Malicious Ramp-induced Temporal Data Attack in Power Market with Look-ahead Dispatch

Dae-Hyun Choi and Le Xie
Department of Electrical and Computer Engineering, Texas A&M University, College Station, TX, USA
Email: cdh8954@neo.tamu.edu, Lxie@ece.tamu.edu

Abstract—We present a new class of cyber attack on state estimation, which may lead to financial arbitrage in power markets with time-coupled look-ahead dispatch models. It is shown that in look-ahead dispatch, attackers can manipulate the limits of ramp constraints of generators, withhold their generation capacity, and consequently make a profit. The feasibility and economic impact of such cyber attacks on real-time electricity market operations are illustrated in the IEEE 14-bus system.

I. INTRODUCTION

THE electricity grid has been facing an increasing number of potential cyber attacks [1]. The strong coupling of power systems with the cyber infrastructure such as sensor and communication network opens the possibility of malicious cyber attacks. The main objective of this paper is to investigate the impact of cyber attacks on state estimation, which in turn, affect the result of an emerging economic dispatch model in the power system. Impact of such cyber attacks can be illustrated in a conceptual three-layer framework, which consists in the physical, measurement, and control/computation layer as shown in Figure 1. Bad/malicious data may be injected into the measurement layer, which leads to a distorted estimation of the states of the physical layer. As a result, the attacker could impact the feedback from control/communication layer back to the physical layer, resulting (1) power grid physical insecurity, and/or (2) financial misconducts in the power markets. This paper is an effort toward understanding the impact of (2) in a more realistic power market setting.

Recently, many researchers have been paying attention to investigate the vulnerability of power system operation (state estimation in particular) to cyber attacks. False data injection attacks against state estimation was formulated and analyzed in [2], [3]. Efficient algorithms to find sparse attacks (compromising a small set of measurements) and PMUs placement algorithms to prevent such sparse attacks are developed in [4], [5]. A distributed joint detection-estimation framework for malicious data injection attack problem is presented in [6]. In [7], it is shown that the attacker can hack the power grid without prior knowledge of the power network topology, which can be estimated using linear independent component analysis (ICA). On the other hand, the economic impact of false data injection attacks against state estimation on real-time market operations is first examined in [8]. Heuristic attack strategies based on virtual bidding mechanism for finding undetectable and profitable attacks are provided. In [9], more general malicious data attack problem is formulated in the real-time electricity market. However, in [8], [9], false data injection attacks are characterized in static economic dispatch model without modeling inter-temporal constraints.

In this paper, we formulate a new type of potential cyber attacks in more realistic economic dispatch model, i.e., look-ahead dispatch. Compared with conventional static dispatch, look-ahead dispatch computes the optimal dispatch in an extended period of time, taking into account inter-temporal ramp rates of generators of different technologies. This is motivated by the increasing penetration of variable resources such as wind and solar [10]. Major independent system operators (ISOs)/regional transmission organizations (RTOs) have been implementing look-ahead dispatch in the past few years in order to improve the market dispatch efficiency [11], [12], [13]. We show how the attacker could withhold generation capacity and make a profit by stealthily manipulating inter-temporal constraints (i.e., ramp constraints of generators) of look ahead dispatch. The proposed attack problem is different from the existing capacity withholding literature in that for the purpose of withholding capacity, the proposed approach manipulates the limit of ramp constraints by injecting undetectable malicious data into sensors, whereas the conventional capacity withholding approach uses learning algorithm (e.g., SA-Q-Learning algorithm) for a generation company to report capacity noticeable lower than its maximum capacity [14], [15].

The main contributions of this paper are suggested as two fold:
1) We formulate a malicious ramp-induced data (RID) attack problem in look-ahead dispatch. The attacker could stealthily change the ramp constraints of generators through manipulating sensors’ data, aiming at increasing the nodal price by withholding capacity of generator.

2) We propose a RID attack strategy with which the attacker can make a profit without being detected by RTOs in the real-time electricity market. Numerical examples are provided in the IEEE-14 bus system.

