MITSUBISHI ELECTRIC RESEARCH LABORATORIES
http://www.merl.com

Dynamic State Recovery for Cyber-Physical Systems under Switching Location Attacks

Liu, C.; Wu, J.; Long, C.; Wang, Y.

TR2016-104 June 2016

Abstract

Malicious data attacks have raised widespread concerns on data integrity and security of cyber-physical systems. This paper discusses a state recovery problem, where the underlying cyber-physical system is subject to switching location attacks. Compared with the fix location attack, the switching location attack changes the attack locations at a constant/variable frequency. This paper develops nonzero sub-row and nonzero entry sparsity models to characterize the switching location attacks. Moreover, state recovery constraints are deduced for different attack modes, which prove the higher efficient state recovery compared with the fix location and static decoders. According to the different sparsity models, l1=l2 and l1 decoders are designed, respectively, which can recover the initial state accurately within relaxation conditions. Numerical simulations in a randomly chosen system and a 14-bus electric power system show the proposed dynamic decoders can provide effective system resilience under switching location attacks.

IEEE Transactions on Control of Networked Systems

Dynamic State Recovery for Cyber-Physical Systems under Switching Location Attacks

Chenshen Liu, *Student Member, IEEE,* Jing Wu, *Member, IEEE,* Chengnian Long, *Member, IEEE,* Yebin Wang, *Member, IEEE*

***Abstract*—Malicious data attacks have raised widespread concerns on data integrity and security of cyber-physical systems. In this paper, we discuss a state recovery problem, where the underlying cyber-physical system is subject to attacks at different locations with constant switching frequency. Nonzero sub-row and nonzero entries sparsity models are presented based on corresponding switching frequency, which is the fundamental difference between switching location and other attacks. Moreover, state recovery constraints are deduced based on corresponding attack modes, which further proves the higher efficiency compared with fix location and static decoders. According to the different sparsity models, l_1/l_2 and l_1 decoders are designed, respectively, which can recover the initial state accurately within relaxation conditions. Numerical simulations in a randomly chosen system and a 14-bus electric power system show our proposed dynamic decoder can provide an effective system resilience under switching location attacks.**

***Index Terms*—Dynamic State Recovery, Switch Location Attacks, Block Sparsity, Dynamic Decoder**

I. Introduction

INTEGRATING the computation and communication techniques into control systems, Cyber-Physical Systems (CPSs) widely exist in critical infrastructure such as electrical, water, chemical, oil and gas, etc. Even though CPSs can greatly improve the stability and efficiency, the tight coupling between IT systems and control systems brings new security challenges. For example, authentication, encryption and integrity weakness checks in communication protocols [1] make CPSs vulnerable to malicious data attacks.

Utilizing the vulnerabilities of the integrated IT systems, attackers can easily implement malicious data attacks. In order to circumvent security methods, such as dynamic security policies [2] and current fix location based state recovery [3], attackers can change the attack set continuously. As shown in Fig. 1, utilizing the authentication weakness [4] and the *restart communications option* vulnerability [5] in Modbus/TCP protocols, attackers can implement the IP spoofing attack [6] (the blue arrows) with a denial of service (DoS) attack (the red arrows) in SCADA systems [7], which can successfully inject malicious packets. By altering the target addresses, attackers can easily change the target from RTU-1 (the solid line) to RTU-n (the dash line). Since vast of false response packets must be injected for malicious data injection in SCADA systems using Polling techniques [7], the compromised RTUs with limited packet generation capacity and limited communication bandwidth [8] can attack only part of the devices in the IP spoofing & DoS attack, which makes the attack sparse. In this paper, we assume that attackers can implement sparse switching location attacks, i.e., attackers can compromise any subset of sensors with the constraint of amount and change the set of attacked sensors with a constant/variable frequency, limited by the system facilities and possible attack techniques.

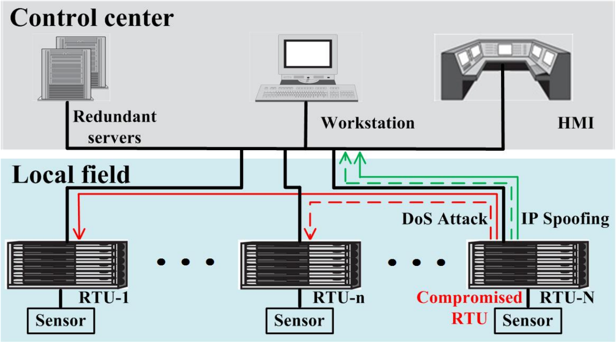

Fig. 1. An IP spoofing & DoS attack example.

In literature, malicious data attacks have been extensively studied recently. For example, *Liu et al.* [9] and *Mo et al.* [10] discussed the feasibility of the malicious data attacks in static and dynamic systems, respectively. To resist such attacks in static system, measurement low-rank property based attack identification and miss data recovery methods were presented in [11] and [12], respectively, where the sparsity of measurement is utilized. Using the sparsity of attack vectors (or system failure), i.e., the nonzero entries in attack vector is sparse, a static decoder was designed to recover the system state [13], where only the current compromised measurements are used. Based on both the measurement low-rank property and attack sparsity, a false data detection mechanism was designed by solving a matrix separation problem [14]. To decrease the measurement amount in sparse state recovery, a model-based compressive sensing method, such as block-sparsity, was presented in [15] and [16], which provide concrete guidelines on model-based recovery algorithm design with provable performance guarantee. However, the static sparsity based secure mechanisms given above fail to use the system dynamics, which will increase the resilience of the system. Based on

This work was supported by the National Nature Science Foundation of China (61473184).

Chensheng Liu, Jing Wu, and Chengnian Long are with the Department of Automation, Shanghai Jiao Tong University, Shanghai, 200240, China. E-mail: longcn@sjtu.edu.cn

Yebin Wang is with Mitsubishi Electric Research Laboratories, Cambridge, MA 02139, USA. E-mail: yebinwang@merl.com

the block-sparsity in static system, [3] and [17] expanded the method into dynamic systems, where fix location decoders can recover the initial state by the compromised measurement sequences. However, the fix location decoder is designed under the assumption that the set of attacked sensors does not change over time [3], i.e., if $K \subset \{1, \cdots, p\}$ is the set of attacked sensors, then for all t, $supp(e^{(t)}) \subset K$, where $supp(e^{(t)})$ is the set of attacked sensors. Aimed to deal with sensor attack scenarios with fixed attacked sensors, the fix location decoder fails to tackle switching location attacks, which brings new challenges in state recovery. First of all, the switches of attack set destroy the original fix location sparsity, which damages the system resilience greatly, especially when the switch frequency is high. Since attackers may switch the attack set in different manners, different sparsity models and recovery methods must be studied, correspondingly.

In this paper, we discuss state recovery in switching location attacks using system dynamics and attack sparsity. As the fundamental motivation, nonzero sub-row and nonzero entries sparsity models are described based on different attack manners, which is the basis of this paper. Corresponding to the different sparsity models, state recovery constraints are deduced, which reflect the system resilience and guarantee the state recovery accuracy. As one of the main contributions, we theoretically proved that the dynamic decoder outperforms the fix location and static decoders in switching location attacks. Two different decoders are designed according to the different sparsity model. With the relaxed conditions, two practical decoders are presented based on the l_0 ones, which can recover the initial state accurately. Finally, numeral simulations show the efficiency of dynamic decoder in switching location attacks.

