Abstract: Advanced metering infrastructure (AMI) plays a key role in power systems. Since smart meters and meter collectors are synchronised to the time synchronisation devices (TSDs) in the head end system (HES) of AMI, they are vulnerable to global positioning system (GPS) spoofing-based time synchronisation attack (TSA). Impacts of GPS spoofing-based TSA on AMI are investigated in this study. It is uncovered that, since AMI is a distributed networked system and metering data and control commands transmitted in AMI could be of large latency, data and commands with large latency over the specific threshold are considered to be invalid according to validity verification mechanism of average distributed system. Therefore, the disorder in time synchronisation induced by GPS spoofing-based TSA could disable functions of HES of AMI, such as meter reading and remote control. A time jitter detection-based approach is developed to identify and prevent from GPS spoofing-based TSA. A high-precision oven-controlled crystal oscillator with cumulative error compensation is utilised to identify time jitter of the satellite clock and help ride through sustained GPS spoofing-based TSA. Simulation on FPGA demonstrates the effectiveness of the proposed approach.

1 Introduction
Cybersecurity of Smart Grid is considered to be one of the vital issues [1]. As a key component of Smart Grid, advanced metering infrastructure (AMI) is a valuable target for malicious adversaries [2]. In order to harden cybersecurity defence of AMI, cyber-based data encryption and authentication [2], and wireless virtual private networks [3] are employed to protect the integrity and privacy of data communication. Firewall and Intrusion Detection Systems are deployed to harden the head end of AMI and block external malicious intrusion [4, 5]. However, a novel cyber-attack, global positioning system (GPS) spoofing-based time synchronisation attack (TSA), which results in disorder in time synchronisation [6, 7], could negatively impact the AMI by bypassing existing cyber defense techniques.

GPS-based time synchronisation devices (TSDs) are widely used in power systems to keep monitoring and control systems synchronised precisely [8]. Since the GPS-based TSD communicates via civilian GPS signal with plain-text, they are vulnerable to GPS spoofing attacks [9]. Malicious adversaries could send the forged satellite signal in the physical proximity of a substation or control centre [10] to make the blunder of GPS-based time references, Fan et al. [11] inducing malfunction of monitoring and control systems. For example, the transmission system operator (TSO) of power utilities implements unit commitment according to pre-planned generation plans. In 2013, TSDs of the control centre of Sichuan Province in China output time reference of a wrong date, and TSO implemented unit commitment of that day, which results in unexpected tripping of several generators in two hydropower plants.

Global Navigation Satellite System (GNSS) signal is so weak that GPS receivers misinterpret forged satellite signals as authentic signals and, as a consequence, report a wrong time or location. GPS spoofing can be implemented according to the spoofer mechanism as follows [12]:

- **Suppression:** The attacker applies a strong interference signal to suppress authentic satellite signal, so that the target receiver loses the lock to the authentic satellite signal.
- **Record-and-replay attack:** The attacker delays and amplifies the received satellite signal and then forwards it out, so that the target receiver receives and generates the wrong positioning and timing information.
- **Generate spoofing attack:** The attacker synthesises and broadcast forged satellite signal to cheat satellite receiver. Once the target satellite receiver tracks to the forged satellite signal, TSD is induced to receive and output wrong positioning and timing information.

The growing dependence of critical infrastructure on GPS makes GPS spoofing-based cyber-attack a realistic threat [6–14]. Iranian military forces captured an unmanned drone in 2011 by GPS spoofing, which landed in Iran but it thought it was landing at its base in Afghanistan. Humphreys et al. control ships and unmanned vehicles with false GPS signals [7, 12]. A low-cost software-defined controller-based GPS simulator with hardware of 300 USD is developed in [13] and posted to GitHub, a publicly-accessible online software repository. With the help of the GPS simulator, one can launch GPS spoofing-based cyber-attack by broadcasting fabricated GPS signals with a few function calls [13]. Since power systems should maintain time synchronisation with high accuracy, it is vulnerable to GPS spoofing-based TSA. The wide-area measurement system (WAMS) is a typical distributed time synchronisation system where phasor measurement units (PMUs) in substations are synchronised with TSDs of substations. PMUs derive precise timing from GPS signals and leave a timestamp in each of its measurements. Recent research indicates that the spurious GPS signal could result in the wrong timestamp in PMU measurement [8–10]. The slight time deviation of a millisecond could result in a notable error in synchrophasor. Therefore, GPS spoofing-based TSA could induce mal-operation of wide-area measurement-based control [8, 15]. There are a variety of ways to defend against the GPS spoofing-based cyber-attack [8, 9]. The multiple antennas-based approaches are proposed in [16] to defend against intentional GPS spoofing. However, the use of multiple antennas just increases the technical difficulty of mounting a successful spoofing attack. A well-designed attack could succeed with additional spoofer transmitters.
Encryption can be employed to detect civil GPS spoofing, but it is cumbersome to use since it requires secure distribution of secret key [17]. Therefore, the way to defend against GPS spoofing-based TSA in the power industry is highly preferred.

