Smart Grid Data Injection Attacks: To Defend or Not?

Anibal Sanjab[1] and Walid Saad[1]
[1] Wireless@VT, Bradley Department of Electrical and Computer Engineering, Virginia Tech, Blacksburg, VA USA,
Emails: {anibals,walids}@vt.edu

***Abstract*—Data injection is a cyber-attack in which an attacker targets the state estimator of the smart grid with the aim to alter the estimation of the system's real-time state. Using data injection, an adversary can manipulate the calculation of the real-time locational marginal prices to reap financial benefit. Even though data injection attacks have attracted significant attention recently, remarkably, all of the existing works focus on cases in which a single adversary is present. In contrast, in this paper, multiple data injection attackers are considered. The problem is formulated as a noncooperative game between the attackers and the smart grid defender. In this game, each attacker chooses a data injection attack while the defender chooses measurements to protect in order to thwart the attacks. The Nash equilibrium of this game is characterized and the effect of the strategies taken by the attackers and defender on the system is analyzed. Our results show how, at the equilibrium, multiple attacks can eliminate the effect of one another thus requiring no defense. However, under different conditions, a defense mechanism can be beneficial in reducing the combined effect of the different attacks on the system. Numerical results using the WSCC 9-bus system are used to validate the derived analytical solution. These results also shed light on the effect of the cost of defense on the attackers' and defender's optimal strategies and utilities. Accordingly, we show that a higher cost of defense makes attackers more likely to attack and worsens the defender's expected utility.**

I. Introduction

The recent introduction of advanced metering infrastructures as well as advanced data collection and communication nodes have rendered the smart electric grid more vulnerable to cyber-attacks [1]. In particular, *data injection attacks* have emerged as a highly malicious type of cyber-attacks in which malicious adversaries target the state estimator of the power system in order to alter the estimate of the real-time system state by manipulating a number of measurements [1].

Data injection has a detrimental effect on the power system since it targets the state estimator, an integral component of the smart grid which is used by the system operator to monitor, protect, control, and economically operate the system [2]. The goals from data injection attacks can be varied and they can range from compromising the security of the grid to impeding the real-time operation of the system or making financial profit through energy prices manipulation.

Data injection attacks are challenging by nature due to their stealthiness which makes the task of detecting them arduous [1]. In fact, data injection attacks can alter the estimation process while remaining unnoticed by the operator.

Recently, data injection attacks have attracted significant attention [1], [3]–[5]. The authors in [1] introduce an optimal data injection scheme and derive an optimized subset of measurements that can be defended to face this attack. The work in [3] introduces a stealthy data injection attack scheme that can evade detection when compromising a number of measurements.

This research was supported by the U.S. National Science Foundation under Grant CNS-1446621.

An analysis of the economic effects of data injection on energy markets is discussed in [4]. In [5], a zero-sum game is formulated between an attacker and a defender in which the attacker modifies an estimated line flow to manipulate prices.

While interesting, this existing body of literature [1], [3]–[5] (and references therein) has primarily focused on investigating a class of stealthy attacks by one attacker and studying their effect on the smart grid's security or economics. However, in practice, due to their efficacy and stealthiness, data injection attacks can occur concurrently from *multiple adversaries* that can target various state estimation sensors. Moreover, [1], [3], [4] focus primarily on the attacker's strategy with no modeling of possible attacker-defender strategic interaction while in [5], the attacker and defender interaction is restricted to modifying the power flow over a given line. *To our best knowledge, somewhat remarkably, no existing work has studied the impact of data injection attacks that are carried out by multiple adversaries*. In fact, due to the networked nature of the smart grid, the manipulation of measurements in one part of the system, by an adversary, impacts the system as a whole. Hence, an attack carried out by one attacker does not only impact the grid's performance, but it also affects the benefits of all other attackers in the system. This interconnection can be, on the one hand, beneficial to the smart grid for cases in which the different simultaneous attacks mitigate the severity of one another leading, thus, to a reduced combined effect. On the other hand, multiple attacks can lead to a more severe combined effect on the electric grid which, in turn, can make the task of defending the system more challenging. Clearly, there is a need for a strategic model to analyze and understand these interdependencies between attackers.

The main contribution of this paper is to introduce a novel game-theoretic approach to analyze data injections attacks that involve a defender and *multiple adversaries*. In the studied game, each attacker chooses a data injection attack to maximize the trade-off between the benefits, earned through prices manipulation, and costs associated with the attack. Meanwhile, the defender chooses a set of measurements to defend in order to block potential attacks and reduce their effect on the system while optimizing a utility that captures both the benefits and costs of the chosen defense strategy. For the formulated game, we characterize the Nash equilibrium and we study its properties by analyzing the overall effect of the defense and attack strategies on the system. Our results show that, at the equilibrium, multiple attacks can eliminate one another thus requiring no defense. On the other hand, under different conditions, defensive actions can be beneficial and can reduce the attacks' effect. Numerical results using the WSCC 9-bus system are used to validate the derived analytical solution. From this numerical application, we also study the impact of the cost of defense on the optimal strategies and utilities of the attackers and defender. Our results show that

978-1-4673-8289-2/15/$31.00 ©2015 IEEE

a higher cost of defense makes attackers more likely to attack and worsens the expected utility of the defender.

The rest of this paper is organized as follows. Section II presents the system model and problem formulation while Section III presents the formulated game and its solution. Section IV provides numerical results while conclusions are presented in Section V.

