2020 International Conference on Information, Cybernetics,
and Computational Social Systems (ICCSS)

Energy Based Optimal Dynamic Stealth False Data Injection Attacks on the Smart Grid

Yifa Liu
the State Key Laboratory of Management and Control for Complex Systems, Institute of Automation, Chinese Academy of Sciences,
Beijing, China
the School of Artificial Intelligence, University of Chinese Academy of Sciences,
Beijing, China

Long Cheng
the State Key Laboratory of Management and Control for Complex Systems, Institute of Automation, Chinese Academy of Sciences,
Beijing, China
the School of Artificial Intelligence, University of Chinese Academy of Sciences,
Beijing, China

long.cheng@ia.ac.cn

2020 7th International Conference on Information, Cybernetics, and Computational Social Systems (ICCSS) | 978-1-7281-6246-1/20/$31.00 ©2020 IEEE | DOI: 10.1109/ICCSS52145.2020.9336868

***Abstract*—The false data injection attack is a typical cyber attack method which seriously endangers the security of power systems. Most studies of false data injection attacks regard it as a one-shot event, including the researches on the development of attack methods. However, this cannot fully demonstrate the threats of false data injection attacks. Therefore, this paper takes the dynamic behavior of the false data injection attack into account and addresses the constrains of attack resources and operations in practice. Then based on the optimal control theory, an optimal dynamic attack strategy is proposed, which significantly improves the attack effect on limited energy conditions, and reduces the possibility of being detected to a certain extent. When some conditions permit, it can be reinforced with other stealth attack methods to completely bypass the detection.**

***Index Terms*—smart grid, security, false data injection attack, optimal control**

I. Introduction

Since the demand for electrical power has soared significantly in recent years [1], especially with ecological and environmental issues emerging [2], the smart grid was proposed to overcome the various limitations of traditional power systems and provide electricity with high quality and quantity [3]. Adopting modern control, sensing, computing, communication technologies, and new equipment, the smart grid is able to integrate utilization of renewable energy on a large scale and use historical data for dynamic optimization of grid operation to improve efficiency and reliability [4].

However, due to the addition of cyber infrastructures, the smart grid is more vulnerable to malicious attacks [5], especially false data injection attacks [6]. There are many smart meters and sensors placed in the field to measure real-time operating status information, and the measurements are collected to the control center. Then an estimator is used to provide the estimation of grid states [7]. If those distributed meters are attacked and tampered with, the control center is to receive false reports and estimate wrong states, which may cause serious damage to the operation of power systems [8].

The false data usually do not match grid operation, hence, after false data injection attacks, the residual between estimation and measurement is surging rapidly [9], and then anomaly detection can find the attacks. However, this is based on the assumption that a false data injection attack creates an obvious error. There are several ways to prevent that, and one way is to inject data consistent with grid operation [10], which is called the stealth false data injection attack and works effectively.

To combat the stealth false data injection attacks, there are also specific defense methods: A data verification method against false data injection was introduced in [11]. Countermeasure for the case where the attacker has structural knowledge was also proposed in [12]. A two-layer game theoretical model for analyzing false data injection attacks against power systems was given in [13]. A list of defense mechanisms against false data injection attacks focused on one certain device [14]–[17].

However, many studies treat false data injection attack as a one-shot event and lack dynamic analysis. From this perspective, this paper gives another workable approach: continuously inject false data that cause inconspicuous errors. With noises already existing in the smart grids and electricity demand fluctuating, if the attacker chooses to launch a long-periodic but gradually increasing attack, the residual detection methods may lose effectiveness.

Furthermore, with limited resources, the challenge for the attacker is to maintain the long period attack to cause as much damage as possible. In this paper, an energy based optimal dynamic stealth attack strategy is proposed, which can cause maximum damage to the grid with limited energies while reducing the residual to conceal.

II. Problem Formulation

A. System model

In smart grids, distribution test feeders are interfaced to the local load through converters. Distributed energy resources are

This work was supported in part by the National Natural Science Foundation of China (Grants 61633016, 62025307, U1913209, and 61873268) and the Beijing Natural Science Foundation (Grant JQ19020).

connected into the main grid network at the points of common coupling and each one needs to control the voltage to keep its reference value [18]. Consider a smart grid with n buses, near the stable operating point X_d, the dynamics of the grid can be linearized into the following state-space equation [19].

$$\dot{X}(t) = A(X(t) - X_d) + BU(t), \tag{1}$$

where $X(t) = [x_1(t)\ x_2(t)\ \cdots\ x_n(t)]^T \in \mathbb{R}^n$ is the vector of states (voltage phase angles), $x_i(t)$ is the state of the i-th bus in the grid, and $U(t)$ is the input vector.

