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

Performance analysis of WM-Bus-based synchronization protocols in Sensor Networks

D. Capriglione[1], L. Ferrigno[1], A. Del Giudice[2], G. Graditi[3], V. Paciello[2], A. Pietrosanto[2]
[1] *DIEI University of Cassino, Via G. Di Biasio, 43, Cassino (FR), Italy.*

[2] *DIIn, University of Salerno, via Giovanni Paolo II,132 Fisciano (SA), Italy*
[3] *ENEA Italian National Agency for New Technologies Energy and Sustainable Economic Development*
Portici (NA), Italy

Abstract **– Smart metering wireless sensor networks need to refer to a common time scale for several reasons. As examples: (i) in power quality, some measures at different nodes of the network are senseless if not synchronized; (ii) in security, in case of lack of synch, a replay attack could result successful; (iii) in billing, different times of the day can be charged differently.**
Generally, the synchronization can be reached in many ways, in this paper the authors make a comparison between different synchronization techniques considering a communication protocol specifically designed for measures with wireless sensors: the Wireless Metering bus.

I. INTRODUCTION

Smart Grid sustainers claim that an opportune fusion of power grids and communication networks is the first step to renew the Power Grid architecture for energy transportation and distribution, making it more efficient, more secure and more controllable. To reach this ambitious goal, the old power network needs to be heavily modified from the point of view of communication capability. The nodes of the network are composed by smart meters that are points of the network from which is possible to make some observations on the state of the Grid. To allow the development of the Smart Grid, all nodes must return measures that are dependable, correct and sometime real-time. There is the need of a dependable information exchange between the nodes of the network, so it is important to adopt a communication protocol that is able to support all the operations useful to make communication efficient and reliable. Some requirements of the communication protocol are here reported:

- Packet integrity check: the lower layers of the protocol should ensure the delivery of data packets exchanging.
- Media compatibility: there is no a priori knowledge of the environment in which the meters are placed, so there is the need of some flexibility in the choice of the physical medium on which the communication takes place. The protocol should be able to work with different physical layers.
- Encryption: security is a crucial point in Smart Grids, the information contains sensitive data that must be protected from malicious “men-in-the-middle” attacks.
- Remote update: it is important to have the possibility to write in the program memory of the meter to update the firmware of the device and also in the data memory to modify parameters useful for the control of the Grid.

Electricity meters are mature enough to send information and receive commands over communication networks, it is not true for water meters. The water distribution network does not provide a physical medium by means two actors of the network could exchange information. This is not acceptable if we want to think about the networks of electricity, water and gas distribution as a unique entity remote controllable and fully stable. The main contribution of the present work is on the implementation of a synchronization algorithm over the WMbus protocol, in particular to permit the time synchronization between water meters. To complete the scenario using the theory of consensus decision making for coordinating networks of sensors, in the final work will be presented some performance results on the possibility of internal synchronization starting from the knowledge of the clock phase shift of some nodes of the WSN.

II. THE PROPOSAL

In the present work the authors want to link many sensor nodes by means of a wireless communication channel and reach the synchronization between the clocks of the nodes using an existent protocol for wireless sensor networks. The context in which the work is conceived is the one of Advanced Metering Infrastructure in which there is the need of distributed

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

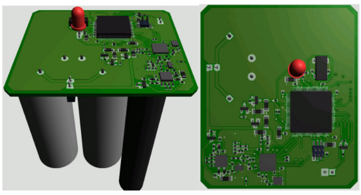

Figure 1 The 3D of the sensor node

measures made by low cost sensors that can communicate wirelessly. The first step is the designing and building of the single sensor node. Every node has been thought as a device that can be attached on common water counters and take a picture of the consumption value. The picture can be stored and sent to a concentrator device on request. The single node at design phase is shown in Figure 1 and described later in detail.

The communication protocol chosen for this application is the Wireless Metering bus protocol [12]. This protocol was specifically designed for wireless metering applications. After these preliminary operations the single node has been replicated to create a network of sensors. The second step has been the selection of the way for time clock synchronization of three nodes with existing protocols for WSN: the TPSN, FTSP to cite a few. During the normal synchronization process, many non-ideal events could occur and introduce uncertainty into the process. Based on previous work done [15],[16], the authors want to investigate some causes of uncertainty that could compromise the synchronization process:

- The finite processing resolution and processing time of the microcontroller;
- The effect of non-ideal clock on time computing;
- The effect of the limited bandwidth that causes latencies and delays.

