin y$$

Applying the Cosine Rule to the triangle formed by the attacker's transmitter, antenna 1 and antenna 2 (triangle T12) yields:

$$c^2(t+\Delta t_2)^2 = l_2^2 + c^2t^2 - 2l_2ct\cos(\theta+\alpha)$$

$$t = \frac{l_2^2 - c^2{\Delta t_2}^2}{2c^2\Delta t_2 + 2l_2c\cos(\theta+\alpha)}$$

Applying the Cosine Sum Identity:

$$t = \frac{l_2^2 - c^2{\Delta t_2}^2}{2c^2\Delta t_2 + 2l_2c(\cos\theta\cos\alpha - \sin\theta\sin\alpha)} \quad Eqn.(1)$$

Applying the Cosine Rule to T13 yields:

$$c^2(t+\Delta t_3)^2 = l_3^2 + c^2t^2 - 2l_3ct\cos\theta$$

$$t = \frac{l_3^2 - c^2{\Delta t_3}^2}{2c^2\Delta t_3 + 2l_3c\cos\theta} \quad Eqn.(2)$$

Combining Eqns. (1) and (2):

$$\frac{l_3^2 - c^2{\Delta t_3}^2}{2c^2\Delta t_3 + 2l_3c\cos\theta} = \frac{l_2^2 - c^2{\Delta t_2}^2}{2c^2\Delta t_2 + 2l_2c(\cos\theta\cos\alpha - \sin\theta\sin\alpha)}$$

Assuming that the denominators do not equal zero:

$$\frac{2c^2\Delta t_3 + 2l_3c\cos\theta}{l_3^2 - c^2{\Delta t_3}^2} = \frac{2c^2\Delta t_2 + 2l_2c(\cos\theta\cos\alpha - \sin\theta\sin\alpha)}{l_2^2 - c^2{\Delta t_2}^2}$$

$$\left(\frac{2l_3c}{l_3^2 - c^2{\Delta t_3}^2} - \frac{2l_2c\cos\alpha}{l_2^2 - c^2{\Delta t_2}^2}\right)\cos\theta + \left(\frac{2l_2c\sin\alpha}{l_2^2 - c^2{\Delta t_2}^2}\right)\sin\theta + \left(\frac{2c^2\Delta t_3}{l_3^2 - c^2{\Delta t_3}^2} - \frac{2c^2\Delta t_2}{l_2^2 - c^2{\Delta t_2}^2}\right) = 0$$

Noting that all terms contained in brackets in the above equation are known constants, this can be represented as:

$$A\cos\theta + B\sin\theta - C = 0$$

where:

$$A = \left(\frac{2l_3c}{l_3^2 - c^2{\Delta t_3}^2} - \frac{2l_2c\cos\alpha}{l_2^2 - c^2{\Delta t_2}^2}\right)$$

$$B = \left(\frac{2l_2c\sin\alpha}{l_2^2 - c^2{\Delta t_2}^2}\right)$$

$$C = \left(\frac{2c^2\Delta t_2}{l_2^2 - c^2{\Delta t_2}^2} - \frac{2c^2\Delta t_3}{l_3^2 - c^2{\Delta t_3}^2}\right)$$

This can be manipulated to obtain the bearing θ by:

$$\theta = 2\left(tan^{-1}\left(\frac{B - \sqrt{A^2 + B^2 - C^2}}{A + C}\right) + \pi n\right)$$

$$A + C \neq 0,\ A^2 + AC + B^2 \neq B\sqrt{A^2 + B^2 - C^2}, \text{for } n \in Z$$

If the timing errors can be determined with a suitable degree of uncertainty, then the range r is obtained by:

$$r = c\left(\frac{l_3^2 - c^2{\Delta t_3}^2}{2c^2\Delta t_3 + 2l_3c\cos\theta}\right)$$

VII. GNSS Receiver Position Variance

In this section, the minimum spacing requirements for the GNSS receive antennas for the spoofing detector are determined. A study was conducted to evaluate the variance in estimated position of a number of GNSS receivers. The objective was to determine the distance that the GNSS receiver would deviate from its median position estimation over a long period of time, thus identifying the maximum deviation and other characteristics. As described in [7], a position fix outside of the maximum variance would be regarded as invalid. Since [7] does not include the necessary statistics, it is necessary to experimentally ascertain these characteristics.

