A Matroid Theory Approach to Constructing the Sparse Attacks on Power System State Estimation

Michael Khokhlov
Institute for Socio-Economic and Energy Problems of the North
Komi Science Centre of Ural Branch of the Russian Academy of Sciences
Syktyvkar, Russia
hohlov@energy.komisc.ru

***Abstract* — The problem of malicious false data injection to the power system state estimators has gained a lot of attention recently. By launching false data injection attacks, an attacker can manipulate the injected data to bypass the bad measurement detection and identification and also arbitrary bias the results of state estimation. Of interest are sparse data injection attacks that involve the compromise as few measurements as possible. In this paper, an approach based on matroid theory to construct sparsest attacks is proposed. It is shown that finding the undetectable attacks is reduced to finding the cocircuits of vector matroid that defined over measurement relations. By applying this approach, an attacker can efficiently generate collection of sparse undetectable data injection attacks and also more sparse unidentifiable attacks, those, while being detected, still allow to change the results of state estimation in a predicted way. Success of these attacks is demonstrated through simulation using 14-bus power system.**

***Index Terms*—Power system, cyber security, false data injection, state estimation, vector matroid.**

I. INTRODUCTION

Modern power grids are increasingly dependent on information and communication technologies in order to achieve higher efficiency, reliability and sustainability. The development and implementation of more advanced sensing, communications and control capabilities for power grids enables better monitoring and smarter control. This greater dependence on information systems however creates a new layer of threat arising from cyber intrusion potentially leading to destructive physical effects.

Recently, there has been considerable research concerning false data injection attacks, a class of the integrity attacks, in which an attacker who is able to compromise the measurement devices and/or to hack the communication networks can inject the malicious measurements transmitted to a control center in order to mislead the Energy Management System (EMS) about operating state of a power grid. A range of objectives pursued by an intruder lies from hiding the facts of electricity theft to provoking a system operator to take a control actions changing the power flow in a way beneficial to a particular participant of electricity market. The consequences of control actions, taken under the influence of false information, may be emergency situations, causing failures of specific components and the whole power systems.

In EMS, a barrier to a measurements information that was corrupted or falsified, is an on-line state estimator, one of the most important function of which is bad data detection and identification [1]-[3]. It is well known that the robustness of any estimator is essentially a function of the local redundancy in the measurements [4]-[8]. These fundamental limitations were exploited in [9], showing that it is possible for an attacker to inject a relative small number of malicious measurements that will bypass any bad data detection algorithm. This result initiated a lot of research targeted towards developing methods for constructing the undetectable attacks, as well as defensive mechanism [10]-[16].

In this paper we examine the false data injection attacks from the attackers' point of view, and propose an approach to constructing those based on the matroid theory. The matroid theory is a branch of mathematics developed from the linear algebra and the graph theory, generalizing the structure of independence relations [17]. This theory has been applied to evaluate the adequacy and reliability of a measurement system for power system state estimation [7], [18], [19]. The method being developed allows generating a collection of sparse undetectable attacks and also more sparse unidentifiable attacks, those, while being detected, still able to change the result of state estimation in a predicted way. The next Section discusses vulnerabilities of state estimation that enables undetectable and unidentifiable attacks. In Section III the proposed method is presented and explained. In Section IV success of attacks is demonstrated through simulation using IEEE 14-bus system

II. PRELIMINARIES

A. False Data Injection

In this paper we adopt a linearization of power system equations around a nominal state and employ the following measurement model:

$$z = Hx + \xi, \tag{1}$$

where x is the n-dimensional state vector to be estimated from a set of m measurements contained in the vector z and corrupted by the Gaussian noise vector ξ, H is $m \times n$ measurement Jacobian matrix. Estimated system states are used to calculate all power flow quantities in the system.

In the presence of malicious false data attack, the corrupted measurement is

$$z = Hx + \xi + a, \tag{2}$$

where vector a is malicious data injected by an attacker. Following [15], we name attack as a pair $A = (S, a)$ consisting of a set S of measurements being modified and attack vector a, so that $i \in S \Leftrightarrow a_i \neq 0$.

