ATLANTIS PRESS
Advances in Intelligent Systems Research, volume 158
Vth International workshop "Critical Infrastructures: Contingency Management, Intelligent, Agent-based, Cloud Computing and Cyber Security" (IWCI 2018)

State Estimation of Electric Power System under DOS-attacks on SCADA system and WAMS

Irina N. Kolosok, Liudmila A. Gurina

Melentiev Energy Systems Institute of Siberian Branch of the Russian Academy of Sciences,
Lermontov str., 130
Irkutsk, Russia
E-mail: gurina@isem.irk.ru

Abstract

The control of EPS includes monitoring, forecasting and planning of the system operation based on its state estimation. Therefore, it is extremely important to obtain accurate estimates of the state variables in both favorable and critical situations that arise due to cyberattacks.
The paper gives an analysis of possible cyberattacks on SCADA system and WAMS. We propose an algorithm for EPS state estimation based on interior point method. It provides the required accuracy of solving at the event of various adverse factors, including cyberattacks.

Keywords: EPS, SCADA, WAMS, cyberattacks, state estimation, interior point method.

1. Introduction

Today electric power system (EPS) are developing in accordance with the concept of Smart Grid, defined in Russia as an intelligent electric power system. Of great importance is the introduction of systems for Wide-Area Monitoring Systems (WAMS) and the EPS control based on modern intelligent information and communication technologies, tools and technologies for measuring, transmitting, processing and presenting information [1]. The use of information and computing facilities in the information-communication infrastructure of EPS is increasing, which increases the vulnerability of EPS to cyberattacks. Therefore, for the reliable operation of EPS, its control should take into account emerging cyber threats that affect the quality of information on operating conditions.

The EPS operational and emergency control is performed using the current operating parameters obtained from state estimation based on the measurements coming from the SCADA and WAMS.

In the case of successful cyberattacks on the SCADA and WAMS, data from measuring devices may be lost, and measurements may contain errors that are not detected by traditional state estimation procedure.

The paper proposes a solution to the EPS state estimation problem based on the interior point method (IPM). Interval formulation of the state estimation problem takes into account not only the network laws (steady-state equations), but also the permissible technological limits of variation in operating parameters (constraints-inequalities).

The proposed approach to solving the state estimation problem makes it possible to obtain estimates of unmeasured variables in the case of a failure of measuring devices and to detect serious errors in measurements in case of cyberattacks on measuring systems.

2. Cyber-security of EPS control system

2.1. Structure of EPS control system in Russia

The research into cyber security of electric power system is focused on two subsystems - information-communication control and controlled (physical) subsystems. The information-communication control subsystem includes the systems of SCADA/EMS, WAMS, WAPS (Wide Area Protection Systems), and WACS (Wide Area Control Systems). The controlled subsystems are represented by the objects of control (electric power plants, substations, transmission and distribution networks).

The SCADA/EMS systems, designed to support the actions of the operator in the operational and emergency control of EPS, include: remote terminal units (RTU), installed at substations of EPS and intended to record telesignals about the status of switching equipment and measurements of operating parameters; communications channel; Master Terminal Unit (MTU), which provides Human Machine Interface (HMI)

between the Engineering Work Station (EWS) and System.

Russian analog of WAMS is the System for Transient Conditions Monitoring. It includes recorders of synchronized phasor measurements (PMU data), phasor data concentrators (PDC), dispatch control at all levels (central (CDC), interregional (IDC) and regional (RDC)), channels for data transfer between the recorders, data concentrators and dispatch control centers of JSC "SO of UES", and facilities for processing the obtained information. WAMS measurements are synchronized using global navigation satellite systems (GNSS), including GPS and GLONASS. Signals from GNSS are received by time server (TS) intended for the generation of accurate time signals and further synchronization of phasor measurement units [2,3].

A hierarchical structure of control system in Russia is presented in Fig.1.

