Vulnerability Analysis of Large-Scale Dynamical Networks to Coordinated Attacks

Sai Pushpak, Amit Diwadkar, Makan Fardad, and Umesh Vaidya

Abstract— **We study the vulnerability of large-scale linear dynamical networks to coordinated attacks. We consider scenarios in which an attacker can tamper with the links connecting the network components and can also manipulate input injections at the nodes. When these two types of attacks take place simultaneously, the attack is referred to as a coordinated attack. We assume that network links are attacked with a certain probability and that malicious data is injected at the input ports. We employ Markov jump linear systems to model link-based attacks and the system input matrix to model data injection attacks. System theoretic vulnerability metrics developed in earlier work are used to analyze network vulnerability to coordinated attacks. These measures of vulnerability allow us to characterize the impact of coordinated attacks and the difficulty associated with detecting them. Finally, we analyze the vulnerability of coordinated attacks on the New England 39 bus power network.**

I. Introduction

Securing critical infrastructure against cyber attacks is a problem of national security interest. As technological developments make attacks more sophisticated, it is imperative to develop systematic methods to understand the vulnerability of systems to attacks, and to develop appropriate mitigation strategies. Understanding the vulnerabilities of a network is an important step in the design of mitigation strategies. In this paper, we demonstrate vulnerability of the network to coordinated attacks arising in the form of simultaneous denial of service (DoS) and data integrity attacks [1].

For large-scale networks, link-based attacks caused by the removal of links or by jamming communication over the link can be understood as denial of service. Similarly, a data integrity attack can be understood as a node-based attack where malicious data is injected at an input node. While the existing literature focuses on considering one of these two types of attacks, in this paper we consider the scenario in which both link-based and node-based attacks occur simultaneously and in a coordinated fashion. We present preliminary results on the identification of the most impactful and vulnerable node-link pairs. While an impactful attack is defined to be one that causes maximum performance degradation or stability violation in the network, the most vulnerable attack is one that is not only impactful but also difficult to detect. We use system theoretic vulnerability metrics developed in [2] for the identification of worst-case attacks. The ultimate goal of this preliminary study is to develop an optimization-based framework for the identification of such coordinated attacks in large-scale dynamical networks. Uncovering the spatial coordination of these two types of attack will help the understanding of network vulnerabilities and aid the design of mitigation strategies.

Several studies on cyber security have been reported in the literature. Stealthy false-data attacks on state estimators has been studied in [3], where the authors define security indices that quantify the amount of effort required to attack without being detected. Static and dynamic approaches to identifying cyber attacks using system theoretic tools, and the fundamental limitations of such approaches, are given in [4]. A detailed study of securing the transmission network from cyber attacks through the use of wide area monitoring systems, such as phasor measurement units (PMU's), is given in [5]. The authors in [6] identify the role of state estimation in power systems and study stealth attacks on them. They propose algorithms that give the placement of encryption devices to increase the system's security. An optimization-based framework for making state estimators in SCADA networks resilient to stealth attacks is discussed in [7]. Using the tools from systems theory, the authors in [2] formulate optimization-based strategies for the mitigation of vulnerabilities to node-based cyber attacks.

We use techniques from Markov jump linear systems (MJLS) to model stochastic attacks on network links. The link is assumed to fail/removed (off) by the attacker with a certain probability and is restored back in operation (on) with a certain probability. With a single link under attack, the Markov chain is defined over two (on & off) states. Similarly the data integrity attack, or the node-based attack, is modeled by affecting the system input matrix. We apply the system theoretic notions of controllability and observability to MJLS for the identification of the most impactful attacks and those that maximally exploit the system's vulnerabilities. The relative controllability and observability of different directions in state space is used to characterize the impact and the difficulty of detecting an attack. To provide additional insight, we present computational results for the New England 39 bus power system network. We identify the most impactful and vulnerable link-node pairs that, when attacked, inflict the most damage upon the network.

II. Cyber-Physical Attack Model

We propose a Markov jump linear system (MJLS) model for modeling coordinated attacks in dynamical networks. The

Financial support from National Science Foundation grants CNS-1329885, CNS-1329915 are gratefully acknowledged. S. Pushpak, A. Diwadkar and U. Vaidya are with the Department of Electrical & Computer Engineering, Iowa State University, Ames, IA 50011. M. Fardad is with the Department of Electrical Engineering and Computer Science, Syracuse University, Syracuse, NY 13244. E-mails: saipushpakn@gmail.com, amitdiwadkar@gmail.com, makan@syr.edu, ugvaidya@iastate.edu.

