Vulnerability Analysis of Satellite based Synchronized Smart Grids Monitoring Systems

Alfredo Vaccaro[(1)] , Ahmed F. Zobaa[(2)], Giuseppina Formato[(3)]

[(1)] Dipartimento di Ingegneria, Università degli studi del Sannio, 82100 Benevento Italy, vaccaro@unisannio.it, **corresponding author**

[(2)] Brunel Institute of Power Systems, School of Engineering and Design, Brunel University, Uxbridge, UB8 3PH, Middlesex, United Kingdom

[(3)] Consorzio di Ricerca Sistema ad Agenti -CORISA, Dipartimento di Informatica, Università degli studi di Salerno, 84084 Fisciano (SA) Italy, gformato@corisa.it

Abstract

The large scale deployment of Wide-Area Monitoring Systems (WAMSs) could play a strategic role in supporting the evolution of the traditional power systems towards smarter and self healing grids. The correct operation of these synchronized monitoring systems requires a common and accurate timing reference usually provided by satellite based Global Positioning System (GPS). Although, these satellites signals provide timing accuracy that easily exceeds the needs of the power industry, they are extremely vulnerable to radiofrequency interference. Consequently a comprehensive analysis aimed at identifying their potential vulnerabilities is of paramount importance for a correct and safe WAMSs operation. Armed with such a vision, this paper presents and discusses the results of an experimental analysis aimed at characterising the vulnerability of GPS-based WAMSs to external interferences. The paper outlines the potential strategies that could be adopted to protect GPS receivers from external cyber-attacks and proposes decentralized defense strategies based on self organizing sensor networks aimed at assuring the correct time synchronization in the presence of external attacks.

***Keywords*—Wide Area Monitoring Systems, Phasor Measurement Unit, Global Positioning System, Radio Frequency Interference.**

1. Introduction

The complexity of modern power systems and the rising level of uncertainties in these networks might radically affect the required security and reliability of their operation. This is mainly due to the increasing level of power systems interconnections, that increases their vulnerability with respect to dynamic perturbations, and the constant growth of the electrical energy demand, which leads power components to operate closest to their thermal limits. Further uncertainties in power systems operation are induced by the unpredictable economic dynamics governing the energy market operators and by the increasing pervasion of distributed generation systems that could sensibly raise the number of power transactions.

In this complex scenario, a significant growth of the number of dispersed generators powered by renewable energy sources connected to the electrical systems is expected in the near future [1,2]. This induces a number of side effects that should be properly managed as far as highly variable power injections and voltages profile perturbation are concerned. Finally, it is expected that the operational

environment of future power systems will becoming increasingly rigorous due to continually evolving functions of a power system from operation jurisdiction to control responsibly, coupled with the rising demand and expectation for reliability [3,4].

In facing these problems, the large scale deployment of the Smart Grids (SGs) paradigm has been recognized as the most promising enabling technology.

This emerging paradigm is based on a fusion of pervasive sensor networks, two-way high-speed communications, high scalable computing systems, monitoring software and related data services to get location-specific and real-time actionable data aimed at providing high value services for both system operators and end-users [5,6]. The cornerstone of the SG is the ability of distributed entities to acquire, process, store and share accurate and heterogeneous information. As a consequence, the development of reliable and flexible Wide Area Monitoring Systems (WAMSs) represents a crucial issue in both structuring and operating the SGs [7,8].

WAMSs are based on system-wide data processing aimed at increasing network capacity and minimizing wide-area disturbances. The main SGs applications that may be effectively deployed by a WAMS are [9]:

- System Integrity Protection Schemes;
- Distribution circuits network management;
- Dynamical loading of power equipments;
- System restoration and smart restoration tools;
- Advance warning systems of impending trouble.

WAMSs require accurate phasor and frequency information from multiple time synchronized sensors distributed along the power network [10,11]. Presently, Phasor Measurement Units (PMUs) provide accurate synchronized information about voltage and current phasors, frequency and rate-of-change-of-frequency using a high common accuracy time reference [12].

The adoption of WAMSs based on PMUs could allow the SGs to be operated closer to its stability limits by: *(i)* monitoring in real time the power flows in interconnected areas; *(ii)* identifying the power system dynamics and *(iii)* detecting inter-area oscillations [13,14,15]. As a consequence, the SGs operator could exploit the transmission and generation capacity more efficiently, the renewable power generators can be used more effectively, and the marginal cost of power generation can be reduced [16,17].

Anyway, to realize these benefits, several open problems need to be addressed.

In particular, the correct operation of PMUs requires a common and accurate timing signal that should be generated by a reliable synchronizing source and referenced to the Coordinated Universal Time [18,19]. This signal must be available without interruption at all PMUs locations and it should satisfy specific requirements in terms of availability and reliability. Moreover, it should be accurate enough to allow the

PMUs to be synchronized with an accuracy suitable to keep the Total Vector Error[1] within one percent [20]. To address these needs, satellite-based timing signals are frequently adopted. These signals provide global absolute time reference which is characterized by a global coverage and an extremely high timing accuracy [21,22]. On the other hand, they greatly rely on information transfer over air communications media. This wireless nature of communications links and the weak power levels of satellite signals make them vulnerable to radiofrequency interference. As a consequence, any electromagnetic radiation source emitting radio signals in the satellite signals frequency bands could affect the correct PMUs synchronization and, consequently, the overall WAMS operation [23]. The occurrence of this kind of disruption mechanism could be not infrequent in future SGs which are considered strategic infrastructures potentially vulnerable to cyber attacks and external interference [24].

