IET Generation, Transmission & Distribution

Review Article

Review on GPS spoofing-based time synchronisation attack on power system

ISSN 1751-8687
Received on 7th February 2020
Revised 26th June 2020
Accepted on 6th July 2020
E-First on 4th September 2020
doi: 10.1049/iet-gtd.2020.0253
www.ietdl.org

Heng Zhang[1], *Shurong Peng*[1] ✉, *Liang Liu*[1], *Sheng Su*[1], *Yijia Cao*[1]

[1]*School of Electrical & Information Engineering, Changsha University of Science and Technology, 410114, People's Republic of China*

✉ *E-mail: 173764138@qq.com*

Abstract: Power utilities implement cyber-security defence with a philosophy of defence in-depth. Firewall and air-gapped systems are widely used to harden cybersecurity defence of critical power system infrastructure. However, cyber-attack, such as global positioning system (GPS) spoofing, that can compromise the air-gap system has not been investigated thoroughly. As a geographically dispersed cyber-physical system, the power system relies heavily on the GPS to keep time synchronisation of different parts with high precision. GPS spoofing-based time synchronisation attack (TSA) could induce disorder in time synchronisation, and negatively impact or even disable monitoring and control function of the power system via their operation mechanism. The principles of GPS-based time synchronisation and GPS spoofing-based TSA are introduced. Time synchronisation and operation mechanism of typical monitoring and control systems of the power systems are analysed. Thereafter, the consequences of TSA against these systems are analysed. Various techniques that can be used to defend against TSA are depicted and their performances are analysed.

1 Introduction

Unlike the traditional power system that distributes electricity from power plants to the end consumers in one direction, the smart grid provides two-way electricity flow and data communication. Since numerous participants, including users, distributed generation systems, and electric vehicles, can be incorporated via communication, the efficiency, reliability, and resiliency of power systems can be enhanced notably. The other edge of the sword is that participants of the smart grid are exposed to malicious cyber-attack [1]. To keep data integrity and confidentiality of users, various authentication and data encryption schemes have been developed [2, 3]. However, as a close-coupled cyber-physical power system (CPPS), the consequence of cyber-attack on power systems is notable different from that of the average information system. While a traditional cyber-attack may leak users' personal sensitive information [4, 5], a CPPS attack could lead to a loss of control in generators and outages of several substations [6], placing the nation's security and public safety at risk.

Currently, cybersecurity is widely accepted as one of the vital issues in power systems. A tremendous number of efforts have been put into the research of cybersecurity of CPPS. The firewalls are widely adopted for access control in power utilities against intruders [7]. Intrusion detection systems that incorporate the operation mechanism of a substation automation system (SAS) have been developed in [8, 9] to detect network activity anomaly caused by malicious intruders. However, all these are reactive countermeasures and they cannot deal with next-generation unknown threats. Trusted computing has been proposed to harden cybersecurity defence of embedded terminal for industrial applications [10]. Since only the authorised software can operate, it enforces specific behaviours and protects the system against unauthorised changes and attacks such as malware and root kits. As a proactive security approach, it can defend against unknown malware. For the critical part of the CPPS, an air-gapped system is used to harden cybersecurity defence according to the philosophy of defence in-depth.

The global positioning system (GPS) can provide positioning, navigation, and timing services. Since civil GPS signals are transmitted as unencrypted plaintext, it is vulnerable to GPS spoofing attacks [11]. Once malicious adversary broadcast fraud GPS signals at high power, a GPS receiver (RX) nearby could output error location or time signal that carries the potential for devastating consequences. GPS spoofing do occur in the real world. In 2011, Iran successfully captured US military drones through the global navigation satellite system (GNSS) spoofing [12]. In 2017, a GPS spoofing attack caused 20 ships around the Black Sea to be positioned incorrectly [13]. Since GPS spoofing is a non-invasive attack that does not intrude into a communication network of power utilities, it can bypass most existing security technologies and cause destructive consequences in air-gapped CPPS [14]. Therefore, the sabotage mechanism of GPS spoofing attack on CPPS and the way to defend against it is highly preferred.

The power system is a geographically dispersed cyber-physical system (CPS). Monitoring and control systems in the power plants, transmission systems, distribution systems, control centres, and user side should operate with precise time synchronisation. GPS is widely employed to maintain high-precision time synchronisation of the power industry and it plays a fundamental role to facilitate the security and stability of power system [11]. GPS spoofing-based time synchronisation attack (TSA) could induce disorder in time synchronisation, and negatively impact or even disable monitoring and control function.

The GPS spoofing-based TSA is reviewed in this paper. The remainder of the paper is organised as follows. The GPS-based time synchronisation and GPS spoofing-based TSA are introduced in Section 2. Based on the analysis of the operation mechanism of specific monitoring and control systems, GPS spoofing-based TSA's on various hierarchical synchronised and distributed synchronised systems are analysed in Section 3. The ways to defend against GPS spoofing-based TSA are reviewed in Section 4 and Section 5 concludes the paper.

2 GPS and GPS spoofing-based TSA

2.1 GPS-based time synchronisation

GPS satellites broadcast radio signals providing their locations, status, and precise time from on-board atomic clocks. The GPS radio signals travel through space at the speed of light. A GPS device receives the radio signals, noting their exact time of arrival, and uses these to calculate its distance from each satellite in view. Once a GPS device knows its distance from at least four satellites, it can determine the precise time and its location on Earth in three

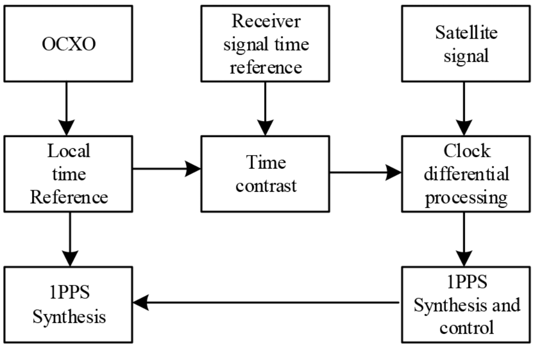

OCXO
Receiver signal time reference
Satellite signal
Local time Reference
Time contrast
Clock differential processing
1PPS Synthesis
1PPS Synthesis and control

Fig. 1 *Schematic diagram of timing module of TSD*

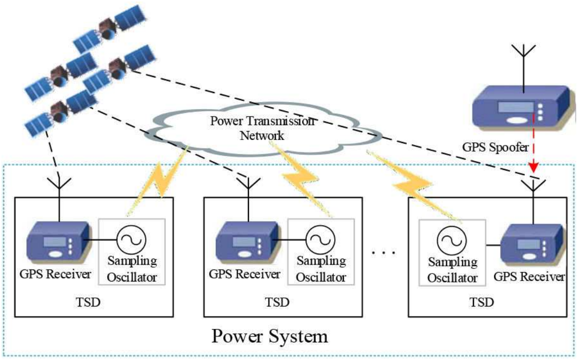


Fig. 2 *Time synchronised in power system with GPS spoofer*

dimensions. A detailed way to calculate location and time is depicted in [15, 16].

GPS is widely employed for time synchronisation in power utilities. The time synchronise device (TSD) with a GPS-based timing module is used to produce accurate time reference. There is a TSD in almost every power plant, substation, and all control centres and head ends of most monitoring and control systems.

The schematic diagram to produce the time reference is shown in Fig. 1. Satellite time reference is used as the main clock source in TSD, while the oven-controlled crystal oscillator (OCXO) based local clock source is used as the time reference when the satellite signals are not available [11]. The GPS RX de-modulate the satellite navigation signal to obtain the data code containing positioning and timing information including time, satellite orbit, and ionospheric delay. It compares the satellite time reference with the OCXO-based local time reference to obtain the result of the pseudo-range measurement. Thereafter, the clock error between the local time reference and the satellite time reference can be estimated according to local coordinates, satellite signals, relevant ionospheric/tropospheric correction parameters, and RX time delay calibration information [16]. Thereafter, the TSD syntheses and outputs the 1 pulse per second (1PPS) signal as time reference [11].

