Multi-agent System for Detecting False Data Injection Attacks Against the Power Grid

Esther Amullen
Tennessee State University
3500 John A. Merritt Blvd
Nashville, TN, 37209
eamullen@my.tnstate.edu

Hui Lin *
University of Illinois at Urbana-Champaign
1308 W. Main St.
Urbana, IL 61801
hlin33@illinois.edu

Zbigniew Kalbarczyk
University of Illinois at Urbana-Champaign
1308 W. Main St.
Urbana, IL 61801
kalbarcz@illinois.edu

Lee Keel
Tennessee State University
3500 John A. Merritt Blvd
Nashville, TN, 37209
lhkeel@tnstate.edu

ABSTRACT

A class of cyber-attacks called False Data Injection attacks that target measurement data used for state estimation in the power grid are currently under study by the research community. These attacks modify sensor readings obtained from meters with the aim of misleading the control center into taking ill-advised response action. It has been shown that an attacker with knowledge of the network topology can craft an attack that bypasses existing bad data detection schemes (largely based on residual generation) employed in the power grid. We propose a multi-agent system for detecting false data injection attacks against state estimation. The multi-agent system is composed of software implemented agents created for each substation. The agents facilitate the exchange of information including measurement data and state variables among substations. We demonstrate that the information exchanged among substations, even untrusted, enables agents cooperatively detect disparities between local state variables at the substation and global state variables computed by the state estimator. We show that a false data injection attack that passes bad data detection for the entire system does not pass bad data detection for each agent.

1. INTRODUCTION

Energy management systems (EMS) in power grids rely on state estimation to obtain information about their operating conditions. State estimation is carried out based on the topology of the power network and data readings taken from measuring units deployed locally at substations. The collected meter measurements are used to estimate state variables which include bus voltage magnitudes and phase angles. Based on state estimates obtained from the state estimator, control decisions and subsequent actions that directly impact the operation of the power grid are made. To handle errors associated with noise and faulty meters in state estimation, bad data detection (BDD) schemes are employed. BDD relies on Chi-square tests and residual signals generated based on the squares of differences between measured data and estimated data [1].

Advanced power grid technology integrates varieties of digital computing and communication technologies, which exposes the power delivery infrastructure to malicious attacks. Attackers with access to the power grid's topology information can carry out false data injection (FDI) attacks. As shown in [2, 3, 4, 5], measurements compromised by FDI attacks can bypass BDD schemes during state estimation. If the control center uses compromised measurements for state estimation, the resulting state estimate will mislead the control center regarding the actual operating condition of the power grid inherently affecting control decisions.

In this paper, we propose a multi-agent system that detects FDI attacks targeting state estimation in power grids. We logically partition a power grid into multiple sub-systems, each comprising a substation and other substations directly connected to it through transmission lines. Because off-shelf computing and communication infrastructures are deployed in substations, we can deploy software-based agents in each substation and allow them to communicate with each other. The agents facilitate exchange of meter measurements among substations that are included in each subsystem. Each agent can perform local state estimation for its sub-system. In the absence of FDI attacks, state estimation results at each sub-system are identical to state estimation results for the whole grid. However, in the presence of FDI attacks compromised measurements can bypass bad data detection during state estimation for the whole grid. State estimation performed at each sub-system is used to analyze the compromised measurements and identify disparities. FDI attacks compromise measurements based on the topological information of the power grid such as connectivity of each substation and susceptance of each transmission line. However, the topological information for each sub-system varies.

*Co-first author

ICSS '16, December 06 2016, Los Angeles, CA, USA
© 2016 ACM. ISBN 978-1-4503-4788-4/16/12...$15.00
DOI: http://dx.doi.org/10.1145/3018981.3018987

As a result, the condition that hides compromised measurements from state estimation for the whole grid can fail in the constructed sub-systems.

To evaluate the proposed strategy for FDI detection, we conduct experiments with the IEEE 9-bus, 14-bus and 30-bus power system benchmarks using MATPOWER [16], an open source MATLAB toolbox. For each system, we generate 1000 attack cases that can bypass BDD schemes during state estimation for the whole grid. Then, we construct sub-systems at each bus in the power system and use state estimation at each sub-system to analyze all FDI cases. In our experiments, we can detect all FDI attack cases with at least one agent.

The rest of this paper is organized as follows; In Section II a survey of related literature is presented. In Section III, preliminary information pertaining to the power grid and state estimation is discussed. In Section IV we discuss our proposed multi-agent system for FDI attack detection. In Section V the experiments used to validate the proposed system are discussed along with the results obtained. In Section VI this paper is concluded with a discussion of our findings and aspects for future research.