Consequently a comprehensive analysis aimed at identifying the potential satellite-based PMUs' vulnerabilities and the main strategies that could be adopted to protect the satellite receivers from external RFI attacks is of paramount importance for a correct and safe SGs operation.

In addressing these needs, this paper presents the results of an experimental analysis aimed at characterizing the vulnerability of a GPS-based PMU to external RFI external cyber attacks. The PMU adopted in this study is the SEL 421 equipped by a high performance GPS receiver. This is an advanced protection, automation, and control system for high-speed distance and directional protection developed by Schweitzer Engineering Laboratories. Several attack scenarios were simulated, and the impact on the PMU operation have been assessed. Starting from these results, the paper analyzes the main strategies that could be adopted to protect GPS receivers from RFI attacks and explores the possibility of decentralizing the WAMS synchronization functions on a network of interactive PMUs equipped by distributed consensus protocols [25]. This decentralized synchronization paradigm could be activated in the case of a GPS unavailability since it doesn't require neither explicit point-to-point message passing nor routing protocols. It spreads information across the wide area communication network by updating each PMU timing signal by a weighted average of its neighbors. Thanks to this feature the PMUs can synchronize their local acquisitions without the need for a synchronization infrastructure.

2. Elements of Synchronized SGs Monitoring

Recent advances in Information and Communications Technology are leading to significant enhancements in the context of synchronized and wide area SGs monitoring. A wide spectrum of advanced technologies and methodologies will support the evolution of traditional monitoring frameworks toward self healing and

[1] It is the magnitude of the vector difference between the phasor estimated by the PMU and its theoretical value expressed in percentage of the theoretical value.

self organizing architectures composed by distributed and cooperative entities. In this domain the large scale deployment of WAMSs has been recognized as one of the most promising enabling technology.

WAMSs integrate pervasive sensor networks, advanced data processing tools and wide area communication systems. They aim at enhancing the conventional functions of existing Supervisory Control and Data Acquisition systems by enabling real-time wide area situational awareness [26]. This is obtained by acquiring and processing synchronized measurements aimed at classifying the current SG operation state and detecting incipient faults [27]. To this aim, WAMSs require reliable and accurate phasor and frequency measurements from a proper number of power system buses. This can be obtained by deploying a network of time synchronized PMUs aimed at measuring the voltage phasor (magnitude and phase) at the installed buses and the current phasors in all the branches incident to these buses [19]. These phasor information are collected by the PMUs, forwarded to the phasor data concentrators and transmitted to the monitoring centre. At this level the data processing and storage applications can be run directly. These applications depend by the number and locations of the PMUs and in particular:

- If a limited number of PMUs are available, WAMS data processing can only partially describe the SG operation state. In this case the typical applications include:
    - Voltage stability monitoring for transmission corridors;
    - FACTS control using feedback from remote PMU measurements.
- On the contrary, more advanced applications based on a detailed network model view can be implemented including[2] [28]:
    - Loadability calculation based on OPF studies;
    - Topology detection and state estimation;
    - Distribution circuits network management;
    - System restoration and smart restoration tools;
    - Advance warning systems of impending trouble.

  These applications allow the WAMSs to evolve toward the so called Wide Area Measurements Protective and Control Systems (WAMPACs).

To implement these functions PMUs require a common and accurate timing reference determining the instant at which the waveforms of the buses voltages and currents are sampled. This may be obtained by synchronising the PMUs clocks to the coordinated universal time by a common timing reference. The latter should be available without interruption at all measurement locations and characterised by a degree of availability, reliability, and accuracy satisfying proper requirements [19].

To address these needs the employment of Satellite based timing signals has been widely adopted for

[2] It is worth nothing that each specific WAMS application requires that a proper number of PMUs are strategically located into the SG.

PMUs synchronization. The main benefits arising by the application of the Satellite technology is that it does not require the deployment of primary time and time dissemination systems assuring, at the same time, a set of intrinsic advantages as far as wide area coverage, easy access to remote sites and adaptable to changing network patterns are concerned.

On the other hand, Satellite-based synchronization signals rely on information transfer over air communications media which makes them vulnerable to both intentional and unintentional radiofrequency interference. Any electromagnetic radiation source can act as an interference source if it can emit potential radio signals in the satellite signals frequency bands [19].

Consequently the research for reliable and effective synchronization techniques aimed at providing redundant PMUs timing signals is of paramount importance for a correct and safe WAMS operation. These "back-up systems" come into effect in the case of a GPS unavailability providing a more reliable timing source. Furthermore, if one signal is degraded or unavailable, the PMU should still operate within overall system requirements.

