2016 IEEE International Conference on Smart Grid Communications (SmartGridComm): Cyber Security and Privacy for the Smart Grid

Combined Data Integrity and Availability Attacks on State Estimation in Cyber-Physical Power Grids

Kaikai Pan*, André M. H. Teixeira†, Milos Cvetkovic* and Peter Palensky*
*Intelligent Electrical Power Grids
Faculty of EEMCS, Delft University of Technology, Delft, The Netherlands
†Engineering Systems and Services
Faculty of TPM, Delft University of Technology, Delft, The Netherlands

***Abstract*—This paper introduces combined data integrity and availability attacks to expand the attack scenarios against power system state estimation. The goal of the adversary, who uses the combined attack, is to perturb the state estimates while remaining hidden from the observer. We propose security metrics that quantify vulnerability of power grids to combined data attacks under single and multi-path routing communication models. In order to evaluate the proposed security metrics, we formulate them as mixed integer linear programming (MILP) problems. The relation between the security metrics of combined data attacks and pure data integrity attacks is analyzed, based on which we show that, when data availability and data integrity attacks have the same cost, the two metrics coincide. When data availability attacks have a lower cost than data integrity attacks, we show that a combined data attack could be executed with less attack resources compared to pure data integrity attacks. Furthermore, it is shown that combined data attacks would bypass integrity-focused mitigation schemes. These conclusions are supported by the results obtained on a power system model with and without a communication model with single or multi-path routing.**

I. Introduction

The evolving cyber-physical power grids more intensively depend on the integration of power systems and Information Communication Technologies (ICT) to realize monitoring and controlling operations. An important instance of such dependency is the State Estimation (SE), which uses measurement data in monitoring systems of power grids and provides timely state information for Energy Management Systems (EMS) in control centers [1]. The measurements are usually collected by the Remote Terminal Units (RTUs) in the substations and transmitted through the ICT infrastructures, e.g., Supervisory Control and Data Acquisition (SCADA) system. Smart sensors, like Phasor Measurements Units (PMUs), and wide area monitoring and control systems are also introduced to facilitate fast data collection and accurate state estimation.

Modern EMS applications, such as automatic generation control, optimal power flow and contingency analysis, rely on the state inputs from SE. Thus, an accurate and secure SE is of great importance for power grid operation. However, the SE is potentially vulnerable to a large number of security threats. Substations needs remote access connection for monitoring and maintenance, which may expose them to cyber attacks. Besides, for most industrial communication protocols, e.g., DNP 3.0, IEC 61850, adequate cyber security features were not always included at the time of publishing [2]. Since recently, SCADA system has been an interesting target of cyber attacks given the success of *Stuxnet malware* [3].

Cyber attacks could be divided into data availability attacks, data integrity attacks and data confidentiality attacks [4], each of which can be launched individually or in coordination with other attacks. The vulnerability of power grids to data integrity attacks was first shown in [5]. According to this reference, the measurements can be injected with false data without triggering the Bad Data Detection (BDD) built in SE. This kind of data integrity attack that avoids BDD is called *stealth attack*. A considerable amount of work has been done on stealth attacks under power system models, e.g., vulnerability analysis using security metrics [6], data-driven attack mechanisms [7] and attack impacts [8]. In order to defend against stealth attacks, data authentication and protection are proposed to safeguard certain measurements from adversarial data injections [9].

It is worth noting that the majority of research in the literature has focused on data integrity attacks on SE from many aspects, especially the stealth attacks. However, in order to launch a stealth attack, the adversary needs intensive attack resources such as the knowledge of the system model and the capability to inject false data on a set of measurements. Actually, a more common threat for the power grids is that the adversary would try to use less resources and multiple kinds of data attacks while still achieving the goal, i.e., remaining hidden and changing state estimates.

In addition, security issues of SE have been researched under power system models. However, due to power grids being cyber-physical systems, SE security also needs to be considered under cyber-physical models. Cyber attacks take place on ICT infrastructures and could influence the physical process. A realistic treatment of attacks and mitigation schemes should be based on the characteristics of the power system and of the communication infrastructures. The work in [10] considered adding jamming attacks to the attack scenario on the design of *detectable attack*. However, this work did not consider the communication models with single or multi-path routing, and as opposed to [10], our work aims to provide new insights on undetectable combined attacks.

978-1-5090-4075-9/16/$31.00 ©2016 IEEE

Contributions and Outline

In this paper, we propose the data attack scenarios that combine data integrity and availability attacks on SE, and also use the cyber-physical models to propose security metrics and mitigation schemes. The goal of the combined data attacks is to manipulate certain measurements and make another set of measurements unavailable to SE so that they can remain hidden and corrupt SE. In addition, the use of less attack resources is preferred by the attacker. Thus, our work is to expose vulnerability of power grids to combined data attacks.