MJLS is described by

$$\begin{aligned} x(k+1) &= A_{\theta(k)}x(k) + Bu(k) \\ y(k) &= Cx(k), \end{aligned} \tag{1}$$

where $x(k) \in \mathbb{R}^n$, $y(k) \in \mathbb{R}^p$, and $u(k) \in \mathbb{R}^q$ denote respectively the network's state, output, and input. $\theta(k)$ is the Markov state and is assumed to take only finitely many values, $\theta(k) \in \{1, \ldots, m\}$. The transition probabilities between the Markov states is given by transition probability matrix $[P]_{ij} = p_{ij}$ for $i, j = 1, \ldots, m$,

$$\text{Prob}\{\theta(k) = j \mid \theta(k-1) = i\} = p_{ij},$$

for all k. Note that the transition probability matrix is row stochastic and hence Markov.

Several forms of attacks are studied in the cyber-physical systems literature, such as denial of service, bad data injection, replay attacks, covert or stealth deception, and link failures [1], [5]. In this paper, we consider coordinated attacks that arise in the form of bad data injection and changes in the structural properties of the network. From a modeling perspective, bad data injection affects the system in the form of additive perturbation, whereas an attack on the system's structural properties multiplies the state. In particular, the additive input $u(k)$ can be used to model bad data injection or changes in set-points for the system, such as changes in active and reactive power settings of generators in power networks. The MJLS is used to model attacks on the structural properties of the network, and is general enough to capture attacks such as denial of service or link removals. Links between subsystems may model physical interconnections or communication pathways. For example, a link may be a physical transmission line in a power network or a communication line in wide area control. The Markov property of the chain itself can be used to model coordinated attacks on different links of the network. In the following example, we explain how the MJLS can be used to model link failure attacks on a network.

Example 1: Consider the case where a single link in a network is subjected to attacks. Let the network with no links removed be modeled by the matrix A_1, and let the matrix A_2 model the network configuration after the removal of the mentioned link. We thus have $\theta(k) \in \{1, 2\}$. The transition probability matrix in this case will be a 2×2 row stochastic matrix of the form

$$P = \begin{bmatrix} p_{11} & p_{12} \\ p_{21} & p_{22} \end{bmatrix}$$

where $p_{12} = 1 - p_{11}$ and $p_{21} = 1 - p_{22}$. Here, p_{12} captures the probability of the link being attacked at any time instant assuming it is intact or secure at the previous time instant. Similarly, p_{21} captures the probability of the link being restored to its nominal state once it fails or is subjected to an attack. Simultaneous attacks on multiple links of the network can be modeled using Markov chains with more than two states.

One of the main challenges in attack modeling using the proposed MJLS framework is that of determining the Markov transition probabilities p_{ij}. Historical data from network attacks and intrusions can be used in evaluating these transition probabilities [8]. Studies have found that the nature of attacks on a network follows a Poisson process with exponential distribution [8]. Furthermore, simulation-based methods, such as stochastic petri nets in the context of cyber attack, can also be employed to determine transition probabilities [9], [10]. The rate of attack is used to model the transition times in stochastic Petri nets and they are solved [11] to obtain the transition probabilities.

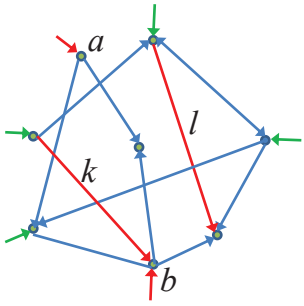

Fig. 1. Coordinated attack on input nodes and links (marked in red) of network.

As shown in Fig. 1, we assume that the network is subjected to coordinated attacks on both its nodes and links. Each node in the network corresponds to a dynamical system with inputs and outputs, and interacts with other subsystems over the network. We assume that the attacker can inject malicious data through input ports and can also remove links connecting different nodes. For example, in Fig. 1 malicious inputs are assumed to be injected at nodes a and b and the links l and k are subjected to attacks; malicious inputs are modeled by $u(k)$ and MJLS model is used to model the link failure attacks in (1).