The remainder of this paper is organized as follows. In Section II, the notation and attack sparsity models are presented. In Section III, the state recovery condition and the theoretical analysis of the dynamic decoder are given. Then the dynamic decoders for two sparsity models are designed in Section IV. Numerical simulations and conclusion are made in Section V and VI, respectively.

II. Model and Notation

A. Notation

In the rest of this paper, we will use the notations defined below. For a vector $x \in R^n$, $supp(x)$ denotes the index set of nonzero elements in x, i.e., $supp(x) = \{i | i \in \{1, \ldots, n\}, x_i \neq 0\}$, where x_i is the ith element in x. For a set S, $|S|$ denotes the cardinality of S. Then the l_0 norm of vector x means $\|x\|_{l_0} = |supp(x)|$. Similarly, the l_1 norm of vector x is defined as $\|x\|_{l_1} = \sum_{i \in \{1,\ldots,n\}} |x_i|$.

Suppose that a matrix $E \in R^{p \times T}$ is divided into $k+1$ parts by cutting the matrix in column, we denotes E_i as the ith part of the matrix E, and $(E_i)_j$ as the jth sub-row of the sub-matrix E_i, where $i \in \{0, \cdots, k\}$, $j \in \{1, \cdots, p\}$. For example, the attack matrix, $E_{s,T}(k)$, in (2) (Section II-B) is divided into 2 parts, and E_1 is the first two columns, and E_2 is the last two columns. Denote $\|E\|_{l_0}$ as the sum of the nonzero entries in matrix E. If $K \subset \{1, \ldots, p\}$, K^c denotes the complementary set of K. Moreover, we denote Q as the sum of the nonzero sub-rows/entries in all the $k+1$ sub-matrices, q as the attack amount limitation, i.e., the number of attacked sensors are no more than q at each time. Throughout the paper, the variable with the superscript $'$ is defined for comparison with the one without it. For ease of reading, the nomenclature is given in Table 1.

TABLE I
Nomenclature table.

1	Q	Summation of the nonzero entries/sub-rows.
2	q	Amount of attacked sensors.
3	q_{max}	The largest correctable attack amount.
4	τ	Switching interval in attacks.
5	k	Switch times within T.
6	K_i	The ith attack set.
7	T	Measurement amount in state recovery.
8	Γ	Time set $\Gamma = \{0, \cdots, T-1\}$.
9	E	Attack matrix.
10	$x^{(0)}$	Initial state of the system.
11	$y^{(t)}$	Compromised measurement at time t.
12	$e^{(t)}$	Attack vector at time t.
13	z	Nonzero initial state.

B. System Model

Considering the following linear dynamic system,

$$\begin{aligned} x^{(t+1)} &= Ax^{(t)} \\ y^{(t)} &= Cx^{(t)} + e^{(t)} \end{aligned} \tag{1}$$

where $x^{(t)} \in R^n$ is the state of the system at time $t \in N$, $y^{(t)} \in R^p$ is the measurement at time t. The matrices A and C have appropriate dimensions and the vector $e^{(t)} \in R^p$ is the attack vector injected by attackers at time t. Since $e^{(t)}$ is injected by malicious attackers, $e^{(t)}$ will not be assumed to follow any particular model, and if the jth sensor at time t is attacked, then $e_j^{(t)}$ is arbitrary, otherwise $e_j^{(t)} = 0$.

In the rest of this paper, we divide switching location attacks into two cases: i) the switching frequency is constant and known to system operators; ii) the switching frequency is constant but unknown or it is variable.

1) Nonzero Sub-row Sparsity: In case i), attackers change the set of attacked sensors with a constant switching frequency, which is known to system operators. Denote τ as the switching interval (the reciprocal of the switching frequency) in attacks. For simplicity, we assume the attack starts at $t = 0$, and the attacks at other time can be analyzed similarly. Given attack vectors $e^{(t)}$, $t \in \Gamma = \{0, \cdots, T-1\}$, and switched times k, the attack vectors satisfy $supp(e^t) \subseteq K_i \subset \{1, \cdots, p\}$, $t \in \{i\tau, \cdots, (i+1)\tau - 1\}$, where K_i as the ith attack set. The possible attack vector set in Γ with attack amount limitation q and switched times k can be defined as

$$\begin{aligned} E_{q,T}(k) = \{(e^{(0)}, \cdots, e^{(T-1)}) | supp(e^{(t)}) \subseteq K_i, |K_i| = q, \\ t \in \{i\tau, \cdots, (i+1)\tau - 1\}, i \in \{0, \cdots, k\}\}. \end{aligned}$$

Denote $E = \{e^{(0)}, \cdots, e^{(T-1)}\}$ as attack matrix within T. Suppose $T = 4$ and $\tau = 2$, the attack matrices in fix location attacks [3] and switching location attacks, namely, $E_{f,T}$ and $E_{s,T}(k)$, can be expressed in the following forms:

$$E_{f,T}=\begin{bmatrix} \times & \times & \times & \times \\ \times & \times & \times & \times \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{bmatrix}; E_{s,T}(k)=\begin{bmatrix} \times & \times & 0 & 0 \\ \times & \times & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & \times & \times \\ 0 & 0 & \times & \times \end{bmatrix} \tag{2}$$

where the locations with "×" denote the attacked sensor measurements. The rows and columns denote sensor location and the sampling time, respectively. Note that the compromised measurements "×" can be arbitrary value.

Similar to the block sparsity expression in [16], the attack matrices can be expressed in sequence as shown below:

$$E_{f,T} = [\underbrace{\times \ \times \ \times \ \times}_{x_f{}^{[1]}} | \underbrace{\times \ \times \ \times \ \times}_{x_f{}^{[2]}} | \cdots]$$

$$E_{s,T}(k) = [\underbrace{\times \ \times}_{x_s{}^{[1]}} | \underbrace{0 \ 0}_{x_s{}^{[2]}} | \underbrace{\times \ \times}_{x_s{}^{[3]}} | \underbrace{0 \ 0}_{x_s{}^{[4]}} | \cdots],$$

where $x_f^{[l]}$ is the lth row in attack matrix $E_{f,T}$, and $x_s^{[l]}$ is the lth sub-row divided by k switches. Denoting

$$\|E_{s,T}(k)\|_{2,0} = \sum_{l=1}^{(k+1)p} I(\|x_s^{[l]}\|_2 > 0)$$

where $I(\|x_s^{[l]}\|_2 > 0) = 1$ if $\|x_s^{[l]}\|_2 > 0$ and 0 otherwise [16]. The sparsity of switching attack is Q-sparse if $\|E_{s,T}(k)\|_{2,0} \leq Q$. Note that the sparsity in fix location attacks is equivalent to that the amount of attack points sparsity. While in switching location attacks, it means that the amount of nonzero sub-rows is sparse. The number of nonzero sub-rows is determined by the switched times k and the attacked sensor amount q. Note that the discussion above is based on the assumption that the switching frequency is constant and known to system operators. When the switching frequency is variable or is not known to system operators, the nonzero sub-row sparsity model is not suitable.

