International Journal of Trend in Scientific Research and Development (IJTSRD)

International Open Access Journal

ISSN No: 2456 - 6470 | www.ijtsrd.com | Volume - 2 | Issue – 2

Data Injection using Kalman- like Particle Filter based Smoother is Diagonalized into Subsystem

Sarumathy. B
Department of CSE, Mailam Engineering College,
Mailam, Tamil Nadu, India

Indra. E
Assistant Professor, CSE, Mailam Engineering
College, Mailam, Tamil Nadu, India

ABSTRACT

Web applications are typically developed with hard time constraints and are often deployed with security vulnerabilities. Automatic web vulnerability scanners can help to locate these vulnerabilities and are popular tools among developers of web applications. Their purpose is to stress the application from the attacker's point of view by issuing a huge amount of interaction within it. Two of the most widely spread and dangerous vulnerabilities in web applications are SQL injection and cross site scripting (XSS), because of the damage they may cause to the victim business. The most common types of software faults are injected in the web application code which is then checked by the scanners. The results are compared by analyzing coverage of vulnerability detection and false positives. Added to this it checks whether the domain or URL gives is present in any of the domain blacklist sites. It also provides I Category- the category classification for the given domain. So this gives the analyst an advantage of having the Domain rating for the given domain with a lookup on top blacklist providing sites and also the Category Classification for the given domain. Three leading commercial scanning tools are evaluated and the results show that in general the coverage is low and the percentage of false positives is very high.

Keywords: *Interarea oscillation, Kalman filter, model prediction, multisensor data fusion, phasor measurement unit (PMU), power system stability, synchrophasor, track-level measurement fusion*

NOMENCLATURE

Acronyms and Abbreviations of Mathematical Formulations

KLPF	Kalman like particle filter.
MHE	Moving horizon estimate.
PMU	Phasor measurement unit.
TFMP	Track-level fusion-based model prediction.
TFC	Track fusion center.
α	Constant matrix with compatible dimension
$f(.)$	Nonlinear function for state transition model.
$x0$	Initial condition of the oscillation state.
w	Random process noise.
t	Time instant.
T	Number of time instants.
z	Observation vector.
p	Number of synchrophasor observations.
X	State matrix for oscillations.
Υ	Observation noise.
N	Number of sensors.

I. INTRODUCTION

Modern electrical grids demand accurate sensor measurements and communication channels to perform effective coordinated operations. Recent deployment of PMUs in transmission networks enables real-time grid dynamics to be recorded and transmitted to local data acquisition servers. Subsequently, signal processing algorithms can be applied to extract system information for online grid operations. However, the close coupling between cyber and physical operations can make system operations vulnerable to cyberattacks[1], [2]. In this paper, the focus is toward cyberattacks in the form of data injections [1]–[10]. Abnormal data superimposed into collected synchrophasor measurements can cause false system information to be interpreted by installed monitoring algorithms. This can then lead to delays in mitigation actions. Among monitoring schemes using PMU measurements, state estimation and oscillation detection are more popular applications. Despite several methods are proposed for bad data detection in state estimation [4]–[6], none explored in the field of oscillation detection. Thus, the motivation of this paper improves the immunity of oscillation detection schemes against data injections.

