20th IMEKO TC4 International Symposium and
18th International Workshop on ADC Modelling and Testing
Research on Electric and Electronic Measurement for the Economic Upturn
Benevento, Italy, September 15-17, 2014

The Impact of GPS Vulnerabilities on the Electric Power Grid

Bernhard Baumgartner[1], Christian Riesch[2], Wolfgang Schenk[3]

[1,2,3] OMICRON electronics GmbH, Oberes Ried 1, 6833 Klaus, Austria
[1] bernhard.baumgartner@omicron.at, [2] christian.riesch@omicron.at, [3] wolgang.schenk@omicron.at

***Abstract* – The failure of time references can result in operational distortions of power plants or substations. Rumours say that simply a truck, illegally equipped with a GPS jammer to camouflage its position, parking outside a substation can cause GPS failure in the substation. Is this really true? How vulnerable are today's GPS synchronized time references? And what are the consequences of short term to long term GPS reception losses? In this paper the authors address these questions for different time synchronisation infrastructures and applications in the power industry. The paper concludes with an assessment of possible countermeasures against GPS Jamming and GPS Spoofing.**

I. INTRODUCTION

When accurate absolute time information is needed, GPS offers an effective and accurate method to obtain precise UTC[1] synchronized time nearly everywhere on the planet. The time accuracy of modern high quality GPS disciplined time references is well within < ±100 ns in comparison to UTC. Nowadays, GPS is widely used as a primary time source for master clocks or station clocks in the electric power industry. The time reference signals provided by these clocks are used to synchronize Intelligent Electronic Devices (IEDs) such as protection relays, fault recorders or Phasor Measurement Units (PMUs) in IEC 61850 [1] infrastructures.

II. TIME SYNCHRONIZATION IN A SMART SUBSTATION

Before discussing the impact of potential GPS vulnerabilities on the secure operation of power utilities it is helpful to understand what technical and regulatory requirements apply to time synchronized measurements and time stamping of data in the modern power grid.
With the adoption of the NERC[2] Standard PRC-018-1 [2] in 2006 it is now a legal obligation that all recorded data in North America must have an accuracy of 2 ms or better in relation to UTC. Such time accuracy is relatively easy to reach, but current and emerging future measurements like sampled values or synchrophasors require an absolute accuracy of 1 µs or better [3]. In the IEC 61850-9-5 the time accuracy requirements for time tagging of events and time synchronized measurements are summarized in five time performance classes which range from 1 ms to 1 µs. [1]
In order to time synchronize all devices involved in the processes and measurements mentioned above, usually GPS disciplined time references, commonly called substation clocks, are used. To ensure that all time synchronized IEDs operate within the accuracy defined by the applicable time performance class, time reference signals are distributed throughout the substation. As shown in Fig. 1 this can happen via a separate time synchronisation network or via the station communication network. In addition, some IEDs can be equipped with their own GPS clocks.

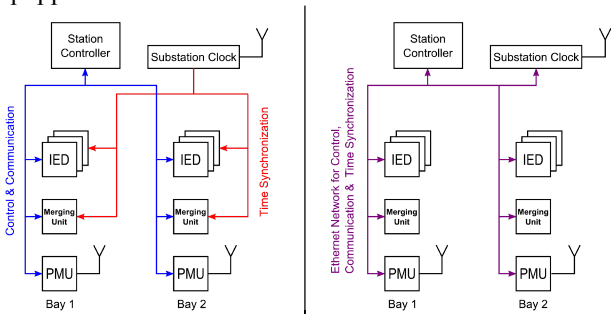

Fig. 1 Time distribution infrastructures in substations

III. SECURITY AND AVAILABILITY OF GPS SIGNALS

When the security and availability of GPS signals is discussed, it is important to distinguish between general GPS reception issues and dedicated man-made attacks like GPS Jamming and GPS Spoofing. This paper focuses only on threats resulting from man-made attacks.