2) Nonzero Entries Sparsity: In case ii), attackers change the set of attacked sensors with a unknown constant or variable switching frequency. Suppose $e^{(t)} \in R^4$, and denote attack matrix with constant switching interval, $\tau = 2$, as E_1. Denote attack matrix with a variable switching interval sequence, $\tau = 2, 3, 2, \cdots$, as E_2. Since system operators don't know the accurate switching frequency, the incorrect division of sub-matrices may introduce unnecessary nonzero sub-rows into the attack matrix. An example is presented below,

$$E_1=\left[\begin{array}{ccc|ccc|c} \times & \times & 0 & 0 & \times & \times & \ldots \\ \times & \times & 0 & 0 & \times & \times & \ldots \\ 0 & 0 & \times & \times & 0 & 0 & \ldots \\ 0 & 0 & \times & \times & 0 & 0 & \ldots \end{array}\right], E_2=\left[\begin{array}{ccc|ccc|cc} \times & \times & 0 & 0 & 0 & \times & \times & \ldots \\ \times & \times & 0 & 0 & 0 & \times & \times & \ldots \\ 0 & 0 & \times & \times & \times & 0 & 0 & \ldots \\ 0 & 0 & \times & \times & \times & 0 & 0 & \ldots \end{array}\right], \tag{3}$$

where the attack matrices are divided by the incorrect switching interval $\tau = 3$. Obviously, unnecessary nonzero sub-rows are introduced into the nonzero sub-row sparsity model.

For attacks in case ii), we describe the sparsity of attack matrices using the number of nonzero entries of the attack matrix, named nonzero entries sparsity here after. Note that, nonzero entries sparsity model is a special case of nonzero sub-row sparsity model, when the constant switching interval is $\tau = 1$.

Based on the system model (1) and the sparsity model, the state recovery that we consider in this paper is to recover the initial state $x^{(0)}$ of system (1) utilizing the compromised measurements $y^{(0)}, \cdots, y^{(T-1)}$, i.e., design a decoder $D : (R^p)^T \to R^n$, such that $D(y^{(0)}, \cdots, y^{(T-1)}) = x^{(0)}$

As shown in (2), there are 4 nonzero sub-row in $E_{s,T}(k)$ corresponding to the attack amount limitation $q = 2$. However, in the view of fix location attacks, there are $q = 4$ attacked sensors. It means that the recovery method based on fix location attack are not qualified in the case with switching location attacks. In the following, we'll analyze the recovery condition with switching location attacks in details in Section III.

III. State Recovery Analysis

In this section, we will address the state recovery condition of the linear dynamic system in (1) with switching location attacks. Without losing generality, the initial state recovery, $x^{(0)}$, is discussed by utilizing the compromised measurement sequences $y^{(0)}, \cdots, y^{(T-1)}$.

A. State Recovery Condition

By the system dynamics in (1), the measurement can be formulated as the function of initial state $x^{(0)}$.

$$y^{(t)} = CA^t x^{(0)} + e^{(t)}, t \in \Gamma \tag{4}$$

Then the process of state recovery is to search an appropriate initial state $x^{(0)}$ to match the compromised measurements, which can be denoted as $D : (R^p)^T \to R^n$. If the system state can be recovered correctly in switching location attacks with q attacked sensors and k switches after T steps, we say that the system is *q-attack k-switch correctable*. The definition is given as follows.

***Definition* 1.** *The system is q-attack k-switch correctable after T steps, if for any $x^{(0)} \in R^n$ and any attack set sequence $(e^{(0)}, \ldots, e^{(T-1)}) \in E_{q,T}(k)$, there exist a decoder $D : (R^p)^T \to R^n$, such that $D(y^{(0)}, \cdots, y^{(T-1)}) = x^{(0)}$.*

Similar to attack identification in [19], Definition 1 transforms q-attack k-switch correctable into the existence of a decoder, which can reconstruct any initial state correctly. Next we will discuss the existence of such a decoder. In order to facilitate the deduction of the following propositions, we give the negative forms of the existence shown as follows:

***Proposition* 1.** *Let $T \in N\backslash\{0\}$, the followings are equivalent:*

1) *There is* no *decoder to recover the initial state in switching location attacks with q attacked sensors and k switches after T steps;*
2) *There exist $x^{(0)}, x'^{(0)} \in R^n$ with $x^{(0)} \neq x'^{(0)}$, and attack vectors $(e^{(0)}, \cdots, e^{(T-1)}) \in E_{q,T}(k)$, $(e'^{(0)}, \cdots, e'^{(T-1)}) \in E_{q,T}(k)$ such that $\forall t \in \Gamma, CA^t x^{(0)} + e^{(t)} = CA^t x'^{(0)} + e'^{(t)}$.*

Proof: The detail proof can be easily derived based on the proof of the attack identification (*Lemma* 3.2) in [19]. Thus, omitted here. ■

Proposition 1 gives a feasible method in deducing the state recovery condition ensuring the existence of such decoders. Based on compressive sensing theory [20], simply, there can't exist two different states such that the compromised measurement sequence in Γ are same. Then we have a necessary and sufficient condition for the existence of such decoders under switching location attacks in case i).

***Proposition* 2.** *Let $T \in N \backslash \{0\}$, the follows are equivalent:*

1) *There exists a decoder to recover the initial state under any switching location attacks with q attacked sensors and k switches after T steps;*
2) *For all $z \in \mathcal{R}^n \backslash \{0\}$, the system with k switch location attack in Γ satisfies:*

$$\sum_{i=0}^{k} \left| \bigcup_{t=i\tau}^{(i+1)\tau-1} supp(CA^t z) \right| > 2 \cdot (k+1)q;$$

Proof: Since the attack matrix $E_{s,T}(k) \in R^{p \times T}$ is divided into $k+1$ parts, as shown in (2), then a new attack matrix, $E'_{s,T}(k) \in R^{(k+1)p \times \tau}$, can be composed by putting the sub-matrices one on another.

1) → 2): Suppose for the sake of contradiction that there exists $z \in \mathcal{R}^n \backslash \{0\}$ such that $\sum_{i=0}^{k} |\bigcup_{t=i\tau}^{(i+1)\tau-1} supp(CA^t z)| \leq 2 \cdot (k+1)q$. Denote S_i, S'_i as disjoint subset of $\{1, \dots, p\}$ with $|S_i| \leq q$, $|S'_i| \leq q$ for all $i \in \{0, \cdots, k\}$. Suppose for all $i \in \{0, \cdots, k\}$, $|\bigcup_{t=i\tau}^{(i+1)\tau-1} supp(CA^t z)| \leq 2q$, then there exist S_i, S'_i such that $S_i \cup S'_i = \bigcup_{t=i\tau}^{(i+1)\tau-1} supp(CA^t z)$, for all $i \in \{0, \cdots, k\}$. Let $e^{(t)} = CA^t z|_{S_i}$, be the vector obtained from $CA^t z$ by setting all the components outside S_i to 0, where $t \in \{i\tau, \cdots, (i+1)\tau - 1\}$, $i \in \{0, \cdots, k\}$. Similarly let $e'^{(t)} = -CA^t z|_{S'_i}$. Then we have $CA^t z = e^{(t)} - e'^{(t)}$, i.e., for all $t \in \Gamma$, $CA^t z + e'^{(t)} = CA^t \cdot 0 + e^{(t)}$. As $z \neq 0$, it is obvious that there are two different initial state z and 0 ($z \neq 0$), with two attack vectors $(e^{(0)}, \cdots, e^{(T-1)}) \in E_{q,T}(k)$, $(e'^{(0)}, \cdots, e'^{(T-1)}) \in E_{q,T}(k)$ such that $CA^t z + e'^{(t)} = CA^t 0 + e^{(t)}$, i.e., there is no decoder that can correct q attack with k switches after T steps. Above all, 1) does not hold.