2.2 GPS spoofing-based TSA

Traditionally, TSDs used in power utilities are designed to implement the function of time synchronisation with high reliability and precision. However, the way to defend against TSA is not considered. Since the TSD used in power systems communicate with unencrypted plaintext civil code, malicious adversaries could launch the GPS spoofing-based TSA in the neighbourhood of a victim GPS RX and compel the TSD to output time reference with deviation. It is not so difficult to launch a TSA as expected. In [15], a low-cost software-defined controller-based GPS simulator with hardware of 500 USD is developed and the related documents are posted to GitHub, a publicly-accessible online software repository. With the help of the GPS simulator, average people without professional knowledge can launch GPS spoofing-based cyber-attack by broadcasting fabricated GPS signals with a few function calls [15]. The GPS spoofing-based TSA can be illustrated with Fig. 2.

GPS spoofing should mislead a GPS RX to acquire the fraud GPS signal instead of the legitimate one. Since the acquisition is implemented by searching for the highest correlation peak in the code-phase-carrier-frequency (CPCF) two-dimensional space, the signal with higher signal-to-noise- ratio (SNR) will have a higher correlation peak. Therefore, spoofing can be implemented in two steps. Firstly, the spoofer launches interference which causes the GPS RX to lose track. Thereafter, it broadcasts a fraud GPS signal when the GPS RX carries out the acquisition processing. Consequently, the GPS RX will track the fraud signal for its higher SNR and correlation peak [17, 18].

The attacker can scan the two-dimensional space of CPCF till the fake correlation peak overlaps the legitimate one as shown in Fig. 3. Firstly, the attacker launches the fraud correlation peak close to the legitimate one and moves slowly towards the legitimate one. Thereafter, the fraud correlation peak moves to the position in which it overlaps the legitimate one. The GPS RX will be captured by and locked to the fraud signal since it has a higher SNR. In the end, the attacker can move the fake correlation peak slowly to the desired point and the legitimate signal will be considered as noise.

Jamming of GPS signals can be divided into two categories: jamming suppression and deception jamming. The jamming suppression is to broadcast a jamming signal at high power to make the victim RX cannot receive the legitimate signal [19]. The jamming suppression-based TSA is relatively simple and the RX can identify jamming suppression with adaptive filtering or spatial filtering technology [20, 21]. The deception jamming can be divided into generation-based spoofing and forwarding spoofing (record legitimate satellite signals and replay it with high power [20]). It is much more difficult to detect and prevent deception jamming-based GPS spoofing. Several kinds of deception jamming are analysed as follows:

- Meaconing is a forwarding spoofing. It captures and retransmits legitimate GPS signals with a delay [20].
- Security code estimation and replay (SCER) is a variation of meaconing [22]. According to [23], spread spectrum codes can be employed to make some segments of navigation signal unpredictable and improves the security of civil satellite signal-based time synchronisation. However, SCER can achieve spoofing of this satellite signal. It involves the rebroadcast of individual satellite signals after a delay. The spoofer estimates the unpredictable $D_i(t)$ bits, and it broadcasts them as soon as it has reliable estimates.
- The open-loop signal simulator simulates the generation of satellite navigation signals received by users in various real environments. They do this by synthesising their false code phases in a way that induces the false position/timing fix at the victim RX while maintaining small pseudo-range residuals [21].
- RX-spoofer captures the victim RX tracking loops and transmits the fraud signals so that they are code phase and Doppler-matched to the legitimate signals at the location of the victim antenna [24].
- Nulling. The spoofer transmits two signals for each spoofed signal. One is spoofing signals, which work together with other spoofing signals to cause position or clock deviation. Another signal is used to eliminate the traces of real signals and delete all traces of repeated signals [25].

A combination of the aforementioned spoofing methods could compel TSD to output the wrong time reference. The deception jamming-based GPS spoofing is listed in Table 1. It can be observed that almost all the deception jamming-based GPS spoofing is a variation or combination of aforementioned spoofing techniques. The first several approaches can be implemented easily with off-the-shelf tools. Since more attacking hardware is involved and expertise is required to run attacking hardware with high complexity, the latter approaches are much more difficult.

Traditionally, the GPS signal is supposed to be legitimate and the TSD is designed to operate with high reliability and precision for several hours without GPS signal. Once the GPS RX loses track, the local time reference maintained by a high-precision

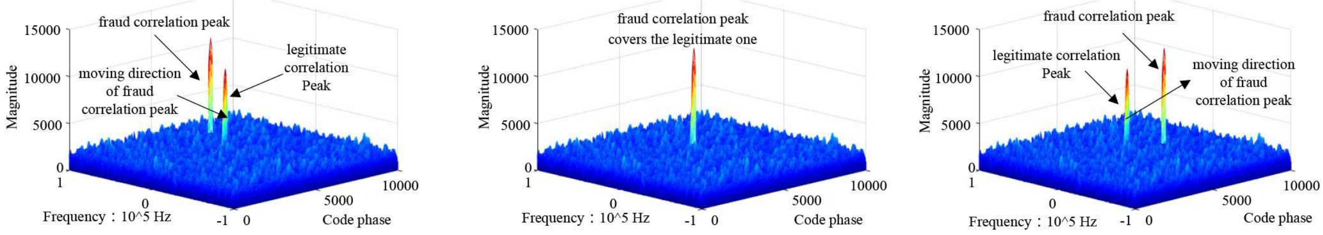


Fig. 3 *Process of tricking power TSD to capture decoy signals*

Table 1 Common attack techniques

No.	Attack techniques key
A1	meaconing, single RX ant., single transmitter (TX) ant.—the capture and retransmission of legitimate GNSS signals after a delay [20]
A2	open-loop signal simulator—simulate the generation of satellite navigation signals received by users in various real environments [21]
A3	RX-spoofer, single TX ant., no SCER—according to the parameters of real satellite signals obtained by the RX, spoofing signals are generated [24], and the single antenna transmits signals
A4	RX-spoofer, single TX ant., SCER—combine SCER on A3 basis
A5	meaconing, multi. RX ants., single TX ant.—on the basis of A1, multiple antennas are used to receive satellite signals
A6	nulling RX-spoofer, single TX ant., no SCER—two kinds of spoofing signals are emitted on the basis of A3. One is spoofing signals, which work together with other spoofing signals to cause position or clock deviation. Another kind of signal is used to eliminate the traces of real signals and delete all traces of repeated signals.
A7	nulling RX-spoofer, single TX ant., SCER—combine SCER on A6 basis
A8	RX-spoofer, single TX ant., sensing of victim ant. motion—combine sensing of victim ant. motion on A3 basis [26]
A9	RX-spoofer, multi. TX ants., no SCER—multiple antennas are used to transmit signals on the basis of A3
A10	RX-spoofer, multi. TX ants., SCER—combine SCER on A9 basis
A11	meaconing, multi. RX ants., multi. TX ants.—multiple antennas are used to transmit and receive signals based on A1
A12	nulling RX-spoofer, multi. TX ants., no SCER—multi-antenna transmit signal based on A6
A13	nulling RX-spoofer, multi. TX ants., SCER—combine SCER on A12 basis

OCXO is output as a time reference. In this way, TSD can output time reference with high precision even though it loses GPS signal for several hours. However, once the GPS RX of TSD suffers GPS spoofing-based TSA, it could output the wrong time estimated according to the spoofed GPS signal or signal with an error. Such incidences do occur occasionally in real-world due to error in GPS signal. For example, television station broadcasts programmes automatically at a predefined time. However, it could broadcast the wrong programme due to time jitters of the TSD. Although a similar thing occurs in the power system too, its impact is not as evident as that in a television station. Since GPS spoofing-based TSA could be accompanied by notable time jitter, power utilities in China regulate that the time jitter of the TSD should be verified with the OCXO-based local time reference. Once there is a time jitter above 1 μs/s between the time reference of the GPS signal and local time reference, the GPS signal is supposed to be abnormal and the local time reference is output as a time reference. However, it cannot identify sustained TSA with slim time jitter below 1 μs/s. Therefore, the ways to verify the genuineness of the GPS signal is highly preferred.

3 Impact of TSA on power systems

As a geographically dispersed CPS, the power system relies heavily on the GPS to keep time synchronisation of different parts. Disorder in time synchronisation caused power systems outages do occur in the real world. For example, the control centre of power utilities implements automatic generation control with a predefined generation plan and adjusts generation according to the state of the system. On 24 January 2013, the Control Center of Sichuan Province in China executed a generation plan of a wrong date due to time jitter of the TSD, which caused the abnormal shutdown of several hydro turbines in Ertan and Waterfall hydro-power plants. Although this accident may not be caused by GPS spoofing-based TSA, it does uncover the potential of TSA on power systems.