3. Vulnerability Analysis of Satellite based WAMSs

The deployment of satellite-based timing signals has been widely explored in wide area synchronized monitoring. Many technologies are currently available for WAMSs synchronization; the most common is based on GPS signal processing. GPS is based on a constellation of 24 satellites and it is steered by a ground-based cesium clock ensemble that itself is referenced to UTC. Each GPS satellite is identified by the PRN code it transmits and broadcasts a spread-spectrum waveform on two carrier frequencies at 1575.42 MHz and 1227.6 MHz providing a correction to UTC time that the receiver automatically applies to the outputs [22]. Thanks to this continuous adjustment, the timing accuracy is limited only by short-term signal reception whose basic accuracy is 0.2 microseconds. The inherent availability, redundancy, reliability, and accuracy make GPS signal processing a technological solution well suited for synchronized WAMSs [20,21].

A further technological option potentially suitable for synchronized SGs monitoring is represented by the INMARSAT system satellites. They will carry a GPS-like transponder broadcasting signals that will be similar to existing GPS transmissions. As a consequence, it can be used with slightly modified GPS receivers.

The European Space Agency (ESA) GALILEO system is the third global satellite time and navigation system to come on line. It comprises a constellation of 30 satellites divided among three circular orbits at an altitude of 23222 km to cover the Earth's entire surface. Galileo will have an integrity signal to ensure the quality of the signals received and to inform the user immediately of any error. The GALILEO time

precision in terms of time errors (95% confidence) for different signals range from 0.7-8.1 ns [29].

Although these satellite based synchronization technologies provide timing accuracy that easily exceeds the needs of the power industry, they can be vulnerable to both intentional or unintentional interferences that could hinder the correct operation of the WAMS. In details, the disruption mechanisms that could trigger these phenomena can be classified as:

- Ionospheric effects: the sunspot activity causes an increase in the solar flux, charged particles and electromagnetic rays emitted from the Sun. This natural process could sensibly affect the transit time of satellite signals through the ionosphere. As a consequence, the satellite receiver of the PMU may experience degraded performance in tracking of the satellites due to scintillations, rapidly varying amplitude and phase of the satellite signal. The equatorial and high latitude regions are most severely affected by this increased ionospheric activity [30,31].
- Unintentional Interference: since satellite signals travel through the upper regions of earth's atmosphere, they can be influenced by solar disturbances. In addition, when there will be restricted lines of sight to satellites (as for example in urban areas or near foliage) the overall quality of the synchronization signal could sensibly deteriorate for short or long term. In this case, it is important to have a reliable estimation of the timing signals availability [31].
- Radio Frequency Interference: any electronic equipment radiating in the satellites frequency band represents a potential source of interference. Although transmitter equipments are designed to not interfere with the wireless telecommunication signals, they can radiate at the same frequency as the satellite signals if they are faulty or badly operated. These interferences, if powerful enough, lead the satellite receiver of the PMU to badly receive the timing signals [30].
- Intentional Interference: satellite based timing signals are extremely weak and they can be deliberately jammed by radio interference. The occurrence of this event could be not infrequent in future SGs which are considered strategic infrastructures potentially exposed to external attacks.

In the authors opinion, intentional interference represents one of the most serious problems to address amongst these disruption mechanisms. This kind of cyber attack has not so far explored in the WAMSs literature although its consequences could be very dramatic for the overall SG operation. In fact, all the main WAMS functions could be seriously compromised if the installed PMUs lose their synchronization signals. PMUs flag the time synchronization conditions to disable the protection and control systems. A comprehensive analysis of the potential cyber attack scenarios is therefore essential in order to try and reduce this risk.

4. Experimental Studies

This section presents the results of an intensive experimental activity aimed at characterising the potential

vulnerabilities of a satellite based PMU to external jamming signals. The test set-up adopted in our experiments is schematically depicted in fig.1. The device under test is the SEL 421. The PMU has been interfaced with a Human Machine Interface computer and synchronized by a high performance Satellite-Synchronized time source. To this aim a SEL 2407 equipped by an active bullet antenna (5 V 40 dB gain) has been adopted. This device generates demodulated IRIG-B outputs with ±100 ns accuracy meeting the requirements for precise-timing applications and exceeding the IEEE C37.90 and IEC 60255 protective relay standards.

In order to analyze the signal received by the GPS antenna, a DC blocking splitter has been adopted. It allows us to divide the GPS signal in two signal paths.

The first signal path is sent directly to the satellite-synchronized clock. This signal allows the satellite-synchronized clock to power the antenna. The second signal path is processed by a GPS amplifier and sent to a spectrum analyzer (namely, the Rohde&Schwarz FSP30). This signal is connected to the DC block port of the power splitter combiner.

The external cyber-attacks have been generated by a vector signal generator (namely, the Rohde&Schwarz SMIQ03B) equipped by a broadband disturbance antenna (namely, the Rohde&Schwarz HL040). The disturbance antenna has been located 5 meters from the GPS antenna. The main features characterising the RF components have been summarised in table I.