2) → 1): Suppose there is no decoder that can correct q attacks with k switches after T steps. It means that there exist two different initial states $x^{(0)}, x'^{(0)} \in R^n, x^{(0)} \neq x'^{(0)}$, and attack vectors $(e^0, \cdots, e^{(T-1)})$, $(e'^0, \cdots, e'^{(T-1)}) \in E_{q,T}(k)$, such that $\forall t \in \Gamma, CA^t x^{(0)} + e^{(t)} = CA^t x'^{(0)} + e'^{(t)}$. Now let $z = x^{(0)} - x'^{(0)} \neq 0$, then we have $CA^t z = e'^{(t)} - e^{(t)}, \forall t \in \Gamma$. Since for $t \in \{i\tau, \cdots, (i+1)\tau - 1\}$, $i \in \{0, \cdots, k\}$, $|S_i| \leq q$, $|S'_i| \leq q$, $|\bigcup_{t=i\tau}^{(i+1)\tau-1} supp(CA^t z)| = |S'_i - S_i| \leq 2q$. Obviously, $\sum_{i=0}^{k} |\bigcup_{t=i\tau}^{(i+1)\tau-1} supp(CA^t z)| \leq 2 \cdot (k+1)q$, 2) does not hold. ■

Actually Proposition 2 can be well understood with the following physical meaning. Suppose that $z \in R^n \backslash \{0\}$ denotes the difference between any two different initial states, and $CA^t z$ is the map from state domain to measurement domain. Then for all $t \in \Gamma$, $CA^t z$ denote the image of state difference, z, in measurement domain. More specifically, the nonzero element in $CA^t z$ means the characteristic of distinguishing the two initial states, and $|supp(CA^t z)|$ denote the number of characteristics in distinguishing the two initial states at time t.

In order to confuse different initial states, attackers must tamper the characteristics in measurement domain for all different states. Due to the limited amount of attacked sensors, for $i \in \{0, \cdots, k\}$, $|S_i| \leq q$, $|S'_i| \leq q$, the maximal number of characteristics being tampered is $2 \cdot (k+1)q$. In order to distinguish the initial states in the worst case, there must be more than $2 \cdot (k+1)q$ characteristics for system (A, C), i.e., $\sum_{i=0}^{k} |\bigcup_{t=i\tau}^{(i+1)\tau-1} supp(CA^t z)| > 2 \cdot (k+1)q$.

As described in Section II-B, nonzero entries sparsity is a special case of nonzero sub-rows sparsity, when the constant switching interval is $\tau = 1$, the necessary and sufficient condition of recovering initial state under switching location attacks in case ii) is a special case of Proposition 2, i.e., for all $z \in R^n \backslash \{0\}$, the system satisfies $\sum_{t=0}^{T-1} |supp(CA^t z)| > 2 \cdot T \cdot q$.

Proposition 2 is deduced based on the assumption that the switching frequency is constant and known to system operators, and attack starts at $t = 0$, i.e., system operators knows the switching time points. If system operators have no idea about the switching frequency and attack starting time, i.e., the condition using fix location decoders [3] under switching location attacks, the recovery condition can be expressed as follows:

***Corollary* 1.** *The initial state $x^{(0)}$ of system (1) can be recovered by decoders based on fix location sparsity model in [3] after T steps under any switching location attacks with q limited attack amount and k switches if and only if for all $z \in R^n \backslash \{0\}$, the following satisfies*

$$\left| \bigcup_{t=0}^{T-1} supp(CA^t z) \right| > 2 \cdot (k+1)q$$

For a given system (A, C), denote q_{max} and q'_{max} as the largest correctable attack amount of switching location attacks corresponding to Proposition 2 and Corollary 1, respectively. Obviously, q'_{max} decrease when the switched times k increase in Γ. Moreover, Since $\sum_{i=0}^{k} |\bigcup_{t=i\tau}^{(i+1)\tau-1} supp(CA^t z)| \geq \left| \bigcup_{t=0}^{T-1} supp(CA^t z) \right|$, the state recovery method using accuracy time point can be more effective than the fix location decoder in switching location attacks, i.e., $q_{max} \geq q'_{max}$. Note that the state recovery condition in [3] is a special case of Proposition 2 and Corollary 1.

Denote M as the measurement matrix consisted of matrix $C, \cdots, CA^{T-1}$ one on another, then M is the system observation matrix when $T = n$. Since for both fix and switching location attacks, the state recovery condition is the sufficient but not necessary condition of the condition that the measurement matrix is column full rank, i.e., $rank(M) = n$. As a simple proof, if $rank(M) < n$, there exists $z \neq 0$ such that $Cz = \cdots = CA^{T-1} z = 0$. It means that the system can correct no attack [3]. Then for a given system and steps T, the largest number of correctable attack can be transferred into the measurement matrix column full rank problem. In detail, by extract the rows corresponding to the attacked sensors, the largest correctable q can be found at the boundary of $rank(M) = n$.

Denote M' as a sub-matrix of measurement matrix M, consisted of rows of matrix M. Let M^c be the rest matrix by extracting the corresponding rows of the attacked sensors from M, and $M'^c = M^c \cap M'$. Then we have $rank(M^c) \geq rank(M'^c)$. It means that for the same attack amount q in switching location attacks, $rank(M^c) \geq rank(M'^c)$, i.e., M can recover no less attack amount than M'. Considering the worst case in switching location attacks, i.e., $\tau = 1$, the efficiency of recovery method based on Proposition 2 and the static decoder in [13], can be analyzed, simply.

***Remark* 1.** *For the dynamic system (1) under switching location attacks with limited attack amount q and $k = T - 1$ switches, decoders in Proposition 2 can recover no less attack than the static decoder.*

B. Recovery Upper Bound and Steps T

As discussed in Section III-A, for a given system (A, C), the recovery upper bound can be transferred into the matrix column full rank problem. Obviously, the problem above is a NP-hard problem, and there is no practical algorithm [18].

In fix location attacks, the largest correctable amount can be reached when $T = n$ based on the Cayley-Hamilton theorem, while for switching location attacks, the result in fix location is not quit suitable here. A simple example is given below.