Our contributions are threefold. First, we formulate security metrics to quantify the vulnerability of power grids to combined data attacks. The security metric for combined attacks is formulated as a mixed integer linear programming (MILP) problem, which is then analyzed and compared to the security metric of data integrity attacks. We show that, when data availability and data integrity attacks have the same cost, the two metrics coincide. Second, we consider the attack scenarios under both power system and communication models. According to the introduced attack costs, we show that the power grids are more vulnerable to combined data attacks. Third, we use security metrics and present how combined data attacks would impact integrity-focused mitigation schemes.

The outline of the paper is as follows. Section II gives a brief introduction of SE on power system model and stealth attack mechanisms. Communication model of power grid is also illustrated. Section III presents the combined data attacks and proposes security metrics with the corresponding computation solutions. The combined data attacks under communication model of power grid is analyzed in Section IV. Routing vector/matrix is developed for formulating security metrics. Section V discusses how combined data attacks can impact mitigation schemes that only tackle integrity violations. Section VI presents the results of security metrics under both power system and communication models with single or multi-path routing. In Section VII we conclude the paper.

II. Power System and Communication Model and Data Integrity Attack

In this section, we review the power system model and state estimation, and present the modeling of communication system of power grid for security research. The typical stealth attack and security metrics are also addressed.

A. Power System Model and State Estimation

A power system model has a number of buses connected by transmission lines. Usually, a bus represents a power substation in electricity grids. If two buses are connected only by a transformer, it can be assumed that these buses represent the same substation [11]. For example, in IEEE 14 bus test system [12], bus 5 and bus 6 represent one substation. It should be emphasized that the measurement data is collected by sensors (i.e., RTUs) at substations. The data collected includes line flow measurements and bus injection measurements. These m measurements are denoted by $z = [z_1, \ldots, z_m]^T$. The system state x is the vector of phase angles and voltage magnitudes at all buses except the reference bus whose phase angle is set to be zero. Using the AC power flow model, the measurements and the state can be modeled as $z = h(x) + e$, where h is the nonlinear measurement function vector $h = [h_1(x), \ldots, h_m(x)]^T$, and e is the measurement noise vector $e = [e_1, \ldots, e_m]^T$, which we assume has a Gaussian distribution of zero mean and covariance matrix Σ.

A linear approximation of the AC power system model at nominal state called the DC power flow model [1] is often used in SE. In the DC model, the vector z refers to active power flow and injection measurements, and the state x refers to bus phase angles. We assume that a power system has $n+1$ buses, and that there are n angles to be estimated not including the reference angle, i.e., $x = [x_1, \ldots, x_n]^T$. We can write

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

where $H \in \mathbb{R}^{m \times n}$ is a constant Jacobian matrix which depends on the impedance of transmission lines, the power system topology, and the placement of the measurements. Usually a large degree of redundancy of measurements is employed to make H full rank. The state estimate $\hat{x}$ is obtained using weighted least squares estimate:

$$\hat{x} = \arg\min_x (z - Hx)^T \Sigma^{-1} (z - Hx). \tag{2}$$

Based on the state estimates, the measurement residues are evaluated as

$$r = z - H\hat{x}, \tag{3}$$

where r is the residue vector. To validate the state estimates, BDD uses the $\mathrm{J}(\hat{x})$ to detect erroneous measurements,

$$\begin{cases} \text{Good data, if} & r^T \Sigma^{-1} r \leq \tau, \\ \text{Bad data, if} & r^T \Sigma^{-1} r > \tau, \end{cases} \tag{4}$$

where τ is the threshold used in BDD to satify the false alarm probability constraints [7].

B. Communication Model

In monitoring systems, wide area networks (WANs) are employed to deliver multiplexed measurements from substations to the control center. The communication lines are usually laid along with the transmission lines between substations with the cables installations. Thus, the measurements sent from a substation would go through several substations, where switches, routers and multiplexers multiplex the data from different substations onto the communication link [9].

With the knowledge above, it is practical to represent each substation as a node that receives and transmits data. With communication links between nodes, mesh topologies are used to improve utilization of available infrastructures. This network is a multi-hop network where packets would be routed through multiple nodes before reaching destination [11]. Figure 1 shows the communication model for IEEE 14 bus test system. There are 10 nodes and 15 communication links on the 14 bus system's WAN. Each node and communication link represents one substation and one communication line in a physical system. Here we assume the control center is located at the reference bus, i.e., bus 1/node 0.

