Delay aware measurements gathering in WAMS communication network

SelvaPrasanth.N
Department of CSE
Francis Xavier Engineering College
riderrishi1998@gmail.com

Selva.N
Department of CSE
Francis Xavier Engineering College
selvavasi07@gmail.com

Mrs.B.Benita B.E
Assistant Professor
Francis Xavier Engineering College

Abstract

Electric power system is an critical infrastructure and the loss of its resilience or operability can lead to the negative consequences for the national economy. Modern power systems based on a sophisticated computerand communication technologies are now characterized by elevated vulnerability to the different types of unauthorized malicious access, i.e. cyber-attack. Wide area measurement system is based on the technology of vector measurements with the phasor measurement units refers to the subsystems of electric power system which are the most vulnerable in terms of the aftermath of cyber attacks. In the earlier research, the authors of different paper suggested a technique for a two-level distributed state estimation which is based on singling out the areas within the scheme of electric power systems which are monitored using PMU. The PMU measurements which coming at a high frequency make it possible to implement the fast linear algorithms of the state estimation for such areas. The paper will present potential consequences of cyber attacks on WAMS, their impact on the quality of measurements coming to the state estimation problem and use of distributed state estimation algorithms for theiridentification.

Index Term– WAMS, PMU measurements, state estimation, cyber attacks, test equation method, bad data detection.

I. INTRODUCTION

The adoption of the complicated technical equipment and the advanced information and communication technologies need to establish an intelligent power system (IPS) with in increases the vulnerability of the entire intelligent power system and its individual infrastructures to the various failures and disturbances, which includes those malicious, or cyber attacks.

State estimation is an mathematical method for the data processing which makes it possible to calculate the state variables of the electric power systems on the basis of measurements, and the filter gross errors in them. The results of the state estimation from the basis for the real-time and the emergency control of electric power systems, their visualization raise the awareness of the dispatching staff on this current state of the electric power system. The most vulnerable in terms of thecyber attack consequences for the state estimation are the facilities of the information-communication control subsystem, such as the SCADA and WAMS, since the input data is used for solving the state estimation problems which are represented by the SCADA measurements (telemetry and remote signals) and phasor measurements which received from the phasor measurement unit, which is the main measuring equipment of WAMS. Due to the cyber attacks on the SCADA and WAMS,measurementdata coming to the state estimation problem are distorted. If no special measures have been taken to identify these distortions and suppress their impact on the state estimation will results, a serious errors and can appear in decisions made by dispatchers using the state estimation result.

Solutions to the state of estimation problem can be considerably improved by the method of combining the SCADA and WAMS measurement. The addition of the PMU measurement makes it possible to improvea observability of the complete calculated scheme, which enhance the efficiency of the method for bad data detection in the measurement of the data, and accuracy of the obtained estimates in it. The measurements from the WAMS are assumed to be accurate and reliable. At the same time the research and experience of the PMU operation will indicate that there can be a different reasons for a failure in PMU operations and bad data in their readings. As is shown in a number of publications the WAMS can be a potential target for the cyber attacks, since to improve the state estimation procedure it will be integrated with the SCADA system.

In this system consideration will be given to the potential cyber attacks on the WAMS, their impact on quality of measurements coming to state estimation problem and on that state estimation results, as well as the use of the bad data detection methods for their identification and the suppression. This system is structured as follows. It defines three infrastructures representing the links of an system for intelligent power system operation control and their vulnerability to cyber attacks. Then Section III consider the variants of cyber attacks on the WAMS, whose consequences affect the reliability of a state estimation problem. Then Section IV focuses on the state of the estimation problem statement and algorithm for the detection of a cyber attack on the WAMS by the state estimation method. Then Section V suggests the implementation of the algorithm based on PMU measurements.