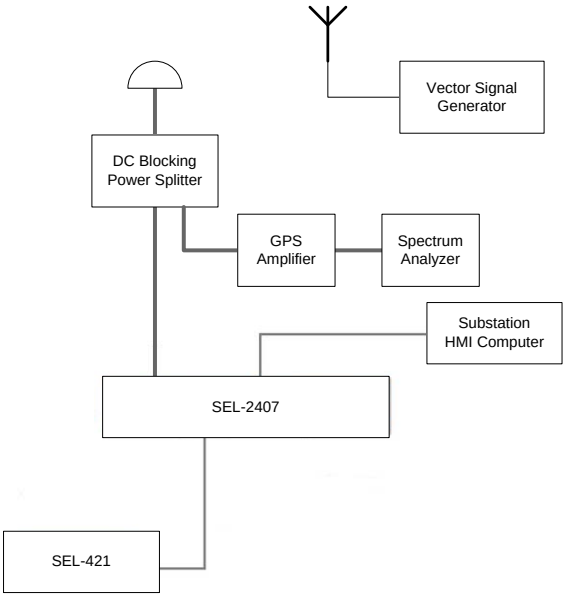

Fig.1: The experimental setup

The first experimental activity aimed at characterising the actual signal received by the satellite-synchronized time source without any external perturbations. The measured GPS signal spectrum in the L1 band is reported in fig.2.

The spectrum analyzer measured the noise floor at about -80 dBm with a 30 kHz RBW. The measured

signal spectral hump is about 5 dBm.

These data are consistent with those obtained in similar experiments reported in the satellite literature [32]. They demonstrate the good level of the GPS signal received by the satellite-synchronized time source.

Table I: Main features of the RF components

DC Blocking RF Splitter Combiner	
Frequency Range	700 - 2700 MHz
Impedance	50 OHMS
Insertion Loss (max):	0.4 dB (ABOVE 3.01 dB SPLIT)
Amplitude Balance (max):	0.2 dB
Phase Balance (max):	3 Degrees
VSWR (max):	1.20 : 1 (IN), 1.20 : 1 (OUT)
GPS Amplifier	
Frequency Range	1200-1600 MHz
Gain	32 dB
Noise Figure	0.95 dB
OIP3	31 dBm
P1dB	17 dBm
VSWR	1.5:1 (IN), 1.9:1 (OUT)
Disturbance Antenna	
Frequency Range	400 MHz to 3.6 GHz
Polarization	Linear
Input impedance	50 Ω
VSWR	<2.5, typ. <2.0
Max. input power	150 W to 50 W CW
Gain	5 dBi to 7 dBi

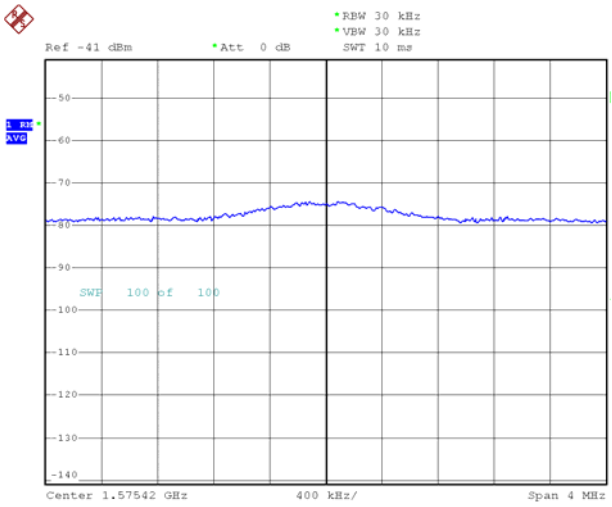

Fig.2: The GPS signal spectrum processed by the Satellite-Synchronized time source without any external perturbation.

To assess the impact of external cyber-attacks on the PMU synchronization, further experiments were conducted. To this aim, we considered several attack scenarios. In the first one we generated a sinusoidal jamming signal and we checked the impact of this disturbance on the PMU synchronization for several signal frequencies and power. The obtained results are summarised in fig. 3 and 4. In details, Fig. 3 shows the spectrum of the signal processed by the satellite-synchronized time source in the presence of a sinusoidal jamming signal. The corresponding impacts of the sinusoidal jamming signal on the PMU synchronization for different frequency and power values are reported in fig. 4.

Analysing these data it is worth observing that the PMU only lost its synchronization during the 4th attack

(characterized by a signal frequency of 1576.2 MHz and a signal power of -40 dBm) and the 5th attack (characterised by a signal frequency of 1576 MHz and a signal power of -26 dBm)[3].

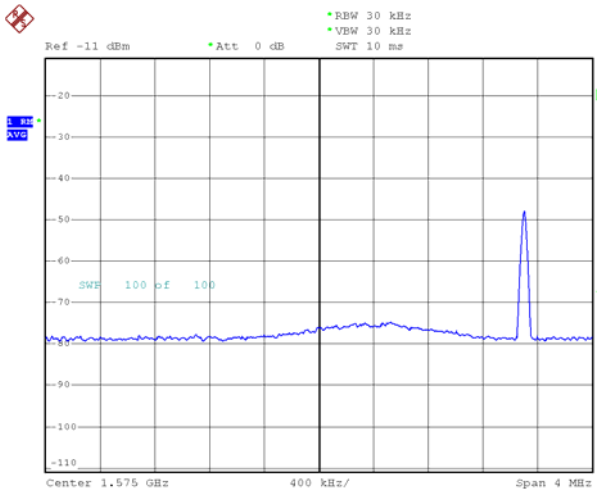

Fig.3: The GPS signal spectrum processed by the Satellite-Synchronized time source in the presence of a sinusoidal Jamming signal