State estimation processes a set of available measurements to detect, identify and remove all bad data so that they would not corrupt the state estimates. An attacker takes advantages of inherent weakness of state estimators to construct an attack vector a that bypasses bad data processing and biases estimated quantities.

In the real world, coordinated attacks that involve a large number of geographically isolated measurements are improbable. Because of that, not every attack can be practically implemented. Attacks that has low set S cardinality and very sparse vector a are more probable to carry out.

B. Vulnarabilities of State Estimation

Fundamental limitations of bad data detection and identification capabilities are imposed by the local redundancy of the available measurements as defined by power grid topology and measurement configuration.

It is well known, that gross error in a critical measurement can be neither detected nor identified [4], and that gross error in critical pair of measurements is detectable but not identifiable [see discussion in 20]. More general, any k-1 gross errors in a critical k-tuple of measurements are detectable but not identifiable [5]. Therefore, by manipulating critical measurements, attacker can bias the result of the state estimation while avoiding detection at the control center [21]. Furthermore, under false data injection into any k -1 measurements of a critical k-tuple, the state estimator can detect that there are bad data but it cannot identify the measurements being attacked. As a result, valid measurements are rejected whereas some falsified ones are kept.

Taking into account that any state estimator can fail when conforming measurement errors form certain structures in data, the capabilities of an attacker to launch successful attacks are further increased. A vulnerability based on this feature was used in [9] to construct undetectable attacks in the absence of critical measurements. It was shown, that bad data are undetectable if an attacker choose the attack vector in such a way that

$$a = Hb, \tag{3}$$

where $b \neq 0$. It was found in [12], that attack vector (3) comprises an undetectable attack $A = (S, a)$ if and only if a power grid becomes unobservable when the measurements of S are deleted. We note here, that by definition [5], minimal set (with respect to inclusion) that satisfies this condition is a critical k-tuple. Therefore, any critical k-tuple of measurements can be used to construct undetectable attacks.

The identification of multiple conforming bad data is one of the most difficult problems in state estimation. Based on the robustness concepts it was shown in [6] that if majority of measurements of a fundamental set associated with a state variable are perfectly conforming, then any estimator will break down. In this paper we use more strong condition. In [7] it was found, that bad data are topologically identifiable if neither critical k-tuple contains majority of bad measurements, that is

$$f_i \leq \left[(k_i - 1)/2\right], \tag{4}$$

where f_i is the number of bad measurements in i-th critical k-tuple of size k_i, $[y]$ denotes integer part of y. It means, that in case $f_i > [k_i / 2]$ there is always a combination of errors that, being adding to f_i measurements, makes bad data identification to fail. Utilizing such vulnerability enables to construct more sparse attacks.

III. Attack Construction Based on Measurement Matroid

A. Relation to Matroid

A matroid can be viewed as an abstraction of the linear independence relation in vector spaces. The structure $M = \{E, \Im\}$ is said to be the matroid of the matrix B if E corresponds to the set of columns of B, and $\Im$ contains all linearly independent subset of columns [17].

We define matroid on the transposed H. Let $Z = \{z_1, \ldots, z_m\}$ be a set of m measurements. Each measurement $z_i \in Z$ is associated with a unique column vector e_i in matrix H^T. We define $\Im = \{J\}$, where $J \subseteq \Im$, such that all column vectors e_i associated with $z_i \in J$ are linearly independent. Then $M = (Z, \Im)$ is vector matroid over Z with a collection of independent sets given $\Im$. We call it measurement matroid.

In [18] a connection is shown between concepts associated with matroid structure and those with power system observability. In particular, a base of matroid M (maximal independent subset $J \subseteq \Im$) corresponds to a set of basis measurements, a cobase − to a set of redundant measurements; a fundamental cocircuit of a matroid M − to a critical k-tuple of measurements, a coloop − to critical measurement, and so on. In order to construct attacks, we utilize the concept of fundamental cocircuits.