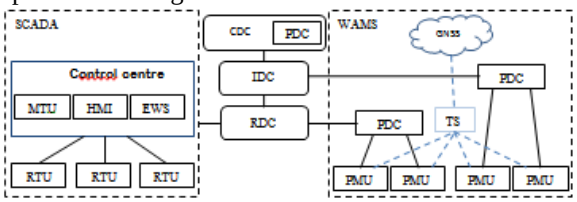

Fig. 1. A hierarchical structure of control system EPS.

The functional components of the control system are a time synchronization subsystem, a measurement subsystem, a data transfer subsystem, and a data processing subsystem.

2.2. Possible cyberattacks on EPS control system

An analysis in [4-8] shows that most cyberattacks are targeted at subsystems of control system:

Reconnaissance attacks allow an attacker to determine weak places and potential targets in the subsystems of data measurements and processing. The targets can represent the determination of IP-addresses of connected PMU, RTU, PDC and MTU. Such information can be used to carry out future False data injection attacks and Denial of service attacks. In the subsystem of data transfer there can be scanning of network, transfer protocols of the network, analysis of network traffic.

False data injection attacks are aimed at breaking integrity, availability and validity of data or operability of the system. Such attacks can be implemented through the false data injection into RTU/PMU, as well as against a PDC that receives synchronized data streams from multiple PMUs and generates a single output stream. This makes the PDC an ideal target for intrusion, to then manipulate a large number of synchronized measurements.

Denial of service attacks (DOS-attacks) are aimed at availability. Denial of service may stop transmitting measurements from the PMU or RTU to control centers, the transmission of control actions, or both. In addition, when performing a denial of service attack, the PMU, PDC and super-PDC of the WAMS or RTU, MTU can stop working, which may result in loss of system observability.

Replay attacks allow attackers to intercept and save data streams for their retransmission and manipulation, and to input false control signals into the system. Successful attacks can cause physical damage to the system.

The main goal of **jamming attack** is to jam data transmission subsystem by interference signals for disruption of communication between the components of the SCADA and WAMS systems.

Attacks aimed at GNSS are called **time synchronization attacks**. These include **spoofing attacks**. Here, the attacker can manipulate time-stamped measurements, which can lead to improper control actions. In such attacks, a GPS signal is forged so that the PMU measurements are sampled with delay, which leads to PMU measurements with incorrect time stamps.

In addition, successful attacks affect the functional capabilities of the EPS control, i.e. operation scheduling, forecasting, monitoring, EPS state estimation, etc. Therefore, it is necessary to develop and upgrade the methods for solving the problems of control that ensure reliable operation of electric power systems under cyber intrusions

The most vulnerable are SCADA and WAMS measuring devices, because their work can be influenced by cyberattacks conducted in all control subsystems, and, as analysis indicates, especially DOS-attacks.

2.3. DOS-attacks on the SCADA system and WAMS

In [8] three categories of DOS-attacks on measuring devices are described:

- bandwidth consumption

- resource starvation
- programming flaws.

The techniques and ways to successfully conduct DOS-attacks are presented in Tables 1-3.

Table 1. Bandwidth Consumption.

<table>
<tr><td>Connecting to network</td><td>Analysis of ports</td><td>Using unused ports</td><td rowspan="4">Bandwidth consumption</td></tr>
<tr><td rowspan="3">Traffic analysis</td><td>Know data packet structure</td><td>Network flooding</td></tr>
<tr><td colspan="2">Insecure firewall</td></tr>
<tr><td colspan="2">Finding protocol loop holes</td></tr>
<tr><td colspan="3">Flood network with random data</td></tr>
</table>

Table 2. Resource starvation.

<table>
<tr><td>Knowledge of operating system</td><td colspan="2">Scheduling flaws in operating system</td><td rowspan="2">Resource starvation</td></tr>
<tr><td>Gain access to network</td><td>Traffic analysis</td><td>SYN flood</td></tr>
</table>

Table 3. Programming flaws.

<table>
<tr><td>Connecting to network</td><td colspan="2">Trapdoor/ Backdoor</td><td>Key value modification</td><td rowspan="2">Programming flaws</td></tr>
<tr><td>Traffic analysis</td><td>Knowledge about transmission protocol</td><td>Knowledge of max size of data to be transmitted</td><td>Buffer our flow</td></tr>
</table>

Figures are to be inserted in the text nearest their first The DOS attacks cause delays in the receipt of data from measuring devices, data loss, or RTU / PMU may stop responding to MTU / PDC requests.