II. System Model and Problem Formulation

A. Energy Markets

Consider a competitive energy market architecture based on day ahead (DA) and real time (RT) markets. In the DA market, hourly locational marginal prices (LMPs), μ^{DA}, are generated by the operator for the next operating day [6]. Market clearing is executed based on the solution of a linearized optimal power flow (DCOPF) problem that outputs the optimal dispatch of each participating generator and the DA LMP at each bus [6]. The DCOPF formulation is as follows [2]:

$$\min_{\boldsymbol{P}} \sum_{i=1}^{G} C_i(P_i), \tag{1}$$

$$\text{s.t. } \sum_{i=1}^{N}(P_i - D_i) = 0, \tag{2}$$

$$P_i^{\min} \leqslant P_i \leqslant P_i^{\max}, \forall i \in \{1, \cdots, G\}, \tag{3}$$

$$\sum_{i=1}^{N}(P_i - D_i)\chi_{l,i} \leqslant F_l^{\max}, \forall l \in \{1, \cdots, L\}, \tag{4}$$

$$-\sum_{i=1}^{N}(P_i - D_i)\chi_{l,i} \leqslant F_l^{\max}, \forall l \in \{1, \cdots, L\}, \tag{5}$$

where N, G and L are the number of buses, generators, and lines respectively. C_i is the offer of generator i while P_i and D_i are, respectively, the power injection and load at bus i. If no generator (load) is connected to bus i, $P_i = 0$ ($D_i = 0$). $P_i^{\min}$ and $P_i^{\max}$ correspond to the lower and upper output limits of generator i. Constraints (4) and (5) represent the limit of the power flow on line l which cannot exceed the thermal limit $F_l^{\max}$. Each line flow is associated with a given reference direction. If the flow is in the opposite direction, it is represented by a negative power quantity. Hence, constraint (4) corresponds to the thermal limit of a line in its assumed reference direction while constraint (5) corresponds to the thermal limit of a line where the flow is opposite to its assumed reference direction. $\boldsymbol{X}$ is the generation shift factor matrix which defines the relationship between the power injection at each bus, $\boldsymbol{P}$, and the flow over each line, $\boldsymbol{F}$:

$$\boldsymbol{F}_{(L\times 1)} = \boldsymbol{X}_{(L\times G)} \times \boldsymbol{P}_{(G\times 1)}, \tag{6}$$

where the elements of $\boldsymbol{X}$ that are associated with the system's reference bus are equal to 0. $\chi_{l,i}$ corresponds to the shift factor of a generation at bus i on a line l.

On the other hand, in RT, an ex-post model uses actual real-time operation conditions estimated using the state estimator, instead of a projection of the system conditions like in DA, to generate real-time LMPs, μ^{RT} [6]. The RT LMPs are generated using an incremental DCOPF which is formulated as follows [6]:

$$\min_{\Delta \boldsymbol{P}} \sum_{i=1}^{G} C_i^{RT}(\Delta P_i), \tag{7}$$

$$\text{s.t. } \sum_{i=1}^{N}(\Delta P_i) = 0, \tag{8}$$

$$\Delta P_i^{\min} \leqslant \Delta P_i \leqslant \Delta P_i^{\max}, \forall i \in \{1, \cdots, G\}, \tag{9}$$

$$\sum_{i=1}^{N}(\Delta P_i)\chi_{l,i} \leqslant 0, \forall l \in \mathcal{C}^+, \tag{10}$$

$$-\sum_{i=1}^{N}(\Delta P_i)\chi_{l,i} \leqslant 0, \forall l \in \mathcal{C}^-, \tag{11}$$

where C_i^{RT} is the real time offer of generator i calculated based on its output in RT and its associated offer curve [6]. $\mathcal{C}^+$ ($\mathcal{C}^-$) is the set of congested lines which flow is in (opposite to) their reference directions. $\Delta P_i^{\min}$ and $\Delta P_i^{\max}$ are used as a bandwidth for solution tolerance. The common practice is to take $\Delta P_i^{\min} = -2$ MW and $\Delta P_i^{\max} = +0.1$ MW [7]. An alternative to using this feasibility bandwidth is also proposed in [7].

The DA and RT LMPs at each bus, i, are outputs of the DA and ex-post DCOPF formulations. These LMPs reflect the cost of energy of an incremental load at bus i as well as the cost of the contribution of this bus to the congestion in the system. The DA and RT LMPs at bus i can be computed as follows:

$$\mu_i^{DA} = \lambda_0 + \sum_{l=1}^{L}(\lambda_l^{DA,-} - \lambda_l^{DA,+})\chi_{l,i}, \tag{12}$$

$$\mu_i^{RT} = \lambda_0 + \sum_{l\in\mathcal{C}_l}(\lambda_l^{RT,-} - \lambda_l^{RT,+})\chi_{l,i}, \tag{13}$$

where $\mathcal{C}_l \triangleq \{\mathcal{C}^+ \cup \mathcal{C}^-\}$ is the set of congested lines, in RT, estimated using the state estimator. $\mathcal{C}_l \subseteq \mathcal{L}$ where $\mathcal{L} = \{1, \cdots, L\}$ is the set of all lines. λ_0 is the energy balance Lagrange multiplier associated with constraints (2) and (8). $\lambda_l^{DA,+}$ and $\lambda_l^{DA,-}$ are the Lagrange multipliers associated, respectively, with constraints (4) and (5) for line $l \in \mathcal{L}$. $\lambda_l^{RT,+}$ and $\lambda_l^{RT,-}$ are the Lagrange multipliers associated, respectively, with constraints (10) and (11) for line $l \in \mathcal{C}_l$. If $l \in \mathcal{L}$ but $l \notin \mathcal{C}_l$, then $\lambda_l^{RT,+} = \lambda_l^{RT,-} = 0$. Moreover, when $l \in \mathcal{C}^+$, $\lambda_l^{RT,-} = 0$; whereas, when $l \in \mathcal{C}^-, \lambda_l^{RT,+} = 0$.