The rest of the paper is organized as follows. Section II provides the overview of state estimation and real-time power market with look-ahead dispatch model, and addresses problem statement. In Section III, the attack model and proposed RID attack strategy are formulated. Section IV evaluates the performance of the proposed RID attacks in the IEEE-14 bus system. The conclusions and future work are discussed in Section V.

II. PRELIMINARIES AND PROBLEM STATEMENT

The notations used in this paper are summarized in Table I.

<table>
<thead>
<tr>
<th>Index</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>$i$</td>
<td>Index for generators $i$</td>
</tr>
<tr>
<td>$n$</td>
<td>Index for buses $n$</td>
</tr>
<tr>
<td>$l$</td>
<td>Index for transmission line $l$</td>
</tr>
<tr>
<td>$K$</td>
<td>Total number of sampling period</td>
</tr>
<tr>
<td>$N$</td>
<td>Total number of buses</td>
</tr>
<tr>
<td>$L$</td>
<td>Total number of transmission lines</td>
</tr>
<tr>
<td>$M$</td>
<td>Total number of measurements</td>
</tr>
<tr>
<td>$G$</td>
<td>Set of generation units</td>
</tr>
<tr>
<td>$G_M$</td>
<td>Set of marginal units</td>
</tr>
<tr>
<td>$L_M$</td>
<td>Set of binding units with lower marginal cost than marginal unit</td>
</tr>
<tr>
<td>$D$</td>
<td>Set of Demands</td>
</tr>
<tr>
<td>$P_{gi}[k]$</td>
<td>Scheduled $i$th generator power at time $k$</td>
</tr>
<tr>
<td>$D_{ni}[k]$</td>
<td>With bus fixed demand at time $k$</td>
</tr>
<tr>
<td>$F_l[k]$</td>
<td>Transmission flow at line $l$ at time $k$</td>
</tr>
<tr>
<td>$R_l$</td>
<td>Ramp rate of generator $i$</td>
</tr>
<tr>
<td>$\Delta T$</td>
<td>Dispatch interval</td>
</tr>
<tr>
<td>$P_{\min}$, $P_{\max}$</td>
<td>Min/max generation limits for generator $i$</td>
</tr>
<tr>
<td>$F_{\min}$, $F_{\max}$</td>
<td>Min/max flow limits at line $l$</td>
</tr>
</tbody>
</table>

### A. State Estimation

We consider a state estimation model based on a linearized DC power flow. The measurements taken by each sensor are written by

$$z = Hx + e$$  \hspace{1cm} (1)

where $x$ is the $N \times 1$ state vector of the entire power system, $z$ is the $M \times 1$ measurement vector, $e$ is the $M \times 1$ random measurement error vector, and $H$ is the $M \times N$ system factor matrix of the state vector $x$. Due to a bijective relationship between bus voltage phase angle and the nodal power injection vector [8], the state vector $x$ in this paper represents the nodal power injections, and the measurement vector $z$ is composed of power injection and flow measurements. Error vector $e$ is assumed to be independent identically distributed (i.i.d.) Gaussian random variables with zero mean and $M \times M$ covariance matrix $R$. The system factor matrix $H$ specifies the relationship between $x$ and its corresponding $z$. Therefore, (1) can be rewritten by

$$z = Hx + e = \begin{bmatrix} I \\ H_{\text{d}} \end{bmatrix} x + e$$  \hspace{1cm} (2)

where $H_{\text{d}}$ and $I$ denote the distribution factor matrix and the identity matrix, respectively. The state estimation problem is to find the optimal estimate of $x$ to minimize the weighted least square of measurement error:

$$\min_{x} J(x) = r^T R^{-1} r$$  \hspace{1cm} (3)

s.t. $r = z - Hx$  \hspace{1cm} (4)

where $r$ is the estimated residual vector. If the system is observable (i.e., the system factor matrix $H$ is full rank), the weighted least squares estimate of $x$ is written as the multiplication form of the $N \times M$ matrix $B$ and $z$,

$$\hat{x}(z) = (H^T R^{-1} H)^{-1} H^T R^{-1} z = Bz$$  \hspace{1cm} (5)