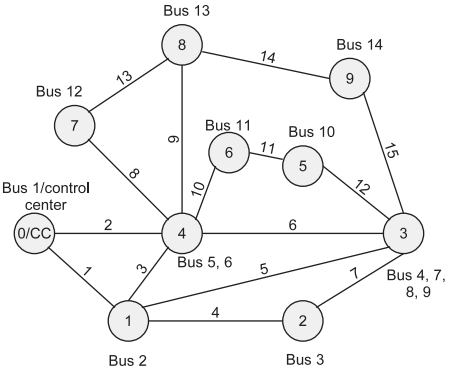

Figure 1. Communication model for IEEE 14 bus test system based on [11].

C. Stealth Attacks

The goal of the adversary is to perturb the state estimates while remaining hidden. The attackers would inject false data on a set of measurements. Thus, the measurements vector z becomes $\bar{z} := z + a$. The *attack vector* a is added to the original measurement vector. As shown in [5], the attacker corrupts certain measurements using the attack vector $a = Hc$, where $c \in \mathbb{R}^n$ is nonzero. The corrupted measurement vector $\bar{z}$ becomes $\bar{z} = H(x+c)+e$. This leads to the state estimate perturbed by a degree of c, while the residues for BDD checking keep the same after measurements corruption. It has be verified that this stealth attack can be performed on SCADA/EMS test bed avoiding BDD [13].

To describe the vulnerability of power grids to stealth attacks, the security metrics are introduced as the minimum number of measurements that need to be corrupted by the attacker in order for the attack to remain unnoticed [6].

$$\begin{aligned} \alpha_j := \min_{c} \quad & \|a\|_0 \\ \text{s.t.} \quad & a = Hc, \quad a(j) \neq 0, \end{aligned} \tag{5}$$

where $a(j)$ denotes the injected false data on measurement j. The result α_j is the security metric that quantifies the vulnerability of measurement j to stealth attack. It is known that this optimization problem above is NP-hard. In [14], the authors proposed an approach using the big M method to set (5) as a MILP problem, which can be solved with an appropriate solver.

$$\begin{aligned} \alpha_j := \min_{c,w} \quad & \sum_{i}^{m} w(i) \\ \text{s.t.} \quad & Hc \leq Mw, && \text{(6a)} \\ & -Hc \leq Mw, && \text{(6b)} \\ & H(j,:)c = 1, && \text{(6c)} \\ & w(i) \in \{0,1\} \quad \text{for all } i. \end{aligned}$$

In (6a) and (6b), M is a constant scalar that is greater than the maximum absolute value of entries in Hc. And $H(j,:)c = 1$ is assumed in (6c) to represent the constraint $a(j) \neq 0$ in (5). Thus the solution of (6) is exactly the solution to (5), and $w(i) = 1$ means that the measurement i is attacked.

III. Combined Data Integrity and Availability Attacks

This kind of data integrity attack above is resource-intensive, since the knowledge of the system model (i.e, H) is needed and data injection needs to take place on certain measurements in a coordinated way. In reality, an adversary would use all tools available and try to reduce attack resources. Besides, monitoring systems are always more vulnerable to data availability attacks (e.g., DDoS attacks, jamming attacks) [15]. Thus, the attack scenario we consider is that the adversary would use combined data integrity and availability attacks. The data availability attack is denoted by $d \in \{0,1\}^n$, where $d(i) = 1$ means the measurement i is unavailable for SE. An intuitive security metric could be the minimum number of measurements to compromise using combined data attacks.

$$\begin{aligned} \beta_j := \min_{c,d} \quad & \|a\|_0 + \|d\|_0 \\ \text{s.t.} \quad & a = H_0 c, && \text{(7a)} \\ & H_0 = (I - \text{diag}(d))H, && \text{(7b)} \\ & a(j) \neq 0, && \text{(7c)} \\ & d(i) \in \{0,1\} \quad \text{for all } i. \end{aligned}$$

In (7a) and (7b), H_0 denotes the Jacobian matrix of the remaining measurements, which is obtained from H by replacing some rows with zero row vector due to data availability attacks on the corresponding measurements. The combined data attacks can remain hidden as the attack vector a still lies on the column space of the remaining Jacobian matrix H_0. To solve this NP-hard optimization problem, we propose a computation solution which also uses the big M method:

$$\begin{aligned} \beta_j^{'} := \min_{c,w,d} \quad & \sum_{i}^{m} w(i) + \sum_{k}^{m} d(k) \\ \text{s.t.} \quad & Hc \leq M(w+d), && \text{(8a)} \\ & -Hc \leq M(w+d), && \text{(8b)} \\ & H(j,:)c = 1, && \text{(8c)} \\ & w(i) \in \{0,1\} \quad \text{for all } i, && \text{(8d)} \\ & d(k) \in \{0,1\} \quad \text{for all } k, && \text{(8e)} \end{aligned}$$

where $w, d \in \{0,1\}^m$, with $w(i) = 1$ and $d(k) = 1$ meaning data integrity attack and data availability attack on measurement i and k respectively. Here we also assume $H(j,:)c = 1$ in (8c) to represent the constraint $a(j) \neq 0$ in (7c).