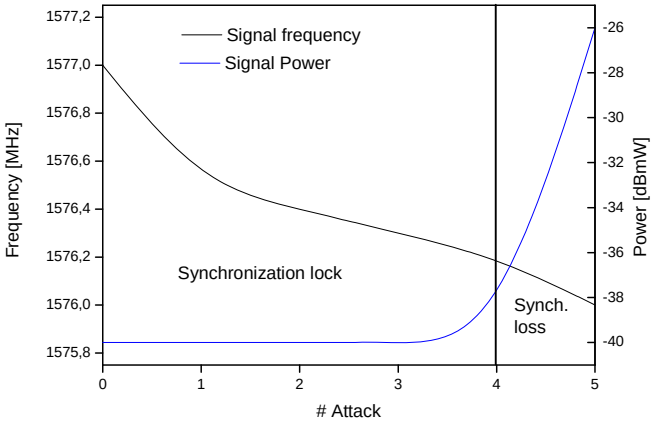

Fig.4: Impact of a sinusoidal jamming signal on the PMU synchronization

In the second attack scenario, the effect of a digital jamming signal on the PMU synchronization has been assessed. In particular the jamming signal adopted in this experiment is characterized by a carrier frequency of 1575 MHz (L1 band) modulated by a Binary Phase Shift Keying (BPSK) code. The effect of this disturbance on the PMU synchronization has been experimentally assessed. The obtained results are summarized in fig. 5 and 6. In particular, fig.5 shows the spectrum of the signal processed by the satellite-synchronized time source in the presence of the BPSK jamming signal while fig.6 shows the impacts of the BPSK jamming signal on the PMU synchronization for different signal powers.

By analyzing these data it is important to emphasize that the PMU lost synchronization only during the first attack (characterized by a jamming signal power of -40 dBm). Therefore, we can argue that this value

[3] It is important to emphasize that -40 dBm corresponds to a signal power of about 100nW.

represents the lower power threshold for a modulated jamming signal in the L1 band.

This conclusion has been also confirmed by further experimental results obtained by using different modulation techniques.

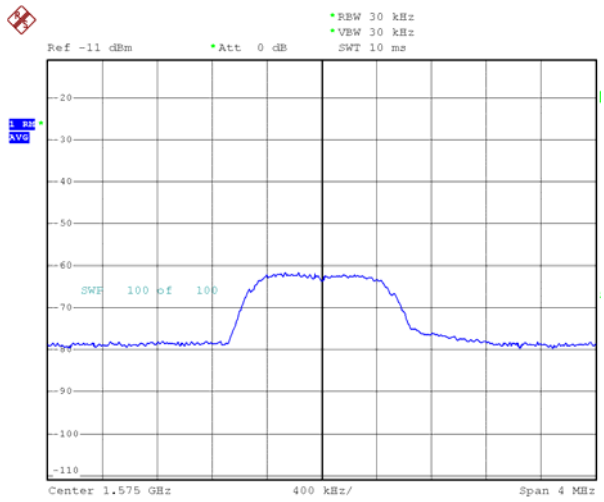

Fig. 5: The GPS signal spectrum processed by the Satellite-Synchronized time source in the presence of a BPSK Jamming signal

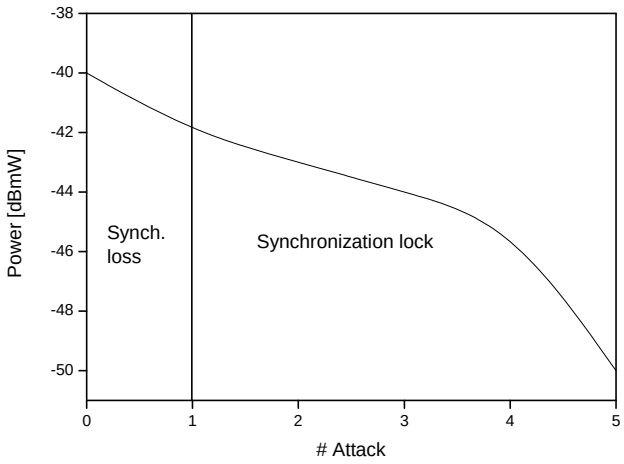

Fig.6: Impact of a BPSK jamming signal on PMU synchronization

5. Possible Countermeasures Against External Attacks

The defense strategies that could be adopted to protect satellite-based WAMSs from cyber-attacks are based on the general principle of raising the power levels required by the jammers to interfere with the receivers. The latter makes the cyber-attack unsustainable in terms of the energy required to run, or easily detectable.

To implement this defense paradigm several mitigation techniques could be deployed. They include [19]:

– The employment of a “Controlled Reception Pattern Antenna” aimed at determining the direction of the attack source and modifying its reception pattern to filter signals received from that

direction;

- The implementation of a narrowband interference processing aimed at measuring the frequency of the attack signal and then ignore it. This technique only works well when the frequency band of the attack signal is much narrower than that of the satellite signal;
- The adoption of a jamming signal to thermal noise 'powermeter' that measures the total amount of power received by the antenna. Based on the amount of power expected from thermal noise, it estimates the amount of received jamming power. In this way, the receiver can monitor the likelihood of becoming jammed and inform the user of its reliability [23].