B. Real-time Power Market with Time-coupled Look-ahead Dispatch Model

Recently, due to high inter-temporal variability of renewable resources such as wind and solar, RTOs are making the transition from static dispatch to look-ahead dispatch for more flexible operations in support of high penetration of variable resources [11]. In this realistic economic dispatch model, we demonstrate that the proposed cyber attacks lead to a financial misconduct. Look-ahead dispatch formulation is simply presented as follows:

$$\min_{P_{gi}[k]} \sum_{k=1}^{K} \sum_{i \in G} C_i(P_{gi}[k])$$  \hspace{1cm} (6)

s.t.

\begin{align*}
(\lambda[k]) & : \sum_{i \in G} P_{gi}[k] = D_n[k] \quad \forall k = 1, \ldots, K \\
(\omega[k]) & : |P_{gi}[k] - P_{gi}[k-1]| \leq R_i \Delta T \quad \forall k = 1, \ldots, K \\
(\tau_i[k]) & : P_{g\min} \leq P_{gi}[k] \leq P_{g\max} \quad \forall k = 1, \ldots, K \\
(\mu_l[k]) & : F_{l\min} \leq F_{l}[k] \leq F_{l\max} \quad \forall k = 1, \ldots, K, \forall l = 1, \ldots, L
\end{align*}  \hspace{1cm} (7) \hspace{1cm} (8) \hspace{1cm} (9) \hspace{1cm} (10)

In this formulation, the objective function is to minimize the total generation costs in (6). (7) is the system-wide energy balance equations. (8) and (9) are the ramp constraints and the physical capacity constraints of each generator, respectively. (10) is the transmission line constraints, which contribute to network transmission congestion. In this paper, we call one-step look-ahead dispatch with $K = 1$ as static dispatch.

According to the definition of the nodal price [16] and assuming that bus 1 is the slack bus, the LMP for each bus $n (n = 2, \ldots, N)$ at time $k$ is computed with the Lagrangian
multipliers of look-ahead dispatch formulation as follows:
\[
\lambda_i[k] = \lambda[k] - \mathbf{H}_{da}^T (\mu_{\text{max}}[k] - \mu_{\text{min}}[k])
\]  
(11)
where \(\lambda[k]\) is the LMP for the slack bus 1 at time \(k\), \(\mathbf{H}_{da} = [\frac{\partial C_i(P_{gi}[k])}{\partial P_{gi}[k]} \ldots \frac{\partial C_i(P_{gi}[k])}{\partial P_{gi}[k]}]^T\), \(\mu_{\text{max}}[k] = [\mu_{1,\text{max}}[k], \ldots, \mu_{L,\text{max}}[k]]^T\), and \(\mu_{\text{min}}[k] = [\mu_{1,\text{min}}[k], \ldots, \mu_{L,\text{min}}[k]]^T\).

Alternatively, by the first-order KKT condition of look-ahead dispatch formulation, the LMP for each generator \(i\) connected to bus \(n\) is expressed as
\[
\lambda_i[k] = \frac{\partial C_i(P_{gi}[k])}{\partial P_{gi}[k]} - \mathbf{H}_{da}^T (\mu_{\text{max}}[k] - \mu_{\text{min}}[k])
\]  
\[+ (\tau_{i,\text{max}}[k] - \tau_{i,\text{min}}[k]) + (\omega_{i,\text{max}}[k] - \omega_{i,\text{max}}[k + 1])
\]  
\[+ (\omega_{i,\text{min}}[k + 1] - \omega_{i,\text{min}}[k])
\]  
(12)
We note that LMP formulation in static dispatch (one-step look-ahead) does not include the future time Lagrangian multipliers, \(\omega_{i,\text{max}}[k + 1]\) and \(\omega_{i,\text{min}}[k + 1]\).