III. Vulnerability Analysis for Coordinated Attack

In this section, we present a novel metric based on notions from system theory to analyze the vulnerability of networks to coordinated attacks. The basic idea for the metric is adopted from [2]. The vulnerability metric proposed in [2] was developed for linear time invariant (LTI) system and it captures both the impact of an attack and the difficulty of detecting it. It was shown that while the impact of an attack is captured by the controllability gramian, the difficulty of detecting it is captured by the observability gramian. Information from these two gramians was combined to define the vulnerability measure for dynamical networks. The objective of this section is to generalize this measure for the analysis of coordinated attacks in the context of MJLS (1). To achieve this, we need to extend the definitions of controllability and observability gramians to MJLS. Controllability and observability gramians for MJLS are well-defined only under the assumption of stability of the MJLS. Since an MJLS is a stochastic dynamical system, we use following definition of mean square exponential stability [12], [13].

Definition 2: A Markov jump linear system

$$x(k+1) = A_{\theta(k)}x(k)$$

with Markov state $\theta(k) \in \{1, \ldots, m\}$ and transition probability matrix P is said to be mean square exponentially stable if there exist a positive constant $\beta < 1$ such that for every initial condition $x(0)$ we have

$$E_{\theta_0^{k-1}}[x(k)^\top x(k)] \leq \beta^k x(0)^\top x(0). \tag{2}$$

Here, θ_0^{k-1} stands for the sequence $\{\theta(0), \ldots, \theta(k-1)\}$.
Assumption 3: We assume that the MJLS (1) is mean square exponentially stable as given by Definition 2.
The conditions for mean square exponential stability of any MJLS are given in [12]. Conditions to check controllability and observability for Markovian systems similar to LTI systems have been discussed in [14], [15], [16]. In this paper, we consider controllability and observability gramians for MJLS as given in [12].

A. Controllability and observability gramians for MJLS

Definition 4: The controllability gramian for the j^{th} Markov state is given by

$$X_c^j = E\left[\sum_{k=-\infty}^{-1} \mathcal{A}\left(\theta_{k+1}^{-1}\right) BB^\top \mathcal{A}\left(\theta_{k+1}^{-1}\right)^\top\right],\ \theta(0) = j, \tag{3}$$

where

$$\mathcal{A}\left(\theta_{k+1}^{-1}\right) := \prod_{l=k+1}^{-1} A_{\theta(l)} = A_{\theta(-1)}A_{\theta(-2)}\cdots A_{\theta(k+1)},$$

and $\mathcal{A}(\theta_0^{-1}) := I$, I being the identity matrix [12]. The collection of controllability gramians X_c^j for $j = 1, \ldots, m$ corresponding to each Markov state satisfy

$$X_c^j = \sum_{i=1}^{m} p_{ij}\left(BB^\top + A_i X_c^i A_i^\top\right).$$

Let x_0^j be the state of system (1) at time $k = 0$ and residing in the j^{th} Markov state. Suppose the system was driven to x_0^j from $k = -\infty$ with the initial condition $x(-\infty) = 0$, by the control sequence $\{u(k)\}_{k=-\infty}^{-1}$. Then the expected value of the system state x_0^j is given by

$$\bar{x}_0^j = E_{\theta_{-\infty}^{-1}}\left[\sum_{k=-\infty}^{-1} \mathcal{A}(\theta_{k+1}^{-1})Bu(k)\right]. \tag{4}$$

Then we have the following lemma.
Lemma 5: The control sequence $\{u(k)\}_{k=-\infty}^{-1}$, with mean square energy $E_{\theta_{-\infty}^{-1}}\left[\sum_{k=-\infty}^{-1} u(k)^\top u(k)\right] = 1$, that drives the system (1) to $\bar{x}_0^j$ with minimum mean square input energy, is given by $u(k) = B\mathcal{A}\left(\theta_{k+1}^{-1}\right)^\top X_c^{-1}\bar{x}_0^j$. Furthermore, the mean value $\bar{x}_0^j$ can then be expressed in terms of the controllability gramian as

$$\bar{x}_0^j \in \left\{X_c^{j\frac{1}{2}} x_c \mid x_c \in \mathbb{R}^n,\ \|x_c\|_2 = 1\right\}, \tag{5}$$

with energy of the mean state $\bar{x}_0^j$ given by $\|\bar{x}_0^j\|_2^2 = x_c^\top X_c^j x_c$.