II. CYBER SECURITY OF ELECTRIC POWER SYSTEM.THE MOST VULNERABLESUBSYSTEMS

Electric power system is the critical infrastructure and the loss of its resilience and operability can be the result in negative consequences for national economy. To study the cyber security problem, it should be sensible to divide the electric power system into the two subsystems,controlled, and consider it as the two-level model. The controlled subsystems are represented by the objects of control (electric power plants, substations, transmission and distribution networks), i.e. physicalinfrastructure.

The comprehensive approach to understanding the security problem of electric power system should employ

the notion of a cyber- physical infrastructure [1] which represents theinterconnection of information-communication and physical infrastructures.

To develop the measures to ensure cyber security of the electric power system it is necessary to determine the cyber vulnerability the considered infrastructures, taking into the account their interdependence, analyze the impacts on potential consequences due to the cyber attacks.

A cyber attack on information-computation subsystem can result in the failure of any component in the measurement, computation and communication systems. Actions of intruders can be weaken the information-communication subsystem, so to lead the data loss or unreliability, implementation of the negative control actions, etc. Attacks on information communication infrastructure can cause the emergency conditions of the physical system.

In turn, the failure of a component the physical infrastructure can lead to the emergency conditions in the electrical part and to facilitate failure of the control system of information – communication infrastructure [2].

Malicious intrusion in a cyber - physical infrastructure can violate the operability of the information-communication infrastructure and the physical infrastructure or of both ofthem.

With a growing use of information and computation devices we can make anything in the information-communication infrastructure, its vulnerability to cyber attacks will increase regularly. Therefore, it is necessary to identify potential cyber attacks on those control system and methods for their identification to prevent the manipulation of the electric power system control. In this research we have to analyz the vulnerabilities and the weaknesses of the information-communication infrastructure in case of the cyber intrusions in terms of the state estimation results on the basis of WAMS measurements.

III. WAMS AND STATE ESTIMATION PROBLEM. POTENTIAL CYBERATTACKS

A. WAMS architecture

The Wide-Area Monitoring System represents the set of recorders of synchronized phasor measurements (PMU), phasor data concentrators (PDC), channels for the data transfer among the recorders, data concentrators and dispatching centers of JSC “SO UES”, as well as systems for processing they obtained information. WAMS measurements are synchronized by a system of GPS/GLONASS. The hierarchical architecture of WAMS [3] is presented in Fig. 1.

Phasor measurement units measure the magnitudes and the phases of nodal voltages and currents in lines, which can incident to these nodes. PDC collects, filters, processes and retransmits data. Besides, PDC we can register abrupt surges, distortions, parameters of the switches, parameters of the loads and lines, and identify the generator parameters.

Super-PDC processes data which provides a dispatcher or an operator with graphical interface and the access to the data archive.

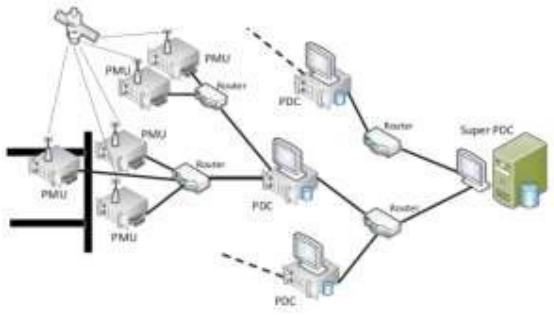

Figure1. Hierarchical architecture of WAMS

In The existing SCADA measurements and PMU measurements, Duplicating them make some energy companies to think that WAMS are not a strategically important system and the technical means of WAMS are not the cyber critical components of the energy infrastructure. However, the WAMS is vulnerable to cyber attacks.