2. RELATED WORK

Liu et al. [2], study the problem of False data Injection (FDI) attacks that target measurement data used in DC state estimation and demonstrate that if an adversary has knowledge of the network topology, he can craft an FDI attack to bypass the BDD schemes in place. Since Liu et al. introduced the idea of undetectable FDI attacks, a lot of research effort has gone into this area. [6] shows that encrypting a carefully selected set of measurement devices can enable detection of FDI attacks against DC state estimation. The authors show that the number of measurements that need to be protected to achieve FDI attack detection is equal to the number of total state variables. The strategy in [6] is extended in [7] to maximize the number of encrypted meters. Dan et al. [7] take into account the fact that the power network has a large number of measurement devices and encryption of as many devices as state variables is not always practical or economically feasible. They propose algorithms to deploy encrypted devices in parts of the network that their usefulness is maximized. In addition [8] provides solutions that an operator can use to arbitrarily select critical meters to protect so that an undetectable FDI attack cannot be launched. Furthermore a detection framework employing a security manager, a managed switch and security agents running alongside critical nodes (controllers and edge nodes) was proposed by Wei et al. [9]. Each critical node is monitored by a security agent connected to the security manager through a managed switch capable of separating external and internal transmission. The security manager is protected by conventional IT solutions and provides access control, firmware monitoring, vulnerability patches and security policies to security agents which in turn monitor the critical nodes.

In [10] Yang et al. studied false data injection attacks and defense mechanisms. Specifically, they design attack strategies the inflict maximum damage and propose a defense mechanisms to make critical sensors more resilient to such attacks. The authors also design spatial- and temporal-based detection algorithms that the control center can employ to detect and identify stealthy attacks. A heuristic based false data injection attack detector is proposed in [11]. Kosut et al. leverage the sparse nature of the FDI attack and propose a detection test based on the L_∞ norm computation as opposed to the L_2 norm. The authors show that the L_∞ norm accurately detects the presence of an injected sparse vector. In [12], a strategy based on formation control is proposed to identify corrupted measurements from phasor measurement units (PMUs). Specifically a flocking-based modeling paradigm is used to identify corrupted data during grid transient state. However, transient periods in the power grid are brief, limiting this technique to narrow scenarios. [13], exploits the constraints in power network topology to enhance the state estimator's capacity for bad data detection. Liu et al. proposed an adaptive partitioning state estimation (APSE) technique to detect bad data injections in the smart grid. Specifically, the APSE partitions the power network into several subsystems, and the Chi-squares test for bad data detection is used to detect bad data for each subsystem. Upon detection of bad-data, the subsystems are re-partitioned over several iterations until the bad data is located.

The multi-agent system for FDI attack detection proposed is practical to deploy because it leverages on the existing communication channels among substations stipulated in the IEEE standard [14]. In addition, communication among substations does not need to rely on encryption because any attack on communication compromises every measurement making it easily detectable by the multi-agent system during state estimation. In contrast to the APSE method proposed in [13], our solution is scalable since the node degree does not increase with the scale of the power system [15]. Moreover Liu et al. show that the APSE can only detect bad data within a single transmission line and not the entire network. The iterative nature of the APSE also makes it costly to compute. Using the DC power flow model for the IEEE 9-bus system benchmark [16], we demonstrate that an undetectable FDI attack vector that bypasses the L_2 norm based bad data detector for the entire power grid is detectable by the L_2 norm bad data detector for each agent.

3. PRELIMINARIES

3.1 Overview of the Power Grid Infrastructure

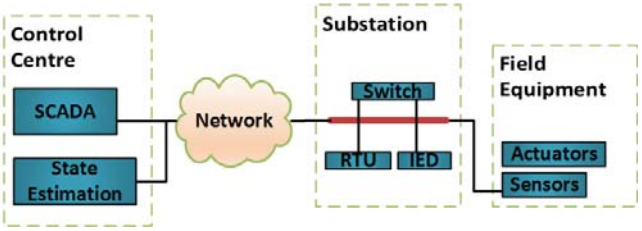


Figure 1: Structure of a Power Grid including communication infrastructure

Figure 1 shows the basic structure of a power grid including the communication infrastructure commonly employed. The key components of the smart grid are: control center, substations and field equipment. The control center comprises a Supervisory Control and Data Acquisition (SCADA) Unit and a state estimator. The control center receives data

such as meter readings, and alarms from the substations through a network. The data received at the control center is used by the state estimator to estimate the operation condition of the power grid. The SCADA unit uses information provided by the state estimator to issue commands (open/close relays, adjust generator or load) to substations. Substations are made up of power equipment and communication equipment such as remote terminal units (RTU) and Intelligent Electronic Devices (IED) (examples of IEDs are; Phasor measurement units (PMU), relays) that can communicate with each other. Devices in substations directly interact with field equipment to effect commands issued by the SCADA unit.