This paper makes two contributions to the subject of cybersecurity defence of GPS spoofing-based TSA.

• We survey the GPS spoofing-based TSA's impact on AMI. Unlike WAMS, smart meters, meter relays, and meter collectors of AMI are synchronised to the TSD in the head-end system (HES) of AMI. GPS spoofing-based TSA could cause large time deviation among HES, smart meters, meter relays, and meter collectors, which could disable monitoring and control function of AMI via data and control command validation mechanism. Once smart meters are compelled to operate with large time deviation, it could even cause electricity tariff loss to the power utility.

• We propose a time jitter detection-based approach to defend against GPS spoofing-based TSA. A high-precision oven-controlled crystal oscillator (OCXO) is utilised to identify time jitter of the satellite clock. The cumulative error of OCXO is compensated to help ride through GPS spoofing-based TSA.

The remaining of this paper is organised as follows. The time synchronisation mechanism of AMI is described in Section 2. The impact of GPS spoofing-based TSA in AMI is analysed in Section 3. The time jitter detection-based approach to defend against GPS spoofing-based TSA is developed in Section 4 and simulation of FPGA is given in Section 5. Section 6 concludes the paper.

2 Time synchronisation of AMI and GPS spoofing-based TSA

2.1 Structure of AMI

AMI is a two-way communication system connecting smart meters, meter relays, meter collectors, with the HES [2, 18]. It is a flexible and general-purpose communication system that can be used for many applications, including advanced energy monitoring and recording, sophisticated tariff/rate data collection, load management and control, etc. AMI enables consumers to better manage their energy usage, and allows the grid to be run more efficiently in terms of cost and energy delivery. These advanced capabilities allow utilities to provide and configure the smart meters in the field, offering new tariff programs, and energy monitoring and control.

The general architecture of AMI is shown in Fig. 1. Usually, tens of meters communicate with a meter relay via power line communication (PLC) and tens or hundreds of meter relays communicate with a meter collector via PLC as well to upload metering data. The meter collector communicates with HES via GPRS/UMTS/4G wireless communication. Since smart meters communicate with the HES via public shared communication, they are exposed to malicious cyber-attack. To guarantee secure communication, a specific IC is utilised to implement authentication and encryption/decryption in smart meters [18]. In order to harden cybersecurity of HES, firewall and intrusion detection system are deployed in HES to detect and prevent malicious intrusion.

2.2 Time synchronisation of AMI

In order to implement monitoring and control function correctly, AMI should keep synchronisation with high precision across the HES, smart meters, meter relays, and meter collectors [15]. AMI is usually synchronised hierarchically in three steps, as shown in Fig. 2.

• There are several GPS-based TSDs in the HES. The TSDs produce a pulse-per-second (PPS) signal with a received GPS signal. After that, PPS is transmitted to synchronise devices in HES via IRIG-B protocol.

• Meter collectors maintain internal clock and they are synchronised to the HES periodically, usually once a day. Meter collectors send a heartbeat signal to the HES once every several minutes. HES estimates whether the time deviation between meter collector and HES is above a given threshold (such as 5 s) once a day. If the time deviation is above 5 s and below 5 min, HES sends a command to the meter collector and the meter collector synchronises its internal clock to that of HES automatically by itself. If the time deviation is above 5 min, field crews will synchronise the collector manually on site.