Distributed meters, such as phasor measurement units, are used to measure the system states in different locations. The measurement based on power flow model can be derived by

$$P_{ij} = \frac{V_i V_j}{X_{ij}} \sin(\theta_i - \theta_j), \tag{2}$$

where P_{ij} is the active power flow from the i-th bus to the j-th bus, X_{ij} is the reactance of the transmission line between the i-th bus and the j-th bus, V_i and θ_i are the voltage magnitude and phase angle of the i-th bus, respectively.

This paper mainly focuses on the D-C (*i.e.* direct current, but it does not mean a direct current power system) power flow model, where it is usually assumed that

- the bus voltage magnitudes are already known and close to unity,
- the voltage phase differences between (any) two buses are small.

Then (2) can be further simplified into $P_{ij} = (\theta_i - \theta_j)/X_{ij}$. Now the states of grid $(x_1, x_2, \cdots, x_n)$ can be defined as the phase angles $(\theta_1, \theta_2, \cdots, \theta_n)$.

Similarly, the measurement equation can be formalized as

$$Z(t) = HX(t) + E(t),$$

where $Z(t) = [z_1(t)\ z_2(t)\ \cdots\ z_m(t)]^T \in \mathbb{R}^m$, $m > n$ is the measurement vector, $z_i(t)$ is the measurement of the i-th meter, $E(t) = [e_1(t)\ e_2(t)\ \cdots\ e_m(t)]^T = \sigma^{\frac{1}{2}} d[b_1(t)\ b_2(t)\ \cdots\ b_m(t)]^T/dt$ is the vector of measurement noises, $b_1, b_2, \cdots, b_m$ are mutually independent standard Brownian motion and $\sigma \in \mathbb{R}^{m\times m}$ is a positive definite matrix.

As it is hard to directly get the states X (measuring high voltage power line phase angle is not a simple thing), the control center uses the measurement Z to estimate the states, namely $\hat{X}$ as the state estimation.

In order to minimize the mean square measurement error

$$\begin{aligned} j &= \lim_{\Delta t} \frac{1}{\Delta t} \int_{\tau=t}^{t+\Delta t} [Z(\tau) - H\hat{X}(\tau)]^T d\tau \int_{\tau=t}^{t+\Delta t} [Z(\tau) - H\hat{X}(\tau)] d\tau \\ &= \lim_{\Delta t} \frac{1}{\Delta t} \int_{\tau=t}^{t+\Delta t} [\hat{X}(\tau) - (H^T H)^{-1} H^T Z(\tau)]^T d\tau H^T H \\ &\quad \times \int_{\tau=t}^{t+\Delta t} [\hat{X}(\tau) - (H^T H)^{-1} H^T Z(\tau)] d\tau + \lim_{\Delta t} \frac{1}{\Delta t} \\ &\quad \times \int_{\tau=t}^{t+\Delta t} Z^T(\tau) d\tau [I - H(H^T H)^{-1} H^T] \int_{\tau=t}^{t+\Delta t} Z(\tau) d\tau, \end{aligned}$$

the (best) state estimation $\hat{X}$ can be obtained as

$$\hat{X}(t) = (H^T H)^{-1} H^T Z(t). \tag{3}$$

And the according residual is

$$\begin{aligned} r(t) &= Z(t) - H\hat{X}(t) \\ &= HX(t) + E(t) - H(H^T H)^{-1} H^T (HX(t) + E(t)) \\ &= [I - H(H^T H)^{-1} H^T] E(t), \end{aligned}$$

where I is the identity matrix.

The purpose of the control is to maintain the states at the stable point X_d, and note that the control center can only use measured and estimated information, so the feedback control law is designed as

$$U(t) = -K(\hat{X}(t) - X_d). \tag{4}$$

Applying controller (4) into system (1) leads to the following closed-loop system

$$\begin{aligned} \dot{X}(t) &= A(X(t) - X_d) - BK(\hat{X}(t) - X_d) \\ &= A(X(t) - X_d) - BK((H^T H)^{-1} H^T Z(t) - X_d) \\ &= (A - BK)(X(t) - X_d) - BK(H^T H)^{-1} H^T E(t). \end{aligned}$$

B. False Data Injection Attacks Against State Estimation

When the attacker launches a stealth false data injection attack on the meters, their measurements are tampered with,

$$\begin{aligned} Z_a(t) &= Z(t) + DT(t) \\ &= HX(t) + E(t) + DT(t), \end{aligned}$$

where $Z_a(t)$ is the measurement vector after tampering, which is sent to the control center instead, $DT(t)$ is the false data added into the original measurements, in which $T(t) \in \mathbb{R}$ is the magnitude of malicious attack and $D \in \mathbb{R}^m$ is the attack direction. The attack direction D may be limited. In the actual manipulation, the attacker carries out attacks by hacking distributed meters in the field, hence, it is hard to choose the attack direction at will. In this paper, D is assumed to be given fixed.