B.Potentialcyber attacks onWAMS

Analysis of the potential cyber attacks [4]-[6] has shown that the greatest harm to the WAMS can be done in the following way**:**

1)The devices of PMU, PDC and communication infrastructure proper:

- **Reconnaissance attacks** allow an adversary to identify the weaknesses and potential targets in the WAMS architecture. The aim of the attacks can be the identification of the IP addresses of connected PMUs and PDCs. This information can also be used for future attacks onWAMS.
- **Communication links damage.** Some companies use the overhead fiber optic lines as the main communication lines for the WAMS. They are installed in the parallel to transmission lines. Therefore, they are exposed to the attacks like a cut-off (loss of line connection).

2)Integrity, accessibility and reliability ofdata:

- **False data injection.** Sensor is a measurement injection and command injections. The false data injection attacks can be the directed against one or several PMUs, as well as against the PDC which receives the flows of the synchronized data from several PMUs and forms an single output flow. This makes PDC an ideal target for intrusion in order to manipulate the large amount of synchronized measurementsafterwards.
- **Denial-of-service attacks.** Denial of service (DoS) can also stop the transmission of PMU measurements to the control centers, andthetransfer of the control actions, or both. The DoS attack can also generate redundant data which

will result in the traffic overload and in depletion of resources of the most important communication line or router. In this case, these measurements can have a long communication delay or be even denied by a router. Moreover, this denial-of-service attack can terminate the operation of PMU, PDC and super- PDC. For the WAMS, this means loss of the power systemobservability.

3) Reliability of GPS.

Some cyber attacks are designed to do the harm to GPS. These are desynchronization, and the forced shift of measurement phase from real value. The authors of [7] show that the GLONASS hardware is an extremely vulnerable to the impact of this interfering signals, which can create a background (masking interference) as well as an intelligent impact (simulating interference). Here they can make some shift of the system time in the PMU devices which may lead to the wrong actions of personnel and the even disconnection of certain components or emergency islanding of networking. Vulnerability of GLONASS leads to the misinformation through the replacement of accurate time instant by a random time instant during and intelligent attack. In [7] the authors suggest developing software for GLONASS receivers to detect and exclude simulation interference.

- **Spoofing attacks.** Spoofing attacks are aimed at GLONASS/GPS synchronization systems. An attacker can easily perform these attacks to synthesize and transfer fake GPSsignals.
- **Replay attacks.** An intruder records valid the GPS signals, and then transmit them with a delay as the corrupted signals, i.e. the information of the direct retransmission isdistorted.
- **Jamming.** Intruder transmits the high-power interfering signals by using the GPS frequency band to prevent the nearby GPS receivers from the receiving and monitoring the GPS signals. The authors of [7] say about low the immunity of GLONASS/GPS synchronization and the systems to interference which can be taken for realsignals.

The specific feature of the technological control in the modern electric power system is imperative transmission of the large data volumes to the upper levels of control. Normally, the data are transmitted through the via corporate network, but recently a points of interface with the Internet have appeared by which makes the network more accessible and thus the vulnerable. In some cases it is suggested to apply the cloud technologies, particularly in WAMS, for the collection and transmission of synchronized vector measurements from PMU level to the PDC and super-PDC level. With an constantly growing number of the cyber attacks on the information structure of energy facilities, the authors of [8] suggest enhancing their cyber security through an reduction in visible zones of potential attacks which make the methods of traffic engineering, the development of the next generation commercial the anti-viruses and systems to detect the intrusion and block the network attacks, and detect the emergence of new networkdevices.

Technical and the information vulnerability of state estimation problem and its informationenvironment is described

State estimation is an traditional technique for detecting and the suppressing bad data..

Research in [9] shows that if the adversary has an comprehensive idea of the power system topology and values of the transmission line conductance, he can attack the injecting false data in such a way so that the attack remains unnoticed.

In this case, the test which are normally used in the electric power system state estimation is used to detect bad data on the basis of discrepancy analysis cannot detect these data.