A. GPS Jamming

GPS jammers are devices used to intentionally disturb the reception of GPS signals. This is done by the transmission of a noise signal in one or more of the GPS frequency bands. Studies show that the use of GPS jammers is becoming more common. One recent study on

[1] UTC … Universal Coordinated Time Scale
[2] North American Electric Reliability Cooperation

ISBN-14: 978-92-990073-2-7

GPS vulnerabilities was the "Sentinel Project." Its final report was published 4 April 2014 and documents thousands of jamming events recorded in the UK throughout the past two years. [4]

To find the real jamming range of commercially available GPS jamming devices the equipment described in Table 1 was examined:

Table 1 – Manufacturer data for GPS Jammer #1 & #2

GPS Jammer #1	
Type:	Plug-in Jammer – small cylindrical device to be plugged into the cigarette lighter socket of a car
Interception Frequency:	1560 MHz – 1580 MHz[3] 1565 MHz – 1585 MHz[4]
Power Source:	DC: 12V
Output power	n. A. in data sheet
Jamming Range	0.5-15 m
Size (L x Dia.):	90 x 25 mm
Cost:	~ 50 €

GPS Jammer #2	
Type:	Battery powered hand-held jammer – multiband jammer in a cuboid housing with four Antennas
Interception Frequencies:	1500 MHz – 1600 MHz (L1) 1220 MHz – 1230 MHz (L2) 1200 MHz – 1210 MHz (L3) 1250 MHz – 1280 MHz (L4) 1170 MHz – 1180 MHz (L5)
Power Source:	Internal re-chargeable Battery
Output power	2 W[5]
Shielding radius	up to 15 m
Size (HxLxW):	113 x 60 x 30 mm
Cost:	~140 €

Before the test was performed the output signals of the Jammers were verified (see Table 2)

Table 2 – Measured output signal characteristics of the examined GPS jammers

GPS jammer #1	Specified	Measured
Output power	n.A.	37 mW
Frequ. range	1565 - 1585 MHz	1402 - 1661 MHz

GPS jammer #2	Specified	Measured
Output power	2W[6]	L1 only: 0.56 W
Frequ. range	1500 - 1600 MHz	1510 - 1645 MHz

[3] According to webpage
[4] According to the label on the device
[5] For all four outputs together
[6] For all four output amplifiers

Examined GPS clocks (devices under test):
For the field test the following devices were used:

- **Clock A:** Professional 19" GPS time reference for rack mounting with a 20 m antenna cable and an active GPS Antenna
- **Clock B:** Professional antenna-integrated GPS-time reference for industrial applications
- **Receiver C:** Hand-held GPS navigation receiver

All Devices Under Test (DUTs) were located at the same position for the tests. It was ensured that all DUTs always had an equal same distance to the GPS jammer for all tests.

Test 1: GPS jamming with the hand-held GPS jammer #2
The target of the first test setup was to determine from what distance the reception of professional GPS clocks can be disturbed to the point that they are no longer locked to GPS.
Both clocks (A & B) were mounted at the same location and monitored simultaneously via an Ethernet connection. Target of the measurement was to find out from what distance the GPS clocks can be "switched-off" using the hand held GPS jammer #2. "Switched off" means that fewer than four satellites can be received and that the clock switches to "hold over"[7] operation. The GPS navigation receiver (DUT C) was used in parallel to find out how a commercial navigation receiver reacts to GPS Jamming.

The test was performed via the following method:

- Step 1: All DUTs are locked to GPS (8 or more satellites are used)
- Step 2: The Hand-held Jammer is switched on at the respective distance (free line of sight)
- Step 3: The result is recorded
- Step 4: The Jammer is switched off and all steps are repeated

Since all examined devices solely used the L1 band the distortions were only emitted in the GPS band L1. The other bands were not affected. Table 3 shows the results of the field test with the hand held jammer. For distances under 70 meters all DUTs were "switched off" by the 0.5 W output signal of the GPS jammer #2. Test 1 also showed the sensitivity to jamming is different for different DUT architectures. The GPS Clock B (antenna-integrated model) was the most robust device; it remained continuously locked to GPS as soon as the GPS jammer was more than 70 meters away. Receiver C worked as soon as the jammer was more than 250 meters away. The GPS Clock A (professional 19" rack version) only worked if the GPS jammer was more than 380 meters away.