Since the RT LMPs calculation relies on the outcome of the state estimator, data injection attacks which target the state estimation can impact the LMPs in (13). Accordingly, next, we introduce the model of data injection attacks.

B. State Estimation and Data Injection Attacks

Using a state estimator, multiple power measurements throughout the smart grid are used to estimate the system states [8]. The measurement vector, $\boldsymbol{z}$, is related to the vector of system states, $\boldsymbol{\theta}$, through the following linearized model:

$$\boldsymbol{z} = \boldsymbol{H}\boldsymbol{\theta} + \boldsymbol{e}, \tag{14}$$

where $\boldsymbol{H}$ is the measurement Jacobian matrix and $\boldsymbol{e}$ is the vector of random errors assumed to follow a normal distribution, $N(0, \boldsymbol{R})$. Using a weighted least square estimator the estimated system states are given by [8]:

$$\hat{\boldsymbol{\theta}} = (\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{H})^{-1}\boldsymbol{H}^T\boldsymbol{R}^{-1}\boldsymbol{z}. \tag{15}$$

The estimated measurements, $\hat{\boldsymbol{z}}$, and the residuals, $\boldsymbol{r}$, can be computed as follows [8]:

$$\hat{\boldsymbol{z}} = \boldsymbol{H}\hat{\boldsymbol{\theta}} = \boldsymbol{S}\boldsymbol{z},\ \boldsymbol{r} = \boldsymbol{z} - \hat{\boldsymbol{z}} = (\boldsymbol{I}_n - \boldsymbol{S})\boldsymbol{z} = \boldsymbol{W}\boldsymbol{z}, \tag{16}$$

where I_n is the identity matrix of size $(n \times n)$, n being the number of measurements.

When data attacks are performed by M attackers in the set $\mathcal{M} = \{1, \ldots, M\}$, the measurements are altered via the addition of their attack vectors $\{\boldsymbol{z}^{(1)}, \boldsymbol{z}^{(2)}, ..., \boldsymbol{z}^{(M)}\}$ which leads to the following measurements and residuals:

$$\boldsymbol{z}^{att} = \boldsymbol{z} + \sum_{i=1}^{M} \boldsymbol{z}^{(i)}, \ \boldsymbol{r}^{att} = \boldsymbol{r} + \boldsymbol{W} \sum_{i=1}^{M} \boldsymbol{z}^{(i)}. \tag{17}$$

By attacking the system measurements, the adversary seeks to manipulate the real-time LMPs, μ^{RT}, to make a financial benefit through virtual bids similarly to the case in [4].

Virtual bidding is a platform through which entities that do not own any physical generation nor load can participate in the energy market settlements through virtual supply and demand offers. Accordingly, an entity that buys (sells) virtual power at a given bus in DA has to sell (buy) that same power at the same bus in RT. In this regard, virtual bidders aim to profit from potential mismatch between DA and RT LMPs [6].

III. Proposed Game and Solution

A. Game Formulation

Given the coupling in the goals and actions of the M attackers as well as the defender, we use noncooperative game theory [9] to analyze their optimal decision making processes. In particular, we formulate a static, strategic noncooperative game $\Xi = \langle \mathcal{P}, (\mathcal{A}_i)_{i\in\mathcal{P}}, (U_i)_{i\in\mathcal{P}} \rangle$, where $\mathcal{P} \triangleq \mathcal{M} \cup \{0\}$ is the players' set, composed of all M attackers and the defender that is referred to via index 0, $\mathcal{A}_i$ is the set of actions available to player $i \in \mathcal{P}$ which consists of choosing an attack/defense vector, $\boldsymbol{a}_i \in \mathcal{A}_i$, and U_i is the utility function of player i. In this game, each attacker, $m \in \mathcal{M}$, selects an attack vector, $\boldsymbol{z}^{(m)} \triangleq \boldsymbol{a}_m \in \mathcal{A}_m$ that maximizes its utility U_m. This utility function must capture the financial benefit earned by means of virtual bidding. *Virtual bidding* is a process in which m buys and sells P_m MW at, respectively, buses i_m and j_m in DA; whereas, in RT, m sells and buys P_m MW at, respectively, buses i_m and j_m. Thus, the goal of each attacker is to optimize the following:

$$\max_{\boldsymbol{a}_m \in \mathcal{A}_m} U_m(\boldsymbol{a}_m, \boldsymbol{a}_{-m}) = \big[(\mu^{RT}_{i_m} - \mu^{DA}_{i_m}) + (\mu^{DA}_{j_m} - \mu^{RT}_{j_m})\big] P_m - c_m(\boldsymbol{a}_m), \tag{18}$$

$$\text{s.t. } \|\boldsymbol{W}_j \boldsymbol{a}_m\|_2 + \sum_{l=1, l\neq m}^{M} \|\boldsymbol{W_j} \boldsymbol{a}_l\|_2 \leqslant \epsilon_m, \ \forall j \in \mathcal{K}_m, \tag{19}$$

$$\|\boldsymbol{a}_m\|_0 \leqslant B_m, \tag{20}$$

where $c_m(\boldsymbol{a}_m)$ is the cost of attack, $\mathcal{K}_m$ is the set of attacked measurements by attacker m and $\boldsymbol{a}_{-m}$ denotes the strategy vector of all players except m whose strategy is denoted by $\boldsymbol{a}_m$. This limit on the residuals of the attacked measurements in (19) can reduce the possibility of being identified as outliers, following from (17), where ϵ_m is a threshold chosen by m. (20) limits the number of measurements that m can concurrently attack, where B_m is the maximum number of such measurements and $\|\boldsymbol{a}_m\|_0$ is the number of non-zero elements in $\boldsymbol{a}_m$.