In total nine GNSS receivers were studied. Each receiver is connected to a GNSS antenna secured to an external wall with a clear view of the sky. Where possible, the receivers have been configured for static timing applications as this is representative to how substation clock equipment is configured. Position is reported by the receiver at 1 second intervals, and is recorded for a period of 24 hours. A Python script tabulates the recorded latitudes and longitudes in decimal degrees and finds the median value. This median value is taken as the center, considered as the 'true' location, and a table of deviations from this center value is created. The deviation in decimal degrees is converted to meters. The approximation of

TABLE I
UNITS FOR MAGNETIC PROPERTIES

Receiver	A	B	C	D	E	F	G	Clock 1	Clock 2
Year (approx.)	2015	2015	2015	2009	2009	2005	1994	2014	2006
Price (approx. USD)	$90	$90	$90	$20	$20	$100	n/a	>$1000	>$1000
GNSS	Multi (3)	Multi (3)	Multi (3)	GPS	GPS	GPS	GPS	Multi (2)	GPS
Channels	72	72	72	50	50	12	8	16	12
SBAS	Yes	Yes	Yes	Yes	Yes	Yes	*No*	Yes	*No*
Deviation									
Max (m)	3.10	3.97	4.88	10.45	7.07	8.02	179.86	6.52	126.10
R99.7 (m)	2.95	3.11	3.78	8.35	5.72	7.88	167.58	6.23	95.67
R95 (m)	2.11	2.10	2.39	5.50	4.87	6.80	57.90	4.29	52.03
DRMS (m)	1.15	1.15	1.30	3.29	2.91	4.02	29.84	1.75	22.91
Median (m)	0.89	0.89	1.00	2.44	2.07	3.65	14.99	0.00	8.56
Standard Dev (m)	0.59	0.58	0.66	1.74	1.61	1.47	21.30	1.53	17.05

Receivers A through F represent chipsets or OEM units designed for integration into systems. Receiver G is a popular early model GPS receiver for marine uses (no longer available). Clock 1 and Clock 2 are products sold for use as 'substation clocks'. 'R95' is the radius within which 95% of values lie, based on distance from the normalized location. 'DRMS' is the distance root-mean-square of the whole set.

'SBAS' – Satellite Based Augmentation System, improves position accuracy (sometimes known as Differential GNSS). 'Multi (2)' allows GPS and GLONASS simultaneously. 'Multi (3)' allows GPS and Galileo, and one of either GLONASS or BeiDou, to be received simultaneously. In this case GPS, GLONASS and Galileo are used.

1° = 111,120 m is applied to the latitude. Longitude is adjusted by the cosine of the latitude, in this case 54°N, yielding 65,315 m. Fig. 6 charts the deviation from median observed for Receiver B.

There are numerous methods and statistics for characterizing GNSS position variance [28], [29]. In addition to maximum deviation, it is usual to also consider the Circular Error Probable (CEP) and the Distance Root Mean Square (DRMS). Two CEPs are considered, R99.7 and R95. R99.7 indicates the radius within which 99.7% of all position estimates lie. Likewise, R95 indicates the radius in which 95% of position estimates lie. DRMS determines the RMS of the magnitude of the full set of location deviations.

The results for the nine GNSS receivers are presented in Table 1. Receivers A through F are OEM style chips or devices intended for integration into systems. Clock 1 and Clock 2 are 'substation clock' products for the electrical utility market. Receiver G is an early model GPS receiver popular in marine applications; it is no longer available to purchase but serves for comparison. The OEM receivers are all sub $100; this indicates low volume pricing offered by the vendors' websites and is similar to retail pricing at the time of writing. The substation clocks are considerably more expensive, but are complete systems ready for integration with substation equipment. The year given represents the first date, often the first firmware release, which the authors identified on the equipment vendors' websites for that model. All receivers stream position via serial NMEA sentences at an update rate of once per second, with the exception of Clock 1 which instead provides location information via Simple Network Management Protocol (SNMP). Clock 1 is therefore polled for position information once per second.