In [8], the authors propose the measures to prevent cyber invasions into control systems: data encryption, restriction of network access by means of firewalls, protection of the operating system, etc.

From a functional point of view, as noted above, successful cyberattacks affect the quality of EPS operation and the accuracy of solutions to control problems. This paper considers the problem of EPS state estimation.

3. State Estimation based on SCADA system and WAMS data

The state estimation problem is a search for the calculated values (estimates) of measurable variables of state $\hat{y}$ that are closest to the measured values $\bar{y}$ with respect to some criterion which is most often represented by the sum of squared deviations of estimates from measurements [9]:

$$J(y) = (\bar{y} - \hat{y})^T R^{-1} (\bar{y} - \hat{y}), \quad (1)$$

and satisfies the steady state equations

$$w(y, z) = 0, \quad (2)$$

relating the measured y and unmeasured z state variables. In (1), R_y is the covariance matrix of measurement errors; its diagonal elements are equal to the variances of measurements σ^2, $\bar{y}$ is vector of SCADA and WAMS measurements, including magnitudes U_i and phases δ_i of nodal voltage, generation of active P_{gi} and reactive Q_{gi} power at nodes, and power flows in transformers and lines P_{ij}, and Q_{ij}, currents at nodes and in lines I_i and I_{ij}, φ_{ij} – angles between current and voltage:

$$\bar{y} = \{P_i, Q_i, P_{ij}, Q_{ij}, U_i, \delta_i, I_i, I_{ij}, \varphi_{ij}\}.$$

Pseudo-measurements of nodal loads are used in addition to measurements of generation to obtain nodal injections P_i, Q_i.

3.1. Constraints in the state estimation problem

In the general case, when solving the problem of state estimation, it is necessary to take into account several types of constraints.

1. Equality constraints. The estimates of the measured y and unmeasured z state variables should satisfy the steady state equations (2).

2. Inequality constraints. The estimated values of some state variables obtained during the state estimation must be within certain technological limits. Thus, generation of active and reactive power at nodes should be within the limits determined by the power generation schedule; for power flows in transformers and lines, the limits determined by line transfer capability can be assigned; at load nodes it is necessary to provide correct direction (sign) of the nodal injection, etc.

Therefore, when solving the state estimation problem, in addition to the equality constraints, it is also necessary to take into account inequality constraints given for both measured y:

$$y_{\min} \le y \le y_{\max}, \tag{3}$$

and unmeasured variables of state z:

$$z_{\min} \le z \le z_{\max}, \tag{4}$$

where $y_{\min}$, $y_{\max}$, $z_{\min}$, $z_{\max}$ are a priori known lower and upper limits for the variation in the values of variables included in the vectors y and z, respectively.

It is worth noting that the information on constraints and their consideration when solving state estimation problem is extremely useful: it allows us a priori to reveal serious error in measurements; the limiting values of reactive power generation can be used as pseudo-measurements at unobservable nodes; the constraints contain reliable information about physically possible technological limits of equipment. Therefore, their consideration makes it possible to improve the quality of estimates and obtain a solution reflecting the physical state of the EPS. It is especially important to use them in the light of emerging trends of growing cyber threats and cyberattacks on the control systems of EPS, which contributes to the corruption and loss of measurement information.

In such cases, the state estimation problem can be solved by the interior point method [10-12], that takes into account not only the constraints (2) [9], (4) [13,14], but also the constraints (5) in case of information loss due to cyberattacks.

4. The interior point method

The problem can be formulated as follows:

Minimize (1)

Subject to (2)-(4).

The equality constraints (2) can be represented as:

$$Ay + Bz = \pi,$$

where A, B are coefficient matrices for measured and unmeasured variables, respectively, $\pi \neq 0$ is loss of active/reactive power or voltage dip in lines. If, for example, loop equations are considered as constraints, then $\pi = 0$.