In this game, the system operator (defender) chooses a defense vector $\boldsymbol{a}_0$ that determines how secured measurements are placed over some measurement locations to block potential attacks. The notion of placing secured measurements to prevent data injection attacks is discussed in [1]. The objective of the defender is to minimize a cost function reflecting the change between the DA and RT LMPs, on all N buses in the system, as follows:

$$\min_{\boldsymbol{a}_0 \in \mathcal{A}_0} U_0(\boldsymbol{a}_0, \boldsymbol{a}_{-0}) = P_L \sqrt{\frac{1}{N} \sum_{i=1}^{N} (\mu_i^{RT} - \mu_i^{DA})^2} + c_0(\boldsymbol{a}_0), \tag{21}$$

$$\text{s.t } \|\boldsymbol{a}_0\|_0 \leqslant B_0, \tag{22}$$

where $c_0(\boldsymbol{a}_0)$ is the cost of defense, P_L is the total load in the system and B_0 is the limit on the number of measurements that the defender can defend concurrently. In (21), μ_i^{RT} depends on the strategies taken by the defender, $\boldsymbol{a}_0$, and attackers, $\boldsymbol{a}_{-0}$.

Before deriving and analyzing the game solution, we next investigate the coupling in between the actions and utilities of potential data injection attackers in a smart grid setting.

B. Attackers' Coupling

Given the networked nature of the power system, the attackers' actions are highly coupled. In fact, an attacker manipulating a set of measurements would alter the whole estimation outcome and, thus, affect the actions and utilities of other attackers. In the case of M attackers, the resulting estimates, $\hat{\boldsymbol{z}}^{att}$, are calculated as follows:

$$\hat{\boldsymbol{z}}^{att} = \hat{\boldsymbol{z}} + \sum_{m=1}^{M} \boldsymbol{S}\boldsymbol{z}^{(m)} \Rightarrow \Delta\hat{\boldsymbol{z}} = \sum_{m=1}^{M} \boldsymbol{S}\boldsymbol{z}^{(m)}, \tag{23}$$

where $\Delta\hat{\boldsymbol{z}}$ is the corresponding change in the generated estimates due to the M attacks. Hence, the success of attacker m in manipulating a targeted measurement z_i is highly influenced by the remaining attackers. In fact, as shown next in Proposition 1, m's action effectiveness can be significantly attenuated by other attackers' actions.

Proposition 1: Depending on their targeted measurements, the attackers' actions can eliminate the impact of one another.

Proof: Consider the case of two attackers where attacker 1 (attacker 2) aims at increasing the estimated flow, $\hat{z}_i$ ($\hat{z}_j$), over line l_i (l_j) to create a false congestion. Hence, the aim of attacker 1 (attacker 2) is to achieve $\Delta\hat{z}_i \geqslant F^{\max}_{l_i} - \hat{z}_i$ ($\Delta\hat{z}_j \geqslant F^{\max}_{l_j} - \hat{z}_j$). Following from (23), the change to $\hat{z}_i$ and $\hat{z}_j$ introduced by the two attacks is expressed as:

$$\Delta\hat{z}_i = s_{i,i} z_i^{(1)} + s_{i,j} z_j^{(2)}, \ \Delta\hat{z}_j = s_{j,j} z_j^{(2)} + s_{j,i} z_i^{(1)}, \tag{24}$$

where $s_{i,j}$ is the element (i, j) of matrix $\boldsymbol{S}$. When the measurement errors are independent and identically distributed (i.e. $\boldsymbol{R} = \sigma^2 \boldsymbol{I}_n$), $\boldsymbol{S}$ is a symmetric matrix. This property can be easily proven based on (15) and (16) by showing that $\boldsymbol{S}^T = \boldsymbol{S}$ when $\boldsymbol{R} = \sigma^2 \boldsymbol{I}_n$. Due to the symmetry of $\boldsymbol{S}$, $s_{i,j} = s_{j,i}$. Consider the case in which $s_{i,j} < 0$, both attackers' actions mitigate the effect of one another. In fact, since $s_{i,j} < 0$, $z_j^{(2)}$ ($z_i^{(1)}$) reduces $\Delta\hat{z}_i$ ($\Delta\hat{z}_j$) preventing it from causing any congestion over line l_i (l_j). On the other hand, if $s_{ij} > 0$, each of the attackers' actions would help the other achieve its goal. This result obviously generalizes to the case of M attackers. ■

In addition to the coupling in their actions, the utilities of the different attackers are also highly interdependent. In fact, as shown in Proposition 2, an attacker can make financial benefit (or incur financial loss) due to the actions of other attackers.

Proposition 2: By properly choosing the nodes on which to place a virtual bid, an attacker can profit from other attackers' actions.