Proof: Due to the assumption of mean square stability, the controllability gramian exists and is positive definite [12]. Choose the control input as

$$u(k) = B^\top \mathcal{A}(\theta_{k+1}^{-1})^\top X_c^{j^{-1}} \bar{x}_0^j. \tag{6}$$

Then the expected value of the input energy is,

$$\begin{aligned}
&E\left[\textstyle\sum_{k=-\infty}^{-1} u(k)^\top u(k)\right] \\
&= E\left[\textstyle\sum_{k=-\infty}^{-1} \bar{x}_0^{j^\top} X_c^{j-1}\mathcal{A}(\theta_{k+1}^{-1})BB^\top\mathcal{A}(\theta_{k+1}^{-1})^\top X_c^{j^{-1}}\bar{x}_0^j\right] \\
&= \bar{x}_0^{j^\top} X_c^{j^{-1}} X_c^j X_c^{j^{-1}} \bar{x}_0^j \\
&= \bar{x}_0^{j^\top} X_c^{j^{-1}} \bar{x}_0^j \\
&= x_c^\top x_c,
\end{aligned}$$

where $\bar{x}_0^j = X_c^{j\frac{1}{2}} x_c$. Consider the expected input energy to be bounded, $E\left[\sum_{k=-\infty}^{-1} u(k)^\top u(k)\right] = 1$, then we have $||x_c||_2^2 = 1$. Applying the control (6), we have

$$\begin{aligned}
E\left[\sum_{k=-\infty}^{-1} \mathcal{A}(\theta_{k+1}^{-1})Bu(k)\right] &= X_c^j X_c^{j^{-1}} \bar{x}_0^j \\
&= \bar{x}_0^j.
\end{aligned}$$

The control chosen can indeed be shown to have minimum mean square energy along similar lines to that in deterministic LTI systems [17]. Thus, given finite input energy, the final reachable mean states can be charecterized in terms of the controllability gramian and hence (5) can be satisfied. ■
We thus define the controllability ellipsoid at the j^{th} Markov state to be

$$\mathcal{E}_c^j = \left\{X_c^{j\frac{1}{2}} x_c \mid x_c \in \mathbb{R}^n,\ \|x_c\|_2 = 1\right\}.$$

The observability gramian for the i^{th} Markov state is defined as follows.
Definition 6: The observability gramian at the i^{th} Markov state is given by

$$X_o^i = E\left[\sum_{k=0}^{\infty} \mathcal{A}\left(\theta_0^{k-1}\right)^\top C^\top C\mathcal{A}\left(\theta_0^{k-1}\right)\right],\ \theta(0) = i, \tag{7}$$

where

$$\mathcal{A}\left(\theta_0^{k-1}\right) := \prod_{l=0}^{k-1} A_{\theta(l)} = A_{\theta(k-1)}A_{\theta(k-2)}\cdots A_{\theta(0)},$$

and $\mathcal{A}(\theta_0^{-1}) := I$, [12]. The set of observability gramians X_o^i for $i = 1, \ldots, m$ satisfy

$$X_o^i = C^\top C + A_i^\top \sum_{j=1}^{m} p_{ij} X_o^j A_i.$$

Let x_o be the state of the system at time $k = 0$ in the i^{th} Markov state i.e., $\theta(0) = i$. Suppose the system is evolved from time $k = 0$, then the output at k^{th} time instance is $y(k) = C\mathcal{A}(\theta_0^{k-1})x_o$ for $\|x_o\|_2 = 1$. Then we have the following lemma.