Power oscillations are electromechanical dynamics between synchronous generators in an interconnected grid. The frequency of local oscillation ranges from 0.8 to 2 Hz, while the frequency of intraarea mode are from 0.1 to 0.8 Hz [11], [12]. Interarea oscillations are difficult to monitor and are prone in systems that are operating near their technical transfer capacity. As a result, monitoring algorithms to detect interarea oscillation using synchrophasor measurements are proposed in recent time [12]–[18]. The objective is to detect lightly damped oscillations at early stage before they trigger angular and voltage instabilities. Interarea oscillation was responsible for the North America northwestern blackout [12]. The present research trend is moving toward recursively monitoring oscillations under ambient situations. Recursive techniques can be categorized into: 1) curve-fitting; and 2) an *a priori* knowledge-based. The first refers to publications that extract oscillatory parameters directly from measurements [14]–[16]. The latter are associated with methods that approximate parameters using previous knowledge of the system as well as the collected measurements [17]. An *a priori* knowledge based approach provides higher estimation accuracy under ambient or noisy conditions when accurate model is provided [18]. In this case, approximating electromechanical oscillations as a sum of exponentially damped sinusoidal signals is considered an accurate model representation in oscillation monitoring research [13]. Hence, the emphasis of this paper is toward enhancing *a priori* knowledge-based techniques. Despite published methods in oscillation detection can operate under noisy conditions, they are not proven to be resilient against data-injection attacks. Such attack is an emerging threat due to the increasing dependency of digital measurements for monitoring and control applications in recent years [7]. Majority of published monitoring methods are formulated based on the assumption of the measurements are not contaminated by human interventions. According to [3] and [8], cyberattacks through introducing periodic or continuous bias to system measurements are possible. There are no guarantees that all cyberattacks can be prevented. Any successful attack will cause existing monitoring schemes to generate inaccurate system information, which may then lead to cascading failures [7], [9], [10]. In recent literature, several methods are proposed to identify abnormal data segments and isolate attacked sensors [4], [7]–[10]. However, they usually require a large data batch and are computational intensive. Although an attacked sensor can be eventually identified, the time between the start of the attack until successful isolation can be in minutes or hours. This is a significant time window to trigger wide-area blackouts as operators are still being fed with false information. Referring to [12] and [19], it only takes minutes to make interarea oscillation become lightly damped and generate wide-area angular and voltage instabilities. Coming from the system operational perspective, the key objective is to minimize the potential damage of data-injection attack through novel processing of information collected from distributed sensors. To the authors' knowledge, such enhancement in oscillation monitoring algorithms has not been proposed. Therefore, this paper contributes toward proposing a signal processing solution to enhance the resilience of existing oscillation monitoring methods against contaminated measurements. Since data-injection attacks in electrical grids can be considered as a regional event, the use of distributed architecture such as [18] is an adequate option against data contaminations. However, given the uncertainties of datainjection attack in the prescribed error statistics, it can be inappropriate to spend a huge amount of computational power to filter erroneous information as used by the algorithmic structure. Referring to [13], monitoring algorithms shall meet: 1) robustness against random fluctuations and bias; and 2) the computational cost of the propagation of estimation of each electromechanical oscillations. To achieve the robustness, while optimizing the computational complexity, constraints of perturbation and random fluctuations shall be considered. The aim is to maintain the accuracy of extracting oscillatory parameters as well as detecting potential monitoring nodes that are being attacked. In this paper, we integrated a modified KLPF-based smoother from

[18] into the proposed TFMP approach. This concept is inspired from multisensory data fusion theory [21] and derived to support the formulation of providing immunity toward data-injection attacks. Here, the TFC represents the collection of measurements from all local sensors. The concept is developed in a distributed feedback environment.

To understand the integration of data-injection attacks into the oscillation monitoring application, an overview of the proposed multisensor TFMP is illustrated in Fig. 1. The considered scenario assumed that the attacker is smart enough to inject data that can imitate regular variations of small-signal system dynamics. TFMP can resolve this concern by manipulating estimated oscillation parameters from all local sensor monitoring nodes. In this paper, a local sensor monitoring node refers to a site where KLPF-based smoother will be applied to extract oscillation parameters from PMU measurements collected at a substation. Furthermore, each monitoring node is assumed to be able to interact with its neighbors through substation communication channels. The estimated parameters are then communicated to the TFC and followed by track association and track fusion at the global level. Note the TFC is developed to compute and minimize the errors of filtering, prediction, and smoothing within each local sensor monitoring node.