Proof: A created or eliminated congestion on one line of the system has a global effect on the LMPs of the whole system. Following (18), attacker m's financial return in the presence of M attackers is governed by:

$$\zeta_m = (\mu_{i_m}^{RT} - \mu_{i_m}^{DA}) + (\mu_{j_m}^{DA} - \mu_{j_m}^{RT}). \tag{25}$$

Replacing the expressions of the DA and RT LMPs from (12) and (13) in (25) returns:

$$\zeta_m = \sum_{l=1}^{L}[(\chi_{l,i_m} - \chi_{l,j_m})\times \tag{26}$$
$$((\lambda_l^{RT,-} - \lambda_l^{DA,-}) + (\lambda_l^{DA,+} - \lambda_l^{RT,+}))].$$

Hence, depending on the sign of $(\chi_{l,i_m} - \chi_{l,j_m})$ (dictated by the choice of virtual bid nodes i_m and j_m) a change in the congestion status of line l between DA and RT, due to the various attacks, can either return a financial benefit or loss to attacker m even without choosing to carry out any attack. ■

For example, consider the case in which attacker m's virtual bidding nodes, i_m and j_m, have generation shift factors with respect to a line l such that $(\chi_{l,i_m} - \chi_{l,j_m}) > 0$. If no congestion exists over line l in DA, $\lambda_l^{DA,-} = \lambda_l^{DA,+} = 0$. Moreover, if the combination of $\mathcal{M} \setminus \{m\}$ attackers cause congestion in the reference direction over line l in RT, $\lambda_l^{RT,-} = 0$ and $\lambda_l^{RT,+} > 0$. Then, the combined attack of the $\mathcal{M} \setminus \{m\}$ attackers causes financial loss to attacker m. However, in the case in which $(\chi_{l,i_m} - \chi_{l,j_m}) < 0$, that same attack results in a positive profit for m. Hence, the combined effect of other attackers on m's utility is a main factor in its decision to either attack or not.

C. Game Solution

In this section, for tractability and illustration purposes, we consider a case study consisting of two attackers and one defender, i.e. $\mathcal{P} \triangleq \{0, 1, 2\}$, where each attacker/defender is able to attack/defend one measurement at a time, i.e. $B_0 = B_1 = B_2 = 1$. The considered power grid is assumed to have two vulnerable lines. Vulnerable lines are defined as lines that are subject to data injection attacks due to their relatively low security measures. The action space of each of the two attackers is $\mathcal{A}_m \triangleq \{z^{(m)}, z_{\text{no}}^{(m)}\}$, for $m \in \{1, 2\}$, where m chooses to carry out attack, $z^{(m)}$, over a chosen vulnerable line or not to launch any attack $z_{\text{no}}^{(m)}$. The defender's action space is $\mathcal{A}_0 \triangleq \{a_{0,1}, a_{0,2}, a_{0,\text{no}}\}$ where $a_{0,1}$ and $a_{0,2}$ denote the actions of placing a secured measurement at the location attacked by either attacker 1 or 2, and $a_{0,\text{no}}$ denotes the action of not defending any of the measurements. The case in which the two attackers target the same measurement is a trivial case that is not considered since it leads to a high associated measurement residual violating constraint (19).

One suitable solution concept for this game is the so-called pure-strategy Nash equilibrium (PSNE) which is a state of the game in which none of the attackers nor the defender can unilaterally change their action choice; given the action choices of their opponents.

To find the PSNE, we use the matrix representation in Table I which enables us to view the utilities of the three players for the different attack and defense strategies where $c_i(a_i)$ has been simply denoted as c_i. $f_{i,j}$ refers to the benefit (or loss) that attacker i reaps when j carries out a successful attack, which can be obtained from (18) and (26). Moreover, d_1 and d_2 denote, respectively, the utility function of the defender when either attacker 1 or 2 launches its attack while no defense is taken. To derive the game's solution, we assume that the cost of attack is such that $c_1 < |f_{i,j}|$ and $c_2 < |f_{i,j}|$ for $i, j \in \{1, 2\}$.

TABLE I
PLAYERS' UTILITIES(U_0, U_1, U_2)

For defense strategy $a_0 \triangleq a_{0,\text{no}}$		
P_1 \ P_2	$z^{(2)}$	$z_{\text{no}}^{(2)}$
$z^{(1)}$	$(0, -c_1, -c_2)$	$(d_1, f_{1,1} - c_1, f_{2,1})$
$z_{\text{no}}^{(1)}$	$(d_2, f_{1,2}, f_{2,2} - c_2)$	$(0, 0, 0)$
For defense strategy $a_0 \triangleq a_{0,1}$		
P_1 \ P_2	$z^{(2)}$	$z_{\text{no}}^{(2)}$
$z^{(1)}$	$(d_2 + c_0, f_{1,2} - c_1, f_{2,2} - c_2)$	$(c_0, -c_1, 0)$
$z_{\text{no}}^{(1)}$	$(d_2 + c_0, f_{1,2}, f_{2,2} - c_2)$	$(c_0, 0, 0)$
For defense strategy $a_0 \triangleq a_{0,2}$		
P_1 \ P_2	$z^{(2)}$	$z_{\text{no}}^{(2)}$
$z^{(1)}$	$(d_1 + c_0, f_{1,1} - c_1, f_{2,1} - c_2)$	$(d_1 + c_0, f_{1,1} - c_1, f_{2,1})$
$z_{\text{no}}^{(1)}$	$(c_0, 0, -c_2)$	$(c_0, 0, 0)$

In this game solution, similarly to Proposition 1, when both attackers launch their respective attacks, their actions eliminate one another. Clearly, the PSNE of this game depends on the sign of $f_{i,j}$. In this regard, we examine two cases.