The following results investigate the relation between the security metrics of these attacks scenarios.

Theorem 1. *For any measurement index $i \in \{1,\ldots,m\}$, the security metrics for combined data integrity and availability attacks formulated in* (7) *and* (8) *have the same value.*

Proof. The proof follows by re-writing (7) as (8). First, note that the first constraint of (7), $a = (I - \text{diag}(d))Hc$, can be formulated as a set of inequality constraints with auxiliary binary variables by using the big M method, yielding $-Mw \leq (I - \text{diag}(d))Hc \leq Mw$, where $w \in \{0,1\}^m$ and $\|a\|_0 = \sum w(i)$.

Since d is a vector of binary variables, the pair of inequality constraints pertaining the i-th measurement can be written as $|(1-d(i))H(i,:)c| \leq Mw(i)$. The latter can be read as

$$\begin{cases} H(i,:)c = 0, & \text{if } w(i) = d(i) = 0, \\ |H(i,:)c| \leq M, & \text{if } w(i) = 1 \text{ or } d(i) = 1, \end{cases}$$

which can be rewritten as $|H(i,:)c| \leq M(d(i)+w(i))$. Hence, recalling that $a(i) = (1-d(i))H(i,:)c$, we conclude that the constraints of (7) can be equivalently re-written as the constraints of (8). The proof concludes by noting that the objective functions of both problems saitfy the equality $\|a\|_0 + \|d\|_0 = \sum w(i) + \sum d(i)$. ■

Lemma 1. *For any measurement index $i \in \{1,\ldots,m\}$, the security metrics for pure data integrity attacks (α_i) and for combined data integrity and availability attacks (β_i) have the same value.*

Proof. The proof follows straightforwardly from Theorem 1, which establishes that $\beta_j = \beta_j'$: comparing (8) and (6), we can easily see that the result β_j' is equal to α_j. ■

An important issue for the attacker is to reduce the attack cost. When considering combined data attacks, we need to compare the attack cost of various scenarios. To simplify discussion, we assume that the data availability and integrity attacks have the attack costs C_A and C_I, respectively, per measurement. The worst case for power grids is that the attack will use the minimum attack resources. Under these attack costs, we formulate the security metric as

$$\begin{aligned} \overline{\beta}_j := \min_{c,w,d} \quad & \sum_i^m C_I w(i) + \sum_k^m C_A d(k) \\ \text{s.t.} \quad & (8a) - (8e). \end{aligned} \tag{9}$$

As previously discussed, it is reasonable to assume that the data availability attack costs less attack resources on measurements compared with data integrity attack. If we take the values that satisfy $C_A < C_I$, the optimal solution of w^* and d^* in (9), w.r.t. measurement j, would lead to $\sum w^*(i) = 1$ and $\sum d^*(i) = \alpha_j - 1$. Thus we have the following proposition.

Proposition 1. *When $C_A < C_I$, the optimal combined data attack strategy is to inject false data on the targeted measurement j and make other certain measurements unavailable to the SE, yielding the optimal attack cost $\overline{\beta}_j = C_I + (\alpha_j - 1)C_A$.*

IV. Combined Data Attacks under Communication Model

In previous section we have shown security metrics β_j and $\overline{\beta}_j$ for combined data attacks. The metrics does not consider the model of communication system of power grid and hence lacks the level of details for an accurate representation of the cyber-physical power grids. In this section we include the communication model into the security metrics for combined attacks. To launch such attacks, the adversary would get access to the ICT infrastructures by exploiting vulnerabilities in power grids, e.g., compromising remote access points, obtaining access to corporate networks. Thus, using the WANs communication model, the adversary shall gain access to the nodes(substations or control center) and communication links.

After accessing one node, the adversary may use data integrity attacks on some measurements that are collected on this node or routed through this node, by compromising the substation network or sensors. The adversary may also use various data availability attacks on these measurements, such as jamming the substation network, launching DDoS attacks on substation server, router, switches or multiplexer [9]. After obtaining access to a communication link, the adversary could only use data availability attacks not integrity attacks on the measurements that traverse this link.

In the following, we introduce security metrics for combined data attacks under communication models. This method is similar to the one in [9].