Remark 1: The duration of the continuous attack is much smaller than the cycle of variations in power demands, therefore, it can be considered that the stable point remains unchanged during the attack.

Replace the original measurement Z with the maliciously tampered one in (3), the estimation of states and residual after false data injection attacks are

$$\begin{aligned} \hat{X}_a(t) &= (H^T H)^{-1} H^T Z_a(t) \\ &= (H^T H)^{-1} H^T (HX(t) + E(t) + DT(t)), \end{aligned} \tag{5}$$

$$\begin{aligned} r[k] &= Z_a(t) - H\hat{X}_a(t) \\ &= (I - H(H^T H)^{-1} H^T)(E[k] + DT[k]). \end{aligned}$$

Then applying (5) into (4), and together with system model (1), the dynamic behavior of the system after being attacked can be written as follow

$$\begin{aligned} \dot{X}(t) &= A(X(t) - X_d) - BK(\hat{X}_a(t) - X_d) \\ &= A(X(t) - X_d) - BK[(H^T H)^{-1} H^T (HX(t) \\ &\quad + E(t) + DT(t)) - X_d] \\ &= (A - BK)(X(t) - X_d) - BK(H^T H)^{-1} H^T E(t) \\ &\quad - BK(H^T H)^{-1} H^T DT(t). \end{aligned}$$

C. Attack Strategy Optimization with Energy Constraints

The target of the attacker is to cause as many messes as possible: that is deviating the power system away from the operation point. The objective function is given as $J = (X-X_d)^T F(X-X_d)$, where $F \in \mathbb{R}^{n\times n}$ is a positive definite matrix. Besides, limited by attack resources, the attacker cannot carry out attacks at any level. It needs to deploy the resources rationally to best achieve its goal. Therefore, the optimization problem is formulated as follows

$$\begin{cases} \max & J = (X(t_f) - X_d)^T F(X(t_f) - X_d), \\ s.t. & \int_{t_0}^{t_f} T^2 dt = M, \end{cases}$$

where t_0 and t_f are the initial and termination time, respectively, F is the weight matrix, and $M \in \mathbb{R}$ is the total attack resources quantified by energy.

III. Main Results

A. Preprocessing

In (6), it is hard to handle an integral equation constraint, so let $S(t) = \int_{t_0}^{t} T^2 d\tau$ be the energy consumed, and then $S(t_0) = 0,\ S(t_f) = M$.

In particular, compared with the false data, the measurement noise plays a minor role. As the noise is with zero mean, $E(\int X dt|_{\substack{E\equiv 0\\ A=0}}) = E(\int X dt|_{A=0})$. So, in this section, the minor effect of noise is ignored.

To guarantee the attack magnitude T to be continuous, its derivative is taken as the input, *i.e.* $\dot{T} = u$. Denote $Y = X - X_d$, and together with attacked system (6), the optimal attack strategy problem can be transformed into the following form

$$\begin{cases} \min & -J = Y(t_f)^T(-F)Y(t_f), \\ s.t. & \dot{Y}(t) = (A-BK)Y - BK(H^TH)^{-1}H^TDT(t), \\ & \dot{T}(t) = u(t), \\ & S(t_0) = 0,\ S(t_f) = M. \end{cases}$$

B. Hamilton Function and Terminal Conditions

Consider the following standard optimal control problem

$$\begin{cases} \min & -J = \begin{bmatrix} Y(t_f) \\ S(t_f) \\ T(t_f) \end{bmatrix}^T \begin{bmatrix} -F & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} Y(t_f) \\ S(t_f) \\ T(t_f) \end{bmatrix}, \\ s.t. & \begin{bmatrix} Y(t_0) \\ S(t_0) \end{bmatrix} - \begin{bmatrix} Y_0 \\ 0 \end{bmatrix} = \mathbf{0}, \\ & \dfrac{d}{dt}\begin{bmatrix} Y(t) \\ S(t) \\ T(t) \end{bmatrix} - \begin{bmatrix} A-BK & 0 & -BK(H^TH)^{-1}H^TD \\ 0 & 0 & T(t) \\ 0 & 0 & 0 \end{bmatrix} \\ & \qquad \begin{bmatrix} Y(t) \\ S(t) \\ T(t) \end{bmatrix} - \begin{bmatrix} 0 \\ 0 \\ 1 \end{bmatrix} u(t) = \mathbf{0}, \\ & S(t_f) - M = 0, \end{cases}$$

where Y_0 is the initial state deviation, *i.e.* $Y_0 = X(t_0) - X_d$.