Lemma 7: Consider the output sequence $\{y(k)\}_{k=0}^{\infty}$. The expected total energy in the output is given by $E_{\theta_0^\infty}\left[\sum_{k=0}^{\infty} y(k)^\top y(k)\right] = x_o^\top X_o^i x_o \triangleq x_0^{i^\top} x_0^i$. Furthermore, the state x_0^i can be expressed in terms of the observability gramian as

$$x_0^i \in \left\{ X_o^{i^{\frac{1}{2}}} x_o \mid x_o \in \mathbb{R}^n,\ \|x_o\|_2 = 1 \right\}.$$

Proof: The proof can be argued by duality based on the proof of Lemma 5. ∎

We thus define the observability ellipsoid at the i^{th} Markov state to be

$$\mathcal{E}_o^i = \left\{ X_o^{i^{\frac{1}{2}}} x_o \mid x_o \in \mathbb{R}^n,\ \|x_o\|_2 = 1 \right\}.$$

The degree of observability of any state x_0 at the i^{th} Markov state can be characterized by ${x_0}^\top X_o^i x_0$ [17], [18]. Both the controllability and observability gramians are well defined under the assumption that the MJLS is mean square exponentially stable.

B. Vulnerability metric

The controllability and observability gramians as defined in the previous section can be used to define the vulnerability of a dynamical network to coordinated attacks. Since the input $u(k)$ models data injection attacks, the impact of the data injection attacks and the link failure attack is captured by the controllability gramian. For a particular j^{th} Markov state the information about the relative degree of damage the malicious input can inflict along different directions in state space is captured by the eigenvectors and eigenvalues of the controllability matrix X_c^j. In particular, the impact of the attack is largest along the direction of the eigenvector corresponding to the maximum eigenvalue. Similarly, the relative degree of observability along different directions in the state space for a particular i^{th} Markov state is captured by the eigenvectors and eigenvalues of the observability gramian X_o^i. The controllability and observability gramians are now combined to define the metric for vulnerability.

An attack is deemed as exploiting vulnerability if it has large impact and at the same time is difficult to observe [2]. Using this idea, we define the vulnerability of any state x at the i^{th} Markov state as

$$V_i(x) = \frac{x^\top X_c^i\, x}{x^\top X_o^i\, x}.$$

Now, since $X_o^i > 0$, we can write $X_o^i = X_o^{i^{\frac{1}{2}}} X_o^{i^{\frac{1}{2}}}$. By choosing $z_i = X_o^{i^{\frac{1}{2}}} x$ and assuming $\|z_i\| = 1$, we have

$$V_i(z_i) = z_i^\top X_v^i z_i,$$

where $X_v^i = X_o^{i^{-\frac{1}{2}}} X_c^i X_o^{i^{-\frac{1}{2}}}$, is the vulnerability matrix at i^{th} Markov state. Identical to the definitions of controllability and observability ellipsoid, which provide the relative degree of controllability and observability of states, we can define a vulnerability ellipsoid as follows.

Definition 8 (Vulnerability ellipsoid): The vulnerability ellipsoid at the i^{th} Markov state is given by

$$\mathcal{E}_v^i = \{ X_c^{i^{\frac{1}{2}}} X_o^{i^{-\frac{1}{2}}} x \mid x \in \mathbb{R}^n,\ \|x\|_2 = 1 \}.$$

Let $\lambda_1 \geq \lambda_2 \ldots \geq \lambda_m$ and $p_1, \ldots, p_m$, be the eigenvalues and eigenvectors of the vulnerability matrix X_v^i. The relative degree of vulnerability in different directions of state-space can be identified using the eigenvalues and eigenvectors of vulnerability ellipsoid. Consider the case when $\lambda_k > \lambda_\ell$, then states aligned with p_k are more vulnerable to attacks than those aligned with p_ℓ. In fact the direction corresponding to maximum (minimum) eigenvalue of X_v^i is the most (least) vulnerable. We reiterate the fact that the vulnerability ellipsoid only provides relative vulnerability of states, not the absolute vulnerability. This necessitates the definition of various measures of vulnerability.

Using the measures of vulnerability defined in [2], we define measures of vulnerability for a given Markov state i as follows

Measures of average vulnerability

$$V_1^i = \text{trace}(X_v^i), \quad V_2^i = \|X_v^i\|_F^2,$$

Measure of worst-case vulnerability

$$V_\infty^i = \lambda_{\max}(X_v^i).$$

Next, we define various measures of vulnerability with respect to the Markov states. We use the term *mean* while referring to Markov states and the term *average* while referring to states in state space. We present here some important measures of vulnerability over the Markov space.