3.2 DC State Estimation

In State estimation based on the DC power flow model, we can correlate the measurement vector z and the state vector x of a power system using the following linear regression model.

$$\mathbf{z} = \mathbf{H}\mathbf{x} + \mathbf{e} \tag{1}$$

where $\mathbf{H}$ is the $m \times n$ measurement Jacobian matrix which encapsulates the topological information of the power system [17], e.g., susceptance of each transmission line. We represent $\mathbf{z}$ as an $m \times 1$ vector with each entry being a meter measurement. In this work, The vector $\mathbf{z}$ comprises the measurements of real power flows at the receiving and sending end of each transmission line and real power injections at each bus. $\mathbf{x}$ is an $n \times 1$ vector with each entry being the phasor angle at each substation. Also, $\mathbf{e}$ is an $n \times 1$ measurement error associated with each entry in $\mathbf{z}$; we assume the measurement error is Gaussian noise. Using the weighted least square criterion [18], a state estimate $\hat{\mathbf{x}}$ can be computed as follows.

$$\hat{\mathbf{x}} = (\mathbf{H^T R H})^{-1}\mathbf{H^T R z} \tag{2}$$

where $\mathbf{R} = diag(1/\sigma_i^2)$, σ^2 is the variance of the meter errors and $i = 1, ..., m$.

Meter errors, incorrect configurations and maliciously injected measurements introduce bad data which affects estimated states [1]. There are several techniques in place for detecting bad data in the power grid. A widely used technique computes a residual between the observed and estimated measurements and uses its L_2 norm to detect bad data. When bad data is present, the L_2 norm increases beyond a preset threshold τ and converges in the absence of bad data.

$$||\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}|| > \tau \tag{3}$$

3.3 False Data Injection (FDI) Attack

An FDI attack against the power grid modifies the measurement vector $\mathbf{z}$ transmitted to the control center by injecting an attack vector $\mathbf{a}$ such that an incorrect measurement vector $\mathbf{z_a}$ is received. [2]

$$\mathbf{z_a} = \mathbf{H}\mathbf{x} + \mathbf{e} + \mathbf{a} \tag{4}$$

In [2], Liu et al show that while a randomly selected attack vector $\mathbf{a}$ is generally detectable by the residual generation based bad data detection system, instances of the attack vector $\mathbf{a}$ maybe undetected. Specifically if $\mathbf{a}$ is a linear combination of the rows in the topology matrix $\mathbf{H}$ it will bypass the BDD system. To construct an undetectable attack vector $\mathbf{a}$, the attacker needs to create an $n \times 1$ vector c such that the entries in $\mathbf{c}$ correspond to targeted state estimates in $\mathbf{x}$ resulting into

$$\mathbf{a} = \mathbf{H}\mathbf{c} \tag{5}$$

If $\mathbf{a} - \mathbf{H}\mathbf{c} = \mathbf{0}$, the attack vector $\mathbf{a}$ is undetectable by the BDD system provided the original measurement z passes BDD. The L_2 norm of the residual from theorem 1 of [2]

$$||\mathbf{z_a} - \mathbf{H}\hat{\mathbf{x}}|| = ||\mathbf{z} + \mathbf{a} - \mathbf{H}(\hat{\mathbf{x}} + \mathbf{c})|| \tag{6}$$

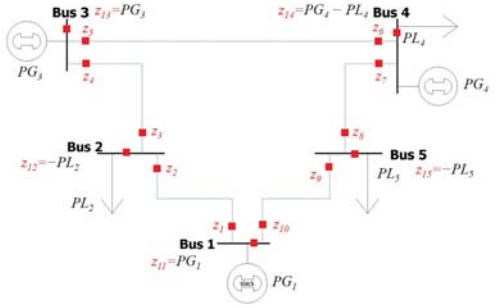
$$= ||\mathbf{z} - \mathbf{H}\hat{\mathbf{x}} + (\mathbf{a} - \mathbf{H}\mathbf{c})|| \tag{7}$$