The study presented in [3] demonstrates that state estimation using only PMU requires the network where PMU data are adequately delivered with less than 30 ms from all PMUs to PDC and super-PDC which sorts a data according to this time stamp and transmits them to estimators. The authors of [3] have made an considerable contribution to the research into which the consequences of cyber attacks on the state estimation procedure: that they use a two- module simulation system (PSLF&NS2) used to consider a physical damage of the network cable; simulate launch of the DoS by blocking network traffic with routing device overload; present a man-in –the-middle attack where adversary intercepts PMU data packets and replaces them with the fake data, which leads them to the wrong state estimation. The simulation results to show that: 1) the emergency in a line can make the system an unobservable; 2) In case of a routing device failure, the state of estimation behavior becomes unstable; 3) The state estimation based on the PMU measurements is robust against the single PMU data spoofing.

Some papers addressing cyber attacks [3,10,11] show that communication network is exposed to such attacks as denial of service, the replay attack, interference in the operation of sensors or recorders. For the state of estimation problem, such events mean that the failure to receive data corresponding to current time instant. In this kind of situation in SCADA systems using the telemetry, previously the remote meters are marked certain measurements as invalid or entire snapshot –as an failed snapshot. In the case of an failed snapshot, the state estimator was not able to start, hence the diagnostics could have been seen in the snapshot archives. It is necessary to envisage the same kind of marking the failed snapshots which are formed by the level of PDC and super- PDC in WAMS, and accordingly, not to start state estimation during whole period of technicalfaults.

Another type of cyber attack is a false data injection in state estimation problem, when there are no failures in communication network. If such information comes from the single recorders, the state estimator can handle with this problem independently, by a priori finding as an erroneous measurement and by replacing it with the pseudo measurement. In this case, if that state variable is assigned a fake value (spoofing attack), then this value can be identified as an systematic error of measurement. However, the time of the cyber attacks can be short and hence the insufficient to identify such a systematic error.

Moreover, a "properly" built attackon the recorder will create another incorrect value, which is randomly differing from the previous one.

In case where the attack has been carried out on a large number of recorders, then the number of erroneous measurements can lead to the situation and where the computational process of the state estimation does not converge. A simple check before the state estimation of whether or not the current measurements lies within some technological limits so we can immediately diagnose if the information failure has occurred. In the state estimator settings it is envisaged to block the large number of the errors, thus it is possible to avoid the state of estimator start which will lead to the failure in its performance. A great number of the rejected measurements can make this system unobservable for the state estimation. Problem planner of the computational environment should have to give a feedback with the state estimator, i.e. the state of estimation launch is cancelled in a event that the indicator should becomes nonzero. One of a measures to withstand the loss of observability by state estimation is to add WAMS recorders at the energy facility, where in this case of rejection of the certain measurements they can be replaced by the values calculated by an backupPMU.

IV.ANALYSIS OF CYBER SECURITY OF STATE ESTIMATION PROBLEM AT CYBER ATTACKS ATWAMS

Currently, there is algorithms for solving the problem of state estimation using only PMU or by only the SCADA measurements, or a combination of both.

This analysis of the main algorithms is based on the combination of SCADA and PMU measurements shows that they have to main drawbacks characteristic of the traditional of state estimation [12]. Therefore, the main attention of the researchers and practitioners is paid now to the state of estimation algorithms and based on the PMU measurements only.

If there is an sufficient amount of the phasor measurement units to provide an observability of the electric power system scheme, the state estimation can be performed using PMU data only. Then the vector of measurements in this case has the form:

iteration. Thanks to the considerably higher accuracy of PMU measurements compared to traditional measurements, the accuracy of the estimates increases.

Unfortunately, modern electric power systems even in most developed countries are still insufficiently furnished with the phasor measurement units to perform linear state estimation for entire scheme. The algorithms of the distributed state estimation on basis of SCADA and PMU are promising under terms of their practical application. The main idea of these algorithms consists in the following: local areas which completely observed using PMU measurements are now singled out in the scheme of electric power system, and they are based on linear algorithms local state estimation is performed by these areas. Then, the obtained estimates are transmitted to an dispatching office of electric power system, where these state of the entire system is estimated using the SCADA measurements in the rest of the scheme.