Measures of mean average vulnerability

$$V_1 = \frac{1}{m}\sum_{i=1}^{m} V_1^i = \frac{1}{m}\sum_{i=1}^{m} \text{trace}(X_v^i).$$

$$V_2 = \frac{1}{m}\sum_{i=1}^{m} V_2^i = \frac{1}{m}\sum_{i=1}^{m} \|X_v^i\|_F^2.$$

Measure of worst-case vulnerability

$$V_\infty = \max_i V_\infty^i = \max_i \lambda_{\max}(X_v^i).$$

In a similar way, using the controllability gramian, we can quantify various measures of impact along different directions in the network. Furthermore, we can define other measures of impact, which can be used for various objectives. These may be used along with vulnerability measures to perform threat mitigation, by designing sensor placement through an optimization framework, as shown for deterministic attacks in [2].

In order to inflict maximal damage on the network, the attack must be along the direction of largest vulnerability, that is along the most strongly controllable and weakly observable direction. The impact of such an attack is captured by the vulnerability ellipsoid, and we refer to this type of attack as a *stealth attack*. Similarly, in the case where the system is full state observable, the goal of the attacker could be to maximize the penetration of the malicious input. The impact in this case is completely captured by the controllability ellipsoid and we call this a *penetration attack*. In the ensuing section we provide simulation results for coordinated attacks on the New England 39 bus power network. We analyze the

vulnerability of the network to both the stealth attack and the penetration attack.

IV. Coordinated cyber attacks on a power network

In this section, we analyze the impact of coordinated attacks on the New England 39 bus network. The measuring devices here can be phasor measurement units (PMU's) that are placed at generator or load buses, and can measure frequencies, voltages, angles, currents, etc. As measurement units are placed at various locations within the network for anomaly detection, an attack with high impact requires sufficient penetration while avoiding detection.

Consider the power system model with a constant impedance load. For the purpose of numerical computations, we use the New England 39 bus power system model consisting of 29 load buses and 10 generator buses; numerical data is taken from [19]. The topology of the network is captured by the weighted Laplacian that has susceptance as its weight between the load buses and susceptance as well as transient reactance between the generator-load buses [4]. Consider the simplified structure-preserving power network model [4] consisting of dynamic linearized swing equation discretized with sample time $\Delta = 0.01$,

$$\begin{bmatrix}\delta(k+1)\\ \omega(k+1)\end{bmatrix} = \begin{bmatrix} I & \Delta I \\ -\Delta M^{-1}\mathcal{L} & I - \Delta M^{-1}D\end{bmatrix}\begin{bmatrix}\delta(k)\\ \omega(k)\end{bmatrix} \quad (8)$$

$$+ \begin{bmatrix}\mathbf{0}\\ \Delta F_\omega\end{bmatrix} u(k), \quad (9)$$

$$y(k) = \begin{bmatrix} C_\delta & C_\omega\end{bmatrix} x(k) \quad (10)$$

where M is the inertia matrix, D is the damping matrix of the generator buses, and stiffness $\mathcal{L} = L_{gg} - L_{gl}L_{ll}^{-1}L_{lg}$, where

$$L = \begin{bmatrix} L_{gg} & L_{gl} \\ L_{lg} & L_{ll}\end{bmatrix},$$

is the graph Laplacian matrix of the power system network giving the interconnections between the generator and load buses. In the linearized swing equation model, δ and ω represent the generator rotor angles and frequencies respectively. In the above described model, the load bus voltage angles ϕ have been incorporated into the swing equations by using the algebraic equation connecting load angles ϕ and generator angles δ. In the system of equations described in (8), any deviation of the load bus voltage angles ϕ is captured through the change in the generator rotor angles δ, via an algebraic equation [4].

Given a network interconnection, one can form the corresponding graph Laplacian L, which is then used to construct $\mathcal{L}$ through a Schur complement. Thus, for the Markov jump linear system model, positive probability of attack (removal) of k links in the network leads to 2^k Markov states, each related to a possible combination of "on" or "off" states for every link. For computational experiments we assume the probability of attack on a link to be $p_{12} = 0.8$, and the probability of restoring the link to be $p_{21} = 0.2$, where we have used the notational convention from Example 1.

Mean square exponential stability of the resultant Markov jump linear system is verified by applying Theorem 3.9 [12]. The gramians at each Markov state are obtained by posing them as a convex optimization problem with optimization variables as gramians at each Markov state. These are solved using CVX, a package used along with MATLAB for solving convex problems [20], [21].