$$= ||\mathbf{z} - \mathbf{H}\hat{\mathbf{x}}|| \leq \tau \tag{8}$$

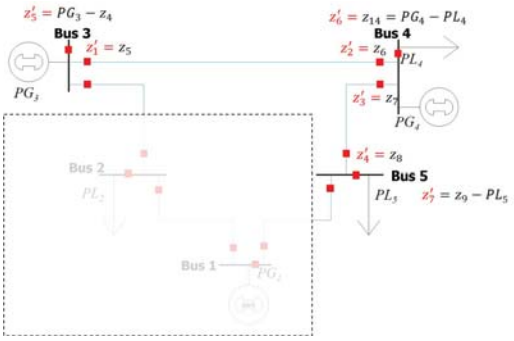
4. PROPOSED MULTI-AGENT SYSTEM FOR FDI ATTACK DETECTION

4.1 Multi-agent System Architecture

In today's power grids, inter-substation communication plays a key role in ensuring local protection at each substation[14]. When a relay in a substation performs protection activities such as opening a circuit breaker to remove a transient short-circuit fault, the substation reports this event to all its neighboring substations. The purpose of this communication is to ensure that when protection activities fail, neighboring substations can perform back-up protection to prevent faults from propagating to large areas.



(a) An example 5-bus System



(b) A sub-system from bus 4

Figure 2: Use agent to build a sub-system from a power grid

Current power grids rely on off-the-shelf computing and communication networks to deliver measurements to control centers. On top of this computing infrastructure, we can install a software agent in each substation. Each agent

stores the measurements from its substation. In addition to delivering these measurements to the control center, it delivers them to agents deployed at the neighboring substations periodically.

Based on the measurements collected from neighboring substations, each agent can build its own sub-system in which the system state, i.e., the phasor angle of each substation, is consistent with the state from the whole system. In Figure 2a, we use a 5-bus system as an example to explain the concept. This power system has 5 buses, 5 transmission lines, 3 load units, and 3 generators. With respect to the DC power flow model, we can have 15 measurements (considering real power flows at the receiving and sending ends of each transmission line and real power injections at each bus). In the figure, we highlight the measurements with red rectangles and letters. Note that the measurement of power injected at a bus is calculated by taking away power consumptions from power generations. For example, at bus 4, we have $z_{14} = PG_4 - PL_4$, where PG_i and PL_i represent power generations and consumptions at bus i.

In Figure 2b, we demonstrate how the agent at bus 4 build a sub-system exclusively based on the measurements from bus 3 and bus 5. The purpose of building the sub-system is that (1) the agent uses the state estimation of the sub-system to obtain the same phasor angle of the involved buses as estimated by the control center when no attacks occur; and (2) the agent can detect compromised measurements in this sub-system while the false data injection attack can bypass state estimation for the whole grid. The sub-systems are created based on the procedure stated in Table 1.

Table 1: Procedure to Build Sub-systems for Agents

Procedure: generate sub-system for agent at bus i

(1) Include bus i and its neighboring buses;
(2) Include the transmission lines that connect the buses selected at (1);
(3) Keep unchanged the real power flow measurements at the sending and receiving end of selected transmission lines;
(4) **For** bus $j \neq i$
(5) **For** transmission line k not selected at (2)
(6) **If** power flow P at line k is delivered into bus j
(7) Increase power injection at bus j by P
(8) **Else**
(9) Decrease power injection at bus j by P
(10) **EndIf**
(11) **EndFor**
(12) **EndFor**

Using the procedure in Table 1, we build a sub-system for bus i which comprises bus i itself, its neighboring buses, and transmission lines that connect them. In this sub-system, we still use the measurements at the receiving and sending end of transmission lines from the whole power grid. However, the power injection at the neighboring buses of bus i is adjusted with the power flowing to the rest of the power systems (blocked by a transparent rectangle in Fig. 2b), based on steps (4)-(12) in Table 1. Following this procedure, we can build the sub-system for each bus. In the sub-system, the power flow equations are maintained for each bus, from which we can obtain the same phasor angles as those obtained during state estimation for the whole grid.

4.2 Threat Model

We don't trust the communication networks that connect control centers and power grid devices in substations. Consequently, we assume that attackers can compromise measurements while they are delivered to the control center. Also, we assume that measurements exchanged between agents at different substations are not trusted. Even though, agents at substations collect untrusted measurements from other substations, the compromised measurements which are crafted based on the topology of the whole power grid can fail to bypass the bad data detection during state estimation performed at the sub-systems.

We assume that an agent uses local sensors to collect trusted measurements from its own field site. In other words, we don't consider the attack case in which attackers can physically manipulate sensors.