Some receivers can observe multiple GNSS constellations concurrently. Channels indicate the maximum number of channels the receiver has available to track GNSS satellites and for activities such as signal-to-noise ratio (SNR) estimation; fewer satellites may be in view in the sky at a given time. Most of the receivers support Satellite Based Augmentation Systems (SBAS). These are differential GNSS (DGNSS) services which help with position estimation by transmitting correction information related to common sources of error in GNSS signals. The error corrections are calculated by ground stations and sent to GNSS receivers by geostationary satellites. In North America, SBAS service is provided by the Wide Area Augmentation Service 'WAAS'. Since the authors are located in Europe, the European Geostationary Navigation Overlay Service (EGNOS) is used.

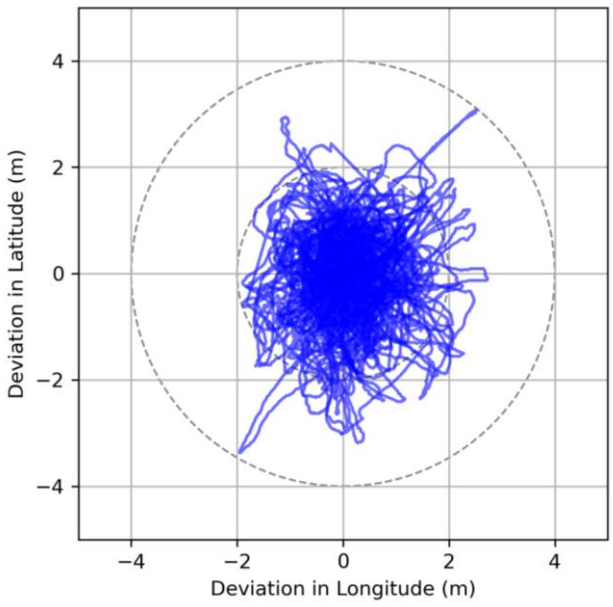

Fig. 6 Deviation in position reported by a stationary GNSS receiver, Receiver B from Table 1. The outer circle has a radium of 4 m.

The data in Table 1 shows that the modern chipsets, A, B, C, achieved maximum deviations of less than 4.88 m. If two such receivers of these types were placed 10 m apart, for example, then their position estimates will not overlap. This validates the application of these chips for use in the spoofing detector described in Section V. As evidenced by Fig. 6, the maximum

deviations are outliers. The R99.7 for these receives is < 4 m.

The slightly older receivers, D, E, F, exhibit a greater variation in position estimation, with a maximum of 10.45 m observed on receiver D. Although the R99.7 and R95 are somewhat lower, these receivers would require a larger antenna spatial separation to be used in the spoofing detection method. Clock 1 performed less well than receivers A, B, C but better than D, E, F. It should be noted that Clock 1 does not appear to be intended for use reporting position; there is no convenient way to obtain this data other than via SNMP. The clock is likely operating in a 'survey-in' or 'fixed position' mode. Regardless, its variation is acceptable and could be used for spoofing detection with antennas placed 14 m apart.

Clock 2 did not perform adequately for use in the spoofing detection method, exhibiting a rather large maximum deviation of over 126 m. This is comparable to receiver G. Note that neither Clock 2 nor receiver G supports SBAS. This would appear to be a necessary requirement to yield suitable position estimation performance. SBAS appears to be common on GNSS chipsets starting from circa 2005, so this is not anticipated to be a problem for new equipment.

A brief survey of local substations show their control buildings are of dimensions 12 x 16 m or greater, and thus Clock 1 could be applied to antennas placed in a triangular formation on these buildings' roof tops.