To quantify the impact of the penetration and stealth attacks, controllability and vulnerability ellipsoids are computed respectively. Fig. 2 shows the impact of the penetration attack (under full observation) on the network. We assume lower security indices [3] and hence the input data is injected at only one node every time. Observe that most of the network is impacted by the penetrated attack. In other words, the penetration attack spreads to most of the network even in the presence of full observation. The impact is maximum when the malicious data is injected at the generator bus 37 and the generator load line $25 \leftrightarrow 37$ is attacked. The impact of the penetration attack on all the node-link pairs is shown in Fig. 2.

Now, in order to analyze the impact of stealth attack on the network, we assume that the states of generator buses $30, 31, 32, 38$ and 39 are observable. In this case, it turns out that if the malicious data is injected at generator bus 37 and if either of the transmission links $15 \leftrightarrow 16$ or $16 \leftrightarrow 17$ are attacked, then those combinations are more vulnerable. The vulnerability of the network due to stealth attacks is shown in Fig. 3. From Figures 2 and 3, notice that some node-link combinations that have less impact due to the penetration attack have high impact due to the stealth attack. The most vulnerable node-link pairs due to the stealth attack are marked in the one-line diagram of the New England 39 bus network as shown in Fig. 4.

V. Conclusion

We use Markov jump linear systems to model stochastic coordinated cyber attacks on dynamical network. Network vulnerability is defined using the notions of controllability and observability from systems theory. Various measures of vulnerability with respect to Markov states are defined. Denial of service and data integrity attacks are studied using the MJLS model proposed in this paper. Finally, the penetration and stealth capabilities of the coordinated (denial of service and data integrity) attacks on the New England 39 bus system are studied and relevant observations are discussed. The notion of vulnerability and the nature of coordinated attacks studied in this paper can be used in future work to develop mitigation strategies, in particular to understand the problem of PMU-based sensor placement in power networks. An optimization framework can be set up to mitigate the impact of an attack as shown in [2]. We reserve the idea of incorporating stochastic node-based attacks in the MJLS model for future work.

References

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

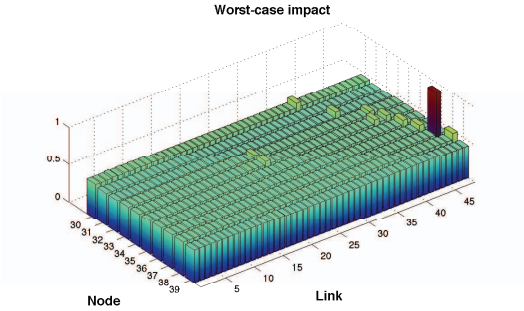

Fig. 2. Impact of the coordinated attack on the node-link pairs.

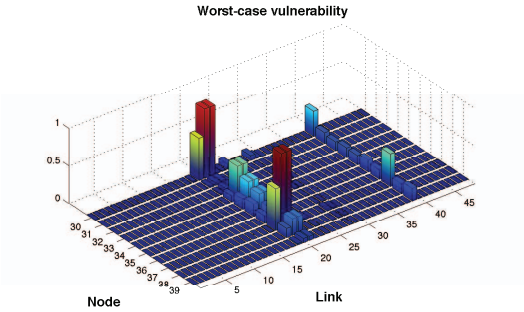

Fig. 3. Vulnerability of the coordinated attack on the node-link pairs.

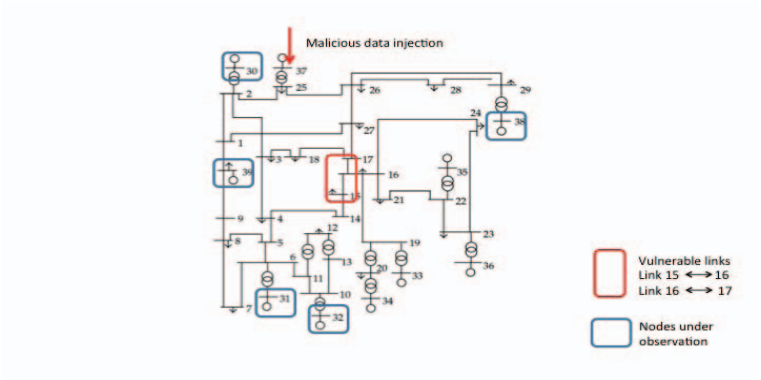

Fig. 4. Most vulnerable node-links and the nodes at observation.