4.3 Formal analysis

In this section, we demonstrate how we use state estimation at the sub-systems to detect false injection attacks that are designed to bypass bad data detection during state estimation for the whole power grid. Consider a power system with n substations, m measurements and b transmission lines. As shown in Section 3.2, the measurement vector z and the state vector x are correlated by the Jacobian matrix: $\mathbf{z = Hx + e}$. By following the procedure outlined in Table 1, we can divide a power system of n substations into n sub-systems. Let $\mathbf{i}$ denote the i^{th} substation where $i = \{1, \ldots, n\}$. Based on the topology of the i^{th} sub-system, we can construct its own Jacobian matrix $\mathbf{H'_i}$. The entry in the state vector $\mathbf{x'_i}$ is directly taken from the corresponding entry from $\mathbf{x}$. However, as shown in Table 1, the entry in the measurement vector $\mathbf{z'_i}$ is calculated from the entries in $\mathbf{z}$. Consequently, for the i^{th} sub-system, the measurements and state variables are correlated by its Jacobian matrix: $\mathbf{z'_i = H'_i x'_i + e'_i}$.

When attackers perform FDI attacks, they decide the attack vector $\mathbf{a}$ based on the measurement Jacobian matrix $\mathbf{H}$ of the entire power grid. As shown in Section 3.2, in order to bypass the bad data detection, the attack vector $\mathbf{a}$ needs to satisfy the condition $\mathbf{a = Hc}$ [2].

When measurements are compromised, a corrupted measurement vector $\mathbf{z_a = z + a}$ is obtained. Under our threat model, the compromised measurements are delivered to the control center and the agents deployed at the substations. Consequently, in the sub-system, we construct the compromised measurement $\mathbf{z'_{a,i}}$ based on the procedure in Table 1. Based on the measurements collected by the agent in each substation, we can perform state estimation and bad data detection on each sub-system. The approach we propose requires the attack vector to satisfy the condition $\mathbf{a' = H'_i c'_i}$ at each subsystem a long with $\mathbf{a = Hc}$. Because $\mathbf{a = Hc}$ does not ensure that $\mathbf{a'_i = H'_i c'_i}$ for each sub-system (where $\mathbf{a'_i = z'_{a,i} - z'_i}$), we can detect a false data injection attack if the compromised measurements fail to bypass bad data detection for at least one agent.

5. EXPERIMENTAL EVALUATION

5.1 Case study

To demonstrate how agents use state estimation at their sub-systems to detect false data injection attacks, we use the IEEE 9-bus system , whose transmission topology is shown in Fig. 3. This power system has 9 buses, 9 transmission lines, 3 generation, and 3 load units.

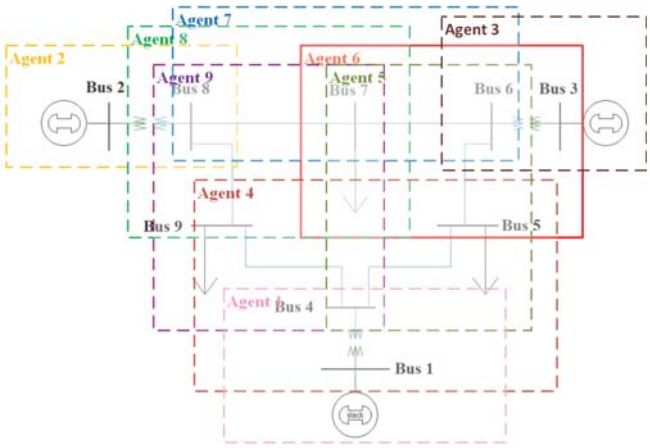


Figure 3: Distribution of agents for a 9-bus system

There are 8 state variables (we assume that the phasor angle of the slack bus is 0) and 18 measurements. We extract the measurement matrix H from MATPOWER. In Table 2, we show the values in one randomly selected attack vector a. The attack vector is injected into the observed measurement z to obtain z_a.