A. Routing Vector and Matrix

We can describe the communication model in Section II as an undirected graph $\mathsf{G} = (\mathsf{V}, \mathsf{E})$ where V is the set of nodes and E is the set of connected communication links. For each node $n \in \mathsf{V}$, single or multi-path routing schemes can be used. Hence, any measurement i can have single or multiple routes to the control center. We establish a binary vector called *routing vector* for each route of measurement i,

$$r_{i,p} = [r_{vi,p}, r_{ei,p}], \tag{10}$$

where $r_{i,p}$ denotes the routing vector for the pth route of measurement i. In $r_{i,p}$, $r_{vi,p}$ denotes the vector corresponding to nodes, i.e., $r_{vi,p} = [r_{vi,p,1}, \ldots, r_{vi,p,N}]$ and the entries are equal to 1 if this route traverses the corresponding nodes. $r_{ei,p}$ denotes the vector corresponding to communication links, i.e., $r_{ei,p} = [r_{ei,p,1}, \ldots, r_{ei,p,E}]$ and the entries are equal to 1 if this route traverses the corresponding communication links. N and E denote the whole number of nodes and links.

For a given communication model, using the graph and routing schemes, we can obtain all of the routing vectors. Based on the routing vectors, if there are m measurements in the power grid, we can establish a binary matrix called the *routing matrix*,

$$R = [R_v, R_e]. \tag{11}$$

In (11), R denotes the routing matrix $R \in \{0,1\}^{P \times (N+E)}$ for model that has a total of P routes, and R_v denotes the matrix corresponding to nodes, i.e., $R_v = [\ldots, r_{vi,p}^T, \ldots]^T$. R_e denotes the matrix corresponding to communication links, i.e., $R_e = [\ldots, r_{ei,p}^T, \ldots]^T$. Using the routing vector and matrix, we map routes of measurements to nodes and communication links.

B. Security Metrics for Combined Data Attacks

First, we quantify the vulnerability of each measurement to combined data attacks by the minimum number of nodes and communication links that have to be compromised in order to remain hidden for BDD. We use two binary vectors $x \in \{0,1\}^N$ and $y \in \{0,1\}^E$. If $x(n)$ is 1 then certain node is attacked; otherwise $x(n)$ is 0. If $y(l)$ is 1 then certain communication link

is attacked; otherwise $y(l)$ is 0. We know that data integrity attacks can only be made on nodes, while data availability attacks can be made both on nodes and links. Then the security metric becomes

$$\begin{aligned}\gamma_j := \min_{c,d,x,y} \quad & \|x\|_0 + \|y\|_0 \\ \text{s.t.} \quad & a = H_0 c, && \text{(12a)}\\ & H_0 = (I - \text{diag}(d))H, && \text{(12b)}\\ & a(j) \neq 0, && \text{(12c)}\\ & a(i) = 0 \text{ if } r_{vi,p} = 0, \text{ for all } i \neq j, p, && \text{(12d)}\\ & d(i) \leq r_{vi,p}x + r_{ei,p}y \quad \text{for all } i \neq j, p, && \text{(12e)}\\ & d, x, y \quad \text{are all binary vectors,}\end{aligned}$$

where the two constraints (12d) and (12e) use the routing vectors to map the combined data attacks on measurements to attacks on nodes and communication links. These two constraints indicate that to launch data integrity attack on measurement i, all of its routes should include at least one attacked node. And, to launch data availability attack on measurement i, all of its routes should include at least one attacked node or one attacked communication link. Using the similar approach in Section III we get

$$\begin{aligned}\gamma_j' := \min_{c,w,d,x,y} \quad & \sum_n^N x(n) + \sum_l^E y(l) \\ \text{s.t.} \quad & Hc \leq M(w + d), && \text{(13a)}\\ & -Hc \leq M(w + d), && \text{(13b)}\\ & H(j,:)c = 1, && \text{(13c)}\\ & Aw \leq R_v x, && \text{(13d)}\\ & Ad \leq R_v x + R_e y, && \text{(13e)}\\ & w, d, x, y \quad \text{are all binary vectors,} && \text{(13f)}\end{aligned}$$

where $A \in \{0,1\}^{P \times m}$ in (13d) and (13e) is a constant binary matrix mapping the measurements to all the corresponding routes. For instance, if single-path routing is employed, A is an identity matrix. Constraints (13d) and (13e) correspond to the constraints (12d) and (12e) respectively. And we can also conclude the following result.