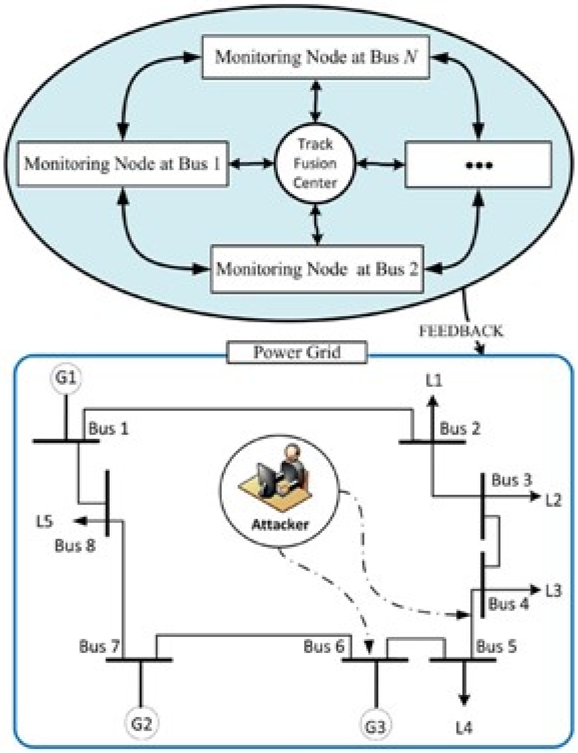

Fig 1: Proposed TFMP scheme to estimate and detect data-injection attacks during power oscillations monitoring

The paper is organized as follows. The proposed scheme is formulated in Section II. In Section III, the implementation and evaluation on a test case is discussed, and finally the conclusions are drawn in Section IV.

II. LITERATURE SURVEY

1. T. T. Kim and H. V. Poor, "Strategic protection against data-injection attacks on power grids," IEEE Trans. Smart Grid, vol. 2, no. 2, pp. 326–333, Jun. 2016.

Data injection attacks to manipulate system state estimators on power grids are considered. A unified formulation for the problem of constructing attacking vectors is developed for linearized measurement models. Based on this formulation, a new low-complexity attacking strategy is shown to significantly outperform naive ℓ_1 relaxation. It is demonstrated that it is possible to defend against malicious data injection if a small subset of measurements can be made immune to the attacks. However, selecting such subsets is a high-complexity combinatorial problem given the typically large size of electrical grids. To address the complexity issue, a fast greedy algorithm to select a subset of measurements to be protected is proposed. Another greedy algorithm that facilitates the placement of secure phasor measurement units (PMUs) to defend against data injection attacks is also developed. Simulations on the IEEE test systems demonstrate the benefits of the proposed algorithms.

2. O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Limiting false data attacks on power system state estimation," J. Fourier Anal. Appl., vol. 14, pp. 877–905, Dec. 2016

Malicious attacks against power system state estimation are considered. It has been recently observed that if an adversary is able to manipulate the measurements taken at several meters in a power system, it can sometimes change the state estimate at the control center in a way that will never be detected by classical bad data detectors. However, in cases when the adversary is not able to perform this attack, it was not clear what attacks might look like. An easily computable heuristic is developed to find bad adversarial attacks in all cases. This heuristic recovers the undetectable attacks, but it will also find the most damaging attack in all cases. In addition, a Bayesian formulation of the bad data problem is introduced, which captures the prior information that a control center has about the likely state of the power system. This formulation softens the impact of undetectable attacks. Finally, a new L∞ norm detector is introduced, and it is demonstrated that it outperforms more standard L2 norm based detectors by taking advantage of the inherent sparsity of the false data injection.

3. M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, "Sparse attack construction and state estimation in the smart grid: Centralized and distributed models," IEEE J. Sel. Areas Commun., vol. 31, no. 7, pp. 1306–1318, Jul. 2015.