Table 2: Data for FDI attack generation

c	$a = Hc$	z	$z_a = z + a$
1	-17.3611	0.6700	-16.6911
0	10.8696	0.2897	11.1593
1	0.0000	-0.6103	-0.6103
0	0.0000	0.8500	0.8500
0	0.0000	0.2397	0.2397
0	0.0000	-0.7603	-0.7603
0	-16.0000	-1.6300	-17.6300
0	0.0000	0.8697	0.8697
	-11.7647	-0.3803	-12.1450
	-17.3611	0.6700	-16.6911
	16.0000	1.6300	17.6300
	0.0000	0.8500	0.8500
	39.9954	0.0000	39.9954
	-10.8696	-0.9000	-11.7696
	0.0000	0.0000	0.0000
	0.0000	-1.0000	-1.0000
	-16.0000	0.0000	-16.0000
	-11.7647	-1.2500	-13.0147

Based on the state estimation performed for the whole power system, we cannot detect this attack vector because the L_2 norm (weighted sum of squared errors) is within the BDD threshold (with the threshold τ set at 1.0228^{-2}). In Figure 4, we show that state estimation performed by agents can detect this attack vector. The x-axis indicates the index of the agent; the y-axis indicates the weighted sum of squared errors of the state estimation performed at the corresponding agent. Because in the sub-system monitored by agents $1, 2, 3, 4, 5, 6, 7, 8$, and 9, we have $a'_i \neq H'_i c'_i$. The L_2-norm at these agents becomes very large making it possible to detect compromised measurements.

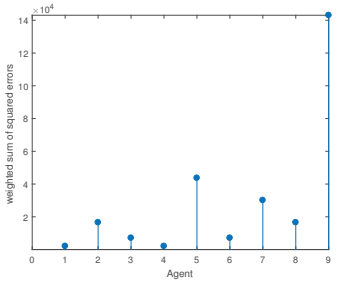


Figure 4: Bad-data detection results for agents in IEEE 9-bus system

5.2 Evaluation of Detection Results

To further evaluate the proposed multi-agent systems, we select IEEE 9-bus, 14-bus, and 30-bus systems, whose baseline profiles are included in MATPOWER [16]. For each power system case, we randomly construct 1000 attack vectors, a using Equation 4, such that Equation 5 is satisfied.

In each power system case, we perform on behalf of each agent the state estimation of its corresponding sub-system. If the $L2$-norm from the state estimation is larger than the BDD detection threshold, we detect the false data injection attacks.

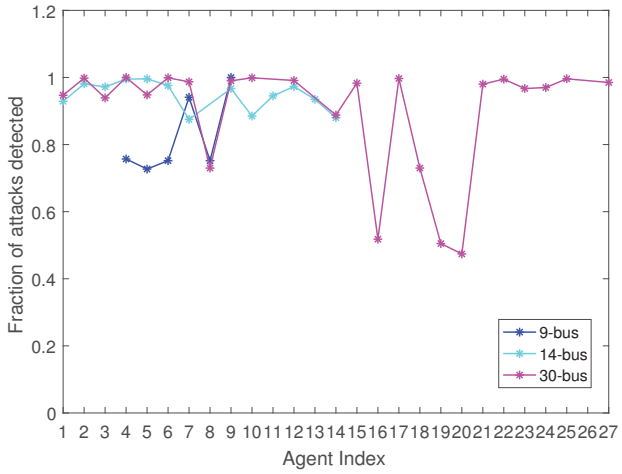


Figure 5: Probability for successful attack detection by individual agents for the 9-bus, 14-bus and 30-bus system

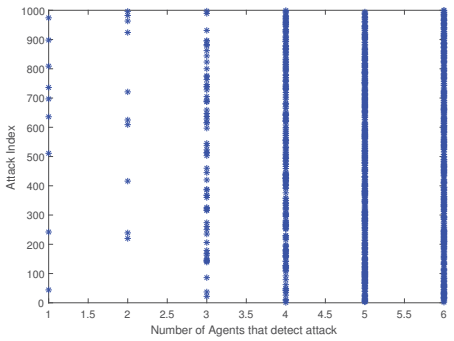
Figure 5 shows the probability that agents can successfully detect an attack for the IEEE 9-bus, 14-bus, and 30-bus power systems. The markers show the actual probability (number of successful detections/number of attacks) computed for a corresponding agent. The x-axis is the agent index, and the y-axis is the fraction of attack cases consid-

ered. From the results obtained, agents with more interconnected substations have a higher FDI attack detection probability in comparison to agents with less than 3-substations interconnected. Individual agents achieve detection for the overall system, with probabilities 0.82, 0.94 and 0.90 for the 9-bus, 14-bus and 30-bus systems respectively for FDI attacks completely undetectable by the power system in the absence of the proposed multi-agent system. Although at individual agents detection is not always 100%, overall detection is always successful since the proposed strategy achieves detection by evaluating the bad data detection result from each agent. In Figure 6 every instance of the FDI attack generated is detected by at least one or more agents making detection successful if carried out collectively. 1000 attack scenarios are simulated against the system and detection results for each agent for each attack scenario evaluated.