[7] Hold over means that the clock's output signal are derived from its internal reference oscillator

Table 3 - Measurement results of field test with hand-held GPS jammer #2

Dist.	Clock A		Clock B		Receiver C	
	# Sat.	Status	# Sat.	Status	# Sat.	Status
70 m	0	UL[8]	2-3	UL	2-3	UL
100 m	0	UL	7	locked	2	UL
120 m	0	UL	7	locked	3-4	UL
135 m	0	UL	≥ 8	locked	3-4	UL
200 m	3	UL	≥ 8	locked		locked
234 m	0	UL	≥ 8	locked	3	UL
300 m	2	UL	≥ 8	locked		locked
350 m	3	UL	≥ 8	locked		locked
380 m	3	UL	≥ 8	locked		locked
400 m	5	locked	≥ 8	locked		locked

Test 2: Plug-in GPS Jammer #1 operated inside a car
In test 2 the plug-in GPS jammer #1 was operated inside a car. Again all DUTs were located at the same position and were locked to GPS. Then the car was slowly driven towards the DUTs until a GPS loss occurred.

Table 4 – Results of test 2 – plug-in GPS jammer #1 operated inside a car

	DUT A (19" version)	DUT B (Antenna integrated)	DUT C (Handheld GPs)
Distance for GPS loss	4.5 m	< 1 m	< 1 m

The results summarized in Table 4 show that a plug-in GPS jammer operated in a car can also cause the loss of GPS reception outside the car.

Test 3: Hand held GPS jammer #2 operated inside a car
For this test the GPS jammer #2 was placed within a parked car. As in Test 1, the distortions were only emitted in Band L1. It was seen at what distance the GPS receiver (DUT C) was no longer disturbed.

Table 5 – Results of test 3 – hand-held GPS jammer #2 operated inside a car

	DUT C (Handheld GPs)
Distance for GPS loss	50 m

Despite of the shielding effect of the car the GPS reception of DUT C was disturbed up to a distance of 50 meters.

Summary of GPS Jamming test results
The examined hand-held GPS jammer #2 had a significantly higher effective range than that stated by the manufacturer. It must be assumed that if the plug-in GPS jammer #1 is operated outside a car its effective jamming range will be also significantly higher than the 15 meters stated by the manufacturer.

Table 6 – Effective jamming ranges

	Jamming range according to data sheet	Measured jamming range
Plug-in GPS Jammer #1	0.5 – 15 m	5 m[9]
Hand-held GPS jammer #2	up to 15 m	~ 380 m ~ 50 m[10]

The impact of GPS jamming depends on several factors:
- the power of the GPS jammer
- the robustness of the GPS receiver against GPS jamming
- the over-all reception conditions at the GPS antenna location

Based on the findings of the conducted tests, small plug in GPS jammers are little threat as long as they are operated inside a car. However, stronger hand-held GPS jammers can seriously disturb GPS reception even when operated inside a car. If a hand-held jammer is operated in direct line of sight to the GPS antenna outside a car it can be considered a serious threat.

B. GPS Spoofing

GPS Spoofing is a method where artificially generated GPS signals are used to hi-jack a GPS receiver with the intent of providing a GPS receiver with counterfeit time and location information. So far GPS spoofing has been mainly performed by university researchers to prove that GPS spoofing is possible and can be a considerable threat to critical infrastructures such as the power grid or transport systems. As of this paper no GPS spoofing attacks other than those conducted for research projects are known. However, the tests executed by the university researchers clearly show that GPS spoofing has the potential for criminal or terror activities. [5]
GPS spoofing is much more complex then GPS jamming and requires a detailed knowledge of the GPS system as well as the actual position of the GPS receiver to be hi-jacked. In his paper "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer" [5]. Professor Todd E. Humphreys and his team of the University of Texas at Austin investigated several concepts for GPS spoofing. The most likely concept to be used for a professional spoofing attack is the so called "Portable Receiver/Spoofer." A portable receiver/spoofer receives an authentic GPS signal, alters it, and re-sends it to the GPS receiver being attacked. Receiver/spoofers are not commercially available for the time being, but Professor Humphrey's team demonstrated that specialists can build such a device based on a software defined GPS receiver and of-the-shelf hardware components that total in about 1500 US$. [5]

[8] UL … unlocked

[9] Operated inside a car

IV. THE IMPACT OF GPS VULNERABILITIES ON POWER GRID INFRASTRUCTURES

A. Examined timing infrastructures

To assess the impact of different GPS vulnerabilities the following three timing scenarios as shown in Fig. 2 were investigated:

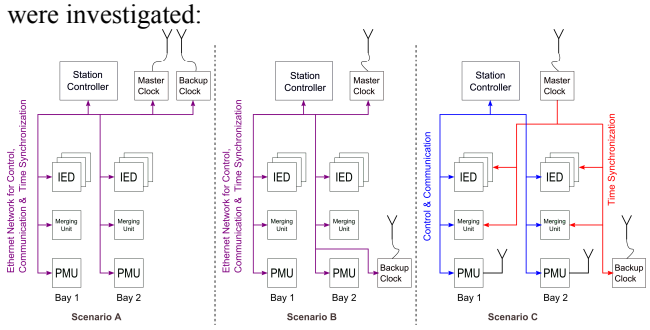

Fig. 2 - Investigated Timing Scenarios A – C

- **Scenario A:** Substation with central master clock and back-up clock located at the same spot. The reception antennas are mounted at the same position.
- **Scenario B:** Substation with central master clock and back-up clock located at different buildings. The reception antennas were mounted at different positions.
- **Scenario C:** Substation with central master clock and back-up clock located at different buildings. The reception antennas were mounted at different positions and two PMUs with integrated GPS receivers were used.

B. The impact of GPS jamming

When a GPS clock is successfully attacked with a GPS jammer it loses satellite reception. As a result it will provide an alarm and continue to operate with the accuracy of its own internal oscillator. Depending on the quality of the internal oscillator and its hold-over stability[10] the accuracy of the timing signals provided by the GPS clock can remain within a few µs for several hours. Fortunately, a GPS jamming attack will not remain unnoticed due to the alarm mentioned above. The station operator and as well as other stations in the grid receiving data from the affected station will know that the data might contain inaccuracies due to GPS reception loss.

Impact on Scenario A:
In this scenario all GPS antennas are located at the same position. Since usually the same GPS clock models are used for the master clock and the backup clock it can be considered that both clocks loose GPS reception at the same time. As a result all clocks inside the IEDs in the system will remain locked to either the master clock or the back-up clock which are both in hold-over mode. This means that all clocks will follow the hold-over drift of the active station clock's internal oscillator. In this situation all time stamped values and measurements can be continued to be used within the substation since all clocks remain in sync with each other. However, since the time information is no longer locked to UTC the entire substation will drift away time wise from the rest of the grid[11].

Impact on Scenario B:
When an intentional jamming attack is launched against a substation it is very likely that the GPS jammer is powerful enough to block reception for all GPS clocks in the substation. However, positioning the master clock and the backup clock at different locations drastically increases the availability of either the main or the backup system in case of unintentional jamming. If, for example a truck equipped with a GPS jammer parks near a substation and if the GPS antennas are more than 50 meters apart it is very likely that either the main or the backup clock will remain operational. In this case all time stamp data can continue to be used. If both GPS clocks are affected the result is the same as that in scenario A. Based on these findings it is suitable to position the main and back-up clock at different locations. However, for standard time distribution infrastructures using IRIG-B[12] or 1 PPS[13] signals the insertion of time reference signals at two different locations is not trivial due to the propagation delays in the distribution network. With the precision time protocol in accordance to IEEE 1588-2008 such distributed infrastructures can be easily implemented since changing propagation delays are automatically compensated. [8]

Impact on Scenario C:
For this scenario in general the findings are the same as those for scenario B. The main difference is that not all IED clocks are locked to the same master clock, since the PMUs have their own GPS receivers. This may result in a situation where some IEDs in the system have accurate time information locked to UTC while other IEDs are locked to a clock drifting slowly away from UTC. If all clocks are affected by the jamming attack, IEDs locked to the active substation clock can drift away from UTC differently than the devices equipped with their own GPS receiver. In such a case the use of their data for automatic substation control is not recommended.

C. Countermeasures against GPS jamming

The results of the field test clearly show that some GPS clock models are less sensitive to GPS jamming than others. Therefore, it is recommended that upon

[10] A free running oscillator changes its frequency over time due to ageing drift and temperature changes. The hold-over stability of an oscillator defines how much its frequency changes over a defined period.