By a series of elementary operations matrix H^T can be reduced to matrix C, known as standard representation matrix of the matroid M:

$$C = \left[I_n \mid D\right], \tag{5}$$

where I_n is $n \times n$ identity matrix, whose columns correspond to the basis measurements, and D is some $n \times (m-n)$ matrix, whose columns correspond to the redundant measurements. The index set of the columns with nonzeros in a row of C is the fundamental cocircuit that corresponds to the critical k-tuple of measurements. Note, the standard matrix C is not unique, i.e. we can shuffle basis vectors to derive different matrix representations of the same matroid.

Zero injections associated with network buses that have neither load nor generation can not be corrupted and should be contracted from the measurement matroid.

B. Undetectable attacks

Proposition 1. If S consists of measurements of i-th fundamental cocircuit of the matroid M, and vector a is set in proportion to the corresponding transposed vector row of matrix C, that is $a = \lambda C_i^T$, where λ is any number, then the attack $A = (S, a)$ is undetectable.

Proof: Standard representation matrix C can be computed from the sparse LU decomposition of the rectangular matrix H:

$$H = LU = \left(LL_1^{-1}\right)\left(L_1 U\right) = C^T T^{-1}, \qquad (6)$$

where $L = \begin{pmatrix} L_1^T & L_2^T \end{pmatrix}^T$ is $m \times n$ matrix, whose first n rows form a lower triangular matrix L_1, U is $n \times n$ upper triangular matrix. It follows from the equation (7) that the матрица C is related to the matrix H through transformation matrix T, so that the attack vector is $a = \lambda C_i^T = \lambda H T_i$ where T_i is i-th column vector of T. Recalling the condition (3) we conclude that attack is undetectable.

The remarkable property of the undetectable attacks, formed based on the measurement matroid is their irreducibility. An attack $A = (S, a)$ is called irreducible [15] if there is no undetectable attack $A' = (S', a')$ with $S' \subseteq S$.

The fundamental system of cocircuits produced from the standard representation matrix (5) provides the an attacker n different undetectable attacks at once. To generate all possible attacks one needs to enumerate all cocircuits of the measurement matroid M. This can be done in incremental polynomial time [22], although the exponential increase of number of cocircuits as the number of measurements grows makes this task practically impossible. At the same time, calculating the linear combination of every two row vectors of one standard matrix (5) can provide a considerable diversity of attacks, which includes all the attacks $A = (S, a)$ with $|S| = 1$ and $|S| = 2$, if those exist. Alternatively, a multitude of different standard representation matrix (5) of the measurement matroid can be calculated, then a collection of attacks extracted from those by eliminating the repeated ones.

C. Unidentifiable attacks

As discussed in Section II, in order to cause a misidentification of bad data, it is sufficient to compromise a majority of measurements of a critical k-tuple.

Let us consider the set of measurements of an arbitrary critical k-tuple and divide the set into two disjoint subsets S and T. An attack $A = (S, a)$ is topologically unidentifiable, if $|S| > |T|$ and upon deleting the measurements of set T it becomes undetectable, i.e. there exist a vector $b \neq 0$, that $a_i = H_i b$, $i \notin T$.

Indeed, the measurement equations (2) under an unidentifiable attack

$$\begin{cases} y_i = H_i x + \xi_i + a_i, & i \in S \\ y_i = H_i x + \xi_i, & i \in Z \setminus S \end{cases} \qquad (7)$$

can be overwritten in an equivalent form:

$$\begin{cases} y_i = H_i (x + b) + \xi_i, & i \in Z \setminus T \\ y_i = H_i (x + b) + \xi_i - H_i b, & i \in T. \end{cases} \qquad (8)$$

Obviously, the number of measurements that are not consistent with the state x is $|S|$. Whereas the number of measurements that are not consistent with $(x + b)$ is less than that, as by assumption $|T| < |S|$. Any high-breakdown point estimator will give an estimate close to $(x + b)$, which may be far away from x.