All these issues can cause problems to the synchronization process, delaying the convergence or worsening the error probability. Starting from

III. THE SYNCHRONIZATION PHASE

The problem of synchronization is very important in wireless sensor networks and it is strongly felt in networks of devices involved in Advanced Metering Infrastructures. The new architecture of the network is conceived as distributed rather than centralized. There are a lot of nodes disseminated in the space of kilometers that can collect measures or register events. The synchronization of a network of nodes can be external or internal. With the term external synchronization we refer to a process in which the correct value of time comes from outside the network, on the other hand when there is no need of the absolute time reference and the application only cares about the consistency of times between all the nodes, it is possible to use an internal synchronization. The quality of the power delivered to civil houses or industries is going to be an important parameter in the market of energy. For Power Quality we intend the analysis of all the disturbances that could bring the Grid out of the following nominal conditions of the supply voltage:

- Constant amplitude and correctness of nominal value;
- Constant frequency and correctness of nominal value;
- Sinusoidal waveform;
- Absence of interruptions.

After retrieving measures from the nodes, next step is a fusion of the collected information, it is then necessary to refer all the measures to a common time line. There are different synchronization techniques some of them wired in the sense that the synchronization process takes place by means of communication protocols that works by wire, other techniques are wireless, all of them presents advantages and disadvantages. As first difference between wired and wireless synchronization we can observe that in case a meter is not reachable by a wireless signal it is not possible to communicate with it and consequently it is not possible to synchronize its clock. On the other hand wireless communication channels are often the only way to reach places where is not possible to pose cables. At the moment the most performant synchronization technique seems to be the synchronization based on GPS satellite receivers that give the possibility to reach maximum errors in the order of hundreds of nanoseconds. There are wired techniques not that performant but often acceptable for the application considered. Generally the common communication protocols for telecommunication systems do not include a native synchronization method. Even protocols like SML, DLMS/COSEM, IEC 61805 that are specific protocols designed for application dedicated to the metering of gas, water and electricity, do not offer a synchronization procedure enough accurate. Some protocols that can be exploited for synchronization purposes in smart metering applications are:

A. FTSP

The FTSP synchronizes the time of a sender to possibly multiple receivers utilizing a single radio message time-stamped at both the sender and the receiver sides. MAC layer time-stamping can eliminate many of the errors. However, accurate time-synchronization at discrete points in time is a partial solution only. Compensation for the clock drift of the nodes is inevitable to achieve high precision in-between synchronization points and to keep the communication overhead low. Linear regression is used in FTSP to compensate for clock

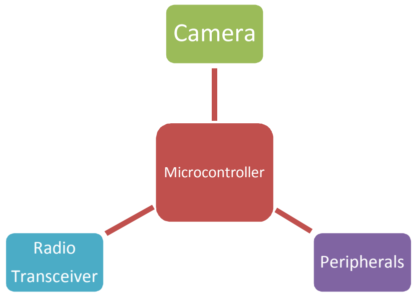

Figure 1 The sensor Node architecture

Drift.

Typical WSN operate in areas larger than the broadcast range of a single node; therefore, the FTSP provides multi-hop synchronization. The root of the network—a single, dynamically (re)elected node—maintains the global time and all other nodes synchronize their clocks to that of the root.

B. TPSN

Timing-sync Protocol for Sensor Networks is based in a sender-receiver scheme and sees the network of the nodes as a tree. The synchronization comes in two phases: the first in which the root creates a tree model of the network where at each node is assigned a level; in the second phase devices of the layer n synchronize their clocks with devices of level n-1.

C. Average Time Synchronization Protocol

The Average Time Synchronization algorithm in [13] can provide average time synchronization in a cluster of the network. Without a root node or an external time reference, average time synchronization means that all the nodes' local clocks synchronize to their average, which enhances the robustness and scalability of the network. In the consensus algorithm the gossiping of the neighbor nodes gives the possibility to reach a common status. If as gossiping function is choose the average clock time the whole synchronization algorithm is known as Average Time Synchronization Protocol [14].

IV. THE SENSOR NODE

The testing network is composed by tens of wireless nodes. Every node is composed by four main devices:

- ARM Microcontroller;
- RF Transceiver;
- RF Front-End;
- Camera sensor.