Other mitigation paradigms consist in physically shielding the satellite receiver's antenna from interference sources. These approaches may be useful only under some circumstances since they require a-priori knowledge of the attack source location.

Further countermeasures are based on the redundancy of the synchronization source. In this context the employment of local oscillators (i.e. quartz or rubidium oscillators) and/or multiple (complementary) timing signals have been proposed as possible solution strategies [33,34]. These "back-up systems" come into effect in the case of signals unavailability providing a more reliable timing source. Furthermore, if one signal is degraded, the receiver should still operate within overall system requirements. A promising solution in this field is the ensemble time base generation, in which various weighting factors based upon the predicted or measured accuracy and stability of various different time sources are taken into account to provide a disciplined time scale generator.

Anyway, in the author opinions, the identification for more effective strategies aimed at reducing the vulnerability of satellite based WAMSs to external attacks in a SGs context is still embryonic and needs both theoretical and practical improvements. In this domain, the most promising enabling technologies include [35]:

- The conceptualization of decentralized paradigms aimed at distributing the synchronization function at PMUs level;
- The deployment of pervasive communication networks aimed at allowing PMUs to communicate with remote centers, with other PMUs and with all the systems at substation level.

These technologies suggest a shift towards decentralized and self healing synchronizing architectures for WAMSs. In addressing this need the large scale deployment of cooperative and self organizing smart sensor networks could play a strategic role.

6. Toward a Self Healing Synchronized Architecture

The recent advances in bio-inspired computing and self organizing sensor networks have opened the door

for reliable and cost effective technologies for decentralized information processing and data analysis. This is mainly due to broad application of distributed decision making in coordinating networks of dynamic agents aimed at enhancing operational effectiveness in networked autonomous systems [25].

Armed with such a vision in this section we explore the possibility of decentralizing the WAMS synchronization functions on a network of interactive PMUs equipped by distributed consensus protocols [25]. The idea is to start from the information spreading theory for coordinating a networks of cooperative smart PMUs [36,37]. The synchronized functions are executed by equipping each PMU by a dynamical system (oscillator) initialized by local information. The oscillators of nearby PMU are mutually coupled by proper local coupling strategies derived from the mathematics of populations of mutually coupled oscillators [38]. This bio-inspired paradigm allows all the PMU to reach consensus on general functions of the variables sensed by all the PMUs. Thanks to this feature, the local sensor acquisitions can be time synchronized and each PMU can compute the most important variables characterizing the global power grid operation without the need for a fusion centre.

In details we assumed that the local clock of the $i-th$ PMU is described by the following linear equation:

$$\tau_i(t) = \alpha_i t + \beta_i \quad (1)$$

Where τ_i is the value of the local clock while α_i and β_i are the skew and offset coefficients respectively. Since the value of the reference time is not available at the $i-th$ PMU, it is not possible to directly compute these coefficients.

To address this issue we focused on the Average Time Syncronization protocols (ATS) [39], which are a class of distributed algorithms based on the average consensus theory.

The idea is to extract indirect information on the unknown clock parameters of the $i-th$ PMU by measuring the time offsets with its neighbors and to synchronize all the PMUs to the following virtual reference clock:

$$\tau_v(t) = \alpha_v t + \beta_v (2)$$

According to this paradigm, each PMU tries to estimate the unknown clock parameters by a linear regression of its local clock:

$$\hat{\tau}_i(t) = \hat{\alpha}_i t + \hat{\beta}_i (3)$$

Where $\hat{\alpha}_i$ and $\hat{\beta}_i$ are the skew and the offset estimation respectively. These parameters are estimated by a local exchange of information between the PMUs according to distributed consensus protocols [31,39]. In particular, when the dynamical systems synchronize, all PMUs will have a common global reference time, namely:

$$\lim_{t\to\infty} \hat{\tau}_i = \tau_v i = 1,..., N \quad (4)$$

and, by observing that:

$$\hat{\tau}_i(t) = \hat{\alpha}_i \alpha_i t + \hat{\alpha}_i \beta_i + \hat{\beta}_i \quad (5)$$

It results:

$$\lim_{t\to\infty} \hat{\alpha}_i \alpha_i = \alpha_v \quad (6)$$

$$\lim_{t\to\infty} \hat{\alpha}_i \beta_i + \hat{\beta}_i = \beta_v \quad (7)$$

These equations demonstrate as the PMUs can be time synchronized by adapting their clocks according to local coupling strategies without the need for any cluster header. When this network of coupled oscillator clocks synchronize, then each clock will show the same value, without changing the value once reached. Thanks to this feature, the built in PMUs oscillators are able to lock to a common phase, despite the differences in the frequencies of the individual clocks.

This decentralized paradigm raises the synchronization redundancy by assuring the time synchronization of the PMUs also in the case of an unavailability of the primary timing signals.

Intense experimental activities aimed at characterizing the actual performances of this solution on real power networks are currently under development by the authors.