• Smart meters and meter relays maintain their internal clock too and they are usually synchronised to the meter collectors once a day. Smart meters sign a time stamp on the metering data. It is required that the time deviation between smart meters and meter relays and collectors should be kept within a threshold, such as 10 s. Meter collectors broadcast time signals to associated meter
relays and smart meters once a day. The smart meters and meter relays estimate its time deviation from that of meter collector. If the time deviation is over 10 s and below 5 min, the time deviation is reported to the HES and the smart meters and meter relays could synchronise themselves to the meter collector automatically. If the time deviation between smart meters and meter relays and meter collector is over 5 min, field crews need to synchronise the smart meter and meter relay manually on site.

3 Impact of GPS spoofing-based TSA in AMI

Civil GNSS satellite signal, which is open to the public, is utilised in GPS-based TSDs for time synchronisation. The TSDs could suffer GPS spoofing-based TSA. Malicious adversaries could broadcast forged satellite fraud signals to cause disorder in time synchronisation of AMI, and after that, attack by hierarchical time synchronisation mechanism and data validity verification mechanism. The impacts of TSA in AMI are summarised as follows.

3.1 Disable monitoring and control function

As a distributed networked system, metering data and control commands transmitted in AMI could be of large latency. According to the validity verification mechanism of the average distributed system, data and command with large latency are considered as invalid. The timestamp is utilised to calculate the latency of uploaded metering data and control command sent to meters to verify the validity of data and command.

In AMI of South Grid of China, the threshold of latency of metering data and control command is 5 min. Once TSDs in HES of AMI suffer TSA and operate with a time deviation above 5 min, all devices in the HES will be synchronised to the TSD and there are the latency >5 min between HES and smart meters. Therefore, all the uploaded metering data have a time deviation over 5 min and they are discarded as invalid data. Similarly, all the downstream control commands have a latency above 5 min and they should be discarded according to the validation mechanism.

Therefore, once TSD in HES of AMI suffers GPS spoofing-based TSA and operates with a time deviation over 5 min, the monitoring and control function of HES of AMI, including meter reading and remote control, will be disabled. Therefore, it is highly preferred to detect and prevent from GPS spoofing-based TSA of AMI.

3.2 Tariff loss

Time-of-use (TOU) tariff is widely used for commercial and industrial users of power utilities to relieve peak capacity constraints. The accurate timestamp of electricity usage plays a key role in determining the electricity charge precisely. Smart meters and meter relays of AMI are synchronised with the meter collectors and the meter collectors are synchronised to the HES as depicted in Section 2.2. According to the synchronisation mechanism of AMI, the internal clock of meter collectors, smart meters, and meter relays could be speedup/slow down 5 min a day at most, once malicious adversaries implement sustained GPS spoofing-based TSA for several days by broadcasting GPS spoofing signals with a time deviation of 5 min. Therefore, the internal clock of a smart meter could be a speedup/slow down for an hour after 12 days. Metering data is marked with the wrong timestamp once the internal clock of a smart meter operates with a large time deviation. Therefore, the power utility will suffer from loss of electricity revenue since the electricity tariff of a user is estimated according to its metering data and TOU.

A power utility with an average power of 44 096 MW is utilised to calculate and demonstrate the potential electricity revenue loss caused by sustained GPS spoofing-based TSA. The TOU electricity tariff and load profile are plotted, as shown in Fig. 3. The red curve denotes the load profile. The blue curve denotes the exact TOU tariff and the dashed line denotes tariff with a deviation of an hour. The peak tariff, off-peak tariff, and standard tariff are $145.5/MWh, $48.5/MWh, and $97.0/MWh, respectively. Once the AMI suffers sustained TSA and smart meters operate with time deviation, the daytime with the higher load will be charged with lower off-peak tariff and the night-time with the lower load will be charged with higher peak tariff. Therefore, power utility could suffer a revenue loss as a consequence.

The electricity usage and tariff in each hour in a typical day are listed in Table 1. The data with bold denote the off-peak hour and those with bold italic denote the peak hour.

The accumulated electricity usage, and electricity tariff in peak hour, off-peak hour, and other time span in a typical day without TSA are accumulated. The overall tariff without TSA is calculated and listed in Table 2. Given all smart meters operate with a time deviation of an hour after 12 days of sustained TSA, the overall electricity tariff on the 12th day with sustained TSA is also calculated, as shown in Table 2. It can be observed that the electricity tariff is $10 533 764. The power utility suffers a revenue loss of $52 428 in a day. Given electricity consumption is evenly distributed in an hour, 5-min time deviation related electricity revenue loss in the 1st day of TSA is around 1/12 of loss $52 428. The tariff loss caused by the time deviation for a 5-min deviation for a day is $4369.