The advantages of the local linear state estimation is based on the PMU data and are obvious. However, there are a pitfalls related to the difficulties in detecting the bad data in such measurements, which can be caused, in a particular by cyber attacks onWAMS.

As the authors of [13] show, loss of synchronization is the most unfavorable in terms of impact on state estimation results. It can be caused by the cyber attacks or interference to GPS receiver, or by the external problems with synchronization due to the computational load of measurement devices, which leads to an delay in the angle measurement. It is very important to note that if an angle shift occurs in some of PMU channel, this shift occurs in all the phase channels. This happens only because all phase channels use one and same GPS time signal and the identical code of processing the numerical signal. The same research shows that the bad data in the measurements of the phase angles of current and the voltage are not identified by the traditional methods for the analysis of the estimation residuals and, hence the cyber attacks aimed at loss of synchronization will not be detected.

One more problem is that propagation of bad data when measurements are now converted from a polar to Cartesian coordinates [14]. In case of the synchronization loss and emergence of the bad data in phase angles of voltage and

$$\bar{y}=\{\delta_I, U_i, I_{ij}, \varphi_{ij}\}, \quad (1)$$

where U_i, δ_i – Magnitudesand the phasesofnodalvoltages, I_{ij} – magnitudes of currents in branches and φ_{ij} – angles between currents in a branch which coming to the *i*-th node and the voltage of this node. In addition tothese measurements, PMU can also calculate active P_{ij} and reactive Q_{ij} flows in these branches. Some of the PMUs instead of angles φ_{ij} measures phase angles of currents ψ_{ij}.

These angles are connected by relation: $\varphi_{ij}=\delta_i-\psi_{ij}$.

When the state estimation problem is solved in the rectangular coordinates then the model of measurements

$\bar{y}=y(x)$,where $x=\{U_{ai}, U_{ri}\}$ is a state vector, becomes *linear*. The state vector estimates can be obtained in one current all the four measurements $U_{ai}, U_{ri}, I_{aij}, I_{rij}$ in Cartesian coordinates will have been erroneous. The authors of [15] show that PMU measurement form which is an mostresistant the synchronization losses is the voltage of magnitude and phase, and the pseudomeasurements P_{ij}, Q_{ij} calculated by using the PMU measurements.

In this system we have to suggest using the method of test equations to analyze and validate the PMU measurements.

method was developed to detect the bad data in SCADA measurements [15], then the adapted to check the PMU measurements and analyze the cyber security of SCADA [16, 17].Test equations are now steady state equations which include only measured state variables *y*

$$w_k(y)=0 \quad (2)$$

Test equations are used to carry out an priori validation of the remote measurements. Substitution of the values of measurements in these equations will leads to the discrepancy, by the comparing with the threshold d , i.e. checking the condition

$$|w_k|<d, \quad (3)$$

we can judge the whether or not the measurements that belong to the test equation are valid.

Since the test equation method is a priori validation method which will operates prior to the state estimation algorithm, i.e. calculation of the estimates, any representation form of the PMU measurements can be used to implement it.

A great variety of the steady state equations including the PMU measurements makes it very possible to use the equations which may contain only measured variables at once as the test equations. The second approach is used to convert PMU measurements into the pseudo measurements of active and the reactive power flows in branches. Depending on the validation results the vector of the measurements for local state estimation from an area is formed

Moreover, up to date the SCADA and the WAMS are independent from one another. Therefore, if a local area or an object observable with WAMS measurements, they are the rule observable with SCADA measurements as well. Therefore, we suggest, when we needed, performing a single (by one timestamp) independent test for the validity and state estimation is based on the SCADA and WAMS measurements to additionally need to find out if there is an malicious impact on one or another system.