The interior point algorithm consists of two stages:

Stage 1. Calculation of initial parameters meeting the conditions of feasibility;

Stage 2. Optimization in the feasible region consists in iterative finding:

$$\begin{aligned} y^{(k+1)} &= y^{(k)} + \lambda^{(k)} \Delta y^{(k)}, \\ z^{(k+1)} &= z^{(k)} + \lambda^{(k)} \Delta z^{(k)}, \end{aligned} \tag{5}$$

where $\Delta y^{(k)}$, $\Delta z^{(k)}$ is direction of improving the solution in iteration k, $\lambda^{(k)}$ is the step value in this direction.

In stage 1, the vectors $\Delta y^{(k)}$, $\Delta z^{(k)}$ are the solution to the auxiliary problem

$$F^{(k)} = \frac{1}{2}\sum_{j=1}^{m}\frac{(\Delta y_j^{(k)})^2}{d_j^{(k)}} + \frac{1}{2}\sum_{j=1}^{n}\frac{(\Delta z_j^{(k)})^2}{g_j^{(k)}} \to \min, \tag{6}$$

$$A\Delta y^{(k)} + B\Delta z^{(k)} - \pi = r^{(k)}, \tag{7}$$

where $r^{(k)}$ is residual vector at the k-th iteration.

Square weighted coefficients $d_j^{(k)}$, $g_j^{(k)}$ defined as

$$d_j^{(k)} = (\min\{y_{\max j} - y_j^{(k)},\ y_j^{(k)} - y_{\min j}\})^2,\ j = 1,...,m,$$

$$g_j^{(k)} = (\min\{z_{\max j} - z_j^{(k)},\ z_j^{(k)} - z_{\min j}\})^2,\ j = 1,...,n.$$

Denote the diagonal matrices

$$D = diag(d^{(k)}),$$

$$G = diag(g^{(k)}).$$

The problem is solved by Lagrange multiplier method. Proceeding from the optimality conditions, we express

$$\Delta y = D^{(k)} A^T u,\ \Delta z = G^{(k)} B^T u, \tag{8}$$

where u is Lagrange multipliers vector.

Substituting (7) into (6), we obtain a system of linear equations with respect to u,

$$AD^{(k)}A^T u + BG^{(k)}B^T u = r^{(k)}, \tag{9}$$

Find vector u, proceeding from (8), we determine the direction of improving the solution $\Delta y^{(k)}$, $\Delta z^{(k)}$.

In stage 2, we solve the problem

$$F^{(k)} = \frac{1}{2}\sum_{j=1}^{m}\frac{(\Delta y_j^{(k)})^2}{d_j^{(k)}} + \frac{1}{2}\sum_{j=1}^{n}\frac{(\Delta z_j^{(k)})^2}{g_j^{(k)}} + J(y^{(k)} + \Delta y) \to \min,$$

$$A\Delta y + B\Delta z = 0, \tag{10}$$

where

$$J(y^{(k)}+\Delta y)=J(y^{(k)})+\frac{1}{2}\sum_{j=1}^{n}\sigma_j^{-2}(\Delta y_j)^2+c^{(k)}\Delta y,$$

$$c^{(k)}=\nabla J(y).$$

Using the Lagrange multiplier method, we obtain

$$\begin{aligned}\Delta y&=((D^{(k)})^{-1}+R^{-1})A^T u^{(k)}+c^{(k)},\\ \Delta z&=G^{(k)}B^T u^{(k)}.\end{aligned}\qquad(11)$$

The step value is determined by the rule

$$\lambda^{(k)}=\min\{1,\tilde{\lambda}^{(k)}\},$$

where

$$\tilde{\lambda}^{(k)}=\gamma\max\{\lambda: y_{\min}\le y^{(k)}+\lambda\Delta y^{(k)}\le y_{\max},$$
$$z_{\min}\le z^{(k)}+\lambda\Delta z^{(k)}\le z_{\max}\},\ \gamma\in(0,1).$$

The iterative transition is carried out according to the rules (5).