The picture below shows the architecture of a single node. It is important to note that the system is very simple and cheap because the cost must be held low. The main feature of the node is the ability to communicate with other nodes so we can observe two main parts: the computing part represented by the microcontroller in which there is the control software which governs all the operations and in which there are multiple versions of the communication protocol and the Radio part which is responsible for establishing of the medium that allow communication in the network of nodes.

A. ARM microcontroller.

The microcontroller is the hearth of the node. It is a high performance ARM®Cortex™-M3 32-bit RISC core, namely STM32F207VC. It works at an operating frequency of 120 MHz.

The core incorporates many peripherals connected by two APB busses, three AHB busses and a 32 bit multi-AHB bus matrix. Between these peripherals there are a Flash memory, an SRAM and many enhanced I/Os modules. The access to memory presents a very low latency thanks to the ART (Adaptive Real-Time memory accelerator). Beyond a very performant core, this microcontroller offers a lot of useful features like: twelve general-purpose 16-bit timers including two PWM timers for motor control, two DACs, three 12-bit ADCs a low-power RTC, two general-purpose 32-bit timers. a true number random generator (RNG) included into the package there are also standard communication interfaces easily handled by the software and also advanced communication interfaces to speed up the information exchange. There are also some advanced peripherals like SDIO, an FSMC (Flexible Static Memory Control) interface and a camera interface for CMOS sensors. This family of microcontrollers pays great attention to power saving that's why there are three operation modes that are conceived to economize battery consumption these are: Sleep, Stop and Standby modes. In our application it is very important to save as much energy as possible because it can be a problem to replace batteries too frequently. Between standard communication interfaces we remember the USB interface and Ethernet communication port.

B. RF 169MHz transceiver

The transceiver is a Texas Instruments high performance RF Transceiver for narrowband communications, in our tests, it works at 169 MHz to match the frequency band of WMbus. This chip is radio transceiver specifically designed for high performance operations and it is suited to work at very low power and low voltage so that it can match our requirement of low power operation of the single node.

Figure 3 The picture of sensor node

Also the price of the chip is cheap enough to be integrated on a PCB that has stringent constraints on the final cost. From this point of view the transceiver permits to save some money (and space on the PCB) for the cost of filters because integrated into the chip there are all filters needed so there is no need of external SAW and IF filters. The device has been designed for applications in the field of industrial, scientific and medical market, it is a short range device and can be used at different frequency bands: 164–192 MHz, 274–320 MHz, 410–480 MHz, and 820–960 MHz. In this application we have chosen the range 164-192 MHz because we want to test the WMbus protocol for data exchange and also because it is a free frequency. The utility of the transceiver is mainly perceived in the handling of data to be transmitted and received. The chip provides hardware support for packet handling data buffering, burst transmissions, clear channel assessment, link quality indication, and Wake-On-Radio. Mainly the chip is controlled through an SPI interfaces. Before starting operations, some registers have to be set in order to allow the correct functioning of the device.

C. RF front-end module

The SKY65367-11 is the interface with the antenna chosen in this work. It is a high performance transmit/receive front-end module and includes a Power Amplifier that is able of more than +29 dBm of transmit output power when the supply has a value of 3.6 V. In case of applications where is important to save battery energy the Power Amplifier can be bypassed. All the functionalities of the chip can be controlled by a three wire interface that permits to the ARM microcontroller to handle the device operations included the deep sleep operation mode that allow to reach very low current consumptions up to 1μA. The receive chain consists of a low-loss Single-Pole, Triple-Throw (SP3T) switch, which provides an insertion loss of approximately 0.5 dB. Three separate VCC pins enable maximum RF isolation.