III. TEST OF THE SUGGESTED TECHNIQUE INA SIMULATION EXPERIMENT

To do calculations based on a suggested technique we use an fragment of a real network observable by the PMU measurements (Fig. 2). The fragment includes two 750 kV lines that can have a common node.

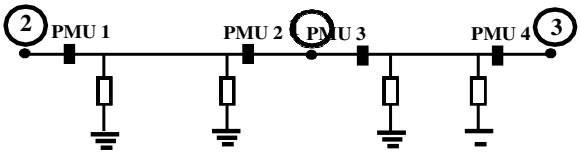

Figure 2. A 3-node scheme consisting of two 750 kV lines

The calculations were done in that simulation experiment when the PMU measurements were simulated by the distorting the parameters of the steady state calculation.

The following types of cyber attacks were simulated:

False data injection (attack 1) was simulated by the technique presented in [4]. A man-in-the-middle attack on block of data which were transmitted PMU-2 to PDC, by doubling the value of all the captured vector measurements. Then the PDC receiving the data failed to distinguish changed packets from the unchanged ones. Moreover, the process of changing the data is occurred according to the requirements for PDC data frame life time, therefore the changed packets were not marked as old and passed in the state estimator.

A denial-of-service attack (attack 2) was simulated by node was simulated to inject the wrong measurements in thedata.ThisnodeinterceptedandmodifiedtheC37.118

the situation where the measurements did not arrive at the PDC. This did not lead to observability loss but on considering reduced redundancy of PMU measurements, which decreased due to the efficiency of the bad data detection algorithm.

Desynchronization attack (attack 3) was simulated by changing the phase voltage angle at the PMU-4 by 9 degrees, which corresponds to the missing one point when taking 40 readings in one 50 Hz cycle. Such an distortion of voltage angle led to an distortion of measurements in other angles: the angle of the current in branch 3-4 and load angle at the node of PMUplacement.

Table 1 presents the state estimation results based on data exposed to attacks, and measures undertaken by the state estimation methods to detect suchdata.

A comment on attack 3: as was said above if an angle shift occurs in certain PMU channel, the same shift will happen in all the phase channels. Therefore, then the same shift in the voltage angle $\delta_3$and current angle ψ_{31}will notaffectthe angle between voltage and the current vectors $\varphi_{31}=\delta_3-\psi_{31}$, hence, this error will not the biggest change the values of active and reactive power. In this case, if the neighboring PMU givesa valid angle measurement, then $\delta_3$will becalculatedcorrectly.

IV. CONCLUSION

The wide area monitoring system (WAMS), which is based on a technology for vector measurements using the PMUs, is one of the most vulnerable subsystems of the intelligent energy system in terms of the cyber attackeffects.The state of estimation results is underlie the real-time and emergency control of the electric power system. Linear state estimation of the local areas observed with PMU measurements is a promising direction in the development of state estimation methods.
The potential cyber attacks on the WAMS have been analyzed. They can cause the greatest damage to the measurement data which coming from the PMU. It is shown that the procedures for the priory detection and the compensation for erroneous measurements is an effective tool for the identification of technical failures and also malicious attacks on WAMS, and the elimination of their impact on the state estimation results.

REFERENCES

[1] S. Sridhar, A. Hanh, M. Govindarasu, "Cyber-Physical System Security for the Electric Power Grid", *Proceeding of the IEEE*, vol. 100, pp. 210-224, Jan.2012.

[2] Voropai N.I., Domyshev A.V., Nepomnyashchy V.A., "Models and methods for the research into the security of electric power systems," in *"Reliability of energy systems: problems, models and methods for solving them,"* Novosibirsk: Nauka, 2014, p.57-74.

[3] Hua. Lin, Yi Deng, Sandeep Shukla, James Thorp, LamineMili, "Cyber Security Impacts on All-PMU State Estimator – A Case Study on Co-Simulation Platform GECO", in *Proc. 5-8 Nov. 2012 Smart Grid Communications (SmartGridComm), 2012 IEEE Third International Conf.*, pp.587-592.