In case 1, we consider the scenario in which the action of one attacker results in a financial loss to the other attacker when the latter chooses not to carry out any attack. Hence, in this case $f_{1,2} < 0$ and $f_{2,1} < 0$. The PSNE of this game is *unique* and it corresponds to the case in which both attackers choose to attack and the defender chooses not to take any defensive actions, $(a_0^*, a_1^*, a_2^*) = (a_{0,no}, z^{(1)}, z^{(2)})$, which results in $(U_0, U_1, U_2) = (0, -c_1, -c_2)$. In fact, at this PSNE, none of the attackers has an incentive to unilaterally deviate from this equilibrium since by unilaterally choosing not to attack, an attacker incurs a bigger financial loss; while by choosing to defend, the defender achieves a worse utility. In fact, *the defender achieves its best possible utility at this equilibrium; hence, any taken defensive action, in this case, serves to worsen its outcome*.

In case 2, we consider the scenario in which attacker 1 is subject to a positive profit due to attacker 2's attack while, on the other hand, attacker 2 is subject to a negative profit due to attacker 1's attack. This case, hence, corresponds to $f_{1,2} > 0$ and $f_{2,1} < 0$. In this case, $(a_{0,no}, z^{(1)}, z^{(2)})$ is not a PSNE. The game's equilibrium highly depends on the considered costs of attack and defense which makes the existence of a PSNE dependent on the considered costs. Therefore, we look at characterizing the Nash equilibrium under mixed strategies. A mixed strategy associates a probability distribution $\alpha_i(a_i)$ with the pure strategies $a_i \in \mathcal{A}_i$ of player $i \in \mathcal{P}$ where $\boldsymbol{\alpha} = [\alpha_0, \alpha_1, \alpha_2]$ is defined to be the vector of all mixed strategies. The expected utility of player i over the vector of all strategies, $\boldsymbol{a} \in \mathcal{A} \triangleq \mathcal{A}_0 \times \mathcal{A}_1 \times \mathcal{A}_2$, is defined as:

$$U_i^E(\boldsymbol{\alpha}) = \sum_{\boldsymbol{a}\in\mathcal{A}} \Big[\prod_{k=0}^{M} \alpha_k(a_k)\Big] U_i(a_i, \boldsymbol{a}_{-i}). \tag{27}$$

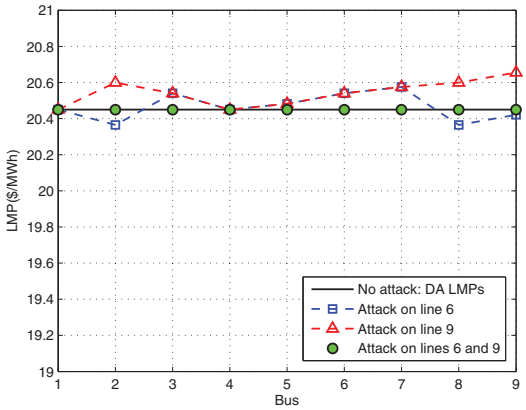

Fig. 1. System LMPs under different attack scenarios.

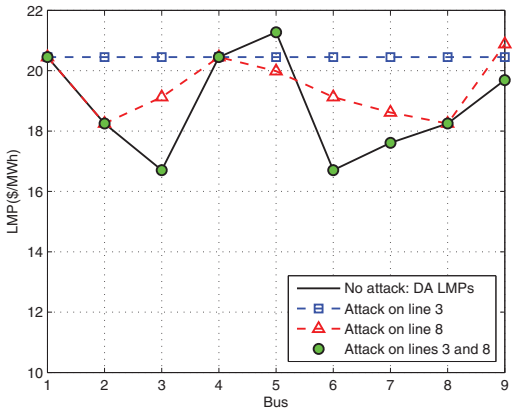

Fig. 2. System LMPs under different attack scenarios.

Consider the equilibrium probabilities to be defined as $p_1 = \alpha_1^*(z^{(1)})$, $p_2 = \alpha_2^*(z^{(2)})$, $q_1 = \alpha_0^*(a_{0,1})$, and $q_2 = \alpha_0^*(a_{0,2})$, the game's proper mixed-strategy Nash equilibrium (MSNE) in which the strategies are such that $0 < \alpha_i^*(a_i) < 1 \, \forall i \in \mathcal{P}$ is derived analytically using the von Neumann indifference principle [9] (derivation details are omitted due to space limitations):

$$p_1 = \frac{d_2\left(d_1 \pm \sqrt{-\frac{d_1(4c_0d_1+4c_0d_2-d_1d_2)}{d_2}}\right)}{2d_1(d_1+d_2)}, \tag{28}$$

$$p_2 = \left(\frac{d_1}{d_2}\right) p_1, \tag{29}$$

$$q_1 = \frac{p_2(f_{1,1}+f_{1,2})(c_1f_{2,2}+c_2f_{1,1}-f_{2,2}f_{1,1})}{f_{1,1}\big(p_1(f_{2,2}f_{1,1}+f_{1,1}f_{2,1})-f_{2,2}f_{1,1}(1-p_2)+f_{2,2}f_{1,2}p_2\big)} - \frac{c_1-f_{1,1}}{f_{1,1}}, \tag{30}$$

$$q_2 = -\frac{(f_{1,1}p_2-f_{1,1}+f_{1,2}p_2)(c_1f_{2,2}+c_2f_{1,1}-f_{2,2}f_{1,1})}{f_{1,1}\big(p_1(f_{2,2}f_{1,1}+f_{1,1}f_{2,1})-f_{2,2}f_{1,1}(1-p_2)+f_{2,2}f_{1,2}p_2\big)} + \frac{c_1}{f_{1,1}}. \tag{31}$$

Remark 1: The proposed game admits *a maximum of two* proper MSNEs under the necessary condition $c_0 \leqslant \frac{d_1d_2}{4(d_1+d_2)}$.