New methods that exploit sparse structures arising in smart grid networks are proposed for the state estimation problem when data injection attacks are present. First, construction strategies for unobservable sparse data injection attacks on power grids are proposed for an attacker with access to all network information and nodes. Specifically, novel formulations for the optimization problem that provide a flexible design of the trade-off between performance and false alarm are proposed. In addition, the centralized case is extended to a distributed framework for both the estimation and attack problems. Different distributed scenarios are proposed depending on assumptions that lead to the spreading of the resources, network nodes and players. Consequently, for each of the presented frameworks a corresponding optimization problem is introduced jointly with an algorithm to solve it. The validity of the presented procedures in real settings is studied through extensive simulations in the IEEE test systems.

4. O. Vukovic, K. C. Sou, G. Dan, and H. Sandberg, "Network-aware mitigation of data integrity attacks on power system state estimation," IEEE J. Sel. Areas Commun., vol. 30, no. 6, pp. 1108–1118, Jul. 2016.

Critical power system applications like contingency analysis and optimal power flow calculation rely on the power system state estimator. Hence the security of the state estimator is essential for the proper operation of the power system. In the future more applications are expected to rely on it, so that its importance will increase. Based on realistic models of the communication infrastructure used to deliver measurement data from the substations to the state estimator, in this paper we investigate the vulnerability of the power system state estimator to attacks performed against the communication infrastructure. We define security metrics that quantify the importance of individual substations and the cost of attacking individual measurements. We propose approximations of these metrics, that are based on the communication network topology only, and we compare them to the exact metrics. We provide efficient algorithms to calculate the security metrics. We use the metrics to show how various network layer and application layer mitigation strategies, like single and multi-path routing and data authentication, can be used to decrease the vulnerability of the state estimator. We illustrate the efficiency of the algorithms on the IEEE 118 and 300 bus benchmark power systems.

III. PROPOSED SYSTEM

his section derives the formulation of the proposed scheme. It begins with outlining the assumed system model, followed by the state representation of electromechanical oscillations. The TFMP algorithm is then built on it for calculating the estimates. An overview of the formulation framework of this section is illustrated in Fig. 2. It summarizes the formulation and equations involved at each step while tackling random data-injection attacks.

Note the formulation is derived from a perspective of a data-based approach. It is not restricted to linearized differential equations, which is merely a simplified model of the true system. In the field of real-time dynamic monitoring, especially for wide-area monitoring system applications, the notion is to become less dependent on classic models and

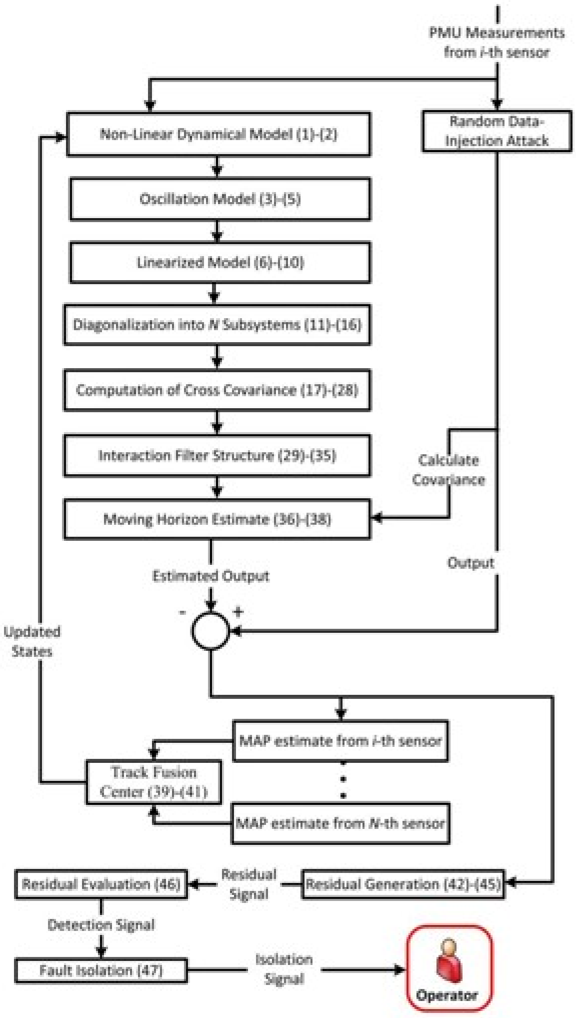
PMU Measurements
from i-th sensor
Non-Linear Dynamical Model (1)-(2)
Random Data-Injection Attack
Oscillation Model (3)-(5)
Linearized Model (6)-(10)
Diagonalization into N Subsystems (11)-(16)
Computation of Cross Covariance (17)-(28)
Interaction Filter Structure (29)-(35)
Calculate Covariance
Moving Horizon Estimate (36)-(38)
Output
Estimated Output
-
+
Updated States
MAP estimate from i-th sensor
Track Fusion Center (39)-(41)
MAP estimate from N-th sensor
Residual Evaluation (46)
Residual Signal
Residual Generation (42)-(45)
Detection Signal
Fault Isolation (47)
Isolation Signal
Operator