![Fig. 3 Synchronisation disorder in TOU electricity tariff](image-url)

### Table 1 Electricity usage and tariff in a typical day

| Time  | Usage, MWh | TOU, $/MWh | Time  | Usage, MWh | TOU, $/MWh |
|-------|------------|------------|-------|------------|------------|
| 0:00  | 4052       | 48.5       | 12:00 | 4518       | 97.0       |
| 1:00  | 3882       | 48.5       | 13:00 | 4463       | 97.0       |
| 2:00  | 3782       | 48.5       | 14:00 | 4475       | 97.0       |
| 3:00  | 3737       | 48.5       | 15:00 | 4541       | 97.0       |
| 4:00  | 3754       | 48.5       | 16:00 | 4746       | 97.0       |
| 5:00  | 3609       | 48.5       | 17:00 | 5003       | 97.0       |
| 6:00  | 3788       | 48.5       | 18:00 | 5306       | 145.5      |
| 7:00  | 3820       | 97.0       | 19:00 | 5259       | 145.5      |
| 8:00  | 4131       | 97.0       | 20:00 | 5179       | 145.5      |
| 9:00  | 4309       | 145.5      | 21:00 | 5004       | 145.5      |
| 10:00 | 4440       | 145.5      | 22:00 | 4762       | 145.5      |
| 11:00 | 4479       | 145.5      | 23:00 | 4060       | 48.5       |

This is an open access article published by the IET under the Creative Commons Attribution License (http://creativecommons.org/licenses/by/3.0/)
and trip several generators in 2013. Since time jitters above a second (per second) of OXCO is output as PPS to maintain the precision of control function of AMI. Therefore, the time jitter-different from that caused by GPS spoofing-based TSA, specific to the PPS leading edge. Therefore, the time jitter-caused by TSA may not be a serious threat in the real world. The ultimate threat of TSA towards AMI arises from disorder in time synchronisation that could disable meter reading and remote control function of AMI.

4 Time jitter-based TSA detection

Since a variety of interference can affect GPS signal, PPS of GPS receiver has a large random error while no accumulative error. In order to maintain the high precision of PPS of GPS, OXCO with small random error is widely used to identify time jitter of PPS [19]. Once the GPS receiver loses lock to the satellite and the PPS has larger error above a specific threshold, the LPS (local pulses per second) of OXCO is output as PPS to maintain the precision of TSD. The cumulative error of OXCO is available via its LPS (local pulses per second) of OXCO is output as PPS to maintain the precision of TSD. Since error induced by environmental interference could be different from that caused by GPS spoofing-based TSA, specific countermeasures should be developed to defend against GPS spoofing-based TSA. After a GPS receiver decodes and processes the satellite navigation message, it generates PPS with a time interval of 1 s [20] and outputs a standard time and a date code corresponding to the PPS leading edge. Therefore, the time jitter-based TSA detection should be divided into two parts, including time jitter above a second and that below a second.

4.1 Time jitter above a second

Since TSD is employed to provide the time reference with high precision, it is usually supposed that the time jitter induced random error is lower than a second. The detection of time jitter caused error above a second is not mandatorily required since time error above a second is rather rare. That is the reason that TSD of the control centre of Sichuan, China, output time reference of a wrong number of smart meters, meter relays, and meter collectors caused by sustained GPS spoofing-based TSA can be detected and prevented by the system operators in time. Therefore, revenue loss caused by TSA may not be a serious threat in the real world. The ultimate threat of TSA towards AMI arises from disorder in time synchronisation that could disable meter reading and remote control function of AMI.

4.2 Time jitter below a second

The high-precision OCXO used in TSDs is of stable frequency. Typical OCXO frequency stability can be within ±1 ppb to ±10 ppb and its LPS are of extremely small random error [19]. Therefore, OCXO has been employed to identify and compensate random error of PPS of GPS [19]. The diagram to identify and compensate time jitter below a second is shown in Fig. 4. The error per second between LPS of OXCO and phase-locked loop (PLL) and PPS of GPS receiver is estimated by time difference measurement module and stored in the register. If the error per second between PPS and LPS is greater than a threshold, i.e. 0.2 µs, the satellite clock is thought to be of a large random error and the TSDs output LPS of OXCO as standard reference time. Therefore, time jitter of GPS signal-induced time error can be controlled to below 0.2 µs per second.