7. Conclusions

The correct operation of synchronized WAMS requires a common and accurate timing reference. This is typically obtained by equipping the remote PMUs by a satellite based synchronization system. Although this technological solution provides timing accuracy that exceeds the needs of the power industry, it is extremely vulnerable to radiofrequency interferences.

Amongst the possible disruption mechanisms that could threaten the correct operation of satellite based systems for WAMSs synchronization, the intentional cyber attack represents one of the most serious problems to address.

This paper presented an experimental analysis aimed at characterizing the potential attack scenarios and the main vulnerabilities of a satellite based PMU to jamming signals. The obtained results have shown that the proper frequency, power and shape of the jamming signal could lead the PMU to lose its synchronization. If this event is not properly managed, it could compromise the correct operation of the overall WAMS. To avoid or mitigate this risk it is necessary to adopt suitable strategies aimed at raising the power levels required by the jammer signal to compromise the correct system operation. This requirement makes the attack too expensive, unsustainable in terms of the power required, and easily detectable and therefore readily intercepted. In this scenario the deployment of decentralized and self

healing synchronization architectures based on cooperative sensor networks represents one of the most promising research direction aimed at reducing the vulnerability of satellite based WAMSs to external cyber-attacks.

8. References

[1] Chun-Xia Dou, Dong-Le Liu, Xing-Bei Jia & Fang Zhao, "Management and Control for Smart Microgrid Based on Hybrid Control Theory" Electric Power Components and Systems, Volume 39, Issue 8, April 2011, pages 813-832

[2] A.F. Zobaa, M.M. Abdel Aziz, S.H.E. Abdel Aleem, "Comparison of shunt-passive and series-passive filters for DC drive loads" Electric Power Components and Systems, Volume 38, Issue 3, January 2010, pages 275-291

[3] V.Madani, R.L.King "Strategies to meet grid challenges for safety and reliability" International Journal of Reliability and Safety, Volume 2, Number 1-2/2008

[4] R. El Ramli, M. Awad & R. A. Jabr, "Ordinal Optimization for Dynamic Network Reconfiguration" Electric Power Components and Systems, Volume 39, Issue 16, October 2011, pages 1845-1857

[5] A.Vaccaro, M. Popov, D.Villacci, V. Terzija, "An Integrated Framework for Microgrids Modeling, Control, Communication and Verification" Invited Paper - IEEE Proceedings Vol.99 Issue 1, pp. 119-132, Jan. 2011

[6] C. Cecati, C. Citro, and P. Siano, "Combined operations of renewable energy systems and responsive demand in a smart grid," IEEE Trans. Sustainable Energy, vol. 2, no. 4, pp. 468–476, Oct. 2011

[7] N. Moaddabi & G. B. Gharehpetian, "Wide-area Method for Self-healing of Smart Grids in Unstable Oscillations" Electric Power Components and Systems, Volume 41, Issue 4, February 2013, pages 365-382

[8] N. Moaddabi, S. H. Hosseinian & G. B. Gharehpetian, "Practical Framework for Self-healing of Smart Grids in Stable/Unstable Power Swing Conditions", Electric Power Components and Systems, Volume 40, Issue 6, March 2012, pages 575-596

[9] V.Madani, A.Vaccaro,D.Villacci, R.L.King, "Satellite Based Communication Network for Large Scale Power System" 2007 iREP Symposium- Bulk Power System Dynamics and Control - VII, Revitalizing Operational Reliability, August 19-24, 2007, Charleston, SC, USA

[10] T.J. Browne, G.T. Heydt, J.W. Stahlhut, W.T. Jewell, "Innovative and emerging concepts in power system instrumentation" Electric Power Components and Systems, Volume 37, Issue 4, March 2009, pages 403-414

[11] Y. Hu, V. Madani, R. Morales, D. Novosel, "Requirements of Large-Scale Wide Area Monitoring, Protection and Control Systems"; Georgia Tech. Conference, (2007).

[12] B. Dickerson "Substation Time Synchronization" Protection, Automation and Control World - Summer 2007. pp.39-45

[13] A.R. Phadke, M. Fozdar, K.R. Niazi "Robust tuning of fixed-parameter static VAR compensator controller for damping inter-area oscillations in power system" Electric Power Components and Systems, Volume 38, Issue 8, May 2010, pages 974-995

[14] H.H. Zeineldin, A. Saif, M.M.A. Salama, A.F. Zobaa "Three-dimensional non-detection zone for assessing anti-islanding detection schemes" Electric Power Components and Systems, Volume 38, Issue 6, April 2010, pages 621-636

[15] M. Hojjat, D.B.M.H. Javidi, "Probabilistic congestion management considering power system uncertainties using chance-constrained programming" Electric Power Components and Systems, Volume 41, Issue 10, June 2013, pages 972-989

[16] S. Pahwa, C. Scoglio, S. Das & N. Schulz, "Load-shedding Strategies for Preventing Cascading Failures in Power Grid" Electric Power Components and Systems, Volume 41, Issue 9, July 2013, pages 879-895

[17] P. Siano, C. Cecati, H. Yu, and J. Kolbusz, "Real time operation of 784 smart grids via FCN networks and optimal power flow," IEEE Trans. Ind. 785 Informatacis, vol. 8, no. 4, pp. 944–952, Nov. 2012