Fig 2: Formulation framework of the proposed scheme.

adopt real-time system identification techniques. The reason Fig. 2. Formulation framework of the proposed scheme is classic differential equations are less representative of continuous random load variations, line temperature variations, and other operational uncertainties. Although using differential equation-based models are suitable for some steady-state or static applications like state estimation or automatic generation control, it is not suitable for monitoring electromechanical interactions of synchronous generators [13]. Therefore, system parameters are not extracted from offline predetermined power system models. Instead, the proposed method extracts desired parameters from PMU measurements. *A. State Representation of Observation Model* A power grid prone to data-injection attacks can be expressed as a nonlinear dynamical system model. Perturbations and random fluctuations are part of noise induced transitions in a nonlinear system with dynamics. It is expressed as $\alpha xt+1 = f(xt,wt)$, $t = 0, 1, . . . , T$ (1) where α is the constant matrix with compatible dimensions to the model dynamics, *f (.)* is the nonlinear function representing the state transition model, $x0 \in$ IR*r* is the initial condition of the oscillation state, and superscript *r* is the size of the oscillation state vector in the subspace IR. In addition, *wt* $\in$ IR*r* is the random process noise, *t* is the time instant, and *T* is the number of time instants. Note (1) represents the equation of a systemwhich has nonlinear dynamics. Perturbations and random fluctuations are part of noise-induced transitions in a nonlinear system. These can be from load variations or switching transients of installed devices. Equation (1) can also be represented by any other dynamical system model. It is not only limited to power systems. It is assumed that the power grid described in (1) will be monitored by *N* number of synchronized sensors in a track-level measurement fusion environment. Computation is conducted at a central station, i.e., TFC, which involves control signals at each local node and predictive estimation sequences are generated in the presence of random noise fluctuations. These local sensors will basically be PMUs installed in highvoltage substations, and all will operate at the same sampling rate. The observations vector for extracting electromechanical oscillations at the *i*th node possibly affected by the attack can be defined as

zit
= *hit*
(xt) + ν *i*
t , *i* = 1, . . . , *N* (2)

where *zit* $\in$ IR*pi* , *pi* is the number of synchrophasor observations made by the *i*-sensor, *hi(.)* is a nonlinear function representing the local observation matrix of *i*th sensor, *xt* is the state matrix for oscillations, and ν *i t* $\in$ IR*pi* is the observation noise of the *i*th sensor. A dynamical power grid will be governed by the following constraints: *xt* $\in$ **X***t*,*wt* $\in$ **W***t*, ν *t* $\in$ **V***t* (3) where **X***t*, **V***t*, and **W***t* are assumed to have Gaussian probability distribution function.