VIII. Implementation & Validation

A prototype of the authors' detector has been implemented using three development kits using the 'u-blox LEA-M8T' GNSS receiver chip. The receivers have been configured to provide position information via RS232 using the 'GPGGA' NMEA sentence at a rate of one report per second, and a 1PPS time pulse. The RS232 outputs of the receivers are connected to a Raspberry Pi 4 single-board computer via USB adapters. The 1PPS signals have been connected to a Keysight DSOX2024A oscilloscope which measures the interval between time pulse arrivals and sends this data to the computer by USB connection. The setup is described in Fig. 7. The antennas of the three detectors are spatially separated, each 12 meters from its neighbors. The receivers are located on a bench with the computer and the oscilloscope. The antenna cable lengths are compensated for in the GNSS receiver firmware, thus the time pulses are coherent in normal operation.

The single board computer is operating a Python script which observes the reported positions (p) of each GNSS receiver (R). A 'geofence', which is a virtual circular perimeter, of radius 5 meters is created about the 'normal' reported position of each receiver. The 'normal' position in this prototype is the median position, but can be changed to a fixed latitude and longitude.

In the event that one or more GNSS receiver reports a position outside of its geofence, then a 'warning' level event is flagged. If a GNSS receiver reports a position inside the geofence of another GNSS receiver, an 'alarm' level event is flagged. Warnings and alarms can be output as a Boolean logic level signal, or as an IEC 61850 GOOSE message over Ethernet. This makes the detector output flexible to integrate with existing substation designs.

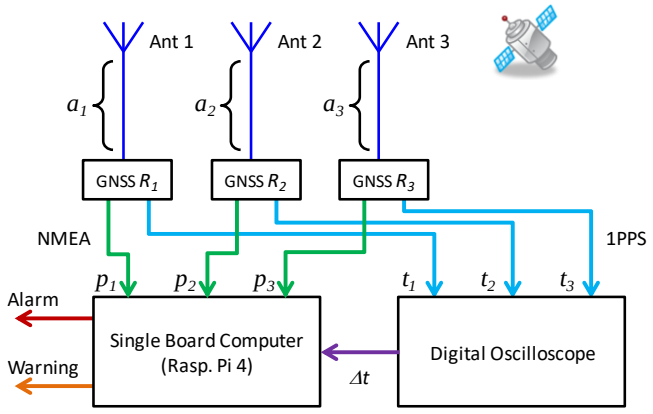

Fig. 7 Configuration of the authors' prototype detector. Cable lengths a_1, a_2, a_3 are compensated for by receivers R_1, R_2, R_3, such that in normal operation time pulses t_1, t_2, t_3 are coherent. Positions p_1, p_2, p_3 are serial messages.

Validation of Position Based Method

Since it is not legal to transmit GNSS signals, it is not legally possible to validate this system using a spoofing signal. However, the effect of a spoofing signal can be achieved by splitting the signal from one GNSS antenna to two or more receivers. Additional lengths of cable can be inserted to mimic the propagation delay.

The authors have used a coaxial cable switch to near instantaneously switch R_2 from its correct antenna to the 'spoofed' signal (antenna R_1), it was found that the reported position would leave the receiver's geofence after 2 to 3 seconds (warning state), and enter the geofence of the 'spoofed' location between 5 to 10 seconds after the 'attack' starts (alarm state).

Although initial inspection of the above results indicate that there is a non-detection period of up-to 10 seconds, during which time sensitive applications are susceptible to spoofing attack, in practice the slew rate of substation clocks and GNSS time solutions mitigate against this. Setting the slew rate to 1 µs/s, for example, presents a worst case time error of 10 µs before the spoofing attack is alarmed. In the case of a PMU, this represents a phase angle error of 0.2°, which remains within specification (< 0.57°) [30]. After the attack is alarmed, substation equipment may switch to holdover mode, or a dedicate hold-over clock could be employed.