Theorem 2. *For any measurement index $i \in \{1, \ldots, m\}$, the security metrics for combined data integrity and availability attacks formulated in* (12) *and* (13) *have the same value.*

The proof of Theorem 2 is similar to the proof of Theorem 1. To reduce attack cost, the adversary prefers to compromise the least number of nodes and communication links. Besides, the attack resources needed for attacking nodes and links are different. Here we assume that attacking all the nodes has the same attack cost C_N, and attacking all the links has the same attack cost C_L. We formulate the security metric with attack cost under communication model as

$$\begin{aligned}\bar{\gamma}_j := \min_{c,w,d,x,y} \quad & \sum_n^N C_N x(n) + \sum_l^E C_L y(l) \\ \text{s.t.} \quad & \text{(13a)} - \text{(13f)}.\end{aligned} \tag{14}$$

Under the communication models, attacking nodes means gaining access to substations and launching attacks on substation local networks, meaning that the adversary needs to compromise a large number of components. As for attacks on links, which means that the data flow through the attacked links is disrupted, they can be accomplished after gaining access to substations, by jamming or flooding the links, or even by physical destruction. Thus it is reasonable to assume that attacking nodes cost more than attacking links.

V. Mitigation Schemes Against Combined Data Attacks

In this section we discuss how the combined data attacks impact the mitigation schemes. (Non) tamper-proof data authentication and/or protection and multi-path routing can be used to protect power grids from data integrity attacks, see [9] for further details. Here we also use these mitigation schemes against combined data attacks.

It should be noted that, when mitigation schemes are considered, the routing vector/matrix method and the computation solution proposed in Section IV can still be used to calculate security metrics by adjusting corresponding entries of routing matrix R_v and R_e in constraints (13d) and (13e). If some nodes use tamper-proof data authentication, all measurements originate from these nodes can not be attacked using integrity attack, but still can be attacked using availability attack on the nodes and links. For example, if node 9 in Figure 1 uses tamper-proof authentication, for measurement i from node 9, we can make the entries of routing vectors to be zero in routing matrix R_v of (13d), but not change the entries of vectors in routing matrix R_v of (13e). Thus $w(i)$ has to be zero according to (13d), meaning that measurement i can not be attacked using data integrity attack. It is similar for the mitigation schemes of protection and non tamper-proof data authentication.

The mitigation schemes for data integrity attacks are not sufficient to protect the grids. Using the example above, although the measurements originating from node 9 can not be injected with data, they can still be made to be unavailable to SE if no special mitigation schemes for data availability attacks are employed. Stealth attacks are still possible since combined data attacks need less measurements to be injected with false data. Thus we can have the following proposition.

Proposition 2. *The mitigation schemes against data integrity attacks are not sufficient to protect the power grids from combined data attacks.*

On the other hand, according to the literature, there are no fully effective mitigation schemes against data availability attacks like DDoS attacks [15], as opposed to data integrity attacks that can be completely mitigated by tamper-proof schemes. Hence, we make the following assumption.

Assumption 1. *Data availability attacks can always be launched in spite of possible mitigation schemes.*

Under this assumption, combined data attacks can still exist as long there is only one measurement whose integrity can be

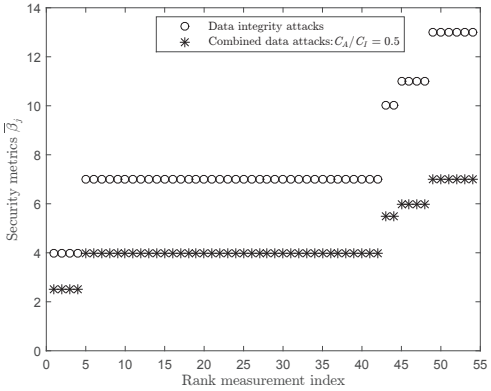

Figure 2. The sorted security metrics $\overline{\beta}_j$ under data integrity attacks and combined data attacks are plotted versus rank measurement index. Here C_I is taken as 1, and C_A is taken as 0.5.

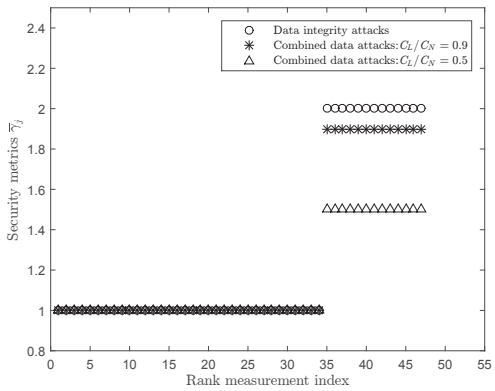

Figure 3. The single-path routing is considered. The sorted security metrics $\overline{\gamma}_j$ under data integrity attacks and combined data attacks are plotted versus rank measurement index. Here C_N is taken as 1, and C_L is taken as 0.9, 0.5 respectively.

attacked, as the adversary can use data availability attacks on the other measurements, which leads to the following result.

Proposition 3. *Combined data attacks are feasible unless all the nodes are protected against data integrity attacks.*

This implies that combined data attacks expand the vulnerabilities and need more advanced mitigation schemes.