Assumption 1: The noises *wt* and ν *t* are all initially assumed to be uncorrelated zero-mean white Gaussian such that IE[*wt*] = IE[ν *t*] = IE[*wg* ν *T h*] = 0, $\forall$ *t*. Note IE denotes the expectation operator, and superscript $*$ denotes the transpose operator. Also, IE[*wgwTh*] = *Rt* δ *gh*, IE[ν *g* ν *T h*] = *Qt* δ *gh*, $\forall$ *t*, where *Rt* represents the residual covariance and δ *gh* is a Kronecker delta which is one when variables *g* and *h* are the same. *Qt* is the process noise correlation

factor. Once the observation model is constructed from synchrophasor measurements collected from the affected location, the corresponding state representation of electromechanical oscillations can then be formulated in the frequency domain. *B. Electromechanical Oscillation Model Formulation* Suppose a measured noise-induced signal contained *K* number of electromechanical oscillations. Referring to (2), the observation output signal *zit* from an *i*th sensor at time *t* can be modeled in the frequency domain as *zit* = *K* _ *k*=1 *ake*(− *σ* k+*j*2 *π fk*)*tTs* + *v i t* , *t* = 1, 2, ... , *T* (4) where *ak* is the complex amplitude of *k*th mode, *σ k* is the damping factor, *fk* is the oscillatory frequency, and *Ts* is the sampling time [17]. Equation (2) has been transformed to (4), i.e., time domain to the frequency domain, using the Laplace transform. The system's poles and zeros are then analyzed in the complex plane. Moreover, it is especially important to transform the system into frequency domain to ensure whether the poles and zeros are in the left or right half planes, i.e., have real part greater than or less than zero. For convenience, the term − *σ k* + *j*2 *π fk* is represented in the rectangular form as *λ k*. In this paper, the *k*th oscillation or eigenvalue within a mentioned signal is described by two states denoted as *xk,t* and *xk*+1,*t*, respectively. They can also be expressed for an *i*th sensor as *xik ,t* = *e*(− *σ* k+*j*2 *π fk*)*tTs* , *xik* +1,*t* = *bk*+1*e*(− *σ* k+1+*j*2 *π fk*+1)*tTs* . (5) The term *bk* represents the complex amplitude of the *k*th mode. Based on (5), a signal consisting of *K* number of exponentially damped sinusoids will be modeled by 2*K* number of states. Note that the *k*th eigenvalue of a particular signal is described by two states denoted as *xk,t* and *xk*+1,*t*, i.e., for *k*th and *k* + 1th mode, respectively. The eigenvalue represents the electromechanical oscillations between synchronous generators in the physical world. Details can be referred to [12] and [13]. In addition, the damping factor *σ k* and the corresponding frequency *fk* of each oscillation will be computed from the state *xt*. Estimating oscillatory parameters in the presence of a random data-injection attack will require the complete observability of the oscillation observation matrix. For a nominal case without data injections, this was previously achieved by using an expectation maximization (EM) algorithm that utilized the initial correlation information extracted from KLPF [18]. Initial correlation information can be defined as the information collected from the initial estimates of the observation model ˆ*H* 0 *t* . The superscript 0 represents the initial estimates. However, considering a datainjection attack situation, taking an averaged form of the log-likelihood function to improve estimate as in [18] is not sufficient. Instead, the initial correlation shall be iteratively calculated by: 1) using the first and second moments of the input model for a node *i*; 2) getting *a priori* information from the constraints; and 3) getting its observation estimates through time and frequency correlation for each *i*th sensor. Note in this paper, monitoring power oscillation is used as an application. The proposed scheme can be utilized by any other application
as well.

PHP 6 AND UNICODE

PHP received mixed reviews due to lacking native Unicode support at the core language level. In 2005, a project headed by Andrei Zmievski was initiated to bring native Unicode support throughout PHP, by embedding the International Components for Unicode (ICU) library, and representing text strings as UTF-16 internally. Since this would cause major changes both to the internals of the language and to user code, it was planned to release this as version 6.0 of the language, along with other major features then in development.