Denote

$$\Theta(Y(t), S(t), T(t), t) = \begin{bmatrix} Y(t) \\ S(t) \\ T(t) \end{bmatrix}^T \begin{bmatrix} -F & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix} \begin{bmatrix} Y(t) \\ S(t) \\ T(t) \end{bmatrix}$$

as the (terminal) payoff in quadratic form, and construct the Hamiltonian

$$\begin{aligned} &\mathbb{H}([Y(t)\ S(t)\ T(t)]^T, u(t), [\lambda_1(t)\ \lambda_2(t)\ \cdots\ \lambda_{n+2}(t)]^T) \\ &= \Lambda_n^T(t)[(A-BK)Y(t) - BK(H^TH)^{-1}H^TDT(t)] \\ &\quad + \lambda_{n+1}T^2(t) + \lambda_{n+2}(t)u(t), \end{aligned}$$

where $\Lambda_n(t) = [\lambda_1(t)\ \lambda_2(t)\ \cdots\ \lambda_n(t)]^T$, $\lambda_i(t)$, $i = 1, 2, \cdots, n+2$ are the Lagrange multipliers (costate variables).

It follows that Hamilton's equation:

$$\begin{cases} \dot{\Lambda}_n^T(t) = -\dfrac{\partial \mathbb{H}}{\partial Y} = -\Lambda_n^T(t)(A-BK) \\ \dot{\lambda}_{n+1}(t) = -\dfrac{\partial \mathbb{H}}{\partial S} = 0 \\ \dot{\lambda}_{n+2}(t) = -\dfrac{\partial \mathbb{H}}{\partial T} = \Lambda_n^T(t)BK(H^TH)^{-1}H^TD - 2\lambda_{n+1}(t)T(t) \\ \dot{Y}(t) = \dfrac{\partial \mathbb{H}}{\partial \Lambda_n^T} = (A-BK)Y(t) - BK(H^TH)^{-1}H^TDT(t) \\ \dot{S}(t) = \dfrac{\partial \mathbb{H}}{\partial \lambda_{n+1}} = T^2(t) \\ \dot{T}(t) = \dfrac{\partial \mathbb{H}}{\partial \lambda_{n+2}} = u(t) \\ \dfrac{\partial \mathbb{H}}{\partial u} \equiv 0 = \lambda_{n+2}(t) \\ \mathbb{H} \equiv 0 = \Lambda_n^T(t)[(A-BK)Y(t) - BK(H^TH)^{-1}H^TDT(t)] \\ \qquad + \lambda_{n+1}(t)T^2(t) + \lambda_{n+2}(t)u(t). \end{cases} \tag{6}$$

And the transversality conditions are

$$\begin{cases} \Lambda_n^T(t_f) = -\dfrac{\partial \Theta}{\partial Y}|_{t_f} = 2Y^T(t_f)F \\ \lambda_{n+1}(t_f) = -\dfrac{\partial \Theta}{\partial S}|_{t_f} - \mu\dfrac{\partial(S(t_f)-M)}{\partial S} = -\mu \\ \lambda_{n+2}(t_f) = -\dfrac{\partial \Theta}{\partial T}|_{t_f} = 0 \\ S(t_f) = M \\ Y(t_0) = Y_0 \\ S(t_0) = 0 \\ T(t_0) = 0, \end{cases} \tag{7}$$

where μ is an undetermined constant.

C. Solution

From (6) and (7), it can be easily obtained that

$$\begin{cases} \lambda_{n+1}(t) \equiv -\mu \\ \lambda_{n+2}(t) \equiv 0, \end{cases}$$

here the attack magnitude can be get

$$\dot{\lambda}_{n+2}(t) = 0 = \Lambda_n^T(t)BK(H^TH)^{-1}H^TD + 2\mu T(t)$$
$$T(t) = -\frac{1}{2\mu}\Lambda_n^T(t)BK(H^TH)^{-1}H^TD. \quad (8)$$

Then substituting (8) into system dynamics leads to the following closed-loop system

$$\dot{Y}(t) = (A-BK)Y(t) + \frac{1}{2\mu}BK(H^TH)^{-1}H^TD\Lambda_n^T(t)BK(H^TH)^{-1}H^TD.$$