C. Problem Statement

\(P_{gi}[0]\) in the ramp constraint of unit \(i\) denotes the initial generation power at \(k = 0\). We note that this initial generation power \(P_{gi}[0]\) is replaced, at every dispatch interval, by its corresponding state estimate \(\hat{P}_{gi}(z)\), which is in advance processed by the state estimator in EMS. Therefore, in static dispatch the generation power of unit \(i\) at \(k = 1\) becomes bounded at every dispatch interval by
\[
\begin{align*}
P_{\text{max}}^{\text{gi}}[1] &= \min \{P_{\text{max}}^{\text{gi}}, P_{\text{max}}^{\text{gi}}(z)\} \quad (13) \\
P_{\text{min}}^{\text{gi}}[1] &= \max \{P_{\text{min}}^{\text{gi}}, P_{\text{min}}^{\text{gi}}(z)\} \quad (14)
\end{align*}
\]
where the maximum and minimum limits of the ramp constraints, \(P_{\text{max}}^{\text{gi}}(z)\) and \(P_{\text{min}}^{\text{gi}}(z)\), are
\[
P_{\text{max}}^{\text{gi}}(z) = \hat{P}_{gi}(z) + R_i \Delta T, \quad P_{\text{min}}^{\text{gi}}(z) = \hat{P}_{gi}(z) - R_i \Delta T \quad (15)
\]
If the attacker stealthily manipulates, through injecting malicious data into \(z\) at \(k = 0\), the estimate \(\hat{P}_{gi}(z)\) so that the capacity limit of unit \(i\) at \(k = 1\) is set to intentionally changed ramp constraint limits (i.e., capacity withholding occurs), the system operator can miscalculate the dispatch instruction such as the optimal generation power and nodal price of each bus. In this paper, we define this type of attack as a ramp-induced data (RID) attack in a potential class of malicious inter-temporal data attacks.

Figure 2 shows a conceptual diagram, which illustrates how the attacker withholds capacity of a marginal unit (a part-loaded generator) by changing the estimate associated with the initial generation power of the marginal unit. Left and right figures describe the generation characteristic of the marginal unit before and after the RID attack, respectively, when no transmission lines are congested. \(W\) is an available generation power window associated with the ramp rate of the generator, and \(\Delta L\) is an incremental or decremental system load from \(k = 0\) to \(k = 1\). In this figure, \(\Delta L\) denotes an incremental system load. As shown in Figure 2, the estimate \(\hat{P}_{gi}[0]\) (for simplicity, we omit \(z\), instead emphasize the initial time) determines the range of \(W\). Without attack, the marginal unit still become a part-loaded generator at \(k = 1\) so that the nodal price at each bus becomes equal to the marginal cost of this marginal unit. On the other hand, if \(\hat{P}_{gi}[0]\) is reduced to \(\hat{P}_{gi,n}[0]\) by the attacker at \(k = 0\) until \(\Delta L\) deviates upwards from the range of \(W\), the attacker withholds capacity of the marginal unit with a new dispatch power \(\hat{P}_{gi,n}[1]\) at \(k = 1\). Thus, an excess power left after capacity withholding is allocated to another generator with the next higher marginal cost, which consequently sets increased LMPs.

III. RAMP-INDUCED DATA ATTACK

A. Attack Model

We assume that the attacker can manipulate the measurements of sensors and consider the attack measurement model as follows:
\[
z_a = \mathbf{H}x + e + a
\]  
(16)
where \(a\) is the false data vector injected by the attacker, which results in the corrupted measurement vector \(z_a\). As shown in [8], the new residual vector \(r_a\) can be decomposed into the two terms:
\[
r_a = r + (\mathbf{I} - \mathbf{HB})a
\]  
(17)
and by triangular inequality of the standard Euclidean 2-norm \(|| \cdot ||_2\),
\[
||r_a||_2 = ||r + (\mathbf{I} - \mathbf{HB})a||_2 \leq ||r||_2 + ||(\mathbf{I} - \mathbf{HB})a||_2
\]  
(18)
For bypassing the bad data detection from the system operators, the attacker seeks to find the attack vector \(a\) such that the value of \(||(\mathbf{I} - \mathbf{HB})a||_2\) added to \(||r||_2\) still makes the following undetectable condition hold true:
\[
||r_a||_2 < \eta
\]  
(19)
where \(\eta\) is the bad data detection threshold.