D. Wireless Mbus

WMbus is a EN standard protocol (EN13757 2005 and 2012) it specifies the RF communication link between meters for water, gas and electricity and it is widely accepted in Europe as communication protocol in applications that aim to put into the same network all the devices present in an Advanced Metering Infrastructure. Originally the bus was designed to work in the 868 MHz band which gives a good tradeoff between the size of the antenna and the RF range. Later two new bands were added 169 MHz and 433 MHz and the introduction of narrowband solutions provides longer RF range with respect to the one at 868 MHz. The radio module allows communications that goes outside the home premises, the distances that can be covered are such that an operator with and hand device can retrieve measures from devices positioned inside residential flats. The frequency bandwidth used in this work is one that goes from 169, 400 MHz to 169, 457 MHz. The European Standards Telecommunications Institute (ETSI) reserved that band for metering applications and fixes to 500 mW (27 dBm) the maximum Equivalent Isotropically Radiated Power (EIRP) and a maximum duty cycle of 10%. France and Italy proposed the Wireless Mbus mode N in CEN area of interest because in both countries the communications for the gas metering system are based on a wireless bus at the frequency of 169 MHz. Mode N is a narrowband protocol that uses a GFSK modulation with different data rates exploiting 6 channels dedicated for data exchange. The channels are spaced 12,5 kHz apart and work with a bit rate of 4,8 kbps (channels 2a and 2b). Furthermore exists a N2g mode that puts together different channels to have an higher data rate. The standard specifies several service classes, the best of these requires a minimum level for the sensitivity of the receiver of -115 dBm with a Packet Error Rate that have to be less than 0,01. At application level there are two communication modes:

- Access Timing: in this mode the meter can be put in sleep mode and it wakes up after a predefined constant period of time to send the measures to the concentrator that is in charge to receive and process measures.
- Synchronous Transmissions: the meter wakes up only when a concentrator or any other authorized devices sends commands directed to the meter requiring the measures.

At application level specific data objects can be used to exchange data and commands between concentrator and meter and is also possible to exploit tunneling techniques to exchange data in DLMS/COSEM data format [6]. From this point of view the WMbus protocol results very interesting since DLMS/COSEM aims to be the communication standard protocol for communications between metering (electricity, water, gas) devices.

The choice of the WMbus as communication protocol has been also driven by the fact that 169MHz is frequency sufficiently low to permit the radio modules to communicate over large distances and the attenuation affect due to walls and other obstacles that can be present inside house premises is less relevant. Typically a meter is positioned inside recesses made into the walls.

V. CASTALIA SIMULATOR

Castalia is a simulator for wireless sensor networks and it exploits the environment and facilities offered by Omnet++ platform. Castalia simulator was designed from scratch and it is highly parametrizable. Castalia features include:

- Channel model. It is not only possible to define connections between nodes but also a map of the path loss even temporally variable. It is also possible to model the movement of a node in the space and the inter nodes interference based on signal strength.
- Radio model. There is the possibility to choice between multiple transmission power levels. It is also possible to define a radio model of the device used on the board.
- Sensing modelling. With Castalia is also possible to define a physical process monitored by the nodes.
- Node clock drift.

The basic structure of Castalia is depicted in the figure

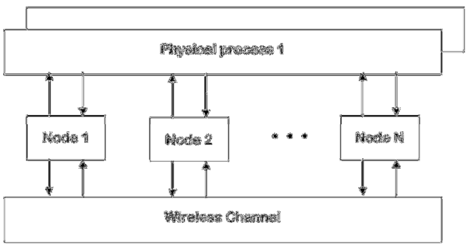

Figure 4 Castalia sctructure

The nodes can communicate only by means of the wireless radio channel. When a node has a message to send, it delivers this to the wireless channel modules which decides who is the receiver of the message on the basis of the content of the packet sent. The nodes sample the physical process to get the readings. The node is an entity composed by modules. The modules is a basic building block of the Omnet++ environment. The modules are defined by the NED language. A module can be simple or based on multiple modules. The complex modules are built with the key word "submodules" and with the explicit connections between modules. Castalia is conceived to work with linux operating systems. In our case we have used the Kali distribution because of the familiarity with this OS. The installation procedure is simple and well documented. Castalia offers two scripts that help in the simulations: "Castalia" and "Castalia Results". The first one is used to run simulations the second to interpret results. To personalize simulations it is necessary to edit a configuration file called "omnet.ini". Inside that file it possible to configure the environment in which the nodes are posed and the behavior of the process to simulate. We have configured different .ini files to run different simulations, what we intend to do is to make a comparison between results obtained by the simulator and experimental results obtained by tries with real boards. The target process is a synchronization using the TPSN protocol in different conditions. In this case the varying parameter is the distance and obstacles between nodes or in other word the signal strength at radio receiver. Castalia offers the possibility to modify the network topology in the .ini file. It is possible to define the area in which the nodes are posed, the number of nodes and the deployment type. We have chosen a fixed number of nodes with a fixed distribution mode and three area extents. The nodes are 9 with a uniform distribution and the areas are 2x2 meters, 10x10 meters and 50x50 meters.The results of simulation are reported in the tables 1,2,3. For the cells without value, it was impossible to synchronize:

Table 1 2x2 configuration

Node	1	2	3	4	5	6	7	8	9
WCE(us)	190	170	169	150	178	169	165	175	134

Table 2 10x10 configuration

Node	1	2	3	4	5	6	7	8	9
WCE(us)	210	195	180	155	189	181	178	190	137

Table 3 50x50 configuration

Node	1	2	3	4	5	6	7	8	9
WCE(us)	--	200	198	158	195	--	--	--	146

VI. PRELIMINARY RESULTS

As preliminary operation, the hardware shown above has been tested with a first version of the software simplified and put in verbose mode to show via RS232 connected to a PC the state of each node. The wireless link between the two nodes is at fixed frequency 169 MHz. Through the PC is possible to issue a request of synchronization from a node directed to the other one. Every synchronization operation happens specifying what kind of protocol is to be used. Two synchronization protocols have been coded: TPSN and FTSP. When the PC starts the operations a node sends to the other one a synchronization request and the two nodes synchronize according to the protocol required. The two nodes always output a square wave signal with the period 1 s, this signal is useful because permits to evaluate the phase shift between the two nodes before and after the synchronization process. The measurement station is composed by:

- Digital counter Agilent (53132A).
- Oscilloscope LeCroy Wave Master (8620A).
- Logic states analyzer Tektronix (TLA5203).

In the Figure 4 is depicted the architecture of the measurement station:

The parameter to evaluate how good the synchronization has been done is the Clock Phase Delay (CPD) representing the delay between the two square wave signals of the nodes. The synchronization interval is variable progressively and is chosen from a script on the PC. The node that requests the synchronization is connected with the PC via RS232. The nodes make multiple synchronizations after variable time intervals. A function generator outputs to the two nodes a precise 1 s waveform that serves as clock to count the time after which the sync process is started. The transceivers mounted on the nodes give the possibility to modify the baud rate of the wireless link Also different values for the baud rate of the wireless link have been explored.

For each baud rate and synchronization interval twenty measurement have been acquired.

Looking at Table 1 it can be highlighted that the CPD worsen as the baud rate decreases. This is strictly related to the time length of the synchronization packet that increases as the baud rate decreases. In particular, once the time sender read its local clock it spends a time related to the time length of the synchronization packet to send the information to the receiver clock. During this time the CPD worsen its value. Similar results are obtained for the FTPS (Table II). In addition it can be highlighted the higher value of the CPD for the FTSP respect width the TPSN synchronization protocol. This is due to the absence of the continuous correction during the regressions.

Looking at Tables 1 and 2, we can see that the CPD seems to be not influenced by the synchronization interval.

In the present work, together with a prototype of a sensor node for water counter, has been presented a comparison of synchronization methods based on 169 MHz radio link. Preliminary tests on distances covered and obstacle immunity have been done showing that the radio frequency chose (169 MHz) is suitable for the environment in which the meters will be placed. In the final work using the theory of consensus, a new synchronization technique will be characterized and exhaustive performance parameters will be examined and reported considering uncertainty causes, distances and obstacle on the path between two nodes.

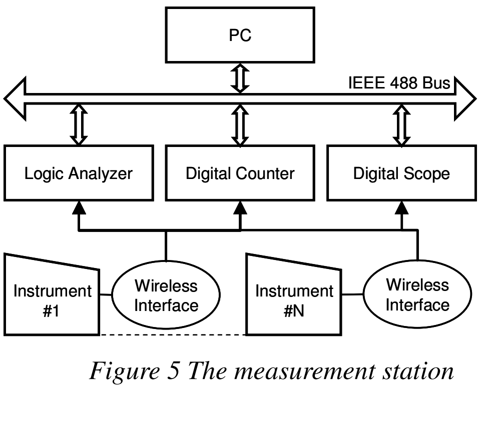

Figure 5 The measurement station

Table 1 Preliminary results for TPSN algorithm.