IV. Numerical Results

In this section, numerical results are provided to study the analytical solutions derived in Section III, for the two discussed cases, through an application of the formulated game to the WSCC 9-bus test system (system information available in [10]). Throughout this section, two attackers and a defender are considered with action spaces similar to the ones considered in Subsection III-C. Since our main focus is on the attackers' and defender's strategies, it is assumed that all market participants abide by their DA schedules and, except for the attacks and defense, no change in system conditions occur between DA and RT. Hence, when no attacks are carried out, the RT LMPs are similar to their DA counterparts.

A. Case One

In this case, line 6, connecting buses 7 and 8, and line 9, connecting buses 4 and 9, are considered to be vulnerable lines. Attacker 1 has virtual bids over buses 7 and 8 according to which attacker 1 buys (sells) virtual power at bus 7 (bus 8) in DA. In RT, attacker 1 must sell (buy) that same virtual power at bus 7 (bus 8). On the other hand, attacker 2 places virtual bids over buses 9 and 4. According to these virtual bids, in DA, attacker 2 buys (sells) virtual power at bus 9 (bus 4), while in RT, attacker 2 sells (buys) that same virtual power at bus 9 (bus 4). As can be seen from Fig. 1, in case of no attacks, no congestion takes place in the system. Hence, the LMPs across all buses are equal and none of the attackers make any profit from their virtual bids while the defender achieves its best utility. Having virtual bids at buses 7 and 8, attacker 1 aims to cause a fake estimated congestion over line 6, in RT, through data injection. As can be seen in Fig. 1, under this attack, $\mu_7^{RT} > \mu_8^{RT}$ which results in a financial benefit to attacker 1 following from (25). However, this attack results in a financial loss for attacker 2, since it results in $\mu_9^{RT} < \mu_4^{RT}$, and also causes a loss to the defender due to the successful manipulation of RT LMPs. Attacker 2, on the other hand, aims to create congestion over line 9. As can be seen from Fig. 1, this attack results in a financial benefit for attacker 2, since $\mu_9^{RT} > \mu_4^{RT}$, but causes a financial loss to attacker 1, since $\mu_8^{RT} > \mu_7^{RT}$, and a loss to the defender. When both attackers choose to launch their attacks, their combined effect on the state estimation results *causes no change in the system LMPs* in between DA and RT, as clearly shown in Fig.1, returning no profit to the attackers while the defender achieves its best utility.

Hence, this case is an illustrative example on case 1 described in Subsection III-C in which the game has a unique PSNE consisting of both attackers choosing to attack and the defender choosing not to take any defensive actions resulting in $(U_0, U_1, U_2) = (0, -c_1, -c_2)$.

B. Case Two

In this case, attacker 1 buys (sells) virtual power at bus 6 (bus 5) in DA; whereas, in RT, it sells (buys) this same power at bus 6 (bus 5). Meanwhile, attacker 2 buys (sells) virtual power at bus 9 (bus 8) in DA; whereas, in RT, it sells (buys) this same power at bus 9 (bus 8). The corresponding LMPs at the different buses under different attack strategies are shown in Fig. 2. The DA results show congestion over line 3 (considered vulnerable) connecting buses 5 and 6 resulting in $\mu_5^{DA} > \mu_6^{DA}$. Attacker 1 aims at removing this congestion in RT, through data injection, which results in a financial benefit for attacker 1 since it leads to $\mu_5^{RT} = \mu_6^{RT} = 0$. As can be seen from Fig. 2, using this attack, the congestion is removed in RT thus yielding constant LMPs at all buses. From the virtual bidding strategies of attackers 1 and 2, and following from (25), this attack results in a financial benefit to attacker 1 but a financial loss to attacker 2, since $\mu_9^{DA} > \mu_8^{DA}$ and the resulting RT LMPs are such that $\mu_9^{RT} = \mu_8^{RT}$. Since this

attack leads to successful LMPs manipulation, it generates a loss for the defender. On the other hand, in DA, there is no congestion on vulnerable line 8 connecting buses 8 and 9. Attacker 2 aims at creating an estimated congestion in RT over this line. As can be seen from Fig. 2 and (25), through this attack, attacker 2 makes a financial benefit due to the manipulation of the LMPs at buses 8 and 9, while attacker 1 also makes a profit since the created congestion results in RT LMPs that yield $\zeta_1 > 0$. Due to successful LMPs manipulation by attacker 2, this attack creates a loss for the defender. When both attackers choose to attack, their attacks mitigate each others' effect thus resulting in no change in LMPs in between DA and RT as can be seen in Fig. 2.

Hence, this case is analogous to case 2, analyzed in Subsection III-C. We next investigate the attackers' and defender's optimal strategies with respect to the cost of defense. This analysis is carried out for $c_0 \leqslant (d_1 d_2)/(4(d_1 + d_2))$ which corresponds to the range specified in Remark 1. For this range, taking no defensive actions is not a PSNE. A similar analysis can be carried out to show the effect of the costs of attack on the MSNE but has been omitted here for space limitation.