Suppose there is a structural system as shown below:

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & \times \\ \times & 0 & 0 & 0 & 0 \\ 0 & \times & 0 & 0 & 0 \\ 0 & 0 & \times & 0 & 0 \\ 0 & 0 & 0 & \times & \times \end{bmatrix}, C = \begin{bmatrix} \times & 0 & 0 & 0 & 0 \\ 0 & \times & 0 & 0 & 0 \\ 0 & 0 & \times & 0 & 0 \\ 0 & 0 & 0 & \times & 0 \\ 0 & 0 & 0 & 0 & \times \end{bmatrix};$$

Assume attackers' switch attack set with a constant frequency and the switch interval $\tau = \tau_{min} = 1$. Based on Proposition 2, the recovered attack amount satisfies

$$q < \min_{z} \frac{1}{2(k+1)} \cdot \sum_{t \in \{0,\cdots,T-1\}} |supp(CA^t z)|$$

For the possible structural $z \in \{(\times, 0, 0, 0, 0), \cdots, (\times, \times, \times, \times, \times)\}$, the recovery upper bound for different T shows in the table below:

TABLE II

THE RECOVERY UPPER BOUND FOR DIFFERENT T

$T =$	1	4	8	12	16
$q <$	0.5	0.5	1.125	1.5833	1.8125
$T =$	20	24	28	32	36
$q <$	1.95	2.0417	2.1071	2.1563	2.1944

As shown in the table above, for most z except for special values in the parameter space of the given system, the recovery upper bound does not reach within $T \leq n$, while the recovery upper bound reaches within $T \leq n$ in fix location attacks [3]. The decision of optimal steps T is still a hard problem with the possible constraint such as the acceptable recovery delay determined by the steps T.

IV. Dynamic Decoder Design

In this section, we will propose the design of the q-attack k-switch state recovery method, named dynamic decoder, corresponding to nonzero sub-row and nonzero entries sparsity models under switching location attacks. As shown in Section III, we know that the initial state $x^{(0)}$ can be recovered using the compromised measurement sequence $y^{(0)}, \cdots, y^{(T-1)}$, when the system (A, C) satisfies

$$\sum_{i=1}^{k+1} \left| \bigcup_{t=(i-1)\tau}^{i\tau-1} supp(CA^t z) \right| > 2 \cdot (k+1)q \tag{5}$$

A. State Recovery for Nonzero Sub-row Sparsity Model

For switching location attacks in case i), the sparsity of the attack matrix refers to that the nonzero sub-row, is sparse. It is natural to minimize the summation of nonzero sub-rows in the attack matrix.

Let $E_{s,T}(k)$ be the attack matrix with attack q limited amount and k switches. Denote E_i and Y_i as the attack matrix and the compromised measurement matrix for $t \in \{i\tau, \cdots, (i+1)\tau - 1\}$, as below:

$$\begin{aligned} E_i &= \left[\, e^{i\tau} \;\cdots\; e^{(i+1)\tau-1} \,\right] \in R^{p\times\tau}, \\ Y_i &= \left[\, y^{i\tau} \;\cdots\; y^{(i+1)\tau-1} \,\right] \in R^{p\times\tau}; \end{aligned}$$

Correspondingly, the state measurement matrix $\Phi_i(x)$ can be expressed as follows:

$$\begin{aligned} \Phi_i(x) &= \left[\, CA^{i\tau}x \;\cdots\; CA^{(i+1)\tau-1}x \,\right] \\ &= \left[\, CA^{i\tau} \;\cdots\; CA^{(i+1)\tau-1} \,\right] \cdot blkdiag(x, \cdots, x), \end{aligned}$$

where $\Phi_i(x) \in R^{p\times\tau}$, and $blkdiag(x, \cdots, x) \in R^{n\tau\times\tau}$ is a block diagonal matrix. Then for $t \in \{i\tau, \cdots, (i+1)\tau - 1\}$, the measurement function can be expressed as

$$Y_i = \Phi_i(x) + E_i$$

As defined in Section II-B-1), indicator function $I(\|x_s^{[l]}\|_2 > 0) = 1$ if $\|x_s^{[l]}\|_2 > 0$ and 0 otherwise [16]. Based on the description above, the initial state can be recovered by solving the following *mixed* l_1/l_2 optimization problem.

$$(D_{1,2}) \min_{\hat{x}\in R^n} \sum_{i=0}^{k} \|Y_i - \Phi_i(\hat{x})\|_{l_1/l_2} \tag{6}$$

where $\|E_i\|_{l_1/l_2}$ is defined as the sum of the l_2 norms of the sum-row in sub-matrix E_i.

$$\|E_i\|_{l_1/l_2} = \sum_{j=1}^{p} \|(E_i)_j\|_{l_2}$$

Even though Proposition 2 can guarantee the accuracy of state recovery by minimizing the summation of nonzero sub-rows, the accuracy of decoder $D_{1,2}$ can not be guaranteed by Proposition 2 directly. In order to prove the accuracy of decoder $D_{1,2}$, the following must be satisfied, for all $i \in \{0, \cdots, k\}$, $K_i \subset \{1, \cdots, p\}$ with $|K_i| = q$, and for all $z \in R^n \backslash \{0\}$, it holds

$$\sum_{i=0}^{k} \sum_{j\in K_i} \|(Y_i - \Phi_i(x))_j\|_{l_2} < \sum_{i=0}^{k} \sum_{j\in K_i^c} \|(Y_i - \Phi_i(x))_j\|_{l_2}.$$

The detail proof can be easily derived based on the proof (*Proposition* 6) in [3], thus omitted here.

B. State Recovery for Nonzero Entries Sparsity Model

For switching location attacks in case ii), the sparsity of the attack matrix is equivalent to the number of nonzero entries of the attack matrix. Different from the method in [3], the state recovery problem can be expressed as the following l_0 optimization.

$$(D_0)\ \min_{\hat{x}\in R^n} \sum_{t\in\Gamma} ||y^{(t)} - CA^t\hat{x}||_{l_0} \tag{7}$$

As shown above, the l_0 dynamic decoder D_0 try to find the initial state $x^{(0)}$ by minimize the summation of the nonzero element in attack matrix $E_{s,T}(k)$. It is obvious that the solution of D_0 is the initial state if (5) holds.

***Proposition* 3.** *If the system can recover the initial state in switching location attacks with q attacked sensors and $k = T-1$ switches, the solution of dynamic decoder D_0 is the initial state $x^{(0)}$.*

Proof: Since the system can recovery the initial state in such switching location attacks, then (5) holds when $k = T-1$. Denote $x^{(0)}$ as the initial state, and denote $(e^{(0)},\dots,e^{(T-1)}) \in E_{q,T}(k)$ as the attack sequence, where $\sum_{t\in\Gamma}\|supp(e^{(t)})\| \le 2\cdot T\cdot \bar{q}$, where $\bar{q}$ is the largest attack amount correctable, determined by (5). Suppose there is another solution, $x'^{(0)}$ for decoder (7). Hence there are two solutions $x^{(0)} \neq x'^{(0)}$ and $(e^{(0)},\dots,e^{(T-1)}) \in E_{q,T}(k), (e'^{(0)},\dots,e'^{(T-1)}) \in E_{q',T}(k)$ generate the same compromised measurement $y^{(0)},\dots,y^{(T-1)}$, with a limitation, $\sum_{t\in\Gamma}\|supp(e'^{(t)})\| \le \sum_{t\in\Gamma}\|supp(e^{(t)})\| \le 2\cdot T\cdot\bar{q}$. Then we have two different initial states and attack sequences corresponding to the same measurement sequence where the nonzero entries are less than $2\cdot T\cdot\bar{q}$. It means that q errors are not correctable after T steps which contradicts the assumption. Thus the above proposition holds. ■

Obviously, the l_0 dynamic decoder (7) is a NP-hard problem. Similar to the l_1 relaxation in [13], the l_0 norm can be relaxed to the l_1 norm.

$$(D_1)\ \min_{\hat{x}\in R^n} \sum_{t\in\Gamma} ||y^{(t)} - CA^t\hat{x}||_{l_1} \tag{8}$$

As shown above the optimality of the dynamic decoder D_0 is guaranteed by proposition 2. It means that once (5) holds, D_0 can recover the initial state $x^{(0)}$ correctly. In order to guarantee the accuracy of the dynamic decoder D_1 a proposition is given below.