Baud Rate	synchronization Interval [s]	CPD [ms]	σ_{CPD} [ms]
250	5	0,633	0,019
	10	0,631	0,020
	30	0,632	0,020
1000	5	0,340	0,017
	10	0,339	0,015
	30	0,339	0,015
3000	5	0,150	0,013
	10	0,148	0,012
	30	0,148	0,012
6000	5	0,094	0,014
	10	0,097	0,015
	30	0,097	0,015

Table 2 The first results for FTSP algorithm.

Baud Rate	synchronization Interval [s]	CPD [ms]	σ_{CPD} [ms]
250	5	7,374	0,48
	10	7,375	0,48
	30	7,371	0,49
1000	5	3,875	0,26
	10	3,871	0,27
	30	3,879	0,29
3000	5	1,545	0,14
	10	1,543	0,15
	30	1,544	0,15
6000	5	0,967	0,12
	10	0,968	0,13
	30	0,968	0,13

VII. REFERENCES

[1] S. Lan, M. Qilong, J. Du, “Architecture of Wireless Sensor Networks for Environmental Monitoring,” Proc. International Workshop on Geoscience and Remote Sensing, 2008, pp. 579-582.

[2] Yik-Chung Wu, Q. Chaudhari, E. Serpedin, “Clock Synchronization for Wireless Sensor Networks: A Survey” , Signal Processing Magazine IEEE 2011, pp. 124-138.

[3] M.D. Lemmon, J. Ganguly, L. Xia, “Model based Clock Synchronization in Networks with Drifting Clocks”. Proc. 2000 Pacific Rim International Symposium on Dependable Computing, Dec. 2000.

[4] Q. Li and D. Rus. Global Clock Synchronization in Sensor Networks, Proc. IEEE Conf. Computer Communications (INFOCOM 2004), Vol. 1, pp. 564–574, Hong Kong, China, Mar. 2004.

[5] F. Cristian. Probabilistic Clock Synchronization. Distributed Computing, 3:146–158, Springer-Verlag, 1989.

[6] A Attianese, A. Del Giudice, M. Landi, V. Paciello, A Pietrosanto, “Synchronization of DLMS/COSEM sensor nodes”, 19th IMEKO TC-4 Symposium Measurements of Electrical Quantities. Barcelona, Spain 18-19 July 2013, pp. 234-239.

[7] K. Arvind. Probabilistic Clock Synchronization in Distributed Systems. IEEE Transactions on Parallel and Distributed Systems, Vol.5, no.5 pp. 474–487, May 1994.

[8] Spinsante, S.; Pizzichini, M.; Mencarelli, M.; Squartini, S.; Gambi, E. "Evaluation of the Wireless M-Bus standard for future smart water grids", Wireless Communications and Mobile Computing Conference (IWCMC), 2013 9th International, On pp.: 1382 - 1387

[9] S. Spinsante, M. Pizzichini, M. Mencarelli, S. Squartini, E. Gambi, "Evaluation of the Wireless M-Bus Standard for future Smart Water Grids", Proceedings of IEEE IWCMC 2013, to appear.

[10] Texas Instruments, CC112X/CC1175 Low-Power High Performance Sub-1 GHz RF Transceivers/Transmitter, 2011.

[11] J. Hayes, K. Tong Lau, D. Diamond, “A wireless sensor network for monitoring water treatment,” Proceedings of IEEE International Conference on Sensor Technologies and Applications, 2007, pp. 514-519

[12] http://www.wmbus.org/

[13]L. Li, Y. Liu, H. Yang, H. Wang, A Precision Adaptive Average Time Synchronization Protocol in Wireless Sensor Networks, in: Proceedings of the IEEE International Conference on Information and Automation, Zhangjiajie, China, 2008.

[14]L. Schenato, F. Fiorentin, “Average TimeSync: A consensus-based protocol for time synchronization in wireless sensor networks” In IFAC workshop on estimation and control of networked systems (2009).

[15]L. Ferrigno, V. Paciello, A. Pietrosanto, "Performance Characterization of a Wireless Instrumentation Bus" IEEE Transactions on Instrumentation and Measurement, Vol. 59, no. 12, pp. 3253-3261, 2010.

[16]L. Ferrigno, V. Paciello, A. Pietrosanto, "Experimental characterization of synchronization protocols for instrument wireless interface", IEEE Transactions on Instrumentation and Measurement, Vol. 60, no. 3, pp. 1037-1046, 2011.