Time synchronisation is fundamental to almost all of the monitoring and control systems in the power industry and they are vulnerable to GPS spoofing-based TSA [27]. The TSA's potential impacts on generation, transmission, and distribution, and utilisation of power system can be illustrated as in Fig. 4.

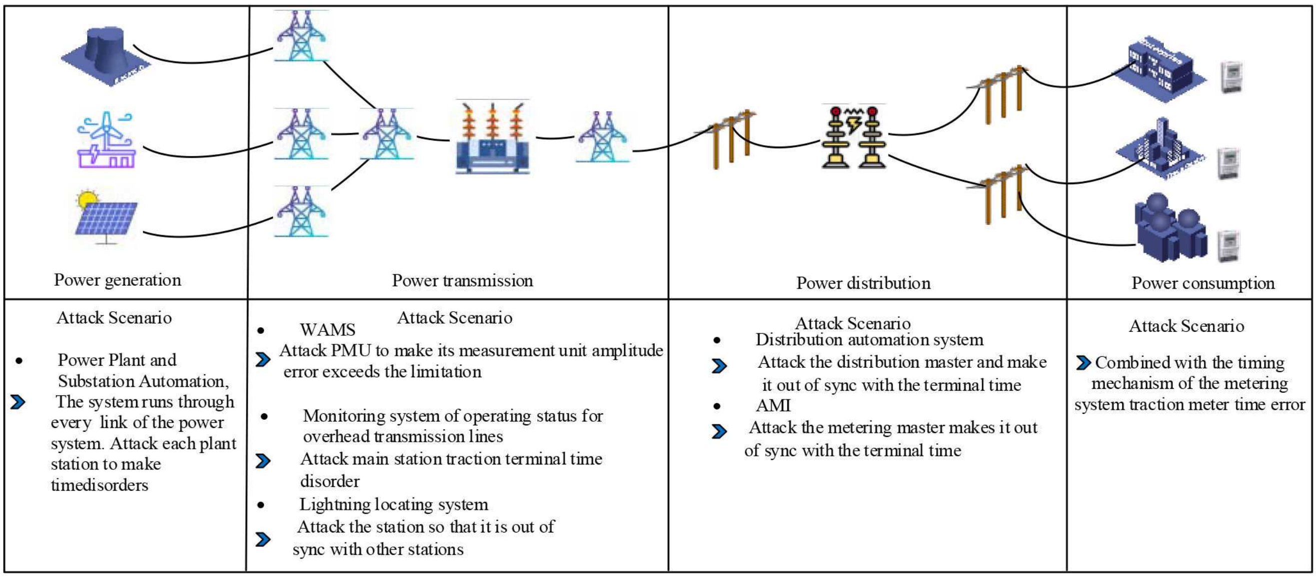
The monitoring and control systems of power industry adopt hierarchical time synchronisation or distributed time synchronisation according to the distribution of system components. Their difference is listed in Table 2.

- The hierarchical synchronised system, including advanced metering infrastructure (AMI), distribution automation system (DAS), condition monitoring system of the overhead conductor etc. There are numerous onsite terminal units and the TSDs are deployed in the head end of the master station. Terminal units require a time precision of second-order and they are synchronised to the head end.
- Distributed synchronized system, including wide-area measurement system (WAMS), lightning location system (LLS), SAS etc. Since TSDs are deployed in almost every substation, power plant, and control centre, system components can be synchronised to the local TSDs. They require a stringent time precision, usually at a millisecond order or higher.

3.1 TSA in a hierarchical synchronised system

• *TSA's impact on DAS*: TSD is deployed at the head end of DAS for wide-area time synchronisation. The onsite terminal units dispersed around the user side are synchronised regularly to the TSD in the head end [27]. Therefore, the time deviation between terminal units and the head end can be limited within a given threshold, usually 3–5 s [11].

Since DAS is a wide-area distributed system, its terminal units could communicate with the head end with large latency, which could result in personal safety accidents of field crews. For example, when a feeder fall outage and field crews work on the isolated feeder section, a closing command issued sometime before to the associated circuit breaker could power the isolated feeder section and cause damage to associated field crews. To avoid such an accident, a latency of 10-s is usually set to verify the validity of a control command. The remote control command issued by the head end is attached with a time stamp. Once field terminals receive a control command, it compares the time deviation of the time stamp to local time. If the time deviation exceeds 10-s, it will



Power generation	Power transmission	Power distribution	Power consumption
Attack Scenario • Power Plant and Substation Automation, › The system runs through every link of the power system. Attack each plant station to make timedisorders	Attack Scenario • WAMS › Attack PMU to make its measurement unit amplitude error exceeds the limitation • Monitoring system of operating status for overhead transmission lines › Attack main station traction terminal time disorder • Lightning locating system › Attack the station so that it is out of sync with other stations	Attack Scenario • Distribution automation system › Attack the distribution master and make it out of sync with the terminal time • AMI › Attack the metering master makes it out of sync with the terminal time	Attack Scenario › Combined with the timing mechanism of the metering system traction meter time error

Fig. 4 *TSA's impact on generation, transmission, distribution, and consumption of power system*

Table 2 Comparison of synchronisation mechanisms in power systems

Type	Hierarchical time synchronisation	Distributed time synchronisation
synchronisation mechanism	synchronised to the TSD in head end	synchronised to the TSDs in substation/ power plant/control centre
related system	AMI, DAS, condition monitoring system of overhead conductor	WAMS, LLS, SAS etc.
precision requirement	above a second	below a second

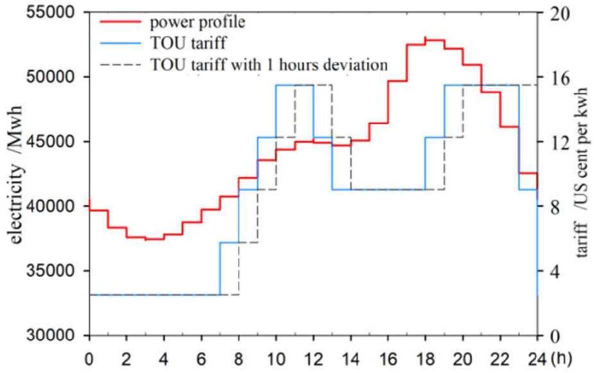


Fig. 5 *Synchronisation disorder in TOU electricity tariff*

not execute the control command. Therefore, once the TSD of DAS suffers TSA and operate with time deviation exceeding 10-s to the associated field terminals. The remote control function of DAS can be disabled.

• *TSA's impact on AMI:* There are three kinds of field terminal units in AMI, i.e. concentrators, meters relays, and meter. They are synchronised in a hierarchical way. The concentrators are synchronised to the TSD in the head end once a day and the meter relays and meters are synchronized to the concentrator everyday [28, 29]. If the time deviation is <10 s, the collectors and meters can be synchronised automatically. Otherwise, field crews should synchronise them by remote control or onsite operation. Once the TSD in the head end suffers TSA and outputs the wrong time, the AMI suffers disorder in time synchronisation and causes negative consequences in two ways.

As a distributed system, metering data and commands transmitted in AMI could be of large latency, too. According to the validity verification mechanism of AMI, data and command with latency >5-min is considered as invalid. Once uploaded metering data with a time deviation over 5-min, it is discarded as invalid data. Similarly, once a meter receives a command with a time deviation over 5-min, the command is discarded too. Therefore, once TSDs in the head end of AMI suffer TSA and operate with a time deviation over 5-min, the meter reading and remote control function of AMI can be disabled [30, 31].

Time of use (TOU) tariff is widely used to relieve peak capacity constraints. The accurate timestamp of electricity usage plays a key role to estimate electricity charges precisely. Smart meters are synchronised to the collectors and collectors are synchronised to the TSDs in the head end in turn. Once TSDs of AMI suffer GPS spoofing-based TSA and compel the head end as well as smart meters to operate with larger time deviation, power utility will from loss of revenue.

A power utility with an average power of 44,096 MW is utilised to calculate and demonstrate the potential electricity revenue loss caused by GPS spoofing-based TSA. The TOU electricity tariff and load profile are plotted in Fig. 5. The red curve denotes the load profile. The blue curve denotes the exact TOU tariff and the dash line denotes tariff with a deviation of an hour. The peak tariff, off-peak tariff, and standard tariff are $145.5, $48.5, and $97.0 MWh, respectively. Once the head-end suffers TSA and operates with time deviation, the daytime with a higher load will be imposed with lower off-peak tariff and the night-time with a lower load will be imposed with higher peak tariff. After time misplacement, the electricity price between 11 and 19 h with a high load will change from the flat price to valley price, resulting in electricity loss as a consequence.