Proposition 2. Let i-th cocircuit, represented by row vector C_i has size k_i. If S consists of a measurement subset of a cocircuits, so that $|S| > [k_i / 2]$, and nonzero elements a_i, $i \in S$, are set in proportion to the corresponding elements of C_i, then the attack $A = (S, a)$ is unidentifiable.

The number of the unidentifiable attacks produced from the standard representation matrix (5) is considerable larger than a number of undetectable attacks. Moreover, an attacker is less constrained in means of implementation of an attack, as the number of measurements to which an unauthorized access is required can be up to 2 times less than in case of an undetectable attack.

We note, that methods for bad data processing used in today's practice do not have high-breakdown point and they can fail when even $|S| \leq [k_i / 2]$, $k_i > 3$. On the other hand, such methods can withstand some unidentifiable attacks [8], [18].

D. Targeted attacks

The discussed attacks are able to change the results of the power system state estimation in an arbitrary way. Of more interest are the targeted attacks in which the attacker aims to find an attack vector that biases certain chosen power system quantity by certain value.

Consider a t-th measured quantity z_t. Let β be the value by which an attacker wants to change the estimate of z_t, and $(c_1, \ldots, c_t, \ldots, c_m)$ be row vector of the cocircuit, contained t-th measurement. Then, entries of the attack vector are:

$$a_i = \beta \, c_i / c_t \qquad (9)$$

If target quantity is not measured, then an enlarged

measurement matroid is used with a ground set extended by additional target element. The matrix underlying the matroid is obtained from matrix H by concatenating the row vector h_{m+1} associated with unmeasured quantity to H.

A target will be achieved by launching any undetectable, also unidentifiable attacks $A = (S, a)$ with $|S| = k_i - 1$, $k_i > 2$. Otherwise, when $|S| < k_i - 1$, desired change in target quantity cannot be guaranteed. This because the state estimator with low breakdown point under multiple conforming bad data can reject valid measurements different from ones of set T, so the bias of the target quantity will differ from β.

E. Protected measurements

Certain measurements in the power grid are protected from attacks by encryption. This imposes a constraint on the attacker by requiring that the values of the attack vector a corresponding to the protected measurements be made 0. This requirement is implemented in different ways for undetectable and unidentifiable attacks. For undetectable attacks, preliminary contraction of protected measurements from matroid is performed in order to avoid generating cocircuits containing protected measurements. Note, that if n basis measurements are protected, then by series of n contraction the measurement matroid is reduced to the empty matroid. In such a case, an attacker is not able to launch an undetectable attack. For unidentifiable attacks, protected measurements are just not included into S.

The system operator can independently verify values of some measured or unmeasured quantities, and the attacker is constrained to not affect the estimates of those quantities. In this case, the contraction of the associated elements of matroid is performed for both undetectable and unidentifiable attacks.

IV. Simulation Results

The method developed is demonstrated using the IEEE 14-bus system of Fig. 1 for which a DC model is considered. We suppose that 20 real power measurements represented by circles in Fig. 1 have no random noise. The aim of an attacker is to increase the estimate for the branch power flow $P_{2\text{-}4}$ by the value $\beta = 10$ from 55.15 to 65.15 MW. The largest normalized residual (LNR) method is used to detect and identify bad data in state estimation. Two cases are considered.

A. Targeted undetectable attacks

The collection of undetectable attacks is extracted from the matrix representation (5) of the measurement matroid modified by adding targeted power flow $P_{2\text{-}4}$ and contracting zero injection pseudo-measurement P_7. Additional attacks are calculated by a linear combination of every two row vectors of the matrix.