Further, it can be obtained that the following state-costate equations

$$\begin{cases} \dot{\Lambda}_n(t) = -(A-BK)^T\Lambda_n(t) \\ \dot{Y}(t) = (A-BK)Y(t) + \frac{1}{2\mu}BK(H^TH)^{-1}H^TD \\ \qquad [BK(H^TH)^{-1}H^TD]^T\Lambda_n(t), \end{cases} \quad (9)$$

and its trajectory can be calculated as

$$\begin{cases} \Lambda_n(t) = \exp(-(A-BK)^T(t-t_0))\Lambda_n(t_0) \\ Y(t) = \exp((A-BK)(t-t_0))Y(t_0) \\ \qquad + \frac{1}{2\mu}\int_{t_0}^{t}\exp((A-BK)(t-\tau))BK \\ \qquad (H^TH)^{-1}H^TD[BK(H^TH)^{-1}H^TD]^T \\ \qquad \exp(-(A-BK)^T(\tau-t_0))\Lambda_n(t_0)d\tau. \end{cases} \quad (10)$$

By the property of the Hamiltonian that $\mathbb{H} \equiv 0$ when terminal time t_f is free, together with (8), the following condition holds

$$-\mu\{-\frac{1}{2\mu}\Lambda_n^T(t)BK(H^TH)^{-1}H^TD\}^2 + \Lambda_n^T(t)(A-BK)Y(t)$$
$$+\Lambda_n^T(t)BK(H^TH)^{-1}H^TD\frac{1}{2\mu}\Lambda_n^T(t)BK(H^TH)^{-1}H^TD = 0$$
$$[\Lambda_n^T(t)BK(H^TH)^{-1}H^TD]^2 = -4\mu\Lambda_n^T(t)(A-BK)Y(t). \quad (11)$$

Note the terminal condition $\Lambda_n^T(t_f) = 2Y^T(t_f)F$ and $S(t_f) = M$,

$$\int_{t_0}^{t_f}[-\frac{1}{2\mu}\Lambda_n^T(t)BK(H^TH)^{-1}H^TD]^2dt = M, \quad (12)$$
$$\Lambda_n(t_f) = 2F^TY(t_f).$$

Finally, combining constrains (11), (12), (13) and system trajectory (10), the necessary condition of optimal attack strategy can be derived as follows

$$\begin{cases} \Lambda_n^T(t_0)\exp(-(A-BK)(t-t_0))BK(H^TH)^{-1}H^TD \\ [BK(H^TH)^{-1}H^TD]^T\exp(-(A-BK)^T(t-t_0))\Lambda_n(t_0) \\ = -4\mu\Lambda_n^T(t_0)\exp(-(A-BK)(t-t_0))BK(H^TH)^{-1}H^T \\ D(A-BK)\exp((A-BK)(t-t_0))\{Y(t_0) + \frac{1}{2\mu}\int_{t_0}^{t} \\ \exp(-(A-BK)(\tau-t_0))BK(H^TH)^{-1}H^TD[BK \\ (H^TH)^{-1}H^TD]^T\exp(-(A-BK)^T(\tau-t_0))\Lambda_n(t_0)d\tau\}, \\ \int_{t_0}^{t_f}\Lambda_n^T(t_0)\exp((-A-A^T+BK+K^TB^T)(t-t_0))\Lambda_n(t_0) \\ \qquad = 4\mu^2M, \\ \{\exp(-(A-BK)^T(t_f-t_0)) - \frac{1}{\mu}F^T\exp((A-BK) \\ (t_f-t_0))\int_{t_0}^{t_f}\exp(-(A-BK)(\tau-t_0))BK(H^TH)^{-1} \\ H^TD[BK(H^TH)^{-1}H^TD]^T\exp(-(A-BK)^T \\ \quad (\tau-t_0))d\tau\}\Lambda_n(t_0) = \exp((A-BK)(t_f-t_0))Y(t_0), \end{cases} \quad (13)$$

where $\Lambda_n(t_0)$, μ, t_f are unknown parameters. Finally, the optimal attack magnitude is

$$T(t) = -\frac{1}{2\mu}\Lambda_n^T(t)BK(H^TH)^{-1}H^TD.$$

IV. Numerical Results

In this section, some numerical experiments are taken to validate the attack strategy proposed in this paper.

In the experiments, the following two indicators are used:

1) With limited energy, how much damage the attack can cause to the power system.
2) How many residuals will be generated during the attack, which is related to the possibility of the attack being detected.

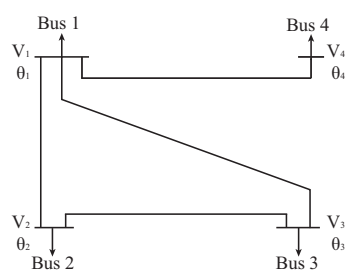


Fig. 1. A 4-bus microgrid system illustration.