[2] U. Vaidya and M. Fardad, "On optimal sensor placement for mitigation of vulnerabilities to cyber attacks in large-scale networks," in *Proceedings of European Control Conference (ECC)*, July 2013, pp. 3548–3553.

[3] H. Sandberg, A. Teixeira, and K. H. Johansson, "On security indices for state estimators in power networks," in *Preprints of the First Workshop on Secure Control Systems, CPSWEEK 2010, Stockholm, Sweden*, 2010.

[4] F. Pasqualetti, F. Dorfler, and F. Bullo, "Cyber-physical attacks in power networks: Models, fundamental limitations and monitor design," in *Proceedings of IEEE Control and Decision Conference*, Orlando, FL, USA, 2011, pp. 2195–2201.

[5] Y. Deng, S. Shukla, *et al.*, "Vulnerabilities and countermeasures–a survey on the cyber security issues in the transmission subsystem of a smart grid," *Journal of Cyber Security and Mobility*, vol. 1, no. 2, pp. 251–276, 2012.

[6] G. Dán and H. Sandberg, "Stealth attacks and protection schemes for state estimators in power systems," in *Smart Grid Communications (SmartGridComm), First IEEE International Conference on*. IEEE, 2010, pp. 214–219.

[7] A. Teixeira, G. Dán, H. Sandberg, and K. H. Johansson, "A cyber security study of a scada energy management system: Stealthy deception attacks on the state estimator," *arXiv preprint arXiv:1011.1828*, 2010.

[8] E. Jonsson and T. Olovsson, "A quantitative model of the security intrusion process based on attacker behavior," *Software Engineering, IEEE Transactions on*, vol. 23, no. 4, pp. 235–245, 1997.

[9] M. A. Marsan, "Stochastic petri nets: an elementary introduction," in *Advances in Petri Nets*. Springer, 1990, pp. 1–29.

[10] H. Choi, V. G. Kulkarni, and K. S. Trivedi, "Transient analysis of deterministic and stochastic petri nets," in *Application and Theory of Petri Nets*. Springer, 1993, pp. 166–185.

[11] S. Pudar, G. Manimaran, and C.-C. Liu, "Penet: A practical method and tool for integrated modeling of security attacks and countermeasures," *Computers & Security*, vol. 28, no. 8, pp. 754–771, 2009.

[12] O. L. do Valle Costa, M. D. Fragoso, and R. P. Marques, *Discrete-time Markov jump linear systems*. Springer, 2006.

[13] G. Kotsalis, A. Megretski, and M. Dahleh, "Model reduction of discrete-time markov jump linear systems," in *Proceedings of American Control Conference*, June 2006.

[14] E. F. Costa and J. B. Do Val, "On the detectability and observability of discrete-time markov jump linear systems," *Systems & Control Letters*, vol. 44, no. 2, pp. 135–145, 2001.

[15] E. Elhamifar, M. Petreczky, and R. Vidal, "Rank tests for the observability of discrete-time jump linear systems with inputs," in *American Control Conference*. IEEE, 2009, pp. 3025–3032.

[16] A. Czornik and A. Swierniak, "On controllability with respect to the expectation of discrete time jump linear systems," *Journal of the Franklin Institute*, vol. 338, no. 4, pp. 443–453, 2001.

[17] G. E. Dullerud and F. Paganini, *A course in robust control theory*. Springer New York, 2000, vol. 6.

[18] U. Vaidya, "Observability gramian for nonlinear systems," in *Proceedings of 46th IEEE Control and Decision Conference*. IEEE, 2007, pp. 3357–3362.

[19] R. D. Zimmerman and C. E. Murillo-Sanchez, 2001. [Online]. Available: http://www.pserc.cornell.edu/tcc/

[20] M. Grant, S. Boyd, and Y. Ye, "CVX: Matlab software for disciplined convex programming," 2008.

[21] ——, "CVX: Matlab software for disciplined convex programming, version 2.0 beta," *Recent Advances in Learning and Control*, pp. 95–110, 2012.