• *TSA's impact on condition monitoring system:* The on-site condition monitoring systems of overhead conductors are synchronised to the TSD in the head end, too. The head end wakes the associated terminals once a day for synchronisation. Once a field terminal operate with a time deviation >2-min to the head end, the terminal will be synchronised to the head end [32, 33].

Once the TSD of head-end suffers TSA, the field terminals will be synchronised to a wrong time reference by the synchronisation mechanism. Therefore, uploaded condition monitoring data (such as ambient temperature, humidity, wind speed & direction, ice accretion, conductor temperature etc.) contains timestamp with a larger deviation [34, 35], which could result in the misleading interpretation of the system situation [36, 37].

3.2 TSA in distributed synchronised system

• *TSA's impact on WAMS*: Phasor measurement units (PMUs)-based WAMS, which measures synchronous phasor of the system with high precision, plays a key role in situation awareness of power systems [38, 39]. WAMS has been applied to dynamic monitoring of power grid operation (online monitoring of voltage stability/transient stability) [40, 41], online disturbance identification, online monitoring analysis, and damping control of low-frequency oscillation [42, 43], online monitoring analysis of grid-related behaviour of grid-connected units [44], load parameter identification [29], state estimation combined with PMU data etc. [45].

Time synchronisation precision plays a key role in accurate monitoring of the dynamic of the system and ensuring the security of the power grid. According to [46], the maximum allowable error of PMU measurement value is 1%. When the phase angle is 0°, the allowable difference in phase angle is 0.573°. In a 60 Hz system, 1 µs time error results in an error of phase angle of 0.022°, and PMU measurement with a time deviation of 26.53 µs exceeds the allowable threshold.

It can be observed from Fig. 6 that PMU synchronises to the TSD within a substation. In [47], consider a power network with N_{b} buses connected via N_{l} transmission lines, the state estimate after the attack is given by (1)

$$\hat{\boldsymbol{v}}_{\mathrm{ML}}^{\mathrm{atk}} = \boldsymbol{G}^{-1} \sum_{n=1}^{N_{\mathrm{b}}} a_n \boldsymbol{H}_n^{\top} \boldsymbol{\Sigma}_n^{-1} (\boldsymbol{\Gamma}_n \boldsymbol{H}_n \boldsymbol{v}_0 + \boldsymbol{w}_n) \tag{1}$$

$$\boldsymbol{G} = \sum_{n=1}^{N_{\mathrm{b}}} a_n \boldsymbol{H}_n^{\top} \boldsymbol{\Sigma}_n^{-1} \boldsymbol{H}_n \tag{2}$$

In formulas (1) and (2), the construction of the coefficient matrix $\boldsymbol{H}_n$ will be based on the complex $2N_{\mathrm{l}} \times N_{\mathrm{b}}$ line to bus admittance matrix, $\boldsymbol{w}_n$ denotes an additive Gaussian noise vector that is assumed to be independent across PMUs with known covariance $\sum_n$. a_n is a binary indicator, which has a value of 1 if a PMU is installed at bus n, and 0 otherwise. $\boldsymbol{\Gamma}_n \in \mathbb{R}^{M_n \times M_n}$ is a block diagonal matrix, consisting of $1 + L_n$ blocks. TSA on bus n shifts the phase of the measured quantities by an unknown quantity $\Delta\theta_n$, where each block is the 2×2 matrix $\begin{bmatrix} \cos\Delta\theta_n & -\sin\Delta\theta_n \\ \sin\Delta\theta_n & \cos\Delta\theta_n \end{bmatrix}$Once TSDs of one or more substations suffer GPS spoofing-based TSA and induced time deviation in phasor measurements, it will result in misleading state estimation and in-appropriate control as a consequence [48, 49]. The potential outcome of TSA has been simulated in [50]. The simulation result indicates that the TSA against WAMS could result in a catastrophic blackout.

- *TSA's impact on SAS*: A series of protection relays operate to isolate fault section once the power grid operates with a short circuit present. The sequences of the event system is extensively employed to identify operation sequence of protection relays in associated power plants and substations [51]. The SAS should be synchronised with high precision to discern the operation sequence of protection relays [11, 25].

Once SAS suffers TSA, it will result in chaos in events sequence, and lead to the wrong conclusion of accident analysis. According to [51], when a transmission line tripped with thunderstorm present, a flashover occurred at 123# tower between phases A and C at 3:16 AM. However, there is no lightning strike at that time in the neighbourhood according to the LLS, while there is a 245.2 KA lightning strike near the tower 122-123# at 3:20:58, which is nearly 5 min later than the time of line tripping. Since the existing time synchronisation technical specification does not explicitly require continuous inspection of the output time reference of TSD, time jitter of TSD might be much more frequent than expected.

- *TSA's impact on LLS*: According to statistics, tripping of transmission lines caused by the lightning stroke accounts for 40–70% of an unplanned outage of transmission lines in China [52, 53]. Existing LLS locates lightning strikes with the time-difference method. It detects very low frequency (VLF) signals generated by lightning at multiple stations, and then calculates and locates the lightning location according to the arrival time of VLF signals caused by the same lightning at each measurement site [54, 55]. The premise for the LLS to locate the lightning strike position accurately is that all measurement sites are synchronised with high precision [56, 57]. When TSDs of single or multiple sites suffer TSA, the lightning positioning error calculated according to the difference in arrival time will increase significantly.

The factors affecting lightning positioning error include the localisation algorithm error, radiation source path error, equipment error (thunder error signal collection, GPS clock error, the thunder peak value judgment), and error caused by the layout of the network of measuring sites. All four positioning errors can be characterised by time uncertainty Δt [58]. Generally speaking, the time error of a GPS RX is below 50 ns [3, 59, 60]. The ultimate time uncertainty Δt is about 100 ns adding up some other factors. According to the geometric model of five stations network as shown in Fig. 7, the positioning error of radiation sources outside the station network is

$$\Delta y = (r/D)c\Delta t \tag{3}$$

$$\Delta r = 8(r/D)^2 c\Delta t \tag{4}$$

It can be seen from (3) and (4) that positioning errors are proportional to $c\Delta t$. The radiation error of the radiation source is proportional to r^2, and the axial error is proportional to r. The axial positioning error of a radiation source at 100 km is 82 m and the radial positioning error Δr is 1.4 km in an area with a diameter of 50 km. Once a monitoring site suffers TSA and produces a time error of 1 µs, the time uncertainty Δt is about 1 µs, the axial positioning error is 820 m, and the radial positioning error is up to 14 km.

To conclude, TSA against LLS will significantly enlarge the positioning error and delay the determination of the time of the

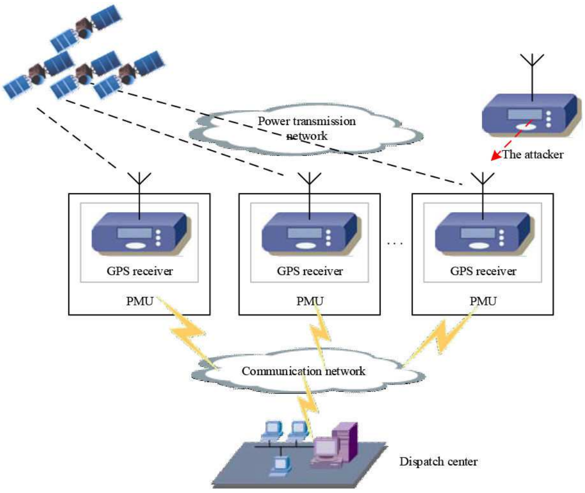


Fig. 6 *PMU-based WAMS under TSA*

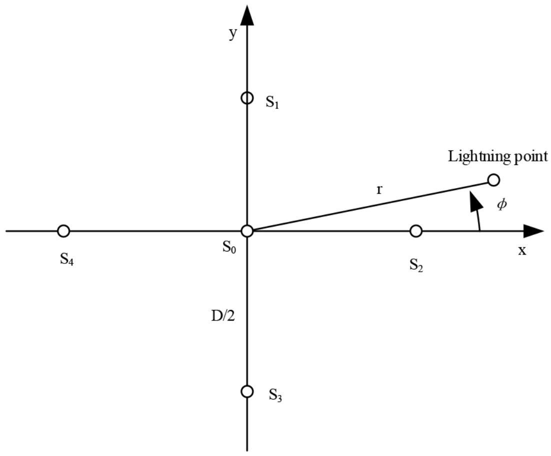


Fig. 7 *Geometric model for station network distribution*

lightning strike point, thus threatening the safe and stable operation of the power grid.