The stopping criterion is the satisfaction of the condition:

$$\xi=\sqrt{2F^{(k)}}<\varepsilon,$$

i.e. it is assumed that the optimal solution is obtained [11].

5. Example

To demonstrate the proposed approach, we considered the IEEE 14-bus test system (Fig. 2). Suppose that a DOS-attack on the SCADA system resulted in a failure of RTU at the second node and a loss of measurements: P_2, Q_2, P_{2-1}, P_{2-3}, Q_{2-3}, P_{2-4}, Q_{2-4}, P_{2-5}, Q_{2-5}.

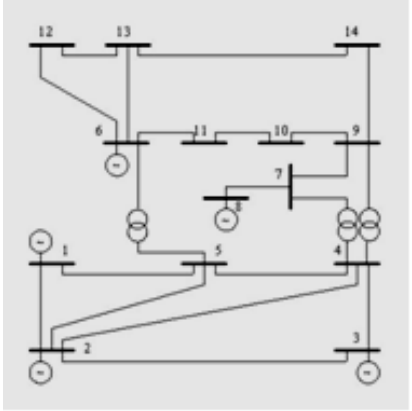

Fig. 2. IEEE 14-bus test system.

The interior point method is suggested to find estimates of measured and unmeasured variables.

The vector $\bar{y}$ forms the following measured variables

$$\begin{aligned}\bar{y}=(&P_1,Q_1,U_1,P_4,Q_4,P_5,Q_5,U_5,P_{11},Q_{11},P_{13},Q_{13},P_{14},Q_{14},\\ &P_7,Q_7,P_8,Q_8,P_3,Q_3,P_6,Q_6,\ P_9,Q_9,P_{10},Q_{10},U_{10},P_{12},\\ &Q_{12},Q_{1-2},P_{1-5},Q_{1-5},P_{3-4},Q_{3-4},P_{4-5},Q_{4-5},P_{4-7},Q_{4-7},\\ &P_{4-9},\ Q_{4-9},P_{5-6},Q_{5-6},P_{6-11},Q_{6-11},P_{6-12},Q_{6-12},P_{6-13},\\ &Q_{6-13},P_{7-8},Q_{7-8},P_{7-9},Q_{7-9},P_{9-10},Q_{9-10},P_{9-14},Q_{9-14},\\ &P_{10-11},Q_{10-11},Q_{13-14},P_{14-13},P_{12-13},Q_{12-13}).\end{aligned}$$

For voltage measurements, constraints (4) were obtained according to [15]:

$$65{,}7\le U_1\le 80{,}3,\ 63\le U_5\le 70,\ 12{,}6\le U_{10}\le 15{,}4.$$

Based on the technological conditions of the EPS operation, the inequality constraints are imposed on unmeasured variables:

$$\begin{aligned}&-12{,}22\le P_2\le 47{,}78,\\ &4{,}91\le Q_2\le 64{,}91,\\ &-182{,}109\le P_{2-1}\le -122{,}109,\\ &43{,}32\le P_{2-3}\le 103{,}32,\\ &-15{,}41\le Q_{2-3}\le 20{,}51,\\ &25{,}42\le P_{2-4}\le 85{,}42,\\ &-16{,}79\le Q_{2-4}\le 19{,}21,\\ &11{,}14\le P_{2-5}\le 71{,}14,\\ &-14{,}97\le Q_{2-5}\le 21{,}027.\end{aligned}$$

Figure 2 presents the results of a comparative analysis of the minimum objective function (1) for deviation of the measurements from reference values for the Lagrange multipliers method (LMM) [9] and the Interior point method (IPM) as well as the estimates of unmeasured variables.

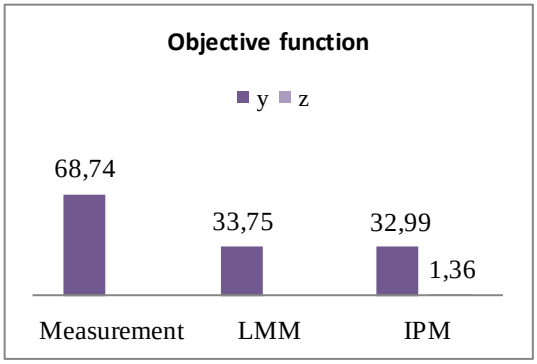

Fig. 3. Objective function minimization diagram.