However, intentional GPS spoofing-based TSA is different from that of random error of the GPS signal. A malicious adversary could implement sustained GPS spoofing-based TSA for a long time, from several hours to several days. Although OCXO is of small random error, its cumulative error escalates with time goes on. The time error of a typical OCXO is around 1 ms a day. That is, once a malicious adversary implements sustained GPS spoofing-based TSA for a day, a TSD that prevents TSA with the aforementioned approach could output time reference with a time error of 1 ms in a day. In 50 Hz power systems, a time error of 1 ms induces a phasor error of 18°, which is much higher than the maximum allowable phase error of 0.57° of IEEE Standard [15]. Once this TSD is utilised for PMUs that are sensitive to time deviation, sustained TSA of a day could induce unallowable error that can cause misleading state estimation. Therefore, the cumulative time error of OCXO should be compensated to mitigate the negative impact of sustained GPS spoofing-based TSA.

The cumulative error of OCXO is available via its countermeasures. Given the daily cumulative error, e.g. 1 ms, distributed evenly on the second order, there is 11.57 ms error per second. The cumulative error of time can be compensated to each second and daily cumulative error of OCXO can be reduced substantially. The process to identify and prevent sustained TSA is shown in Fig. 5, and the steps are as follows:

- The daily cumulative error of the LPS is supposed to be distributed evenly on the second order. The cumulative error of LPS generated by OCXO is compensated in PLL to provide a more precise time reference source.
- The error per second between PPS and LPS is estimated by the time difference measurement module and stored in the register.
- If the error per second between PPS and LPS is >0.2 µs, the satellite clock is thought to be undergoing strong interference in an abnormal state, the TSD output compensated LPS of OCXO as a standard reference time to prevent from sustained GPS spoofing-based TSA.

To conclude, once TSD interprets the received serial message and extracts the date and time stamp, it judges whether there is a time jitter above a second. If so, the TSD output the correct date and time information above a second. Thereafter, it judges whether the

---

Table 2 Revenue with/without GPS spoofing-based TSA

| Time span  | Electricity usage, MWh | Revenue, $/MWh | Revenue, $ |
|------------|------------------------|----------------|------------|
| without TSA |                        |                |            |
| peak       | 38 738                 | 145.5          | 5 636 379  |
| off-peak   | 30 664                 | 48.5           | 1 487 204  |
| standard   | 35 697                 | 97.0           | 3 462 609  |
| overall    | 105 099                | 10 586 192     |            |
| with TSA   |                        |                |            |
| peak       | 38 631                 | 145.5          | 5 620 811  |
| off-peak   | 31 638                 | 48.5           | 1 534 443  |
| standard   | 34 830                 | 97.0           | 3 378 510  |
| overall    | 105 099                | 10 533 764     |            |

---

Fig. 4 Diagram of identification and compensation of time jitter below a second

Since system operators of HES of AMI will check the state of the system in their daily operation, the time deviation of a large number of smart meters, meter relays, and meter collectors caused by sustained GPS spoofing-based TSA can be detected and prevented by the system operators in time. Therefore, revenue loss due to sustained GPS spoofing-based TSA can be detected and controlled. The negative impact of sustained GPS spoofing-based TSA is mitigated by the compensation of time jitter below a second.
Numerical simulation

The proposed approach has been tested on XC7S FPGA, a vivado simulation software from Xilinx. Since the simulation experiment is constrained by computer resources, it is impossible to perform the simulation in a second. Therefore, the signal with a frequency of 100 Hz instead of the second pulse is used in this paper. The simulation lasts for 100 ms. The pulse generator generates a pulse signal every 10 ms with a frequency of 100 Hz instead of PPS. The crystal oscillator clock (100 MHz) is divided by the frequency divider in the PLL to generate LPS, and when the counter in the frequency divider is counted to f4240 H (00000H–f423fH), the time is 10 ms. In order to simulate the error caused by the aging of the crystal oscillator, we added some disturbances, whose characteristics are described in [21].