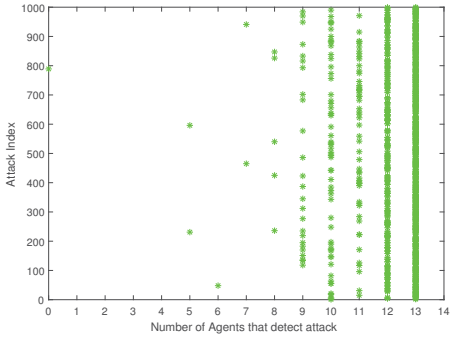
Figures 6a, 6b , 6c, show the number of agents that detect a range of attacks for the 9-bus, 14-bus and 30-bus systems respectively. The x-axis shows the number of agents that can detect an attack, and the y-axis is the index for each of the 1000 FDI attack scenarios considered. In other words, for a point (x_0, y_0) on Figure 6, y_0 cases are detected by less than or equal to x_0 agents. All agents simultaneously carry out detection for all attack cases and the collective result evaluated. For every single FDI attack, there is an agent or group of agents that can detect it.

Figure 7 shows the number of attacks that an agent at each bus detects. The index of each bus is plotted on the x-axis while the y-axis shows the number of attacks that the agent at this bus detects. The detection is distributed over all buses almost evenly. In this case, it is challenging for attackers to bypass the multi-agent detection mechanism. This means that an attack targeting any bus can be detected by at least one agent provided its a member of the subsystem

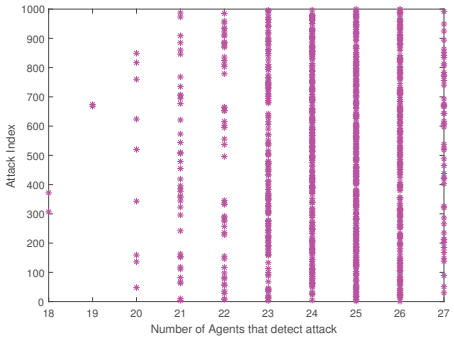
To further evaluate the performance of our FDI attack detection strategy the average time taken by all agents to carry out state estimation (agents carry out state estimation simultaneously) is compared to the time taken for entire grid state estimation. The results obtained indicate that for the IEEE 9-bus, 14-bus and 30-bus system benchmarks considered, the time taken for the agents to carry out state estimation is less than the time it takes for entire grid state estimation. In the 9-bus system, while agents require 0.215 seconds on average, the entire grid requires 0.23 seconds. For the 14-bus system, agents take 0.2000 seconds while the entire grid takes 0.2200 seconds and finally 0.2261 seconds against 0.4300 seconds for the 30-bus system.



(a) 9-Bus System



(b) 14-Bus System



(c) 30-Bus System

Figure 6: Number of agents that detected each individual FDI attack

6. CONCLUSION

A multi-agent system for false data injection attacks in the power grid is proposed. Each substation is assigned an agent created from a topology formed by a substation and its neighboring substations. Agents are equipped with communication capability and facilitate communication among substations. In addition, agents compute state estimates for their respective substation and share this state information with each other. For each agent, the state estimate must pass bad data detection. Measurement data is checked by each of the agents and is only processed for state estimation if it passes state estimation at each Agent. The detection technique is demonstrated using the DC power flow and DC state estimation data of the IEEE 9-bus, 14-bus and 30-bus systems.

In future work the multi-agent system will be extended to include attack identification because the agent detection system currently only detects the presence of the attack but cannot identify the exact measurement affected. The findings presented in this paper are based on simulations, the multi-agent system will be implemented on real-world hardware for further analysis.

7. REFERENCES

[1] E. Handschin, F. C. Schweppe, J. Kohlas and A. Fiechter, "Bad data analysis for power system state estimation," in IEEE Transactions on Power Apparatus and Systems, vol. 94, no. 2, pp. 329-337, Mar 1975.