VI. Case Study

We consider the IEEE 14 bus test system to perform the combined data attacks. In order to expose vulnerability of power grids, we calculated the security metrics under both power system model and the communication model. The communication model in Figure 1 is used. Besides, we calculated security metrics under both combined data attacks and pure data integrity attacks (by making the vector d in the constraints to be zero) to show how combined data attacks differ from data integrity attacks. For the computation, we use the MATPOWER package [16] and optimization solver CPLEX. In the performed experiments, power flow and injection measurements are placed on all the buses and transmission lines to provide large redundancy. Thus there are 54 measurements in the 14 bus system. It should be noted that, the approach we proposed to calculate security metrics do not need the full measurements assumption.

We start with the scenario that no mitigation schemes are employed. First we perform the combined data attacks on the power system model. Figure 2 shows the sorted security metrics $\overline{\beta}_j$ for the 54 measurements under data integrity attacks and combined data attacks. The values of security metrics under combined data attacks are smaller than the ones under data integrity attacks. Thus, the power grids are more vulnerable to combined data attacks comparing with pure data integrity attack. In fact, the results obtained from solving (9) show that $\sum w(i) = 1$, which is consistent with Proposition 1.

Next we consider the combined data attacks on the communication model. Here we calculate attack cost for all the measurements. For pure data integrity attacks, they have to be launched on the nodes. But for combined data attacks, they can take place both on nodes and communication links. We assume that the control center (node 0) in the 14 bus system communication model is protected that can not be compromised by the attacker, but to show the vulnerability of power grids to these attacks, there are no other substations/ nodes are protected.

1) Single-path Routing: We first consider the single-path routing in the communication model, which is common in the real SCADA communication. Figure 3 shows the sorted security metrics $\overline{\gamma}_j$ on all measurements when single-path routing is implemented. As we can see, due to the protection on node 0, there are 7 measurements ($j = 1, 2, 41$ in node 0, $j = 5, 21$ in node 1 and $j = 22, 25$ in node 4) can not be attacked by stealth attacks. We assume $\overline{\gamma}_j = \infty$ for these measurements, which correspond to the indices 48 through 54 of the rank measurement index in Figure 3, and thus they are not shown in the figures. Besides, the security metrics of combined data attacks are smaller than the ones of pure data integrity attacks. It can be inferred from Figure 3 that for combined data attacks under single-path routing, the optimal attack strategy is to attack the node that includes the targeted measurement and attack the communication links if needed.

2) Multi-path Routing: Here we consider the mitigation scheme of multi-path routing. We build two node-disjoint routes for each node. Figure 4 shows results of the sorted security metrics $\overline{\gamma}_j$ when multi-path routing is employed. Comparing Figure 3 and Figure 4 on the data integrity attack scenario, we can see that when multi-path routing is used, it can make some measurements have higher security metrics (from "1" to "2"), meaning that multi-path routing can act as a mitigation scheme against attacks. This is due to the fact that the adversary has to compromise all the routes of the measurement, instead of only one route. Besides, in multi-path routing scenario, the measurements still have smaller security metrics under combined data attacks. Specially from Figure 4, when C_L/C_N is smaller than 0.5 (we take 0.4), all of the

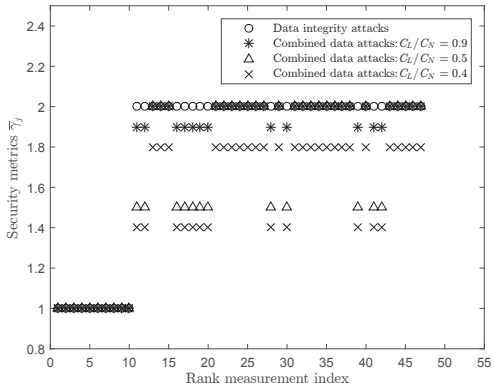

Figure 4. The multi-path routing is considered. The sorted security metrics $\overline{\gamma}_j$ under data integrity attacks and combined data attacks are plotted versus rank measurement index. C_N is taken as 1, and C_L is taken as 0.9, 0.5, and 0.4.

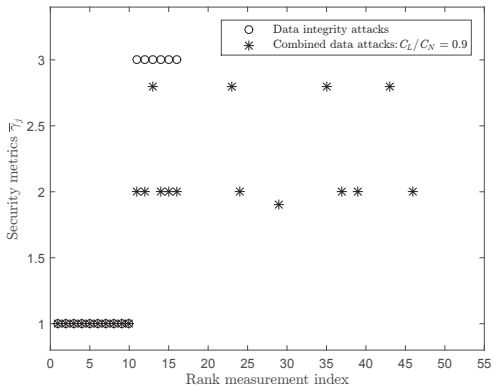

Figure 5. Mitigation schemes based on data authentication are used: node 8 and node 9 use non tamper-proof authentication, other nodes use tamper-proof authentication, and node 0 is protected. The sorted security metrics $\overline{\gamma}_j$ under data integrity attacks and combined data attacks are plotted versus rank measurement index. Here C_N is taken as 1, and C_L is taken as 0.9.

security metrics are smaller than 2. In this case, the optimal attack strategy for the adversary is to attack the node that contains targeted measurement and attack the communication links to make some measurements unavailable.