A. *Validation of Timing Based Method*

As before, for legal reasons the effect on the 1PPS pulses must be studied in a bench top experiment. As with the position based method, a switch is used to swap the antenna feed of GNSS R_2 from its own antenna to that of GNSS R_1, this time with an additional 20 meter length of coaxial cable.

In normal operation, with each receiver fed by its own antenna, a mean time error of 10.3 ns is observed in the 1PPS pulses, with a standard deviation of 11.5 ns. This is well within specification for the GNSS receiver, which suggests 50 ns accuracy for the time pulse. With the addition of the 20 m of extra cable, the mean error increased to 105 ns while the standard deviation remained the same. This is in line with expectations of the propagation delay in the cable. The effect

on the time pulse manifests in approximately 3 to 10 seconds after the 'attack' commences, similar to the position method.

B. Proposed Substation Implementation

The proof-of-concept validation in this section made use of the standard NMEA sentence 'GPGGA' and a 1PPS signal. Both of these signals are readily available from standard substation clocks from established equipment vendors. The computer needed to operate the authors' detector software requires no special interfaces other than common USB and Ethernet ports, so hardened industrial 'substation' computers may be used. In the event that spoofing is detected, the detector software can command substation equipment switch to a suitable holdover clock based on TCXO or atomic oscillator, enabling holdover at ~1 µs for 24 hours [31]. Holdover would be transparent to time sensitive applications, causing no interruptions in substation operations.

Suitable substation GNSS clocks are available at circa $3k each, and substation computers at circa $3k. These costs are considered affordable in the context of most large substations. An equipment vendor could make an integrated solution at a fraction of these costs using the chipsets discussed in Table I.

IX. Conclusions

This paper has introduced a new method of GPS spoofing detection which may be implemented using familiar substation equipment. Where other methods rely on sophisticated baseband methods, the new method takes advantage of the spatial area of an electricity substation to place multiple GNSS receive antennas for spoofing detection. It was found by experiment that antenna separation of 14 m is required for a substation clock under test, but that modern GNSS chipsets could be used in the authors' method with 10 m antenna separation. Mathematical formulae are presented allowing the bearing and ranger of an attacker to be determined.

A prototype detector is validated to be effective in a bench top study. The detector can determine a spoofing attack in as little as 3 to 10 seconds. If the slew rate of the substation master clock can be set, such an attack has negligible impact in this timeframe before the alarm is issued and holdover action is taken. Future work will focus on developing a means to empirically quantify the success rate of spoofing detection, and also false alarm and misdetection events.

Through making use of conventional substation GNSS clocks, the cost of the authors' method is affordable in the context of large substations. More importantly, such clocks are already qualified for substation use, making this method suitable for practical deployment.

References

[1] D. Ingram, D. Smellie, "*White Paper on Implementing PTP in Substations*," Digital Substation, Nov 08, 2016 [Online] http://digitalsubstation.com/en/2016/11/08/white-paper-on-implementing-ptp-in-substations/ [Accessed: May 05 2020]

[2] M. S. Almas, L. Vanfretti, R. S. Singh and G. M. Jonsdottir, "Vulnerability of Synchrophasor-Based WAMPAC Applications' to Time Synchronization Spoofing," in *IEEE Transactions on Smart Grid*, vol. 9, no. 5, pp. 4601-4612, Sept. 2018

[3] X. Fan, L. Du and D. Duan, "Synchrophasor Data Correction Under GPS Spoofing Attack: A State Estimation-Based Approach," in IEEE Transactions on Smart Grid, vol. 9, no. 5, pp. 4538-4546, Sept. 2018

[4] J.S. Warner and R.G. Johnston, "GPS Spoofing Countermeasures," Tech. Report LAUR-03-6163, Los Alamos National Laboratory, 2003 [Online] http://lewisperdue.com/DieByWire/GPS-Vulnerability-LosAlamos.pdf [Accessed May 05 2020]