[11] The occurring drift depends on the duration of the attack and the stability of the clock's internal oscillator

[12] Acc. to IRIG-B Standard 200-04

[13] PPS … pulse(s) per second

installation of new systems GPS clocks are chosen which have high-quality directional antennas and modern sensitive receivers which can deal with low signal to noise ratios. To further minimize the possible impact of unintentional jamming the GPS antennas of the main clock system and the backup clock system should be mounted at different locations. PMUs usually use integrated GPS receivers since the required time accuracy cannot be achieved by standard time code signals like IRIG-B or NTP[14].[3] By implementing a time synchronisation with the precision time protocol according to IEEE 1588-2008 it is possible to lock all PMUs to the substation master clock. As a result time stamped phase information provided by the PMUs can still be used for phase comparison inside the substation.
A sudden loss of GPS satellite lock of one or more GPS receivers without an antenna fault is a strong indication for GPS jamming. To find out where the GPS jamming signal comes from GPS jamming detectors can be used According to manufacturer information, professional GPS jammer detectors and locators can accurately determine which vehicle or individual is hosting the GPS jammer.[4]

D. The impact of GPS spoofing

When a GPS clock is successfully attacked with a GPS spoofer no alarms will sound. The only result is that the time reference signal provided by the attacked clock will slowly drift away from UTC as intended by the operator of the GPS spoofer. Without dedicated countermeasures and detection techniques a GPS spoofing attack on a GPS clock will remain undetected until a malfunction caused by inaccurately time stamped data occurs. In their paper "Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks" the authors Daniel P. Shepherd, Todd E. Humphreys and Aaron A. Fansler prove that that GPS spoofing can cause considerable problems in power grid management.[9]
According to Professor Humphrey's research static GPS receivers as used in GPS disciplined time references can be spoofed more easily than moving receivers. In general, static receivers can be spoofed to provide wrong time information from miles away as long as the position of the GPS Antenna is known and a free line sight is maintained between the receiver and the GPS Spoofer.

Impact on Scenario A:

In scenario A all GPS reception antennas are located in one place. Thus, all GPS receivers will receive and will lock onto the counterfeit signal. Thus, both clocks will drift synchronously away from UTC. Therefore it is likely that the spoofing attack will remain undetected. All time stamp data acquired inside the substation will carry wrong time in information in comparison to UTC, but all clocks in the substation will remain in sync to each other. The trouble starts when data from the substation is used together with data from other places in the power grid for control and automation purposes leading to wrong grid management actions. In comparison to a GPS jamming attack time drift to UTC will be much bigger since it is controlled by the GPS receiver/spoofer and does not depend on the clock's internal hold-over capabilities.

Impact on Scenario B:

For scenario B two different GPS spoofing methods must be considered:

Use of a portable receiver/spoofer close to one of the GPS antennas:
If the spoofing attack is done with a portable receiver/spoofer positioned closely to one of the antennas a simple phase comparison of 1 PPS signals generated by each clock would allow to detect a time drift between the main and the backup clock. The IEDs in the substation are either all locked to the master clock or all locked to the backup clock. Depending on which clock is attacked with the receiver/spoofer either all IEDs or none of the IEDs are affected.

Spoofing from the outside of the attacked site:
Due to the fact that power infrastructures are usually not accessible to the public a spoofing attack conducted from the outside is more likely. In case of such an attack it is very likely that both GPS antennas (despite being mounted at different locations) will receive the spoofed GPS signal and the authentic GPS signal in parallel. Therefore both clocks will show the same drift in comparison to UTC and the spoofing attack will remain undetected. If the spoofing attack remains undetected the impacts would be the same as those outlined for scenario A. All time stamp data acquired inside the substation will carry inaccurate time information in comparison to UTC, but all clocks in the substation will remain in sync to each other since all IED clocks are locked to the same station clock.

Impact on Scenario C:

For a spoofing attack from the outside the findings for scenario C are the same as those for scenario B. If only one clock is attacked with a portable receiver/spoofer placed close to the receiver's antenna all equipment synchronized by this clock will drift. All IEDs connected to other GPS clocks will stay in sync with UTC. Thus not only control and automation processes involving data from other substations but also processes solely relying on time stamped data acquired inside the substation might lead to inaccurate results and false control actions.

E. Countermeasures against GPS spoofing

According to [9] a variety of promising methods are currently developed against civilian spoofing attacks, but most of these techniques require changes in the receiver

[14] NTP … Network Time Protocol acc. to RFC5905

hardware and/or software. It is very likely that it will be years before these techniques are implemented in the field. For the time being there is no off-the-shelf defence available against GPS spoofing.
However, there is a possibility of detecting GPS spoofing attacks in power utilities which use a time synchronisation system accurate enough to lock all IEDs including all PMUs to one central master clock. The precision time protocol according to IEEE 1588-2008 would be a suitable system since it provides a time synchronisation accuracy greater than 1µs for power systems. [10] To detect a spoofing attack in such an environment a free running high stable atomic clock would be needed.