***Proposition* 4.** *The solution of the l_1 dynamic decoder D_1 equals to the initial state in switching location attacks with q attacked sensors and $k = T-1$ switches, if For all $K_t \subset \{1,\dots,p\}, |K_t| = q, t\in\Gamma$ and for all $z \in \mathcal{R}^n\backslash\{0\}$,it holds*

$$\sum_{t\in\Gamma}\sum_{j\in K_t} |(CA^tz)_j| < \sum_{t\in\Gamma}\sum_{j\in {K_t}^c} |(CA^tz)_j|. \tag{9}$$

Proof: (*Sufficiency*) We will proof it by contradiction. Suppose there exist $t\in\Gamma$, $K_t \subset \{1,\dots,p\}$, $|K_t| = q$, and $z\in\mathcal{R}^n\backslash\{0\}$, such that $\sum_{t\in\Gamma}\sum_{j\in K_t}|(CA^tz)_j| \ge \sum_{t\in\Gamma}\sum_{j\in K_t^c}|(CA^tz)_j|$, i.e., (9) does not hold. Let $x^{(0)} = 0$, $supp(e^{(t)}) \subseteq K_t$, $|K_t| = q$, then $y^{(t)} = CA^tx^{(0)} + e^{(t)} = e^{(t)}$. Define $e_j^{(t)} = (CA^tz)_j$, $j\in K_t$, $z\neq 0$, and $e_j^{(t)} = 0$, otherwise. When $\hat{x} = x^{(0)} = 0$ and $\hat{x} = z \neq 0$, we have

$$\begin{aligned}
&\sum_{t\in\Gamma} ||y^{(t)} - CA^tz||_{l_1} = \sum_{t\in\Gamma}\sum_{j=1}^{p} |(y^{(t)} - CA^tz)_j| \\
&= \sum_{t\in\Gamma}\sum_{j\in K_t^c} |(CA^tz|)_j \le \sum_{t\in\Gamma}\sum_{j\in K_t} |(CA^tz)_j| \\
&= \sum_{t\in\Gamma}\sum_{j=1}^{p} |(y^{(t)} - CA^tx^{(0)})_j| = \sum_{t\in\Gamma} ||y^{(t)} - CA^tx^{(0)}||_{l_1}.
\end{aligned}$$

It means that the recovered state $\hat{x} = z \neq x_0$, i.e., decoder D_1 fails to correct q errors after T steps when $k = T-1$. Then the sufficiency hold.

(*Necessity*) Similarly, proof by contradiction. Suppose the l_1 decoder D_1 can not correct q errors after T steps when $k = T-1$. This means there exists $x^{(0)} \in \mathcal{R}^n$, $(e^{(0)},\dots,e^{(T-1)}) \in E_{q,T}(k)$, and $y^{(t)} = CA^tx^{(0)} + e^{(t)}$, such that the recovered initial state $D_1(y^{(0)},\dots,y^{(T-1)}) = \tilde{x}^{(0)} \neq x^{(0)}$, where $supp(e^{(t)}) \subseteq K_t$, $|K_t| = q$. According to the definition of the l_1 decoder D_1, there exists $\tilde{x}^{(0)} \neq x^{(0)}$ such that

$$\sum_{t\in\Gamma} ||y^{(t)} - CA^t\tilde{x}^{(0)}||_{l_1} \le \sum_{t\in\Gamma} ||y^{(t)} - CA^tx^{(0)}||_{l_1}. \tag{10}$$

Let $z = \tilde{x}^{(0)} - x^{(0)} \neq 0$, then $CA^tz = CA^t\tilde{x}^{(0)} - CA^tx^{(0)} = (y^{(t)} - CA^tx^{(0)}) - (y^{(t)} - CA^t\tilde{x}^{(0)})$. Then

$$\begin{aligned}
&\sum_{t\in\Gamma}\sum_{j\in K_t} |(CA^tz)_j| \\
&= \sum_{t\in\Gamma}\sum_{j\in K_t} |(y^{(t)} - CA^tx^{(0)})_j - (y^{(t)} - CA^t\tilde{x}^{(0)})_j| \\
&\ge \sum_{t\in\Gamma}\sum_{j\in K_t} (|(y^{(t)} - CA^tx^{(0)})_j| - |(y^{(t)} - CA^t\tilde{x}^{(0)})_j|)
\end{aligned}$$

For the initial state $x^{(0)}$, and $\tilde{x}^{(0)}$, the inequation (10) holds, then

$$\begin{aligned}
&\sum_{t\in\Gamma}\sum_{j\in K_t} |(y^{(t)} - CA^tx^{(0)})_j| \\
&= \sum_{t\in\Gamma}\sum_{j=1}^{p} |(y^{(t)} - CA^tx^{(0)})_j| \ge \sum_{t\in\Gamma}\sum_{j=1}^{p} |(y^{(t)} - CA^t\tilde{x}^{(0)})_j|.
\end{aligned}$$

We have

$$\begin{aligned}
&\sum_{t\in\Gamma}\sum_{j\in K_t} |(CA^tz)_j| \\
&\ge \sum_{t\in\Gamma}\sum_{j=1}^{p} |(y^{(t)} - CA^t\tilde{x}^{(0)})_j| - \sum_{t\in\Gamma}\sum_{j\in K_t} |(y^{(t)} - CA^t\tilde{x}^{(0)})_j| \\
&= \sum_{t\in\Gamma}\sum_{j\in K_t^c} |(y^{(t)} - CA^t\tilde{x}^{(0)})_j|
\end{aligned}$$

Since $supp(e^{(t)}) = supp(y^{(t)} - CA^tx^{(0)}) \subseteq K_t$, then $\sum_{j\in K_t^c} |(y^{(t)} - CA^tx^{(0)})_j| = 0$. Hence

$$\begin{aligned}
&\sum_{t\in\Gamma}\sum_{j\in K_t} |(CA^tz)_j| \ge \sum_{t\in\Gamma}\sum_{j\in K_t^c} |(y^{(t)} - CA^t\tilde{x}^{(0)})_j| \\
&= \sum_{t\in\Gamma}\sum_{j\in K_t^c} |(CA^tz)_j|,
\end{aligned}$$

which contradict with (9). Then the necessity holds. ■

It is obvious that if the dynamic decoder D_1 can recover the initial state in switch location attacks with q attacked sensors and $T-1$ switches, then the decoder D_0 can as well. Assume for contradiction that there is $z \in R^n\backslash\{0\}$ such that $\max_{t\in\Gamma}|supp(CA^tz)| \le 2q$. Denote K_t as the q largest elements index of $|(CA^tz)_j|$, $j = 1,\dots,p$, then there is $\sum_{t\in\Gamma}\sum_{j\in K_t}|(CA^t z)_j| \geq \sum_{t\in\Gamma}\sum_{j\in K_t^c}|(CA^t z)_j|$. It means that Proposition 4 is the sufficient condition of Proposition 2. When the proposition above satisfies, the original state can be recovered by the l_1 decoder D_1.