[5] D. Borio, F. Dovis, H. Kuusniemi and L. Lo Presti, "*Impact and Detection of GNSS Jammers on Consumer Grade Satellite Navigation Receivers*," in Proceedings of the IEEE, vol. 104, no. 6, pp. 1233-1245, June 2016

[6] Joint Warrior 191 Brief for Fishing Vessels and Ferries, Royal Navy, UK, 14th March 2019

[7] K. Fodero, C. Huntley, P. Robertson, "Secure and Reliable GPS-Based Time Distribution," in *Wide-Area Protection and Control Systems: A Collection of Technical Papers Representing Modern Solutions*, SEL Inc., March 2017

[8] "Tempus Project: A time synchronization platform to protect energy delivery systems from GPS-based attacks", US Dept. of Energy, March 2017, [Online] https://www.energy.gov/sites/prod/files/2017/06/f34/SEL_Tempus_FactSheet.pdf [Accessed: May 21 2021]

[9] K. Zeng, et al, "*All Your GPS Are Belong To Us: Towards Stealthy Manipulation of Road Navigation Systems*," USENIX Security Symposium, 2018

[10] T. Ebinuma, "GPS-SDR-SIM", Github, [Online] https://github.com/osqzss/gps-sdr-sim [Accessed: May 23 2021]

[11] D.P. Shepard, T.E. Humphreys, and A.Fansler, "Going Up Against Time," *GPS World*, August, 2012 [Online] radionavlab.ae.utexas.edu/index.php?option=com_content&view=article&id=275:going-up-against-time&catid=30&Itemid=37 [Accessed May 23 2021]

[12] Q. Meng, L.T. Hsu, B. Xu, X. Luo, A. El-Mowafy.; "A GPS Spoofing Generator Using an Open Sourced Vector Tracking-Based Receiver," in *Sensors*, vol 19, pp. 3993, 2019

[13] S. Bhamidipati, K. J. Kim, H. Sun and P. V. Orlik, "GPS Spoofing Detection and Mitigation in PMUs using Distributed Multiple Directional Antennas," *IEEE International Conference on Communications (ICC)*, Shanghai, China, 2019

[14] M. Schmandt, "*An Introductory Textbook on Geographic Information Systems*", GIS Commons [Online] https://giscommons.org/chapter-2-input/ [Accessed: May 05 2020]

[15] GIS Geography, "GPS Accuracy: HDOP, PDOP, GDOP, Multipath & the Atmosphere",[Online] https://gisgeography.com/gps-accuracy-hdop-pdop-gdop-multipath/ [Accessed: May 05 2020]

[16] "IEEE/IEC International Standard - Measuring relays and protection equipment - Part 118-1: Synchrophasor for power systems - Measurements," in *IEC/IEEE 60255-118-1:2018* , 19 Dec. 2018

[17] R. Charette, "*Will GPS Jamming Cause Future Shipping Accidents?*," IEEE Spectrum, 22 Feb, 2012

[18] D. Goodin, "*A $225 GPS spoofer can send sat-nav-guided vehicles into oncoming traffic*," Ars Technica, 18 July, 2018

[19] M. Pattinson; "STRIKE3: Outcomes of Long Term Monitoring of GNSS Threats and Receiver Testing," 12th Annual Baška GNSS Conference, Baška, Krk Island, Croatia, 06.-09. May 2018

[20] M.L. Psiaki, T.E. Humphreys, "*Protecting GPS From Spoofers Is Critical to the Future of Navigation*," *IEEE Spectrum*, 29 July, 2016

[21] European GSA, "Galileo Commercial Service Implementing Decision enters into force," [Online] https://www.gsa.europa.eu/newsroom/news/galileo-commercial-service-implementing-decision-enters-force [Accessed: May 05 2020]

[22] S. Bhamidipati, K. J. Kim, H. Sun and P. V. Orlik, "GPS Spoofing Detection and Mitigation in PMUs using Distributed Multiple Directional Antennas," *ICC 2019 - 2019 IEEE International Conference on Communications (ICC)*, Shanghai, China, 2019, pp. 1-7, doi: 10.1109/ICC.2019.8761208.