For a successful RID attack, the attacker is assumed to have the knowledge of
1) the system topology (e.g., distribution factor matrix),
which keeps constant at every dispatch interval
2) the ramp rates of attacking power generators
3) the amount of changing system load between two consecutive dispatch intervals

The system topology of the target power system can be exposed off-line by an internal intruder in a control center or can be estimated by linear independent component analysis (ICA) technique proposed in [7]. For assumption (2), typical ramp rates are estimable for typical generators. Assumption (3) is also feasible since the attacker can estimate changing system load from RTOs’ website.

B. Proposed Attack Strategy

In this subsection, we propose a ramp-induced data attack strategy when no transmission lines are congested. The proposed attacks are classified into the following three types:

- **Marginal unit attack**: the attacker compromises the injection measurement sensor associated with the marginal unit.
- **Binding unit attack**: the attacker compromises the injection measurement sensors associated with the binding units.
- **Coordinated attack**: the attacker compromises the injection measurement sensors associated with the binding units as well as the marginal unit.

The marginal unit implies the part-loaded generator, whereas the binding unit does the generator, which produces its minimum or maximum generation output. To accomplish the two main goals of the attacker, undetectability and profitability, the attacker seeks to find the $M \times 1$ attack vector $a$ by compromising sensors associated with the marginal unit $i \in G_M$ or the binding unit $j \in G_B^c$, which is the solution of the following optimization problem:

$$\max_{\alpha \in \text{span}(A)} \delta$$  

s.t.

$$|| (I - H B) a ||_2 \leq \epsilon \tag{21}$$

$$\alpha C_M(a) + \beta C_B(a) \leq \Delta L - R_i \Delta T - \delta \tag{22}$$

$$\delta > 0 \tag{23}$$

where

$$C_M(a) = E[\hat{P}_{gi} - P_{gi}^*]$$

$$C_B(a) = \sum_{j \in G_B^c} E[\hat{P}_{gj} - P_{gj}^*] + R_j \Delta T - F_{gj}^{\text{max}}$$

$C_M(a)$ and $C_B(a)$ are defined as the contributions of the attacker to changing the nodal price, corresponding to the marginal unit $i$ and binding unit $j$ attacks, respectively. $B_i$ is the $1 \times M$ vector of matrix $B$, which corresponds to the injection measurement sensor of a generator $i$. The set $\mathcal{A}$ represents the attack vector space, which describes the attack pattern with respect to the type and number of compromised sensors. $\Delta L - R_i \Delta T$ is the minimum amount of power which the attacker should reduce in order to withhold capacity of unit $i$ at $k = 1$. Constraint (21) assures the undetectability of the attack as the parameter $\epsilon$ is tuned with an appropriate value. That is, the tuned $\epsilon$ makes sure $|| r_a ||_2 < \eta$ in (18). Constraint (22) makes a marginal unit become binding at the maximum limit of its corresponding ramp constraint. Therefore, the attacker aims at maximizing the positive margin $\delta$ in order to withhold capacity of attacking marginal unit and subsequently increase the nodal price with a high probability. The binary values of $\alpha$ and $\beta$ in (22) classify the following three types of attacks:

1) $\alpha = 1$, $\beta = 0$: Marginal unit attack
2) $\alpha = 0$, $\beta = 1$: Binding unit attack
3) $\alpha = 1$, $\beta = 1$: Coordinated attack

IV. NUMERICAL EXAMPLE

In this section, the economic impact of the proposed RID attack on the real-time electricity market operation is illustrated in the IEEE 14-bus system as shown in Figure 3.

![IEEE 14-bus Test system](image)

Fig. 3. IEEE 14-bus Test system.