Since the problem D_1 and $D_{1,2}$ are convex, we solve the problem using CVX [21] in this paper.

V. Numerical Simulations

In this section, we compare the performance of the dynamic decoder, fix location decoder [3], and the static decoder [13] in switching location attacks on a random toy example and an electric power system.

A. Random System

In the simulated system of size $n = 10$, $p = 15$, $T = 12$, $A \in R^{10\times 10}$, and $C \in R^{15\times 10}$ have iid Gaussian entries. In simulation, we generate switching location attacks with q attacked sensors, and k switches, where $q = 1, \cdots, 15$, with switching intervals $\tau \in \{1, 3, 6\}$. For each q and k combination, we simulate the decoders for 200 times. For a given q and τ, the attack set is constant within τ, and the number of attacked sensors is q, i.e., $|K_i| = q$. For each $j \in K_i$, the value of such attack point, $e_j^{(t)}$, is arbitrary with a similar order of the real measurement $y^{(t)}$. The initial state $x^{(0)}$ is generated from the standard Gaussian distribution. Note that the adjacent sets of attacked sensors, K_i and K_{i+1}, are generated randomly, there are both constant and variable switching frequencies in simulations when $\tau = 1$.

In order to verify the effect of the system dynamic in state recovery, we design the static decoder by minimizing the nonzero entries in attack vector $e^{(t)}$ for each time $t \in \Gamma$. The minimal residual is used for static decoders at each time $t \in \Gamma$. To assess the influence of switching location attacks in fix location decoder, the fix location decoder is simulated. To quantize the performance of the decoders, we define the normalized residual of the recovered state as follows:

$$\delta = \frac{\|x^{(0)} - \hat{x}^{(0)}\|_{l_1}}{\|x^{(0)}\|_{l_1}}$$

Define the residual upper bound of the successful recovery as $\delta \leq 1 \times 10^{-3}$, the successful recovery fraction of the decoders are presented in Fig. 2∼4.

As shown in Fig. 2∼4, the dynamic decoder (the red one marked with squares) can recover the initial state perfectly when the attacked sensors are no more than 6, i.e, $q \leq 6$. However, for the fix location decoder (the blue one marked with circle), the largest correctable attacked sensors decrease when the switch times k increase, which is consist with the analysis in *Corollary* 1. Compared with the fix location decoder, the dynamic decoder is more efficient in switching location attacks, because of the utilization of switching location information in the dynamic decoder. Compared with the static decoder, the dynamic decoder can correct more attacked sensors, which is consist with *Remark* 1, because the system dynamic is used in dynamic decoder. In summary, utilizing the switching location attack information and the system dynamic, the dynamic decoder is efficient.

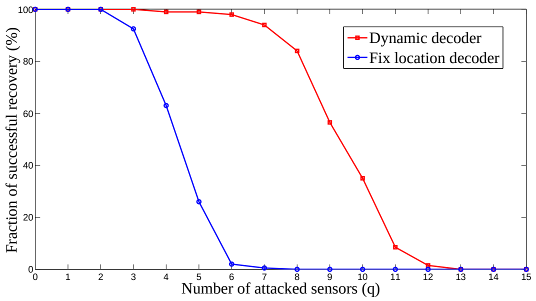

Fig. 2. Performance of the dynamic and fix location decoders in switching location attacks with $\tau = 6$.

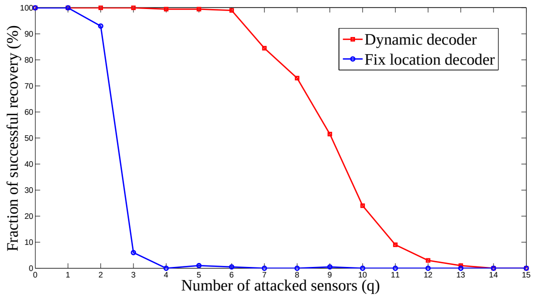

Fig. 3. Performance of the dynamic and fix location decoders in switching location attacks with $\tau = 3$.

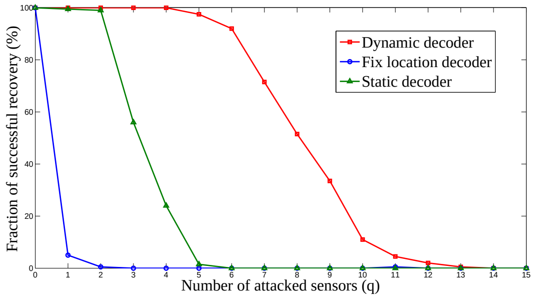

Fig. 4. Performance of the dynamic, fix location, and static decoders in switching location attacks with $\tau = 1$.

B. Electric Power System

In this part, we simulate the performance of dynamic decoder on a 14-bus power system with 5 generators [22]. There are 10 states in the system, i.e., the rotor angle σ and frequency ω of the 5 generators, where $\omega_i = d\sigma_i/dt$. The system matrix A can be deduced from the linearized swing equations [23] by eliminating the bus angle θ. Similar to [24], we assume there are $p = 35$ measurements, consists of 14 bus injection power sensors, 20 power line sensor and 1 rotor angle sensor at generator. Based the DC power flow model, the last five columns in measurement matrix C are zero, i.e., the measurements can only measure the rotor angle σ. In simulations, we generate switching location attacks with q attacked sensors, where $q = 1, \cdots, 34$, $T = 12$, with switching intervals $\tau \in \{1, 3, 6\}$. Similar to the simulations in the random toy example above, we simulate 200 times for each combination of q and τ.

In simulations, the fix location decoder is calculated in a l_1/l_∞ form [3]. For different q and k, we simulate 200 times.

The initial state and the attack vectors are generated randomly, similar to the simulation in a random system. In simulation, we don't allow the last sensor be attacked. The fraction of successful recovery is presented as shown in Fig. 5∼7.

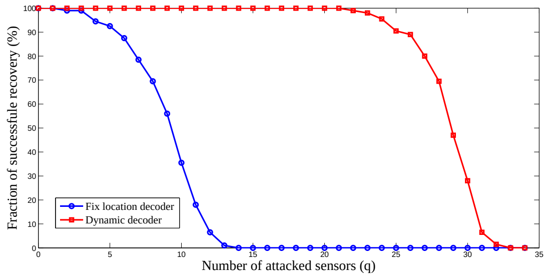

Fig. 5. Performance of the dynamic and fix location decoders in fix location attack and switching location attacks with $\tau = 6$.