Consider the microgrid system with 4 buses in Fig. 1. The base power S_B is 100MW and the base voltage U_B is 230kV. θ_1 is set to reference, which is always 0. The states when the system is operating stably are as follows

$$V^d = \begin{bmatrix} v_1^d \\ v_2^d \\ v_3^d \\ v_4^d \end{bmatrix} = \begin{bmatrix} 230 \\ 18.45 \\ 13.8 \\ 16.5 \end{bmatrix}(kV), \quad \theta^d = \begin{bmatrix} \theta_1^d \\ \theta_2^d \\ \theta_3^d \\ \theta_4^d \end{bmatrix} = \begin{bmatrix} 0 \\ 11.497 \\ 6.682 \\ 2.217 \end{bmatrix}(^\circ).$$

It is assumed that the control objective is to keep the voltage phases to be the reference value θ^d and the voltage magnitudes

have already reached the operating value and are fixed. And the system state is defined as the deviation of the phase angles from the reference values, *i.e.* $X = [x_1\ x_2\ x_3\ x_4] = \pi(\theta - \theta^d)/180\,(rad)$.

Then the linearized differential equation for the power system is described as the following continuous-time state-space model

$$\begin{bmatrix} \dot{x}_2 \\ \omega_2 \\ x_3 \\ \omega_3 \\ x_4 \\ \omega_4 \end{bmatrix} = A \begin{bmatrix} x_2 \\ \omega_2 \\ x_3 \\ \omega_3 \\ x_4 \\ \omega_4 \end{bmatrix} + \begin{bmatrix} 0 & 0 & 0 \\ 2.0723 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 4.4063 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0.561 \end{bmatrix} \begin{bmatrix} T_{m1} \\ T_{m2} \\ T_{m3} \end{bmatrix},$$

where $A =$

$$\begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ -5.4592 & -4.1446 & 2.3385 & 0 & 3.1207 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 5.2010 & 0 & -10.7226 & -8.8126 & 5.5106 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0.952 & 0 & 0.7494 & 0 & -1.7014 & -1.122 \end{bmatrix}.$$

The output feed-back control law is designed as $[T_{m1}\ T_{m2}\ T_{m3}]^T = -K\hat{X}$, where

$$K = \begin{bmatrix} -0.5621 & 0 & 1.1285 & 0 & 1.5059 & 0 \\ 1.1804 & 0 & 1.9728 & 0 & 1.2506 & 0 \\ 1.6970 & 0 & 1.3358 & 0 & -2.4718 & 0 \end{bmatrix}$$

The measurement is based on the bus and branch active power flows as (2),

$$P = \left[P_{12}\ P_{13}\ P_{14}\ P_{34}\right]^T = h(\left[\theta_2\ \theta_3\ \theta_4\right]^T).$$

At the stable operating point, denote $H = \partial h(X)/\partial X|_{X=X^d}$ as the measurement matrix and the measurement vector is selected as $Z = [z_1\ z_2\ z_3\ z_4]^T = [P_{12} - P_{12}^d\ P_{13} - P_{13}^d\ P_{14} - P_{14}^d\ P_{34} - P_{34}^d]^T + E$. Then the measurement equation can be derived by

$$\begin{aligned} Z &= HX + E \\ &= \begin{bmatrix} -24.8601 & 0 & 0 \\ 0 & -17.9574 & 0 \\ 0 & 0 & -123.3828 \\ 2.0172 & -2.0172 & 0 \end{bmatrix} \begin{bmatrix} x_2 \\ x_3 \\ x_4 \end{bmatrix} + E, \end{aligned}$$

where $dE \sim N_4\big(0, diag(1.29, 2.03, 2.49, 1.43)dt\big)$ is the measurement noise vector, whose elements are independent white noises with zero-mean. Then the estimation can be obtained as $[\hat{x}_2\ \hat{x}_3\ \hat{x}_4]^T = (H^T H)^{-1} H^T Z$, $\hat{X} = [\hat{x}_2\ \hat{x}_3\ \hat{x}_4]^T \otimes [1\ 0]^T$, where $\otimes$ is the Kronecker operator.