[18] K. Behrendt, K. Fodero, "The Perfect Time: An Examination of Time Synchronization Techniques" Proc. of the Distributech 06, Feb. 7-9, 2006 - Tampa, Florida

[19] North American SynchroPhasor Initiative (NASPI)-Performance & Standards Task Team (PSTT), " Guidelines for Synchronization Techniques Accuracy and Availability", 2009

[20] IEEE Std C37.118-2005" IEEE Standard for Synchrophasors for Power Systems"

[21] K. E. Holbert, G. T. Heydt, H. Ni, "Use of Satellite Technologies for Power System Measurements, Command, and Control" Proc. of the IEEE 93(5), pp.947-855

[22] M. A. Lombardi, L.M. Nelson, A. N. Novick, V. S. Zhang "Time and Frequency Measurements Using the Global Positioning System" The International Journal of Metrology , July-September 2001, pp. 26-33

[23] The Trusted Information Sharing Network (TISN), "GPS Vulnerability: Information for CIOs" Publications on Critical Infrastructure Protection. Available [Online]: http://www.tisn.gov.au

[24] Y. Yang, T. Littler, S. Sezer, K. McLaughlin, H.F. Wang, "Impact of cyber-security issues on Smart Grid" 2011 2nd IEEE PES International Conference and Exhibition on Innovative Smart Grid Technologies (ISGT Europe), 5-7 Dec. 2011, Manchester (UK)

[25] A. Iacoviello, V. Loia, A. Pietrosanto, A.Vaccaro," Decentralized Consensus Protocols: the enabler for Smarter Grids Monitoring" proc. of the 27th IEEE International Conference on Advanced Information Networking and Applications (AINA-2013) Barcelona, Spain, March 25 - 28, 2013

[26] J. Hauer and J. DeSteese, "Descriptive model of a generic WAMS." Pacific Northwest National Laboratory, June 2007.

[27] V.Terzija, D.Cai, G.Valverde, P.Regulski, A.Vaccaro, M.Osborne, J.Fitch, "Flexible Wide Area Monitoring, Protection and Control Applications in Future Power Networks" The 10th Institution of Engineering and Technology Conference on Developments in Power System Protection DPSP 2010 29 March – 1 April 2010 | The Hilton Deansgate, Manchester,UK

[28] M. Larsson, R. Gardner, and C. Rehtanz, "Interactive simulationand visualization of wide-area monitoring and control applications," Proc. Power Systems Computation Conf, 2005.

[29] P. Mack, F. Capitanescu, M. Glavic, F. Legrand, L. Wehenkel "Application of the Galileo System for a Better Synchronization of Electrical Power Systems" Proc. IEEE Power Tech Conference, Lausanne, July 2007 – 2007

[30] O. Orpen, H. Zwaan "Dual Frequency DGPS Service for Combating Ionospheric Interference" The Journal of Navigation Vol. 54, Nr. 1, pp. 29,36.

[31] Volpe (2001), "Vulnerability assessment of the transportation infrastructure relying on the Global Positioning System (The Volpe report)" John A. Volpe National Transportation System Center. Washington.

[32] Var Rosenbaum, G."Determination of GPS RF signal strengths" 2008 IEEE/ION Position, Location and Navigation Symposium, 5-8 May 2008 pp. 449 – 458, Monterey, CA

[33] A. Dion, V. Calmettes, E. Boutillon, "Reconfigurable GPS-Galileo receiver for satellite based applications" proc. of ION GNSS 2007 : Institute Of Navigation, Global Navigation Satellite Systems Meeting, 27-28 Sep 2007, Fort Worth, Texas, USA.

[34] T. Celano, K. Carroll, C. Biggs, M. Lombardi, "COMMON-VIEW LORAN-C AS A BACKUP TO GPS FOR PRECISE TIME RECOVERY" 35th Annual Precise Time and Time Interval (PTTI) Meeting

[35] A.G. Phadke, J.S. Thorp, "Communication needs for Wide Area Measurement Application" Critical Infrastructure (CRIS) 5th International Conference, Sep 2010

[36] A. Vaccaro, G. Velotto, A. F. Zobaa, "A Decentralized and Cooperative Architecture for Optimal Voltage Regulation in Smart Grids" IEEE trans. on Industrial Electronics, Vol.58 (10), pp. 4593-4602, October 2011

[37] S. Ullo, A. Vaccaro, G. Velotto "The Role of Pervasive and Cooperative Sensor Networks in Smart Grids Communication" MELECON 2010, The 15th IEEE Mediterranean Electrotechnical Conference,25th – 28th April 2010, MALTA.

[38] S. Barbarossa, G. Scutari, "Decentralized Maximum Likelihood Estimation for Sensor Networks Composed of Nonlinearly Coupled Dynamical Systems" IEEE Trans. on Signal Processing, Vol. 55(7), pp. 3456-3470, July 2007

[39] L. Schenato and G. Gamba, "A distributed consensus protocol for clock synchronization in wireless sensor network," in Proc. 46th IEEE Conf. Decis.Control, New Orleans, LA, Dec. 2007, pp. 2289–2294.