4 Defend against GPS spoofing-based TSA

4.1 Defend against TSA with power system state estimation

GPS spoofing-based TSA could cause phase angle error in phasor measurement and result in misleading result of state estimation. Since phasor measurements of neighbouring substations are close-coupled, it is feasible to detect GPS spoofing attacks in a data-driven approach [61].

In [62], state estimation is employed to identify GPS spoofing-based TSA of a single PMU. Numerical simulation indicates that the proposed approach can locate and correct the spoofed synchrophasor data with good accuracy. However, this algorithm cannot achieve correction for TSAs of multiple PMUs. For these unknown spoofed PMU locations and phase angles, an alternating minimisation algorithm for the attack reconstruction of multiple TSAs presented by Risbud *et al,* [63]. Moreover, other works on the attack detection for PMUs in transmission systems such as [64, 65], which have specific requirements for the amount of PMU data. For example, Taha *et al*. [64] required successive PMU measurements across time for dynamic state estimation, and Wang *et al*. [65] achieved the PMU data recovery is only applicable to a transmission line equipped with two PMUs at both ends. A distributed TSA detection approach is proposed in [66]. It can detect the coordinated attack when less than one-third of substations suffer TSA. The state estimation-based approaches can defend against TSA once wide-area phasor data in various substations are available in time. Once there are enough PMUs data, the state estimation-based TSA detection can be applied to unbalanced DAS [67, 68]. However, it should point out that there is usually a high ratio of bad data in phasor measurements, state estimation-based approach may not be appropriate for industrial application, yet.

4.2 Defend against TSA with time jitter detection

Traditionally, the technical guide [69] and specification [46] regulate the way to implement the function of synchronisation with high reliability, while the way to defend against cyber-attack is not considered, i.e. the reason that the TSD could be compromised with TSA at ease.

No matter how the malicious adversary initiate GPS spoofing attack, the time jitter induced by the TSA could be detected by comparing the satellite and local time reference. The time jitter can be identified according to steps as follows [70]:

- The TSD should examine the continuity of the output time above a second order.
- The time deviation between GPS time reference and OXCO-based local time reference should be validated. If the time deviation is >1 μs/s, then the OXCO-based local time reference is output as a time reference.
- Once the time deviation between GPS time reference and local time reference is <1 μs/s, the output time should track the GPS reference signal with a speed below 0.2 μs/s.

In practice, it is common for TSDs to perform local punctuality when the satellite loses lock. A high-precision time-keeping scheme based on pre-set time compensation is proposed in [71]. The synchronisation error of TSD can be kept within 20 s without a satellite signal for a day.

Although time jitter detection-based approach can identify GPS spoofing-based TSA with large time jitter, it may not be used to defend against sustained TSA with small-time jitter. For example, once a sustained TSA causes 0.5 μs timer jitter for 1PPS, it could result in time deviation of 0.5 ms after sustained TSA of 2500 s. A time deviation of 0.5 ms could result in a phase angle deviation of 9°, which may lead to mal-operation of power system controlling, error in lightning location results etc.

4.3 Defend against TSA with satellite signals

Since TSDs are attacked with spoofed satellite signals, it is feasible to detect TSA by identifying the fraud satellite signals. To defend against TSA with satellite signal, we can either encrypt and authenticate the satellite signal or identify features of the satellite signal.

Encryption and authentication of the satellite signal are promising anti-spoofing techniques. Literature [72–75] verifies the effectiveness of using the satellite navigation signal encryption authentication mechanism to detect spoofing from the navigation message information layer and the spread spectrum signal layer, respectively. The navigation message authentication (NMA) defence may require an excess technique to detect a SCER-based attack in which the malicious attacker rapidly estimates the unpredictable bits of the $D_i(t)$ (the *i*th signal's data bit stream) data stream. If the attacker does not use sufficient latency in its attack, then the initial portions of its transmissions of unknown $D_i(t)$ bits will contain errors about half the time. So the RX can implement detection that looks for this initial uncertainty of the unpredictable $D_i(t)$ bits [76]. The SCER detection can issue a spoofing alarm if it sees enough unusual behaviour at the initial portions of these bits. This method can detect and resist satellite navigation spoofing attacks. However, it is rather difficult to implement since the whole satellite navigation signal system needs to be changed.

The fraud satellite signal usually has a notable difference from the legitimate signal. Therefore, it is feasible to anti-spoofing by (i) RX autonomous integrity monitoring (RAIM); (ii) signal amplitude detection; (iii) signal arrival angle detection; (iv) signal arrival time detection; (v) correlation with other GNSS sources.

- *RAIM*: It is the most widely used anti-spoofing strategy in GNSS RXs [77]. Since the movement of satellite follows the Doppler effect, the spatial consistency of all available GNSS signals can be checked to exclude aberrant satellites [78].
- *Signal amplitude detection*: Variation of signal strength of legitimate satellite signal follow specific rule. It can determine whether it is attacked by spoofing by detecting the changes in absolute signal power, carrier to noise ratio (CNR) and power caused by carrier movement in the presence of satellite navigation spoofing [79]. The signal amplitude detection-based approach does not need to change the hardware of a RX. However, it is difficult to adapt to the requirements of different spoofing scenarios because the work rate of the real satellite navigation signal itself may vary with the environment.
- *Signal arrival angle detection*: It detects GNSS spoofing based on the spatial characteristics of spoofing and legitimate signals, which the direction angle of spoofing signals arriving at the RX antenna in different paths is exactly the same, while the direction angle of legitimate signals arriving at the RX antenna in different real navigation satellites is not exactly the same. Spoofing signals generated from a common source can be effectively detected using a synthetic array antenna [80]. Antenna array or moving antenna is used to detect the arrival angle of spoofing signal transmitted by a single antenna [81]. It has good detection performance and can adapt to different spoofing scenarios. However, it increases the cost of system hardware by adding an antenna array or servo control mechanism.
- *Signal arrival time detection*: It uses the difference in the transmission delay between spoofing and legitimate signal to detect the fraud signal [82]. As for the spoofing detection method using the correlator output distribution characteristics [83] and signal quality monitoring [84, 85], it uses the correlation peak anomaly caused by the difference between the arrival time of the spoofing and the legitimate signal. It is useful for the RX in a fixed position. However, it is not fit for a moving RX.
- *Correlation with other GNSS sources*: Augmenting data from auxiliary devices such as inertial measurement unit (IMU) that are immune to the external electromagnetic environment can help to discriminate the spoofing threat [86, 87]. The measurement results of the IMU are compared with the satellite

Table 3 Comparison of the main satellite navigation spoofing detection methods

Detection type	Detection techniques	Spoofing feature	RX required capability	Complexity	Effectiveness	Scope of application
RAIM	RAIM	the change of available signals for spatial consistency	spatial consistency analysis	low	low	low
signal amplitude detection	CNR monitoring	higher CNR	CNR monitoring	low	medium	medium
	absolute power monitoring	higher amplitude	absolute power monitoring	low	medium	high
	power variation versus RX movement	higher power variations	antenna movement/SNR monitoring	low	low	low
signal arrival angle detection	antenna array	spoofing signals coming from the same direction	multiple RX antennas	high	high	high
	moving antenna	spoofing signals coming from the same direction	measuring correlation coefficient	high	high	high
signal arrival time detection	time of arrival discrimination	inevitable delay of spoofing signal	time of arrival analysis	medium	medium	low
	signal quality monitoring	deviated shape of authentic correlation peak	multiple correlators	medium	medium	low
	correlation function distortion monitoring	perturbed correlation functions distribution due to spoofing	distribution analysis of correlation functions	low	medium	medium
correlation with other GNSS source	correlation with other GNSS source	inconsistency of spoofing solution	different navigation sensors	high	high	high
encryption and authentication	NMA	not authenticated	authentication	high	high	high
	delayed-symmetric-key spread spectrum security code (SSSC)	not authenticated	authentication	high	high	high
	dual-RX keyless correlation of unknown SSSC codes	not authenticated	authentication	high	high	high
	symmetric-key SSSC	not authenticated	authentication	high	high	high

navigation and positioning results, which can detect spoofing signals. However, the IMU is of large accumulating error and precise IMU is usually expensive.