The collection obtained includes 11 targeted undetectable attacks that inject malicious errors into 3 or 4 measurements:

1) $a_4 = 10.0$, $a_7 = -62.18$, $a_8 = -41.87$;
2) $a_4 = 10.0$, $a_8 = -41.87$, $a_{10} = -39.27$;
3) $a_4 = 10.0$, $a_8 = -41.87$, $a_9 = -45.08$;
4) $a_4 = 63.72$, $a_5 = -a_6 = 53.72$, $a_8 = -41.87$;
5) $a_5 = -a_6 = -10.0$, $a_7 = 63.72$, $a_8 = -41.87$;
6) $a_1 = a_3 = 11.74$, $a_4 = 25.06$, $a_8 = 20.31$;
7) $a_1 = a_3 = 7.91$, $a_4 = 20.14$, $a_7 = -20.31$;
8) $a_1 = a_3 = -7.80$, $a_7 = -103.47$, $a_8 = -83.16$;
9) $a_1 = a_2 = -44.25$, $a_4 = 69.31$, $a_8 = 20.31$;
10) $a_1 = a_2 = -29.80$, $a_4 = 49.94$, $a_7 = -20.31$;
11) $a_1 = a_2 = 7.46$, $a_7 = -72.66$, $a_8 = -52.36$.

Simulation of these false data injection attacks have shown that each of them bypasses LNR method and successfully modifies the estimate for $P_{2\text{-}4}$ by the given value. Table I presents typical result of the state estimation performed under a 7-th undetectable attack which compromise 3 power injection measurements P_1, P_2, P_4 and power flow measurement $P_{1\text{-}5}$.

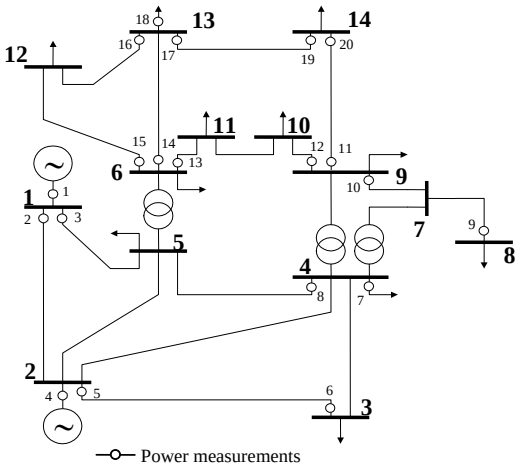

Figure 1. IEEE 14-bus test system

B. Targeted unidentifiable attacks with restrictions

In this case, we suppose that the system operator can independently verify power injections in the buses #1 and #2. Thus an attacker needs to ensure that the estimates for P_1 and P_2 are kept unchanged. To satisfy this restriction, the measurement matroid is modified by contracting these measurements. The collection obtained includes 8 targeted undetectable attacks that inject malicious errors into 4 or 5 measurements:

1) $a_5 = -a_6 = -10.0$, $a_7 = -73.76$, $a_8 = -41.87$;
2) $a_2 = -a_3 = 3.81$, $a_7 = -87.73$, $a_8 = -67.42$;
3) $a_2 = -a_3 = 3.81$, $a_8 = -67.42$, $a_{10} = -55.40$;
4) $a_5 = -a_6 = -10.0$, $a_8 = -41.87$, $a_{10} = -46.57$;
5) $a_2 = -a_3 = 3.81$, $a_8 = -67.42$, $a_9 = -63.60$;
6) $a_5 = -a_6 = -10.0$, $a_8 = -41.87$, $a_9 = -53.47$;
7) $a_2 = -a_3 = -6.25$, $a_5 = -a_6 = -26.39$, $a_7 = -50.85$;
8) $a_2 = -a_3 = -20.12$, $a_5 = -a_6 = -62.78$, $a_8 = 92.98$.

This set of undetectable attacks has 54 unidentifiable attacks. Each of the first 6 attacks shown gives 4 unidentifiable attacks with $|S| = 3$, while each of the last two gives 10 attacks with $|S| = 3$ and also 5 attacks with $|S| = 4$.

Consider the undetectable attack number 7. An unidentifiable attack vector is formed from 3 malicious data

items, $a_3 = -6.25$, $a_5 = -a_6 = -26.39$, injected into power flow measurements $P_{1\text{-}5}$, $P_{2\text{-}3}$ and $P_{3\text{-}2}$. The LNR method detects the bad measurements, but rejects valid ones, $P_{1\text{-}2}$ and $P_{8\text{-}7}$, so that desired change of estimate $P_{2\text{-}4}$ is achieved (see Table I). Note that LNR method does not have high breakdown point, and fails when only two measurements are attacked, for example, under injection $a_5 = -26.39$, $a_7 = -50.85$, but it identifies the attacked measurements correctly when injected data items are the following: $a_2 = -a_3 = -6.25$, $a_5 = -26.39$.