Using PPS as the reference clock source, the time accuracy of compensated and uncompensated LPS is shown in Fig. 6, which shows the error of the LPS at the time of the simulation time of 10, 20 and 80 ms, respectively. Among them, Figs. 6a, c and e are the simulation diagrams without compensation, and Figs. 6b, d and f are the simulation diagrams after compensation. The blue lines denote the rising edges of LPS and the red lines denote the rising edges of the reference time (PPS). When the PPS is normal, we set the terminal of CPUKZH to ‘0’. In addition, when there is no compensation, the CPU does not send a control signal so that the frequency dividing circuit generates PPS according to the set frequency dividing coefficient. After compensation, the CPU sends a control signal to control the pulse controller to generate the frequency dividing control parameter N to correct the error caused by the OCXO frequency drift.

The results show that the error of LPS without compensation at 10, 20 and 80 ms is 9.053, 14 and 41 ns, respectively (see black marks in the upper right corner of Figs. 6a, c and e), which is consistent with the characteristic that the crystal frequency drift has an overall unidirectional drift tendency. And the error of compensated LPS at 10, 20 and 80 ns is 4.953, 6 and 6.135 ns, respectively (see black marks in the upper right corner of Figs. 6a, c and e). The delay of the compensated LPS waveform at 10, 20 and 80 ms, which are ~4.1, 8 and 34.865 ns, respectively. Since the accumulated time error caused by the crystal oscillator is offset to a certain extent, compared with the case without compensation, the timing accuracy of the compensated LPS is better. Moreover, as time goes on, the cumulative error of compensated LPS does not escalate notably, which shows that the method we proposed can not only effectively detect TSA, but also output a clock signal with a low accumulated error under sustained GPS spoofing-based TSA. This effectively improves the time synchronisation security of the AMI.

Based on the above research, the PPS in the simulation is tested for 1 μs jump by the constructed method to identify whether the 1 PPS is abnormal. Specifically, a PPS signal with large interference of 1.5 μs time jitter is injected with a pulse generator at 90 ms. The simulation results of the PPS and LPS are shown in Fig. 7. The red line denotes the PPS with 1.5 μs time jitter and the blue line denotes the compensated LPS signal. It can be observed that the PPS is of notable time jitter of 1.5 μs at 89.9985 ms since the time jitter is larger than the threshold of 0.2 μs, compensated LPS of OCXO is output for a time reference. Since the cumulative error of LPS has been eliminated at large, the time error remains 17 ns, which is much smaller as compared to the PPS. Moreover, since the cumulative error of OCXO has been compensated, TSD can identify time jitter and help ride through sustained GPS spoofing based TSA by output compensated LPS with a slight cumulative error.

Conclusion

The impacts of GPS spoofing-based TSA on AMI are investigated and a time jitter detection-based approach is proposed in this paper. The conclusion of the paper is as follows:

- GPS spoofing-based TSA could disable the monitoring and control function of AMI via data and command validation mechanism. Moreover, the other distributed system adopting data and command latency validation mechanisms, such as wind power plants, small hydropower plants with remote control could be disabled in a similar way.
- Sustained GPS spoofing-based TSA could result in an electricity revenue loss of power utilities once a large number of smart meters are synchronised to operate with time deviation. Since field operators will check the state of the system every day, the impact of sustained TSA on revenue loss is limited.
- Time jitter detection-based approach is proposed to detect and prevent from GPS spoofing-based TSA of AMI. The results show that our method can not only ensure the clock error of power time synchronisation system is within 0.2 μs/s, but also output a high-precision clock signal that meets the time accuracy requirements of the AMI when the satellite clock is abnormal.
Fig. 6 Time error of LPS with/without compensation at different time
(a) 10 ms, error at the arrival of the jitter edge on the LPS without compensation, (b) 10 ms, error at the arrival of the jitter edge on the LPS with compensation, (c) 20 ms, error at the arrival of the jitter edge on the LPS without compensation, (d) 20 ms, error at the arrival of the jitter edge on the LPS with compensation, (e) 80 ms, error on the arrival of the jitter edge on the LPS without compensation, (f) 80 ms, error at the arrival of the jitter edge on the LPS with compensation.
The proposed time jitter detection-based approach can be employed in the other monitor and control system of power systems to prevent from TSA. However, it cannot meet the demand of some of the time-sensitive systems alone. For example, a sustained GPS spoofing could induce a time deviation of 500 μs, which is unacceptable to WAMS-based applications. The authors are investigating the other ways to defend against sustained GPS spoofing-based TSA for these time-sensitive systems.