Based on the aforementioned anti-spoofing techniques, the main satellite navigation spoofing detection approaches can be compared as shown in Table 3. The common TSA detection technologies and their combination are listed in Table 4 in the sequence of complexity. These combinations are representative of good complementary strategies while it is not an exhaustive list of all sensible combinations.

According to Table 1, there are 13 ways of TSA. There are 13 ways to defend against TSA as shown in Table 4, correspondingly. The success rate to detect a TSA is analysed in [25] and the result is shown in Fig. 8. The matrix entries indicate high, mediate, or low detection likelihood for the corresponding attack/detection pair. The red cell indicates a low likelihood of success rate when a detection approach is applied to the corresponding TSA. Yellow cell denotes medium success rate and green cell denotes high success rate.

The attack and defence approaches in Fig. 8 are ranked with order by increasing cost from top to bottom and from left to right. The cost of attack and defence is determined by the cost of developing or buying the hardware, the expertise required to set up it, and the complexity of operating it. Fig. 8 shows an important basis for TSDs vendors to choose a detection technique or a combination of them to defend against potential GPS spoofing attack. The defence technique with less cost can deal with less complex attack techniques. The defence scheme depends on the needed security of the application.

Unlike the average system, cyber-attack against critical electric infrastructures could lead to a catastrophic blackout, which is much placing the nation's security, and public safety at risk. The state-sponsored cyber-attack against power systems could be with sufficient knowledge and budget. Therefore, it is recommended that D9 incorporating NMA, SCER detection, signal amplitude detection, drift monitoring should be employed in TSDs of power systems. However, since the D9 detects GPS spoofing with local information of TSD, it may fail under attack scenarios of A1, A5, and A11. To defend against well organised, complex GPS spoofing attack, state estimation-based approach should be employed to mitigate the potential consequence of attack.

Table 4 Ranking of common detection technologies

No.	Detection techniques
D1	RAIM
D2	signal amplitude detection
D3	correlation function distortion monitoring
D4	drift monitoring (clock offset, IMU/position)
D5	correlation function distortion monitoring, drift monitoring [88]
D6	NMA
D7	NMA and SCER detection
D8	delayed symmetric-key SSSC
D9	NMA, SCER detection, signal amplitude detection, drift monitoring
D10	antenna array
D11	moving antenna
D12	dual-RX keyless correlation of unknown SSSC codes
D13	symmetric-key SSSC

In recent years, big data and artificial intelligence have gained significant advances. The way may be developed with big data and artificial intelligence in combination to detect and defend TSAs.

5 Conclusion

The GPS spoofing-based TSA's impact in the power industry and the way to defend it are reviewed in this paper. The conclusions are as follows:

Attack Detection	A1	A2	A3	A4	A5	A6	A7	A8	A9	A 10	A 11	A 12	A 13
D1	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
D2	🟨	🟩	🟥	🟥	🟨	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥
D3	🟨	🟨	🟨	🟨	🟨	🟥	🟥	🟨	🟨	🟨	🟨	🟥	🟥
D4	🟨	🟩	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨	🟨
D5	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟩	🟩	🟩	🟩	🟨	🟨
D6	🟥	🟩	🟩	🟥	🟥	🟩	🟥	🟩	🟩	🟥	🟥	🟩	🟥
D7	🟥	🟩	🟩	🟨	🟥	🟩	🟨	🟩	🟩	🟨	🟥	🟩	🟨
D8	🟥	🟩	🟩	🟨	🟥	🟩	🟨	🟥	🟥	🟨	🟥	🟩	🟨
D9	🟨	🟩	🟩	🟩	🟨	🟩	🟩	🟩	🟩	🟩	🟨	🟩	🟩
D10	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟨	🟨	🟨	🟨	🟨
D11	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟥	🟨	🟨	🟨	🟨	🟨
D12	🟥	🟩	🟩	🟨	🟥	🟩	🟨	🟩	🟩	🟨	🟥	🟩	🟨
D13	🟥	🟩	🟩	🟨	🟥	🟩	🟨	🟩	🟩	🟨	🟥	🟩	🟨

Fig. 8 *Probability of detection technology*

- In the hierarchical synchronised systems, TSA can cause disorder in time synchronisation of the head end and field unit terminals. Monitoring and controlling function of the head end can be disabled with TSA. Time jitter detection-based approach can be implemented in TSDs to prevent from most of the TSA.
- Distributed synchronised system, such as WAMS, requires high precision in synchronisation and are sensitive to TSA. Time jitter detection-based approach is not enough to prevent sustained TSA alone.
- It is rather difficult to eliminate the likelihood of GPS spoofing-based TSA of a well-organised adversary. The complex defence scheme D9 with a combination of several defence techniques could fail under specific attack scenarios. The state estimation-based approaches using more information should be employed to detect and defend sophisticated GPS spoofing attack.
- GPS spoofing is a major threat to the CPPS. Detection and defending of GPS spoofing attack should be mandatorily required in the related technical specification.

6 References

[1] Tan, S., De, D., Song, W. Z., *et al.*: 'Survey of security advances in smart grid: a data driven approach', *IEEE Commun. Surv. Tutor.*, 2017, **19**, (1), pp. 397–422

[2] Liu, S., You, S., Yin, H., *et al.*: 'Model-free data authentication for cyber security in power systems', *IEEE Trans. Smart Grid*, 2020, pp. 1–1, doi: 10.1109/TSG.2020.2986704

[3] Liu, Y., Cheng, C., Gu, T., *et al.*: 'A lightweight authenticated communication scheme for smart grid', *IEEE Sens. J.*, 2016, **16**, (3), pp. 836–842

[4] Han, W., Xiao, Y.: 'Privacy preservation for V2G networks in smart grid: a survey', *Comput. Commun.*, 2016, **91–92**, pp. 17–28

[5] Nia, M. A., Ruiz-Martinez, A.: 'Systematic literature review on the state of the art and future research work in anonymous communications systems', *Comput. Electr. Eng.*, 2018, **69**, pp. 497–520

[6] Venkataramanan, V., Srivastava, A.K., Hahn, A.: 'Measuring and enhancing microgrid resiliency against cyber threats', *IEEE Trans. Ind. Appl.*, 2019, **55**, (6), pp. 6303–6312

[7] Liu, C., Stefanov, A., Hong, J., *et al.*: 'Intruders in the grid', *IEEE Power Energy Mag.*, 2012, **10**, (1), pp. 58–66

[8] Hong, J., Liu, C.: 'Intelligent electronic devices with collaborative intrusion detection systems', *IEEE Trans. Smart Grid*, 2019, **10**, (1), pp. 271–281

[9] Hong, J., Liu, C., Govindarasu, M.: 'Integrated anomaly detection for cyber security of the substations', *IEEE Trans. Smart Grid*, 2014, **5**, (4), pp. 1643–1653

[10] Chang, R., Jiang, L., Chen, W., *et al.*: 'A trust enclave-based architecture for ensuring run-time security in embedded terminals', *Tsinghua Sci. Technol.*, 2017, **22**, (5), pp. 447–457

[11] Yang, M., Zhang, D., Huang, X.: 'A study on technology of power time synchronization system'. 2011 Int. Conf. on Advanced Power System Automation and Protection, Beijing, 2011, pp. 2272–2277

[12] Kerns, A.J., Shepard, D.P., Bhatti, J.A., *et al.*: 'Unmanned aircraft capture and control via GPS spoofing', *J. Field Robot.*, 2014, **31**, (4), pp. 617–636

[13] Jones, M.: 'Spoofing in the Black Sea: what really happened?', 11 October 2017. Available at https://www.gpsworld.com/spoofing-in-the-black-sea-what-really-happened/

[14] Wang, H., Ruan, J., Zhou, B., *et al.*: 'Dynamic data injection attack detection of cyber physical power systems with uncertainties', *IEEE Trans. Ind. Inf.*, 2019, **15**, (10), pp. 5505–5518

[15] Huang, L., Yang, Q.: 'Low cost GPS simulator: GPS spoofing by SDR'. 2015 DEF CON 23, Las Vegas, NV, USA, 2015

[16] Misra, P., Enge, P.: '*Global positioning system: signals, measurements, and performance*' (Ganga-Jamuna Press, Lincoln, Massachusetts, 2010, 2nd edn.)