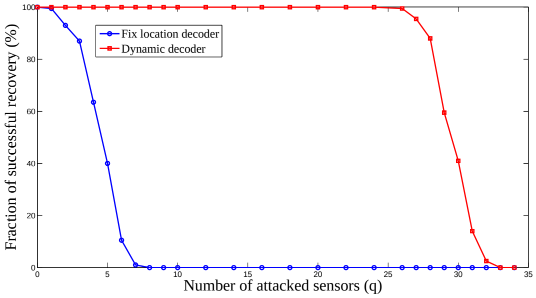

Fig. 6. Performance of the dynamic and fix location decoders in switching location attacks with $\tau = 3$.

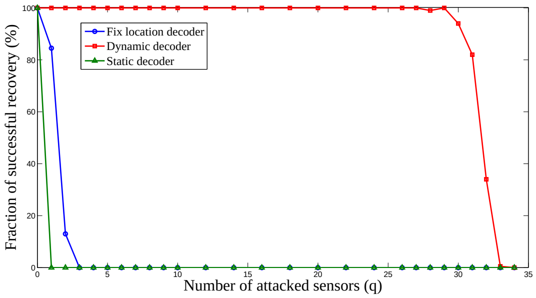

Fig. 7. Performance of the dynamic, fix location, and static decoders in switching location attacks with $\tau = 1$.

As shown in Fig. 5∼7, the dynamic decoder (the red one marked with squares) can recover the initial state perfectly when the attacked sensors are less than 25, because there are much measurement redundancy in the power systems. However, the performance of the fix location decoder in switching location attacks (the blue one marked with cycles) decrease rapidly when the switches increase. Compared with the fix location and static decoder, the dynamic decoder can correct more attacked sensors in power systems.

VI. Conclusion

In this paper, we discussed the state recovery problem in switching location attacks. A state recovery condition and a dynamic decoder are presented utilizing the system dynamics and the sub-row sparsity in attack matrices. The efficiency of the dynamic decoder, compared with the fix location decoder and static decoder, is verified both in theoretical analysis and numeral simulations. Considering that the attackers might not be rational or information incomplete, a more generalized recovery should be studied based on a more generalized sparsity model in a system with noise in the future.

References

[1] *Common Cyber Security Vulnerabilities Observed in Control System Assessments by the INL NSTB Program*, US. Department of Energy Office of Electricity Delivery and Energy Reliability, Nov. 2008, pp. 21-22.

[2] P. Naldurg, R. H. Campbell, and D. Mickunas, "Developing Dynamic Security Policies," in *Proceeding of the 2002 DARPA Active Networks Conference and Exposition (DANCE 2002)*, San Francisco, CA, USA, 2002, pp. 204-215.

[3] H. Fawzi, P. Tabuada, and S. Diggavi,"Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Transaction on Automic Control*, vol.59, no.6, pp.1454-1467, June 2014

[4] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in SCADA networks," *Computers & Security*, vol. 25, no. 7, pp. 498-506, 2006.

[5] DigitalBond Modbus TCP Rules, [Online]. Availiable:http://www.digitalbond.com/tools/quickdraw/modbus-tcp-rules/rule-1111002/

[6] F. Aloula, A. R. Al-Alia, R. Al-Dalkya, M.Al-Mardinia, and W. El-Hajj, "Smart grid security: threats, vulnerabilities and solutions," *International Journal of Smart Grid and Clean Energy*, vol. 1, no. 1, pp. 1-6, 2012.

[7] T. H. Morris, and W. Gao, " Industrial control system cyber attacks," in *Proceedings of the 1st International Symposium for ICS & SCADA Cyber Security Research*, Leicester, UK, September 2013, pp. 22-29.

[8] R. Kalapatapu, "SCADA Protocols and Communication Trends," ISA, 2004.

[9] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceeding of the 16th ACM Conference of Computer and Communications Security*, Chicago, IL, Nov. 2009, pp.21-32.

[10] Y. Mo, E. Garone, and A. Casavola, "False data injection attacks against state estimation in wireless sensor networks, in *the 49th IEEE Conference on Decision and Control (CDC)*, Atlanta, GA, pp. 5967-5972, 2010.

[11] M. Wang, P. Gao, S. G. Ghiocel, J. H. Chow, B. Fardanesh, G. Stefopoulos, and M. P. Razanousky, "Identification of unobservable cyber data attacks on power grids," in *Proceeding of the 2014 IEEE International Conference on Smart Grid Communications*, Venice, Italy, 2014, pp. 830-835.

[12] P. Gao, M. Wang, S. G. Ghiocel, J. H. Chow, B. Fardanesh, and G. Stefopoulos, "Missing data recovery by exploiting low-dimensionality in power system synchrophasor measurments," *IEEE Transaction on Power & Systems*, pp.1-8, 2015.

[13] E. J. Candes, and T. Tao, "Decoding by linear programming," *IEEE Transaction on Information Theory*, vol. 51, no.12, pp. 4203-4215, 2005.

[14] L. Liu, M. Esmalifalak, Q. Ding, V. A. Emesih, and Z. Han, "Detecting false data injection attacks on power grid by sparse optimization," *IEEE Transaction on Smart Grid*, vol. 5, no. 2, 2014.

[15] R. G. Baraniuk, V. Cevher, M. F. Duarte, and C. Hegde, "Model-based compressive sensing," *IEEE Transacion on Information Theroy*, vol. 56, no. 4, pp. 1982-2001, 2010.

[16] Y. C. Eldar, H. Bolcskei, "Block-sparsity: Coherence and efficient recovery," in *the 35th IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Taipei, 2009, pp. 2885-2888.

[17] Y. Shoukry, and P. Tabuada, "Event-triggered projected Luenberger observer for linear systems under sparse sensor attacks," in Proceeding of *53rd IEEE Conference on Decision and Control*, December, Los Angeles, 2014, pp/ 3548-3553.

[18] O. Kosut, L. Jia, R. J. Thomas, and L. Tong, "Malicious data attacks on smart grid state estimation: attack strategies and countermeasures," in *Proceeding of the 1st IEEE International Conference on Smart Grid Communications*, Gaithersburg, ML, Oct. 2010, pp.220-225.

[19] F. Pasqualetti, F. Dorfler, and F. Bullo, “Attack Detection and Identification in Cyber-Physical Systems,” *IEEE Transaction on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[20] M. A. Davenport, M. F. Duarte, Y. C. Eldar, and G. Kutyniok, “Introduction to compressed sensing,” in *Compressed Sensing: Theory and Applications*, Cambridge, U.K.: Cambridge Univ. Press, 2011, pp. 1-68.

[21] M. Grant and S. Boyd, CVX: Matlab software for disciplined convex programming, version 2.1. [Online]. Available: http://cvxr.com/cvx/

[22] IEEE 14-Bus System, [Online]. Available: http://publish.illinois.edu/smartergrid/ieee-14-bus-system/

[23] F. Pasqualetti, A. Bicchi, and F. Bullo, “A Graph-theoretical Characterization of power network vulnerabilities,” in *Proceeding of America Control Conference*, Sanfrancisco, CA, 2011, pp. 3918-3923.

[24] F. Pasqualetti, F. Dorfler, and F. Bullo, “Cyber-physical Attacks in Power Networks: Models, fundamental limitaions and monitor design,” in *Proceeding of the 50th IEEE conference on Decision and Control and European Control Conference*, 2011, pp. 2195-2201.