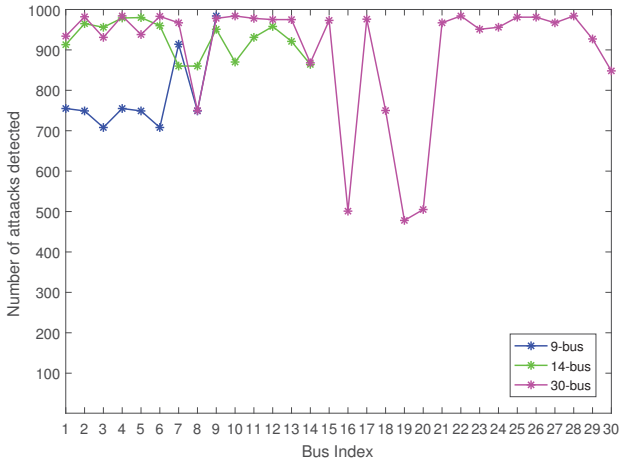


Figure 7: Number of attacks successfully detected at each bus by the corresponding agents

[2] Liu, Yao, Peng Ning, and Michael K. Reiter. "False data injection attacks against state estimation in electric power grids." ACM Transactions on Information and System Security 14.1 (2011).

[3] G. Hug and J. A. Giampapa, "Vulnerability Assessment of AC State Estimation With Respect to False Data Injection CyberAttacks, " Smart Grid, IEEE Transactions on, vol. 3, pp. 1362-1370,2012

[4] O. Kosut, J. Liyan, R. J. Thomas, and T. Lang, "Malicious Data Attacks on the Smart Grid, " Smart Grid, IEEE Transactions on, vol. 2, pp. 645-658, 2011.

[5] Le Xie, M. Yilin and B. Sinopoli, "False Data Injection Attacks in Electricity Markets, " in Smart Grid Communications (SmartGridComm), 2010 First IEEE international Conference on, pp. 226-231, 2010.

[6] Bobba, Rakesh B., et al. "Detecting false data injection attacks on dc state estimation." Preprints of the First Workshop on Secure Control Systems, CPSWEEK. Vol. 2010. 2010.

[7] G. Dan and H. Sandberg, "Stealth Attacks and Protection Schemes for State Estimators in Power Systems," Smart Grid Communications (SmartGridComm), 2010 First IEEE International Conference on, Gaithersburg, MD, 2010, pp. 214-219.

[8] S. Bi and Y. J. Zhang, "Defending mechanisms against false-data injection attacks in the power system state estimation," 2011 IEEE GLOBECOM Workshops (GC Wkshps), Houston, TX, 2011, pp. 1162-1167.

[9] D. Wei, M. Jafari and Y. Lu, "On Protecting Industrial Automation and Control Systems against Electronic Attacks," 2007 IEEE International Conference on Automation Science and Engineering, Scottsdale, AZ, 2007, pp. 176-181.

[10] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang and W. Zhao, "On False Data-Injection Attacks against Power System State Estimation: Modeling and Countermeasures," in IEEE Transactions on Parallel and Distributed Systems, vol. 25, no. 3, pp. 717-729, March 2014.

[11] O. Kosut, Liyan Jia, R. J. Thomas and Lang Tong, "Limiting false data attacks on power system state estimation," Information Sciences and Systems (CISS), 2010 44th Annual Conference on, Princeton, NJ, 2010, pp. 1-6.

[12] J. Wei, D. Kundur, T. Zourntos, and K. Butler-Purry, âĂIJProbing the telltale physics: Towards a cyber-physical protocol to mitigate information corruption in smart grid systems,âĂİ in Proc. IEEE 3rd Int. Conf. Smart Grid Commun. (SmartGridComm), 2012, pp. 372âĂŞ377.

[13] T. Liu, Y. Gu, D. Wang, Y. Gui, and X. Guan, âĂIJA novel method to detect bad data injection attack in smart grid,âĂİ in Proc. IEEE INFOCOM, 2013, pp. 3423âĂŞ3428

[14] IEEE Standard Communication Delivery Time Performance Requirements for Electric Power Substation Automation," in IEEE Std 1646-2004 , vol., no., pp.0 _1-24, 2005

[15] Z. Wang, A. Scaglione and R. J. Thomas, "Generating Statistically Correct Random Topologies for Testing Smart Grid Communication and Control Networks," in IEEE Transactions on Smart Grid, vol. 1, no. 1, pp. 28-39, June 2010.

[16] R. D. Zimmerman, C. E. Murillo-SÃąnchez, and R. J. Thomas, "MATPOWER: Steady-State Operations, Planning and Analysis Tools for Power Systems Research and Education," Power Systems, IEEE Transactions on, vol. 26, no. 1, pp. 12-19, Feb. 2011.

[17] A. Monticelli, State Estimation in Power Systems. Boston: Kluwer Academic Publishers, 1999

[18] A. Wood and B. Wollenberg. Power generation, operation, and control. John Wiley and Sons, 2nd edition, 1996

[19] V. K. Balakrishnan, Graph Theory. New York: McGraw-Hill, 1997