[17] Borre, K., Akos, D.M., Bertelsen, N., *et al.*: '*A software-defined GPS and Galileo receiver*' (Birkhäuser, Boston, 2007)

[18] Zhang, Z., Gong, S., Dimitrovski, A. D., *et al.*: 'Time synchronization attack in smart grid: impact and analysis', *IEEE Trans. Smart Grid*, 2013, **4**, (1), pp. 87–98

[19] Shang, H., An, J., Gong, W.: 'Research on the cascaded suppression method of blanket jamming in satellite navigation receivers'. Proc. ICNS, Wireless Communications and Trusted Computing, Wuhan, Hubei, 2010, pp. 362–365

[20] Bull, T.: 'A new high performance way of detecting and mitigating the Jamming Meaconing and spoofing of commercial GNSS signals'. 2010 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), Noordwijk, 2010, pp. 1–5

[21] Bhatti, J., Humphreys, T.E.: 'Hostile control of ships via false GPS signals: demonstration and detection', *Navigation*, 2012, **64**, (1), pp. 51–66

[22] Humphreys, T.E.: 'Detection strategy for cryptographic GNSS anti spoofing', *IEEE Trans. Aerosp. Electron. Syst.*, 2013, **49**, (2), pp. 1073–1090

[23] Wesson, K., Rothlisberger, M., Humphreys, T.E.: 'Practical cryptographic civil GPS signal authentication', *Navigation*, 2014, **59**, (3), pp. 177–193

[24] Xie, X., Zeng, D., Lu, M.: 'Research on GNSS generating spoofing jamming technology'. IET Int. Radar Conf. 2015, Hangzhou, 2015, pp. 1–5

[25] Psiaki, M.L., Humphreys, T.E.: 'GNSS spoofing and detection', *Proc. IEEE*, 2016, **104**, (6), pp. 1258–1270

[26] Huang, X., Li, W., Yang, S., *et al.*: 'Smart substation IEC61588 time synchronization system and security evaluation'. 2014 IEEE Int. Symp. on Precision Clock Synchronization for Measurement, Control, and Communication (ISPCS), Austin, TX, 2014, pp. 97–101

[27] Ingram, D.M.E., Schaub, P., Campbell, D.A., *et al.*: 'Evaluation of precision time synchronisation methods for substation applications'. 2012 IEEE Int. Symp. on Precision Clock Synchronization for Measurement, Control and Communication Proc., San Francisco, CA, 2012, pp. 1–6

[28] Ullah, R., Faheem, Y., Kim, B.: 'Energy and congestion-aware routing metric for smart grid AMI networks in smart city', *IEEE Access*, 2017, **5**, pp. 13799–13810

[29] Huang, S., Lu, C., Lo, Y.: 'Evaluation of AMI and SCADA data synergy for distribution feeder modeling', *IEEE Trans. Smart Grid*, 2015, **6**, (4), pp. 1639–1647

[30] Luan, W., Sharp, D., LaRoy, S.: 'Data traffic analysis of utility smart metering network'. 2013 IEEE Power & Energy Society General Meeting, Vancouver, BC, 2013, pp. 1–4

[31] Measure and Management System for Electric, Water, Gas and Heat Meter, T/CEC 122.1-2016, October 2016

[32] General technical specification for condition monitoring device on overhead transmission lines, Q/GDW242-2010, 2010.12

[33] So, E., Arseneau, R., Bennett, D., *et al.*: 'Computer-controlled system for calibrating high-voltage revenue metering equipment under actual operating conditions', *IEEE Trans. Instrum. Meas.*, 2011, **60**, (7), pp. 2500–2505

[34] Jiang, X., Meng, Z., Zhang, Z., *et al.*: 'DC ice-melting and temperature variation of optical fibre for ice-covered overhead ground wire', *IET Gener. Transm. Distrib.*, 2016, **10**, (2), pp. 352–358

[35] Huneault, M., Langheit, C., Caron, J.: 'Combined models for glaze ice accretion and de-icing of current-carrying electrical conductors', *IEEE Trans. Power Deliv.*, 2005, **20**, (2), pp. 1611–1616. General technical specification for condition monitoring device on overhead transmission lines, Q/GDW242-2010, 2010.12

[36] Peter, Z., Volat, C., Farzaneh, M., *et al.*: 'Numerical investigations of a new thermal de-icing method for overhead conductors based on high current impulses', *IET Gener. Transm. Distrib.*, 2008, **2**, (5), pp. 666–675

[37] Lu, J., Guo, J., Hu, J., *et al.*: 'Analysis of ice disasters on ultra-high-voltage direct-current transmission lines', *Nat. Hazards*, 2017, **86**, (1), pp. 203–217

[38] Zhong, Z., Xu, C., Billian, B.J., *et al.*: 'Power system frequency monitoring network (FNET) implementation', *IEEE Trans. Power Syst.*, 2005, **20**, (4), pp. 1914–1921

[39] Khandare, B.B., Deshmukh, B.T.: 'A literature review on wide area protection technique using PMU'. 2017 Int. Conf. on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, 2017, pp. 1449–1454

[40] Prabhakar, P., Kumar, A.: 'Voltage stability assessment using phasor measurement technology'. 2014 IEEE 6th India Int. Conf. on Power Electronics (IICPE), Kurukshetra, 2014, pp. 1–6

[41] Gore, R., Kande, M.: 'Analysis of wide area monitoring system architectures'. 2015 IEEE Int. Conf. on Industrial Technology (ICIT), Seville, 2015, pp. 1269–1274

[42] Naidu, O., Gore, R., George, N.: 'Centralized fault location technique for power transmission networks using WAMS data'. 2016 Biennial Int. Conf. on Power and Energy Systems: Towards Sustainable Energy (PESTSE), Bangalore, 2016, pp. 1–6

[43] Gore, R., Valsan, S.P.: 'Big data challenges in smart grid IoT (WAMS) deployment'. 2016 8th Int. Conf. on Communication Systems and Networks (COMSNETS), Bangalore, 2016, pp. 1–6

[44] Kanabar, M., Adamiak, M.G., Rodrigues, J.: 'Optimizing wide area measurement system architectures with advancements in phasor data

concentrators (PDCs)'. 2013 IEEE Power & Energy Society General Meeting, Vancouver, BC, 2013, pp. 1–5

[45] Deng, R., Xiao, G., Lu, R.: 'Defending against false data injection attacks on power system state estimation', *IEEE Trans. Ind. Inf.*, 2017, **13**, (1), pp. 198–207

[46] IEEE Standard for Synchrophasor Measurements for Power Systems, IEEE Std C37.118.1-2011 (Revision of IEEE Std C37.118-2005), 28 December 2011, pp. 1–61

[47] Risbud, P., Gatsis, N., Taha, A.: 'Assessing power system state estimation accuracy with GPS-spoofed PMU measurements'. 2016 IEEE Power & Energy Society Innovative Smart Grid Technologies Conf. (ISGT), Minneapolis, MN, 2016, pp. 1–5

[48] Konstantinou, C., Sazos, M., Musleh, A.S.*, et al.*: 'GPS spoofing effect on phase angle monitoring and control in a real-time digital simulator-based hardware-in-the-loop environment', *IET Cyber-Phys. Syst., Theory Appl.*, 2017, **2**, (4), pp. 180–187

[49] Yasinzadeh, M., Akhbari, M.: 'Detection of PMU spoofing in power grid based on phasor measurement analysis', *IET Gener. Transm. Distrib.*, 2018, **12**, (9), pp. 1980–1987

[50] Almas, M.S., Vanfretti, L., Singh, R.S.*, et al.*: 'Vulnerability of synchrophasor-based WAMPAC applications' to time synchronization spoofing'. 2018 IEEE Power & Energy Society General Meeting (PESGM), Portland, OR, 2018, pp. 1–1

[51] Li, W.: 'Application of lightning location system in fault point inspection of transmission lines', *Low-Carbon World*, 2016, **5**, (18), pp. 41–42

[52] Shao, X., Stanley, M., Regan, A.*, et al.*: 'Total lightning observations with the new and improved Los Alamos Sferic Array (LASA)', *J. Atmos. Ocean. Technol.*, 2006, **23**, (10), pp. 1273–1288

[53] Chen, J., Zhang, Q., Feng, W.*, et al.*: 'Lightning location system and lightning detection network of China power grid', *High Volt. Eng.*, 2008, **34**, (3), pp. 425–431