Then we consider mitigation schemes for data integrity attacks are implemented. We assume that all the substations use non tamper-proof authentication, and multi-path routing is also employed. Figure 5 presents the results of sorted security metrics with data authentication mitigation schemes. It shows that combined data attacks make more measurements vulnerable to attacks and also lead some measurements that can be attacked by pure data integrity attacks have smaller security metrics. In particular, some measurements whose ranked index is higher than 16 cannot be attacked by pure integrity attacks, but are vulnerable to combined attacks. This implies that the mitigation schemes for data integrity attacks are not sufficient for combined data attacks, which is consistent with Proposition 2.

VII. Conclusion

In this paper, we show how combined data integrity and data availability attacks at SE can remain hidden and expose the vulnerability of power grids to combined data attacks using security metrics. The mitigation schemes when considering combined data attacks are also discussed. We demonstrate the attacks and computation solutions for security metrics using IEEE test system. The results from case study prove that power grids are more vulnerable to combined data attacks comparing with pure data integrity attacks since less attack resources are needed and more sufficient mitigation schemes have to be considered. Possible extensions to the work in this paper include the computational efficiency of the algorithm, using various attack cost on different nodes/links and the simulation of combined attacks on test beds.

References

[1] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation*. CRC press, 2004.

[2] J. Hong, Y. Chen, C.-C. Liu, and M. Govindarasu, "Cyber-physical security testbed for substations in a power grid," in *Cyber Physical Systems Approach to Smart Electric Power Grid*. Springer, 2015, pp. 261–301.

[3] T. M. Chen and S. Abu-Nimeh, "Lessons from stuxnet," *Computer*, vol. 44, no. 4, pp. 91–93, 2011.

[4] S. G. I. P. C. S. W. Group *et al.*, "Nistir 7628 guidelines for smart grid cyber security," *Privacy and the smart grid*, vol. 2, 2010.

[5] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM Conference on Computer and Communications Security*, New York, NY, USA, 2009, pp. 21–32.

[6] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *First Workshop on Secure Control Systems (SCS), Stockholm*, 2010.

[7] J. Kim and L. Tong, "Against data attacks on smart grid operations: Attack mechanisms and security measures," in *Cyber Physical Systems Approach to Smart Electric Power Grid*. Springer, 2015, pp. 359–383.

[8] L. Xie, Y. Mo, and B. Sinopoli, "Integrity data attacks in power market operations," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 659–666, 2011.

[9] O. Vukovic, K. C. Sou, G. Dan, and H. Sandberg, "Network-aware mitigation of data integrity attacks on power system state estimation," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 6, pp. 1108–1118, 2012.

[10] D. Deka, R. Baldick, and S. Vishwanath, "Optimal data attacks on power grids: Leveraging detection measurement jamming," in *Proceedings of IEEE International Conference on Smart Grid Communications (SmartGridComm)*, Miami Florida , USA, Nov. 2015, pp. 392–397.

[11] C. B. Vellaithurai, S. S. Biswas, R. Liu, and A. Srivastava, "Real time modeling and simulation of cyber-power system," in *Cyber Physical Systems Approach to Smart Electric Power Grid*. Springer, 2015, pp. 43–74.

[12] R. Christie, "Power systems test case archive." [Online]. Available: https://www.ee.washington.edu/research/pstca/

[13] A. Teixeira, G. Dán, H. Sandberg, and K. H. Johansson, "A cyber security study of a SCADA energy management system: Stealthy deception attacks on the state estimator," *Proceedings of IFAC World Congress*, Aug 2011.

[14] A. Teixeira, K. C. Sou, H. Sandberg, and K. H. Johansson, "Secure control systems: A quantitative risk management approach," *IEEE Control Systems*, vol. 35, no. 1, pp. 24–45, 2015.

[15] J. D. Markovic-Petrovic and M. D. Stojanovic, "Analysis of scada system vulnerabilities to ddos attacks," in *Telecommunication in Modern Satellite, Cable and Broadcasting Services (TELSIKS), 2013 11th International Conference on*, vol. 2. Nis, Serbia: IEEE, 2013, pp. 591–594.

[16] R. D. Zimmerman, C. E. Murillo-Sanchez, and R. J. Thomas, "Matpower: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE Transactions on Power Systems*, vol. 26, no. 1, pp. 12–19, 2011.