A. Optimal Attack Performance under Non-concealed Scenario

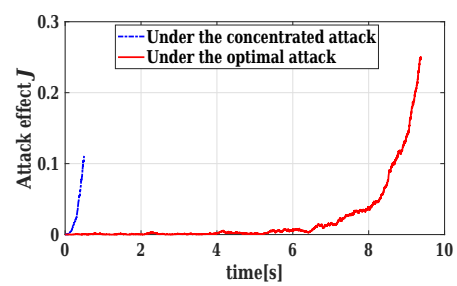
Assume that the attacker can only compromise the meter between bus 1 and bus 2, *i.e.* $D = [1\ 0\ 0\ 0]^T$. Under the traditional attack strategy, the attacker would like to consume all energy with a constant attack magnitude in a short period of time to ensure the success of this attack, that is the concentrated attack strategy.

The following part shows the effects of the two attack strategies, namely one-shot concentrated attack strategy and the energy based optimal attack strategy, respectively. Detailed parameters of both attacks are presented in Table I.

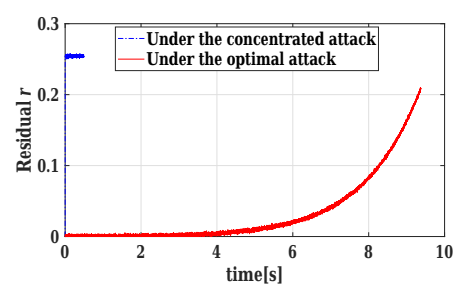
TABLE I
DESIGN PARAMETERS OF ATTACK STRATEGIES

Module	Design Parameters
System assessment	$F = \begin{bmatrix} 167.2703 & 0 & 0 \\ 0 & 175.5506 & 0 \\ 0 & 0 & 30.4878 \end{bmatrix}$ $J = (\theta - \theta^d)^T F(\theta - \theta^d)$
Concentrated attack strategy	$M = 5$ $t_f = 0.5s$ $T(t) = \sqrt{10}, t \in [0, t_f]$
Optimal attack strategy	$M = 5$

Figure 2 shows the results of the system states under different attacks. It can be seen from Fig. 2(a) that the optimal attack strategy can achieve better attack effect and cause more loss than the concentrated attack strategy. In Fig. 2(b), adopting a concentrated attack may significantly increase the residual, which makes the attack easier to be detected, while under the optimal attack, the residual changes more gradually and the maximum value is also reduced.



(a)



(b)

Fig. 2. The optimal dynamic attack can achieve a better attack effect and reduce the residual compared to the traditional concentrated attack: (a) the attack effect; (b) the norm of residual between measurement and estimate.

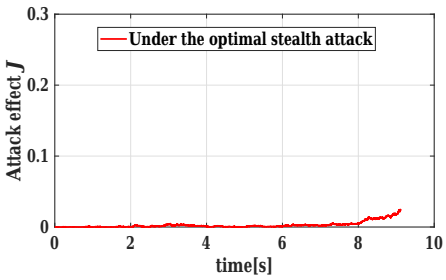
However, the logic of attack cannot be fully described by the figure. It should be indicated that the purpose of the optimal attack strategy is to enhance the impact of the attack, and it is not oriented towards reducing the residual, although it has a lower residual in Fig. 2. The reduction in residual is mainly due to the longer period of sustained attack. From this

perspective, the optimal attack is still successful, but it can also be further optimized to limit the attack magnitude in the design.

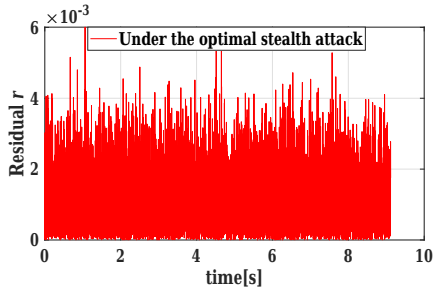
B. The Optimal Stealth False Data Injection Attack

Besides, the optimal attack strategy proposed in this paper does not conflict with the classic stealth false data injection attacks, so they can be used simultaneously, that is to choose a appropriate attack direction $D = Hc,\ \forall c \in \mathbb{R}^n$ [20], thereby greatly increasing the threat. That is the energy based optimal dynamic stealth false data injection attack.

In this case, the attack direction is selected as $D = [0\ 0\ 1\ 0]^T$. This optimal stealth attack produces much fewer residuals as shown in Fig. 3, however, the attack effect is also decreasing sharply in this microgrid. Therefore, to better attack the grid, more energies are still required.



(a)



(b)

Fig. 3. The optimal stealth attack causes fewer residuals: (a) the attack effect; (b) the norm of residual between measurement and estimate.

V. Conclusion

This paper analyzes the utility and advantages of continuous false data injection attacks, and then considering resource constraints, proposes an energy based optimal dynamic stealth false data injection attack strategy. With this method, the attacker can allocate and utilize resources more efficiently to cause greater harm to the power system, while it can bypass the attack detection more easily and improve fault tolerance of the attack.