[54] Chen, L., Zhang, Y., Lu, W.*, et al.*: 'Performance evaluation for a lightning location system based on observations of artificially triggered lightning and natural lightning flashes', *J. Atmos. Ocean. Technol.*, 2012, **29**, (12), pp. 1835–1844

[55] Chen, J., Wu, Y., Zhao, Z.: 'The new lightning detection system in China: its method and performance'. 2010 Asia-Pacific Int. Symp. on Electromagnetic Compatibility, Beijing, 2010, pp. 1138–1141

[56] Cummins, K.L., Murphy, M.J.: 'An overview of lightning locating systems: history, techniques, and data uses, with an in-depth look at the U.S. NLDN', *IEEE Trans. Electromagn. Compat.*, 2009, **51**, (3), pp. 499–518

[57] Guo, J., Gu, S., Feng, W.: 'A lightning motion prediction technology based on spatial clustering method'. 2011 7th Asia-Pacific Int. Conf. on Lightning, Chengdu, 2011, pp. 788–793

[58] Cai, L., Zou, X., Wang, J.*, et al.*: 'Error analysis of total lightning location system based on Monte Carlo method'. 2018 34th Int. Conf. on Lightning Protection (ICLP), Rzeszow, 2018, pp. 1–5

[59] Lu, Y., Liu, Y., Zhou, Z.*, et al.*: 'Distributed lightning current monitoring and its application to lightning protection on transmission line'. 2013 2nd Int. Symp. on Instrumentation and Measurement, Sensor Network and Automation (IMSNA), Toronto, ON, 2013, pp. 833–836

[60] Zeng, R., Zhuang, C., Zhou, X.*, et al.*: 'Survey of recent progress on lightning and lightning protection research', *High Volt.*, 2016, **1**, (1), pp. 2–10

[61] Yan, Y., Qian, Y., Sharif, H.*, et al.*: 'A survey on cyber security for smart grid communications', *IEEE Commun. Surv. Tutor.*, 2012, **14**, (4), pp. 998–1010

[62] Fan, X., Du, L., Duan, D.: 'Synchrophasor data correction under GPS spoofing attack: a state estimation-based approach', *IEEE Trans. Smart Grid*, 2018, **9**, (5), pp. 4538–4546

[63] Risbud, P., Gatsis, N., Taha, A.: 'Vulnerability analysis of smart grids to GPS spoofing', *IEEE Trans. Smart Grid*, 2019, **10**, (4), pp. 3535–3548

[64] Taha, A.F., Qi, J., Wang, J.*, et al.*: 'Risk mitigation for dynamic state estimation against cyber attacks and unknown inputs', *IEEE Trans. Smart Grid*, 2018, **9**, (2), pp. 886–899

[65] Wang, X., Shi, D., Wang, J.*, et al.*: 'Online identification and data recovery for PMU data manipulation attack', *IEEE Trans. Smart Grid*, 2019, **10**, (6), pp. 5889–5898

[66] Wang, Y., Hespanha, J.P.: 'Distributed estimation of power system oscillation modes under attacks on GPS clocks', *IEEE Trans. Instrum. Meas.*, 2018, **67**, (7), pp. 1626–1637

[67] Zhang, Y., Wang, J., Liu, J.: 'Attack identification and correction for PMU GPS spoofing in unbalanced distribution systems', *IEEE Trans. Smart Grid*, 2019, **11**, (1), pp. 762–773

[68] Rahman, W.U., Ali, M., Ullah, A.*, et al.*: 'Advancement in wide area monitoring protection and control using PMU's model in MATLAB/Simulink', *Smart Grid Renew. Energy*, 2012, **03**, (4), pp. 294–307

[69] IEEE Guide for Designing a Time Synchronization System for Power Substations, IEEE 2030.101-2018, 26 July 2018, pp. 1–118

[70] Technical specification of time synchronism system and equipment in smart substation. State Administration of quality supervision, inspection and quarantine of the PRC. GB/T 33591-2017. 2017.12

[71] Zeng, X.J., Yin, X.G., Lin, G.*, et al.*: 'Clock of high accuracy implemented by crystal oscillator in synchronism with GPS clock', *Autom. Electr. Power Syst.*, 2003, **27**, (8), pp. 74–77

[72] Scott, L.: 'Anti-spoofing and authenticated signal architectures for civil navigation systems'. Proc. Int. Technical Meeting of the Satellite Division of the Institute of Navigation (ION GPS/GNSS 2003), Portland, OR, September 2003, pp. 1543–1552

[73] Lo, S., Lorenzo, D.D., Enge, P.*, et al.*: 'Signal authentication: a secure civil GNSS for today', *In-Side GNSS*, 2009, **4**, (5), pp. 30–39

[74] Caparra, G., Sturaro, S., Laurenti, N.*, et al.*: 'Evaluating the security of one-way key chains in TESLA-based GNSS navigation message authentication schemes'. 2016 Int. Conf. on Localization and GNSS (ICL-GNSS), Barcelona, 2016, pp. 1–6

[75] Caparra, G., Ceccato, S., Sturaro, S.*, et al.*: 'A key management architecture for GNSS open service navigation message authentication'. 2017 European Navigation Conf. (ENC), Lausanne, 2017, pp. 287–297

[76] Savasta, S., Presti, L.L., Dovis, F.*, et al.*: 'Trust worthiness GNSS signal validation by a time-frequency approach'. Proc. Int. Technical Meeting of the Satellite Division of the Institute of Navigation (ION GNSS2009), Savannah, GA, USA, 2001, pp. 66–75

[77] John, A.: 'Vulnerability assessment of the transport infrastructure relying on the global positioning system' (Volpe National Transportation Systems Center, 2001)

[78] Kaplan, E., Hegarty, C.: '*Understanding GPS: principles and application*' (Artech House, Norwood, Mass, 1996)

[79] Jahromi, A.J., Broumandan, A., Nielsen, J.*, et al.*: 'GPS spoofer countermeasure effectiveness based on signal strength, noise power, and C/N0 measurements', *J. Satell. Commun. Netw.*, 2012, **30**, (4), pp. 181–191

[80] Nielsen, J., Broumandan, A., Lachapelle, G.: 'Spoofing detection and mitigation with a moving handheld receiver', *GPS World*, 2010, **21**, (9), pp. 27–33

[81] Nielsen, J., Broumandan, A., Lachapelle, G.: 'GNSS spoofing detection for single antenna handheld receivers', *Navigation*, 2012, **58**, (4), pp. 335–344

[82] Maybeck, P.S., DeVilbiss, S.L.: 'Detection of interference/jamming and spoofing in a DGPS-aided inertial system', *IEEE Trans. Aerosp. Electron. Syst.*, 1998, **34**, (4), pp. 1208–1217

[83] Cavaleri, A., Motella, B., Pini, M.*, et al.*: 'Detection of spoofed GPS signals at code and carrier tracking level'. 2010 5th ESA Workshop on Satellite Navigation Technologies and European Workshop on GNSS Signals and Signal Processing (NAVITEC), Noordwijk, 2010, pp. 1–6

[84] Pini, M., Fantino, M., Cavaleri, A.: 'Signal quality monitoring applied to spoofing detection'. Proc. Int. Technical Meeting of the Satellite Division of the Institute of Navigation. 2011, Portland, OR, September 2011

[85] Montgomery, P.Y., Humphreys, T.E., Ledvina, B.M.: 'Receiver-autonomous spoofing detection: experimental results of a multi-antenna receiver defense against a portable civil GPS spoofer'. Proc. Institute of Navigation—Int. Technical Meeting (ITM'09), Anaheim, Calif, USA, 2009, pp. 124–130

[86] Jafarnia-Jahromi, A., Lin, T., Broumandan, A.*, et al.*: 'Detection and mitigation of spoofing attack on a vector based tracking GPS receiver'. Proc. Int. Technical Meeting of The Institute of Navigation, Newport Beach, CA, USA, 2012

[87] Petovello, M.G.: 'Real-time integration of a tactical-grade IMU and GPS for high-accuracy positioning and navigation', PhD thesis, Department of Geomatics Engineering, University of Calgary, 2003

[88] Hu, Y., Cao, K., Bian, S.*, et al.*: 'GNSS spoofing detection algorithm based on clock frequency drift monitoring', *Syst. Eng. Electron.*, 2017, **37**, (7), pp. 1629–1632