We assume a DC state estimation model where nodal power injection measurements are placed at all generation and load buses, and power flow measurements at one end of each transmission line. Therefore, this system has a total of 34 measurements, including 14 power injection and 20 power flow measurements, making the system observable. Table II shows the five generators’ operating characteristics including unit types (generation bus number), physical capacity limits, ramp rates and marginal costs of each generator.

<table>
<thead>
<tr>
<th>Unit Type</th>
<th>$P_{\min}$</th>
<th>$P_{\max}$</th>
<th>Ramp Rate</th>
<th>Marginal Cost</th>
</tr>
</thead>
<tbody>
<tr>
<td>Coal(1)</td>
<td>0MW</td>
<td>200MW</td>
<td>10MW/5min</td>
<td>30$/MWh</td>
</tr>
<tr>
<td>Wind(2)</td>
<td>0MW</td>
<td>300MW</td>
<td>150MW/5min</td>
<td>20$/MWh</td>
</tr>
<tr>
<td>Nuclear(3)</td>
<td>0MW</td>
<td>300MW</td>
<td>8MW/5min</td>
<td>40$/MWh</td>
</tr>
<tr>
<td>Coal(6)</td>
<td>50MW</td>
<td>250MW</td>
<td>15 MW/5min</td>
<td>55$/MWh</td>
</tr>
<tr>
<td>Oil(8)</td>
<td>60MW</td>
<td>150MW</td>
<td>60 MW/5min</td>
<td>60$/MWh</td>
</tr>
</tbody>
</table>

TABLE II
GENERATOR PARAMETERS OF THE IEEE 14-BUS TEST SYSTEM.
The performance of the proposed attack is evaluated based on the one day load profile with a 5-min resolution, which is obtained by interpolating a 15-min daily data obtained from the ERCOT website. The load is scaled down for the load to be consistent with the IEEE 14-bus test system’s peak load data. In this section, three cases are tested:

- Case I: Marginal unit attack (as shown in Figure 3).
- Case II: Binding unit attack
- Case III: Coordinated attack

In Case I and Case II, a single power injection sensor at generation buses 3 and 1, respectively, is compromised. Case III represents the coordinated attack, which compromise both sensors mentioned in Case I and Case II. The common goal of all three cases attacks is to withhold capacity of generator 3 for the purpose of making a profit.

Figures 4 shows the comparison of LMPs between static ($K = 1$) and look-ahead dispatch ($K = 6$) without attack and with attack in Case I,II and III. Since no transmission lines are assumed to be congested, the prices in these figures represent uniform LMPs for all the buses at every dispatch interval. In Figure 4(a), LMPs in look-ahead dispatch show more fluctuating behavior around the nodal price 40$/MWh than ones in static dispatch. This phenomenon is due to the fact that the binding of generator 3 at the up- and down-ramp constraints at time $k + 1$ makes Lagrangian multipliers, $\omega^{3,\text{max}}[k + 1]$ and $\omega^{3,\text{min}}[k + 1]$, become positive, and hence, as shown in equation (12), results in different LMPs at time $k$ compared to LMPs of static dispatch. We observe from Figures 4(b),(c),(d) that LMPs in both dispatch tend to increase after attack. This observation implies that the attacker successfully withholds capacity of generator 3 by lowering its up-ramp constraint limit through manipulating its initial estimate $\hat{P}_{g_3}[0]$.

Table III summarizes the attack performance of Case I,II and III with respect to profitability and undetectability. When the power injection measurement sensor at generation bus $i$ is compromised, the attack profit efficiency at generation bus $i$, $\text{PE}(i)$, is defined as the ratio of the profit after attack to the profit before attack:

$$\text{PE}(i) = \frac{P^*_{g_i,a}[1](\lambda^{(a)}_i - c_i)}{P^*_{g_i}[1](\lambda^{(b)}_i - c_i)} \times 100$$

where $\left(\lambda^{(a)}_i, P^*_{g_i,a}[1]\right)$ and $\left(\lambda^{(b)}_i, P^*_{g_i}[1]\right)$ are a pair of the nodal price and generation output of generator $i$ after attack and before attack, respectively, and $c_i$ is a marginal cost of generator $i$. In addition, the attack becomes undetected if it