PHP 7

As of 2014, work is underway on a new major PHP version named PHP 7. There was some dispute as to whether the next major version of PHP was to be called PHP 6 or PHP 7. While the PHP 6 unicode experiment had never been released, a number of articles and book titles referenced the old PHP 6 name, which might have caused confusion if a new release were to reuse the PHP 6 name. After a vote, the name PHP 7 was chosen.

To simulate deliberate attack scenarios, data injections are carried out in the collected synchrophasor measurements. Since all three electromechanical modes are observable at buses 16 and 17, these two locals are selected as attack nodes. Their neighboring nature as shown in Fig. 3 helped to create a situation of regional attacks on measured data. Simulated attack scenarios at buses 16 and 17 are as follows.

1) ***First Injection:*** Random data injections are introduced at bus 16 from 7 to 12 s.

2) *Second Injection:* Signal with relatively high energy potency are injected at bus 16 from 22 to 27 s.

3) *Third Injection:* Small signature of random sinusoidal waveforms are introduced at bus 16 from 44 to 49 s. Also, ambient disturbance-like injections are introduced at bus 17 from 48 to 55 s.

4) *Fourth Injection*: Small signature of random sinusoidal waveforms are introduced at bus 16 from 44 to 49 s. Also, a data-repetition attack was introduced at bus 17 from 55 to 60 s. This attack replaces the normal oscillation behavior with those recorded at bus 17 from 40 to 45 s.

IV. SYSTEM IMPLEMENTATION

PHP is a server-side scripting language designed for web development but also used as a general-purpose programming language. As of January 2013, PHP was installed on more than 240 million websites (39% of those sampled) and 2.1 million web servers. Originally created by RasmusLerdorf in 1994, the reference implementation of PHP (powered by the Zend Engine) is now produced by The PHP Group. While PHP originally stood for Personal Home Page, it now stands for PHP: Hypertext Preprocessor, which is a recursive backronym.

PHP code can be simply mixed with HTML code, or it can be used in combination with various templating engines and web frameworks. PHP code is usually processed by a PHP interpreter, which is usually implemented as a web server's native module or a Common Gateway Interface (CGI) executable. After the PHP code is interpreted and executed, the web server sends resulting output to its client, usually in form of a part of the generated web page; for example, PHP code can generate a web page's HTML code, an image, or some other data.

My-SQL Database

MySQL is the world's second most widely used relational database management system (RDBMS) and most widely used open-source RDBMS. It is named after co-founder Michael Widenius's daughter, The SQL acronym stands for Structured Query Language.

The MySQL development project has made its source code available under the terms of the GNU General Public License, as well as under a variety of proprietary agreements. MySQL was owned and sponsored by a single for-profit firm, the Swedish company MySQL AB, now owned by Oracle Corporation.

V. CONCULSION AND FUTURE WORK

In this paper, the proposed TFMP-based monitoring scheme is proposed and demonstrated to estimate power oscillations modes during data-injection attacks. The model prediction property of the algorithm has helped to remove bias and noise while accurately extracting the system parameters. It is further facilitated by the derived diagonalized interaction filter, which tackles the error covariance in the form of subsystems, and thus improving the initial oscillatory state estimates. As a result, the incorporation of the proposed algorithm into oscillation detection has provided more accurate results than existing oscillation monitoring schemes in the presence of data-injection attacks. The immunity of monitoring applications against intentional data injections has been enhanced. In the future, studies to quantitatively verify the effectiveness and robustness of the proposed method to more adverse nonregional threats will be conducted.