Thus, the proposed approach allows us to find estimates not only of the measured variables, but also unmeasured, in contrast to the traditional methods of state estimation, in the use of which it is necessary to calculate them.

6. Conclusions

1. The paper provides an analysis of cyberattacks on the SCADA system and WAMS. Particular attention is paid to DOS-attacks, as they may lead to a failure of measuring and processing devices. Thus, the completeness and reliability of data streams on operating parameters is reduced.
2. An algorithm for EPS state estimation based on the method of interior point method is proposed. The algorithm makes it possible to obtain the estimates of measurements in case of their loss.

Acknowledgements

This study is supported by the Siberian Branch of the Russian Academy of Sciences (Project III.17.4.2) of the Federal Program of Scientific Research (№ AAAA-A17-117030310438-1).

References

1. N. I. Voropai, Intelligent electric power systems: conception, state, trends, *Avtomatiz. IT Energet.*, no. 3 (20) (2011). P. 11.
2. A. Zhukov, D. Dubinin, O. Opalev, Development of monitoring and control systems in the UES of Russia on a platform of vector measurements parameters, in *ElectroEnergiya **2**(3)* (2014) 52–65.
3. Y. V. Ivanov, A.S. Cherepov, D. M. Dubinin, Systems Analysis of Architecture and Properties of Transient Conditions Monitoring System Components, in *Energy of Unified Grid*, 3 (26) (2016) 62–70.
4. Yao Liu, Peng Ning, Michael K. Reiter, False Data Injection Attacks against State Estimation in Electric Power Grids, in *CCS'09 Proc*. (USA, Illinois, Chicago, 9-13 November 2009), pp. 21–32.
5. Kebina Manandhar, Xiaojun Cao, Yao Liu, Detection of Faults and Attacks Including False Data Injection Attacks in Smart Grid Using Kalman Filter, *IEEE Transactions of Control of Network Systems. Vol. 1, No 4* (December 2014) 370–379.
6. Liang Heng, Jonathan J. Makela, Alejandro D. Dom´ınguez-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. Power and Energy Conference at Illinois* (PECI) (2014), pp. 1–7.
7. Mohd Rihan, 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.
8. R. Kalluri, L. Mahendra, R.K.S. Kumar, G.L.G. Prasad, Simulation and impact analysis of denial-of-service attacks on power SCADA, in *National Power Systems Conference* (2017), paper № 7858908. DOI: 10.1109/NPSC.2016.7858908
9. A. Z. Gamm, I. N. Kolosok, *Bad data detection in measurements in electric power systems* (Nauka, Novosibirsk, Sib. Enterpr. RAS, 2000).
10. V. I. Zorkaltsev, Solution of linear inequality systems by interior points algorithms, in *Proc. Modern optimization methods and their application to energy* (2001), pp. 142–161.
11. I. I. Dikin, *The interior points method in linear and nonlinear programming, ed.* B.T. Polyak (Moscow, KRASAND, 2010), P. 120.
12. L.A. Gurina, V.I. Zorkaltsev, I.N. Kolosok, E.S. Korkina, I.V. Mokry, *EPS state estimation: algorithms and examples of linearized problems* (Irkutsk, MESI SB of RAS, 2016), P. 37.
13. Chawasak Rakpenthai, Suttichai Premrudeep-reechacharn, Sermsak Uatrongjit, Neville R. Watson, An interior point method for WLAV state estimation of power system with UPFCs, *Electrical Power and Energy Systems, 32* (2010) 671–677.
14. Marcin Połomski, Bernard Baron Optimal, Power Flow by Interior Point and Non Interior Point Modern Optimization Algorithms, *Acta Energetica* 1(14) (2013), pp. 132–139.
15. *State standart 32144-2013. Electry energy. Electromagnetic compatibility of technical equipment. Power quality limits in public power supply systems* (Moscow. Standartinform, 2006).