[23] D.Y. Yu, A. Ranganathan, T. Locher, S. Capkun, D. Basin; "Short paper: Detection of GPS spoofing attacks in power grids," in *Proceedings of the 2014 ACM Conference on Security and privacy in wireless & mobile networks*, pp. 99-104, 23 Jul 2014

[24] S. Bhamidipati and G. X. Gao, "GPS Multireceiver Joint Direct Time Estimation and Spoofer Localization," in *IEEE Transactions on Aerospace and Electronic Systems*, vol. 55, no. 4, pp. 1907-1919, Aug. 2019

[25] A. Khalajmehrabadi, N. Gatsis, D. Akopian and A. F. Taha, "Real-Time Rejection and Mitigation of Time Synchronization Attacks on the Global

Positioning System," in *IEEE Transactions on Industrial Electronics*, vol. 65, no. 8, pp. 6425-6435, Aug. 2018
[26] J. Zidan, E. I. Adegoke, E. Kampert, S. A. Birrell, C. R. Ford and M. D. Higgins, "GNSS Vulnerabilities and Existing Solutions: A Review of the Literature," in *IEEE Access*, 2020, doi: 10.1109/ACCESS.2020.2973759.
[27] A. Jafarnia-Jahromi, A. Broumandan, J. Nielsen, G. Lachapelle; "GPS Vulnerability to Spoofing Threats and a Review of Antispoofing Techniques," in *International Journal of Navigation and Observation*, Hindawi, April 2012
[28] Heng, L., Gao, G.X., Walter, T., Enge, P., "Statistical Characterization of GPS Signal-In-Space Errors," *Proceedings of the 2011 International Technical Meeting of The Institute of Navigation*, San Diego, CA, January 2011, pp. 312-319.
[29] Ranacher, Peter & Brunauer, Richard & Trutschnig, Wolfgang & van der SPEK, Stefan & Reich, Siegfried. "Why GPS makes distances bigger than they are." *International Journal of Geographical Information Science*. 30. 1-18, 2015
[30] "IEEE/IEC International Standard - Measuring relays and protection equipment - Part 118-1: Synchrophasor for power systems - Measurements," in *IEC/IEEE 60255-118-1:2018*, pp.1-78, 19 Dec. 2018
[31] W. Krzewirk, "Chip Scale Atomic Clocks: Effects on Timing Error," Microsemi Corp., 2018 [Online] https://www.microsemi.com/blog/2018/10/05/ [Accessed: June 7 2021]

David M. Laverty (M'10-SM'17) was born in Belfast, Northern Ireland, in 1984. He received the M.Eng and Ph.D. degrees from Queen's University Belfast, UK, in 2006 and 2010 respectively.

He is currently a Reader with the Energy, Power and Intelligent Control (EPIC) Cluster at Queen's University Belfast, with research interests in anti-islanding detection, telecommunications, cyber-security and synchrophasor measurement.

Dr. Laverty is a Senior Member of the IEEE and an Associate Editor for the IEEE OAJPE.

Colin Kelsey was born in 1987 in Newry, Northern Ireland. He received his BSc in Applied Mathematics and Physics, MSc in Plasma Physics and Ph.D. in Plasma Physics from Queens University Belfast in 2009, 2010 and 2014 respectively.

At the time of submission he was working as a Design Engineer at the Biodevices Laboratory in the Nanotechnology and Integrated Bioengineering Centre (NIBEC) at Ulster University, Jordanstown. His research interests include multiphysics modelling and experimental imaging applied to the development and characterization of biomedical devices.

John B. O'Raw (M'07) was born in London, England in 1965. He obtained his PhD degree from Queen's University Belfast, Belfast, UK, in 2020. He is currently lecturing at Letterkenny Institute of Technology, Ireland. Prior to this he worked as a public service IT Manager (1996-2010) and in various roles with ABB specializing in large scale process automation and information systems (1988-1996).