REFERENCES

1. S. Gorman, “Electricity grid in U.S. penetrated by spies,” *Wall Street J.*, Apr. 2009.
2. L. C. Baldor. (Aug. 3, 2010). *New Threat: Hackers Look to Take Over Power Plants*. [Online]. Available: http://abcnews.go.com/ Business/wireStory?id=11316203
3. T. T. Kim and H. V. Poor, “Strategic protection against data-injection attacks on power grids,” *IEEE Trans. Smart Grid*, vol. 2, no. 2, pp. 326–333, Jun. 2011.
4. O. Kosut, L. Jia, R. J. Thomas, and L. Tong, “Limiting false data attacks on power system state estimation,” *J. Fourier Anal. Appl.*, vol. 14, pp. 877–905, Dec. 2008.
5. M. Ozay, I. Esnaola, F. T. Y. Vural, S. R. Kulkarni, and H. V. Poor, “Sparse attack construction and state estimation in the smart grid: Centralized and distributed models,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 7, pp. 1306–1318, Jul. 2013.
6. O. Vukovic, K. C. Sou, G. Dan, and H. Sandberg, “Network-aware mitigation of data integrity

attacks on power system state estimation," *IEEE J. Sel. Areas Commun.*, vol. 30, no. 6, pp. 1108–1118, Jul. 2012.

7. S. Sridhar, A. Hahn, and M. Govindarasu, "Cyber-physical system security for the electric power grid," *Proc. IEEE*, vol. 100, no. 1, pp. 210–224, Jan. 2012.
8. O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 645–658, Dec. 2011.
9. S. Cui *et al.*, "Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions," *IEEE Signal Process. Mag.*, vol. 29, no. 5, pp. 106–115, Sep. 2012.
10. L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Trans. Smart Grid*, vol. 2, no. 4, pp. 659–666,Dec. 2011.
11. P. Kundur, N. J. Balu, and M. G. Lauby, *Power System Stability and Control*, vol. 7. New York, NY, USA: McGraw-Hill, 1994.
12. G. Rogers, *Power System Oscillations*. Boston, MA, USA: Kluwer, 2000.
13. A. R. Messina, *Inter-Area Oscillations in Power Systems: A Nonlinear and Nonstationary Perspective*. New York, NY, USA: Springer, 2009.
14. J. J. Sanchez-Gasca and J. H. Chow, "Performance comparison of three identification methods for the analysis of electromechanical oscillations," *IEEE Trans. Power Syst.*, vol. 14, no. 3, pp. 995–1002, Aug. 1999.
15. S. A. N. Sarmadi and V. Venkatasubramanian, "Electromechanical mode estimation using recursive adaptive stochastic subspace identification," *IEEE Trans. Power Syst.*, vol. 29, no. 1, pp. 349–358, Jan. 2014.
16. R. W. Wies and J. W. Pierre, "Use of least-mean square (LMS) adaptive filtering technique for estimating low-frequency electromechanical modes of power systems," in *Proc. Amer. Control Conf.*, vol. 6. Anchorage, AK, USA, May 2002, pp. 4867–4873.
17. J. C.-H. Peng and N. C. Nair, "Enhancing Kalman filter for tracking ringdown electromechanical oscillations," *IEEE Trans. Power Syst.*, vol. 27, no. 2, pp. 1042–1050, May 2012.
18. H. M. Khalid and J. C.-H. Peng, "Improved recursive electromechanical oscillations monitoring scheme: A novel distributed approach," *IEEE Trans. Power Syst.*, vol. 30, no. 2, pp. 680–688, Mar. 2015.
19. D. N. Kosterev, C. W. Taylor, and W. A. Mittelstadt, "Model validation for the August 10, 1996 WSCC system outage," *IEEE Trans. Power Syst.*, vol. 14, no. 3, pp. 967–979, Aug. 1999.
20. L. Xie, D.-H. Choi, S. Kar, and H. V. Poor, "Fully distributed state estimation for wide-area monitoring systems," *IEEE Trans. Smart Grid*, vol. 3, no. 3, pp. 1154–1169, Sep. 2012.