Fig. 3 shows the variation of the equilibrium's mixed strategies of the two attackers and the defender with respect to the cost of defense. This figure shows that both attackers are more likely to attack when the cost of defense increases. In fact, an increase in c_0 from \$40 to \$60 causes a twofold increase in the probability of attack of any of the attackers. In contrast, the defender's mixed strategy at the equilibrium is less sensitive to c_0. This is due to the fact that the cost of defense, in the studied range, is significantly smaller than the overall effect an attack has on the system. For instance, attacker 1's successful attack yields $U_0 = \$720$ for a total load, $P_L = 315$ MW. Hence, paying a higher cost to defend the system is still beneficial to the defender.

In Fig. 4, we show the optimal expected utility of the defender resulting from the derived MSNE. In this figure, the results are compared to the expected utilities in the cases in which either no defense is taken or the defender is equally likely to defend either one of the attacked measurements. The expected utilities are plotted as a function of the cost of defense. Since the defender aims at minimizing its utility, as shown in (21), Fig. 4 shows performance gains of the derived optimal defense strategy as compared to the other strategies. For $c_0 = \$40$, these gains reach improvement up to 79% compared to the no defense strategy and 85% compared to the uniform defense strategy. Moreover, it also shows that it is better for the defender not to take any defensive actions than to be equally likely to defend any of the measurements. In addition, Fig. 4 shows, as expected, that the defender has a worse expected utility when the cost of defense, c_0, increases which is clear from (21). In fact, a \$20 increase in c_0 (from \$40 to \$60) causes a \$60 increase in the defender's expected utility following the optimal defense strategy.

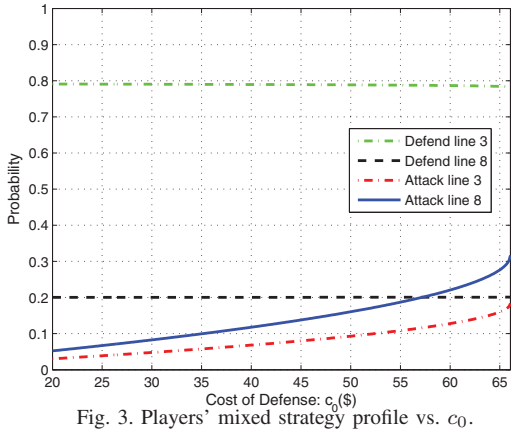

Fig. 3. Players' mixed strategy profile vs. c_0.

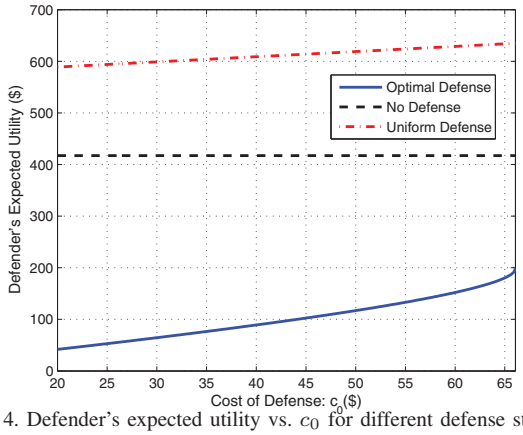

Fig. 4. Defender's expected utility vs. c_0 for different defense strategies.

V. Conclusion

In this paper, we have studied the problem of data injection attacks on smart grid with multiple attackers. The strategic interactions between the defender and the attackers have been modeled using a noncooperative game in which costs of attack and defense have been integrated in the utility functions of the players. For the formulated game, we have derived the optimal defense and attack strategies. Based on the obtained results, we have shown that at equilibrium, under some attack schemes, defensive actions are not needed to defend the system; whereas, for other schemes, defense is needed to reduce the effect of the attacks. Moreover, we have studied the effect of the cost of defense on the attackers' and defender's optimal strategies and utilities. Our results have provided valuable insights on how data injection attacks with multiple adversaries can impact a smart grid.

References

[1] T. Kim and H. V. Poor, "Strategic protection against data injection attacks on power grids," *IEEE Transactions on Smart Grid*, vol. 2, no. 2, pp. 326–333, June 2011.

[2] A. J. Wood and B. F. Wollenberg, *Power generation, operation, and control*. John Wiley & Sons, 2012.

[3] Y. Liu, P. Ning, and M. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security (TISSEC)*, vol. 14, no. 1, pp. 1–33, May 2011.

[4] 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, Dec 2011.

[5] M. Esmalifalak, G. Shi, Z. Han, and L. Song, "Bad data injection attack and defense in electricity market using game theory study," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 160–169, March 2013.

[6] A. L. Ott, "Experience with pjm market operation, system design, and implementation," *IEEE Transactions on Power Systems*, vol. 18, no. 2, pp. 528–534, May 2003.

[7] F. Li, Y. Wei, and S. Adhikari, "Improving an unjustified common practice in ex post lmp calculation," *IEEE Transactions on Power Systems*, vol. 25, no. 2, pp. 1195–1197, May 2010.

[8] A. Abur and A. G. Exposito, *Power system state estimation: theory and implementation*. New York: Marcel Dekker, 2004.

[9] T. Başar and G. J. Olsder, *Dynamic Noncooperative Game Theory*. Philadelphia, PA, USA: SIAM Series in Classics in Applied Mathematics, Jan. 1999.

[10] R. Zimmerman, C. Murillo-Sanchez, and R. 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, Feb 2011.