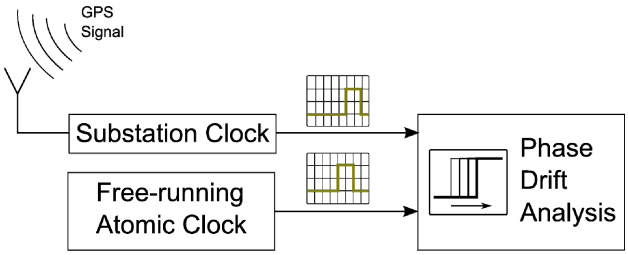

Fig. 3 - Use of an atomic clock to detect GPS spoofing

As shown in Fig. 3 the rising edge of a 1 PPS signal derived from this free running atomic clock can then be compared with the rising edge of the station master clock's 1 PPS signal. Due to the very low ageing of the free-running atomic clock only a very slow drift between the two 1 PPS signals will be detected. In case of a GPS spoofing attack the speed of the detected phase drift between the 1 PPS signals would change drastically since a timing failure of several µs is inserted by the GPS spoofer within minutes. As a result, such a change in drift can be an indication for a GPS spoofing attack, and would allow the station operator to disable automatic control procedures relying on sampled values or synchrophasors.

V. CONCLUSIONS

GPS disciplined clocks are vulnerable to GPS jamming and GPS spoofing. With the growing use of GPS jammers by civilians the danger of unintentional jamming will increase in the future. While the tests performed for this paper indicate that small, low power, plug-in jammers for cars seem to be only a minor threat for power utilities, more powerful hand held jammers like the one examined for this paper can cause GPS reception loss even when operated inside a vehicle parked outside a substation. GPS jamming can be detected and the GPS jammer can be located by using adequate detection and location devices. This will allow the jammer to be removed before the GPS clocks drift far enough from UTC to cause problems.
GPS spoofing can result in severe operational disturbances of power utilities. Further on, there is no off-the-shelf defence against GPS spoofing available. Luckily GPS spoofing is very difficult to implement and requires a high level of system knowledge and technical skills to be implemented. Thus, for the time being, the danger of civilian or terrorist spoofing attacks is quite low, especially since there are more efficient methods available for terrorists to disrupt electric power infrastructures. Nevertheless, the threat of GPS spoofing is not to be neglected[15], countermeasures like the proposed use of free running atomic clocks might be a first step in the right direction to overcome the GPS spoofing threat.

REFERENCES

[1] IEC 61850 Ed.2, "Communication networks and systems in substations", IEC

[2] PRC-018-1, "Disturbance Monitoring Equipment Installation and Data Reporting" NERC, 2006

[3] Baumgartner B, Riesch C, Rudigier M, " Implementation and Transition concepts for IEEE 1588 precision timing in IEC 61850 Substation Environments", SAPSPC 2012, Johannesburg, South Africa.

[4] Curry C. et al., "Sentinel Project – Report on GNSS Vulnerabilities", Chronos Technology, 2014

[5] Humphreys, T.E., B.M. Ledvina, M.L. Psiaki, B.W. O'Hanlon, P.M Kintner, Jr., "Assessing the Spoofing Threat: Development of a Portable GPS Civilian Spoofer," Proceedings of ION GNSS, The Institute of Navigation, Savanna, Georgia, 2008.

[6] A.J. Kerns, D.P. Shepard, J.A. Bhatti, T.E. Humphreys, "Unmanned Aircraft Capture and Control via GPS Spoofing," Journal of Field Robotics, to be published.

[7] Rutkin A. H. "Spoofers Use Fake GPS Signals to Knock a Yacht Off Course"; MIT Technology Review, August 14, 2013

[8] IEEE 1588-2008, "IEEE Standard for a Precision Clock Synchronization Protocol for Networked Measurement and Control Systems", IEEE, 2008

[9] D.P. Shepard, T.E. Humphreys, A.A. Fansler, "Evaluation of the Vulnerability of Phasor Measurement Units to GPS Spoofing Attacks." International Journal of Critical Infrastructure Protection, Vol. 5, December, 2012.

[10] IEEE C37.238-2011, "IEEE Standard Profile for Use of IEEE 1588 Precision Time Protocol in Power System Applications", IEEE, 2011

[15] It has to be assumed, that the military and government agencies of many countries have sufficient funds and access to specialists to conduct an undercover GPS spoofing attack at any time.