<table>
<thead>
<tr>
<th>Case</th>
<th>Static (PE(3))</th>
<th>Look-ahead (PE(3))</th>
<th>$J(\eta_x = 37.6)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>I</td>
<td>131.9</td>
<td>148.9</td>
<td>28.2</td>
</tr>
<tr>
<td>II</td>
<td>101.2</td>
<td>102.6</td>
<td>35.5</td>
</tr>
<tr>
<td>III</td>
<td>108.9</td>
<td>113.8</td>
<td>31.5</td>
</tr>
</tbody>
</table>
satisfies the following Chi-squares test condition [17]:

\[ J(\hat{x}) \leq \chi^2_{(m-s),p} := \eta_X \] (25)

where \( p \) is the detection confidence probability, and \( m \) and \( s \) represent the number of measurements and state variables, respectively. In our simulation, the threshold of the Chi-squares test (with a 99% confidence level) is set to 37.6 with \( m=34 \) and \( s=14 \). For undetectability, the parameter \( \epsilon \) in (21) is set to 3. The second and third columns of Table III indicate the attack profit efficiency at generation bus 3 in static and look-ahead dispatch. We can observe from the comparison of these two columns several facts. First, the values of PE in all three cases of both dispatch are larger than 100. It indicates that the attacker makes an additional profit by using the proposed attack strategy. Second, among the three cases, Case I attack yields the largest PE, whereas Case II attack does the smallest one. The value of PE in Case III is between Case I and Case II. This result is natural since Case II and III attacks require an extra effort for withholding the binding unit’s capacity as well as the marginal unit’s capacity so that these attacks fail with a higher probability than Case I attack. Third, for all three cases, PE in look-ahead dispatch is higher than one in static dispatch. This observation results from the fact that the attack leads to more increase of the nodal price in look-ahead dispatch than in static dispatch. The values of the estimated objective function for each case are shown in the last column of Table III, which indicates that all cases attacks successfully bypass the bad data detection performed in RTOs.

**Table IV**

| Attack            | Relative Effort (ARE) | \( \frac{||a||_{\infty}}{||\hat{a}||_{\infty}} \times 100 \) |
|-------------------|-----------------------|-------------------------------------------------|
| Static (PE(3))    | 111.8                 | 120.8 126.4 126.9 126.9                       |
| Look-ahead (PE(3))| 121.2                 | 125.3 127.0 137.7                              |
| J                 | 21.1                  | 25.4 29.2 33.1                                 |

Table IV shows the sensitivity of the attack performance with respect to the attack effort. In this table, the attacker’s relative effort (ARE) is defined as \( \frac{||a||_{\infty}}{||\hat{a}||_{\infty}} \times 100 \) where \( || \cdot ||_{\infty} \) denotes an infinity norm. We observe from this table that the increase of ARE results in more profit (the third and fourth rows) for both dispatch at the expense of increasing the estimated objective function \( J \) used for the Chi-squares bad data test (the fifth row). This observation implies that the attacker becomes more vulnerable to the Chi-squares detection as ARE increases.

V. CONCLUSIONS

In this paper, we examine the effect of a malicious ramp-induced data attack against state estimation on time-coupled look-ahead dispatch. We propose an undetectable attack strategy with which the attacker could manipulate the limit of ramp constraints of generators for withholding generation capacity and subsequently making a profit from increased nodal price. Numerical examples tested in the IEEE 14-bus system demonstrate the undetectability and profitability of such cyber attacks.

In future work, we will develop a system-theoretical framework to analyze the effect of both spatial and temporal data attacks on real-time electricity market operations. The key challenge lies in how to analytically quantify the impact of manipulated sensor’s measurement on the nodal price in space-time coupled optimization problem. Another important direction is to design robust real-time pricing models as countermeasures to mitigate the financial risks of a variety of malicious data injection attacks.

**REFERENCES**