[4] T.H. Morris, P. Shengyi, U. Adhikari, Cyber Security Recommendations for Wide Area Monitoring, Protection and Control Systems, in *Proc.22-26 July 2012 IEEE Power and Energy Society General Meeting,*pp.1-6.

[5] Liang Heng, Jonathan J. Makela, Alejandro D. Dom´inguez-Garc´ıa,Rakesh B. Bobba, William H. Sanders, and Grace Xingxin Gao, "Reliable GPS-Based Timing for Power Systems: A Multi-Layered Multi-Receiver Architecture," in *Proc. 2014 Power and Energy Conference at Illinois (PECI),* pp.1-7.

[6] MohdRihan, Mukhtar Ahmad, M. Salim Beg, "Vulnerability Analysis of Wide Area Measurement System in the Smart Grid, " *Smart Grid and Renewable Energy* [Online], Sep. 2013, pp. 1-7.Available:http://www.scirp.org/journal/sigre

[7] Nudelman G.S., Oganesyan A.A., "About protection of synchronization systems using GLONASS/GPS signals from intelligent interference impact," in *Proc. of XXII Conference "Relay Protection and Automation of Energy Power Systems,"* Moscow, May 27-29, 2014, pp.427-431.

[8] Nikandrov M.V., Braguta M.V., "Cyber threats to the control systems of modern substation," in *Proc. of XXII Conference"Relay Protection and Automation of Energy Power Systems,"* Moscow, May 27-29, 2014, pp. 424-426.

[9] Md. Ashfaqur Rahman and Hamed Mohsenian-Rad, "False Data Injection Attacks with Incomplete Information Against Smart Power Grids," in *Proc. 2012 IEEE GLOBECOM*, pp.3153-3158.

[10] S. Sridhar, A. Hahn, M. Govindarasu, "Cyber Attack-resilient Control for Smart Grid," in *Proc. 2012 IEEE ISGT*, Washington, USA, pp.1-3.

[11] C. Beasley, G. Kumar Venayagamoorthy, and Richard Brooks, "Cyber Security Evaluation of Synchrophasors in a Power System," *in Proc. 13th Clemson University Power Systems Conference,*2014.

[12] Kolosok I., Khokhlov M., "Specific Features of State Estimation Problem in Control of Electric Power System with Active-Adaptive Properties," in *Proc. of the 5th Intern. Conf. "Liberalization and Modernization of Power Systems: Smart Technologies for Joint Operation of Power Grids"*, Irkutsk, Russia, Aug. 6-10, 2012.- P.100-108.

[13] LuidiVanfretti, Joe H. Chow, "Synchrophasor Data Application for Wide Area System," in *Proc. of the 17th Int. Power System Computation Conference PSSC-2011*, Stockholm Sweden-August 22-26,2011.

[14] Khokhlov M., "Identifiability of errors in synchronized vector measurements," in *Proc. of Conference "Modern approaches to ensuring the electric power system reliability*," Syktyvkar: Komi RC UB RAS, 2014,pp.88-96.

[15] Gamm A.Z., Kolosok I.N., "Test Equations and Their Use for State Estimation of Electrical Power System," in *Proc of Conf. "Power and Electrical Engineering: Scientific Proc. of Riga,"* Technical University. Riga: RTU, 2002, pp.99-105.

[16] Glazunova A.M., Kolosok I.N., Korkina E.S., "Study of test equations method's application for bad data detection in PMU measurements," in *Proc. of PMAPS 2012*, Istanbul, Turkey, June 10-14, 2012,#106.

[17] I. Kolosok, L. Gurina, "Calculation of Cyber Security Index in the Problem of Power System State Estimation Based on SCADA and WAMS Measurements," in *Proc. of 9th International Conference on Critical Information Infrastructures Security*, October 13-15, 2014, Limassol, Cyprus, ID12.