7 Acknowledgments

The authors acknowledge the funding support of the Electric Power Research Institute of China Southern Power Grid under grant ZNKJKXM20170085 and the National Natural Scientific Foundation of China under grant nos. 51777015 and U196620027, Hunan Education Department 15A005.

8 References

[1] Gungor, V.C., Sahin, D, Kocak, T., et al.: ‘Smart grid technologies: communication technologies and standards’, IEEE Trans. Ind. Inf., 2011, 7, (4), pp. 529–539
[2] Huang, X., Hu, Y., Ye, C., et al.: ‘Green-RPL: electric load data compression and classification based on deep stacked auto-encoders’, Energies, 2019, 12, (4), p. 653
[3] Halifax Regional Water Commission: ‘AMI technology assessment & feasibility study consolidated report’, 2014 Available at: https://www.halifax.ca/sites/default/files/documents/home-property/water/AMITechnology-FiantReport.pdf
[4] Teng, J.-H., Chao, C.-W., Liu, B.-H., et al.: ‘Communication performance assessment for advanced metering infrastructure’, Energies, 2018, 12, (1), p. 88
[5] Keemink, S., Roos, B.: ‘Security analysis of Dutch smart metering systems’ (University van Amsterdam, Amsterdam, the Netherlands, 2008)
[6] He, Y., Yan, J.: ‘Cyber-physical attacks and defence in the smart grid: a survey’, IET Cyber-Phys. Syst.: Theory Appl., 2016, 1, (1), pp. 13–27
[7] Bhati, J., Humphreys, T.E.: ‘Hostile control of ships via false GPS signals: demonstration and detection’, J. Inst. Navig., 2017, 64, (1), pp. 51–66
[8] 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
[9] 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
[10] 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
[11] Fan, Y., Zhang, Z., Trinkle, M., et al.: ‘A cross-layer defense mechanism against GPS spoofing attacks on PMUs in smart grids’, IEEE Trans. Smart Grid, 2015, 6, (6), pp. 2659–2668
[12] Humphreys, T.E., Ledvina, B.M., Psaki, M.L., et al.: ‘Assessing the spoofing threat: development of a portable gps civilian spoofer’. Proc. of the ION GNSS Int. Technical Meeting of the Satellite Division, Savanna, CA, USA, 2008, vol. 55, p. 56
[13] Huang, L., Yang, Q.: ‘Low cost GPS simulator: GPS spoofing by SDR’, 2015 DEF CON 23
[14] Rivera, E., Baykov, R., Gu, G.: ‘A study on unmanned vehicles and cyber security’, J. Def. Model. Simul.: Appl., Methodol., Technol., 2015, 12, (4), pp. 1–7
[15] ‘IEEE Std, IEEE standard for synchrophasor measurements for power systems, C37.118-2011 (revision of IEEE Std C37.118-2005)’, 2015
[16] 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. of the Institute of Navigation, National Technical Meeting, Anaheim, CA, USA, 2009, vol. 1, pp. 124–130
[17] Levin, P., De Lorenzo, D., Enge, P., et al.: ‘Authenticating a signal based on an unknown component thereof’. U.S. Patent No. 7,969,354 B2, June 2011
[18] Liu, N., Chen, J., Zhu, L., et al.: ‘A key management scheme for secure communications of advanced metering infrastructure in smart grid’, IEEE Trans. Ind. Electron., 2013, 60, (10), pp. 4746–4756
[19] Chun, S.-H., Chen, R., Xiang, B.-W.: ‘Frequency correction method of OCXO and its application in the data acquisition of electrical prospecting’, WSEAS Trans. Circuits Syst., 2015, 14, pp. 68–81
[20] Milaat, F.A., Liu, H.: ‘Decentralized detection of GPS spoofing in vehicular ad hoc networks’, IEEE Commun. Lett., 2018, 22, (6), pp. 1256–1259
[21] Li, Y., Lu, C., Wang, Y., et al.: ‘High-precision synchronous clock algorithm based on Kalman filtering and neural network’, Power Syst. Technol., 2019, 43, (3), pp. 777–784