In the future work, we would like to take the capability and the tolerance for abnormalities of detection methods into consideration. To extend our results, more constraints in practice will be added into the problem, so as to design a more general dynamic optimal attack strategy. Most importantly, we also plan to investigate the possibility of developing special detection techniques to defend against false data injection attacks.

References

[1] U.S. Energy Information Administration Office of Energy Analysis, (2020). *Annual Energy Outlook 2020 with projections to 2050*[Online]. Available: https://www.eia.gov/outlooks/aeo/pdf/AEO2020%20Full%20Report.pdf.

[2] F. Rahimi and A. Ipakchi, "Demand response as a market resource under the smart grid paradigm," *IEEE Transactions on Smart Grid*, vol. 1, no. 1, pp. 82-88, 2010.

[3] G. Lu, D. De, and W. Song, "SmartGridLab: a laboratory-based smart grid testbed," in *Proceedings of the First IEEE International Conference on Smart Grid Communications*, Gaithersburg, USA, 2010, pp. 143-148.

[4] P. Braun, L. Grüne, C. M. Kellett, S. R. Weller, and K. Worthmann, "A distributed optimization algorithm for the predictive control of smart grids," *IEEE Transactions on Automatic Control*, vol. 61, no. 12, pp. 3898-3911, 2016

[5] M. Jin, J. Lavaei, and K. H. Johansson, "Power grid AC-based state estimation: vulnerability analysis against cyber attacks," *IEEE Transactions on Automatic Control*, vol. 64, no. 5, pp. 1784-1799, 2019.

[6] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on the smart grid," *IEEE Transactions on Smart Grid*, vol. 2, no. 4, pp. 645-658, 2011.

[7] A. Arefi and M. R. Haghifam, "State Estimation in Smart Power Grids," in *Smart Power Grids*, A. Keyhani and M. Marwali, Eds. Berlin: Heidelberg, 2012.

[8] 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, 2013.

[9] H. Yi, M. Esmalifalak, H. Nguyen, R. Zheng, Z. Han, H. Li, and L. Song, "Bad data injection in smart grid: attack and defense mechanisms," *IEEE Communications Magazine*, vol. 51, pp. 27-33, 2013.

[10] Y. Liu, M. K. Reiter, and P. Ning, "False data injection attacks against state estimation in electric power grids," in *Proceedings of 16th ACM Conference on Computer and Communications Security*, Gaithersburg, USA, Nov. 2009, pp. 21-30.

[11] X. Yang, J. Lin, W. Yu, P. Moulema, X. Fu, and W. Zhao, "A novel en-route filtering scheme against false data injection attacks in cyber-physical networked systems," *IEEE Transactions on Computers*, vol. 61, no. 1, pp. 4C18, 2015.

[12] R. Deng and H. Liang, "False data injection attacks with limited susceptance information and new countermeasures in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 3, pp. 1619-1628, 2019.

[13] Q. Wang, W. Tai, Y. Tang, M. Ni, and S. You, "A two-layer game theoretical attack-defense model for a false data injection attack against power systems," *International Journal of Electrical Power & Energy Systems*, vol. 104, pp. 169-177, 2019.

[14] P. Srikantha and D. Kundur, "A DER attack-mitigation differential game for smart grid security analysis," *IEEE Transactions on Smart Grid*, vol. 7, no. 3, pp. 1476-1485, 2016.

[15] Q. Yang, J. Yang, W. Yu, D. An, N. Zhang, and W. Zhao, "On false data-injection attacks against power system state estimation: modeling and countermeasures," *IEEE Transactions on Parallel and Distributed Systems*, vol. 25, no. 3, pp. 717-729, 2014.

[16] A. Farraj, E. Hammad, A. A. Daoud, and D. Kundur, "A game-theoretic analysis of cyber switching attacks and mitigation in smart grid systems," *IEEE Transactions on Smart Grid*, vol. 7, no. 4, pp. 1846-1855, 2016.

[17] S. Sridhar and G. Manimaran, "Data integrity attack and its impacts on voltage control loop in power grid," in *Proceedings of IEEE Power & Energy Society General Meeting*, San Diego, USA, 2011, pp. 1-6.

[18] IEEE PES AMPS DSAS Test Feeder Working Group, Available: https://site.ieee.org/pes-testfeeders/.

[19] H. Li, L. Lai, and H. V. Poor, "Multicast routing for decentralized control of cyber physical systems with an application in smart grid," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 6, pp.1097-1107, 2012.

[20] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," *ACM Transactions on Information and System Security*, vol. 14, no. 1, pp. 13, 2011.