Simulation of all 54 unidentifiable attacks has shown that 47 of those are successful. The LNR method identified 4 attacks. The remaining 3 attacks bypassed the LNR, but the desired change to $P_{2\text{-}4}$ was never achieved.

TABLE I. RESULTS OF THE SIMULATIONS

Paramet.	Meas. point	True value	Case 1		Case 2	
			Estimate	*Residual*	*Estimate*	*Residual*
P_1	1	219.00	226.91	0.0	219.00	0.0
$P_{1\text{-}2}$	2	147.84	147.84	0.0	141.59	6.25
$P_{1\text{-}5}$	3	71.16	79.07	0.0	77.41	0.0
P_2	4	18.30	38.44	0.0	18.30	0.0
$P_{2\text{-}3}$	5	70.02	70.02	0.0	43.63	0.0
$P_{3\text{-}2}$	6	-70.02	-70.02	0.0	-43.63	0.0
P_4	7	-47.80	-68.11	0.0	-47.80	0.0
$P_{4\text{-}5}$	8	-61.75	-61.75	0.0	-61.75	0.0
$P_{8\text{-}7}$	9	0.0	0.0	0.0	-36.87	36.87
$P_{9\text{-}7}$	10	-28.36	-28.36	0.0	-28.36	0.0
$P_{9\text{-}14}$	11	9.64	9.64	0.0	9.64	0.0
$P_{9\text{-}10}$	12	5.77	5.77	0.0	5.77	0.0
$P_{6\text{-}11}$	13	6.73	6.73	0.0	6.73	0.0
$P_{6\text{-}13}$	14	17.25	17.25	0.0	17.25	0.0
$P_{6\text{-}12}$	15	7.61	7.61	0.0	7.61	0.0
$P_{13\text{-}12}$	16	-1.51	-1.51	0.0	-1.51	0.0
$P_{13\text{-}14}$	17	5.26	5.26	0.0	5.26	0.0
P_{13}	18	-13.50	-13.50	0.0	-13.50	0.0
$P_{14\text{-}13}$	19	-5.26	-5.26	0.0	-5.26	0.0
$P_{14\text{-}9}$	20	-9.64	-9.64	0.0	-9.64	0.0
$P_{2\text{-}4}$	-	55.15	65.15	-	65.15	-

V. CONCLUSIONS

The new method based on the matroid theory for constructing the sparse undetectable and sparser unidentifiable false data injection attacks on power system state estimation has been developed. The collection of attacks is generated from the standard representation matrix of the measurement matroid. The method allows constructing targeted attacks and is able to take into account the restrictions imposed by presence of the protected measurements. It has been shown that the number of unidentifiable attacks significantly exceeds the one of the undetectable attacks. Moreover, protection of *n* basis measurements used as a defense mechanism against undetectable attacks is not efficient in case of unidentifiable attacks.

REFERENCES

[1] A. Abur, A. Gómez-Expósito, *Power System State Estimation: Theory and Implementation*, New York: Marcel Deccer, Inc, 2004.

[2] A. Monticelli, *State estimation in electric power systems: A generalized approach*, Boston: Kluwer Academic Publishers, 1999.

[3] A. Z. Gamm, I. N. Kolosok, *Bad Data Detection in Measurements in Electric Power Systems*, Novosibirsk: Nauka, Sib. Enterpr. RAS, 2000. [In Russian]

[4] K. A. Clements, G. R. Krumpholz, P. W. Davis, "Power system state estimation residual analysis: an algorithm using network topology," *IEEE Trans. Power Apparatus and Systems*, vol. PAS-100, no. 11, pp. 1779-1787, 1981.

[5] K. A. Clements, P. W. Davis, "Multiple bad data detectability and identifiability: A geometric approach," IEEE Trans. Power Delivery, vol. PWRD-1, no. 3, pp. 355-360, 1986.

[6] L. Mili, V. Phaniraj, P. R. Rousseeuw, "High breakdown point estimation in electric power systems," *EEE International Symposium on Circuit and Systems*, New Orleans, 1990, pp. 1843-1846, 1990.

[7] M. V. Khokhlov, "Redundancy of measurements as a way to improve measurement system reliability," in *Proc. 79th Int. Scientific Workshop on Methodological Problems in Reliability Study of Large Energy Systems*, *July, 2007*, Issue 58, Moscow-N. Novgorod, pp. 350-363, 2008. [In Russian]

[8] M. V. Khokhlov, "Breakdown properties of robust state estimation of electric power systems," *Electrichestvo*, no. 4, pp. 2-12, 2010. [In Russian]

[9] Y. Liu, M. K. Reiter, P. Ning, "False data injection attacks against state estimation in electric power grids," in *Proc. 16th ACM Conf. on Computer and Communications Security*, New York, NY, USA, 2009.

[10] A. Teixeira, S. Amin, H. Sandberg, K. H. Johansson, S. S. Sastry, "Cyber security analysis of state estimators in electric power systems," in Proc. 49th IEEE Conf. Decision and Control, Dec. 15-17, 2010, Atlanta, GA, USA, pp. 5991-5998, 2010.

[11] R. B. Bobba, K. M. Rogers, Q. Wang, H. Khurana, K. Nahrstedt, T. J. Overbye, "Detecting false data injection attacks on DC state estimation," in *Proc. 1st IEEE Workshop Secure Control Systems*, Stockholm, 2010.

[12] O. Kosut, L. Jia, R. Thomas, L. Tong, "Malicious data attacks on smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645-658, 2011.

[13] T. T. Kim, H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326-333, 2011.

[14] S. Cui, Z. Han, S. Kar, T. T. Kim, H. Poor, A. Tajer, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," *IEEE Signal Processing Magazine*, vol. 29, no. 5, pp. 106-115, 2012.

[15] A. Giani, E. Bitar, M. Garcia, M. McQueen, P. Khargonekar, K. Poolla, "Smart grid data integrity attacks," *IEEE Trans. Smart Grid*, vol. 4, no. 3, pp. 1244-1253, 2013.

[16] M. Ozay, I. Esnaola, F. T. Y. Vural, S. L. Kulkarni, H. V. Poor, "Sparse attack construction and state estimation in the smart grid: centralized and distributed models," *IEEE Journal on Selected Areas in Communications*, vol. 31, no. 7, pp. 1306-1318, 2013.

[17] J. G. Oxley, *Matroid Theory*, New York: Oxford University Press, 1992.

[18] N. Manov, M. Khokhlov, Y. Chukreyev, G. Shumilova, M. Uspensky, M. Chukreyev et al. *Methods and Models for Study of Reliability of Electric Power Systems*, Syktyvkar: Komi SC, Ural Br., RAS, 2010. [In Russian]

[19] M. V. Khokhlov, "Evaluating the reliability of power system observability," in *Proc. 83th Int. Scientific Workshop on Methodological Problems in Reliability Study of Large Energy Systems*, *Sep., 2011*, Issue 62, Ivanovo, pp. 439-449, 2012. [In Russian]

[20] L. Mili, T. Van Cutsem, M. Ribbens-Pavella, "Hypothesis testing identification: A new method for bad data analysis in power system state estimation," *IEEE Trans. Power Apparatus and Systems*, vol. PAS-103, no. 11, pp. 3239-3252, 1984.

[21] M. Göl, A. Abur, "Identifying vulnerabilities of state estimators against cyber-attacks," in *Proc. IEEE PowerTech*, Grenoble, France, 2013.

[22] L. Khachian, E. Boros, K. Elbassioni, V. Gurvich, K. Makino, "On the complexity of some enumeration problems for matroids," *SIAM Journal on Discrete Mathematics*, vol. 19, no. 4, 2005, pp. 966-984.