2018 56th Annual Allerton Conference on Communication, Control, and Computing (Allerton)
Allerton Park and Retreat Center
Monticello, IL, USA, October 2-5, 2018

A Security Index for Actuators Based on Perfect Undetectability: Properties and Approximation

Jezdimir Milošević, Henrik Sandberg, and Karl Henrik Johansson

***Abstract*— A novel security index based on the definition of perfect undetectability is proposed. The index is a tool that can help a control system operator to localize the most vulnerable actuators in the network. In particular, the security index of actuator i represents the minimal number of sensors and actuators that needs to be compromised in addition to i, such that a perfectly undetectable attack is possible. A method for computing this index for small scale systems is derived, and difficulties with the index once the system is of large scale are outlined. An upper bound for the index that overcomes these difficulties is then proposed. The theoretical developments are illustrated on a numerical example.**

I. Introduction

Enabling proper control of critical infrastructures such as power grids or water distribution networks is of utmost importance. However, these systems are complex in nature, and controlling them in an efficient manner is not a trivial task. In fact, it is known that the problem of placing minimal number of actuators in the network to achieve controllability is an NP–hard problem in general [1]. Nevertheless, a number of approaches have been proposed for actuator placement such as to maximize alternative controllability metrics [2]–[5].

In addition to controllability, it is important to consider security aspects of actuator placements. Indeed, incidents testify that control systems can become a target of malicious adversaries [6]–[8]. Furthermore, it has been recognized that cyber-attacks on control systems cannot be treated using the same tools as noise or disturbances, but that new techniques are required [9]. For instance, cyber-attacks impose fundamental limitations for state estimation [10], [11], detection [12], and consensus in multi–agent systems [13], [14]. Motivated by cyber-security issue, we propose a novel security index to characterize the vulnerability of actuators in control systems. Using the index, a control system operator can find the most vulnerable actuators in the system, and then focus a security budget to protect them [15].

A security index was first introduced in [16], to characterize security of sensors monitoring a power network. The power network was modeled as a static linear system, and the static security index was defined for each sensor i in the network. In particular, the static index is equal to the smallest number of sensors that needs to be attacked in order to conduct so called stealthy attacks that affects sensor i. Hence, the index captures both the intent of the attacker and the attack detectability.

Although the static security index proved to be useful to distinguish the most vulnerable sensors in the network, the challenge is to compute it once the number of sensors is large. In fact, it was shown in [17] that calculating the static security index is an NP–hard problem in general. However, for some network topologies, the index can be efficiently computed in polynomial time [17]–[21]. For example, in [18], the authors introduced an upper bound on the static index that can be obtained in polynomial time by solving a minimum s–t cut problem in the graph. They also showed that this bound is tight in several cases of interest.

Security index has also been studied for dynamical systems [22], [23]. In [23], the definition of *undetectability* [12] was used to define a security index. In this paper, we build upon this work. In particular, we propose a novel type of security index for actuators based on the definition of *perfect undetectability* [24], [25].

The contribution of this paper is twofold. Firstly, a novel actuator security index based on the definition of perfect undetectability is proposed. For this index, we derive a sufficient and necessary condition that the solution needs to satisfy (Theorem 1). This condition can be verified efficiently, and can be used to find a security index once the number of sensors and actuators is small. However, two issues appear in large scale systems: (1) The problem of computing the index is NP–hard in general; (2) The index is fragile to system variations. Secondly, motivated by these issues, we derive an upper bound for the security index. For this, we use a *structural model* of the system [26], and the notion of vertex separators introduced in [25] to study structural left invertibility of systems. In particular, we show how vertex separators can be used to define an upper bound of the index (Theorem 2). Interestingly, the problem of finding this upper bound can be reduced to the minimum s–t cut problem (Proposition 1). This results extends the previous work on the static index [17]–[20], where the bound on static index was also obtained by solving minimum s–t cut problem. Besides being fast to calculate, the bound is robust with respect to system variations.

Paper organization. In the remainder of this section, we introduce notation. In Section II, we introduce the model setup and formulate the security index problem. In Section III, we discuss properties of the index. In Section IV, we propose an upper bound of the index, and in Section V, we outline its properties. In Section VI, we illustrate the findings on a numerical example. In Section VII, we conclude the paper.

The work was supported by the Swedish Civil Contingencies Agency (CERCES project), the Swedish Research Council, Knut and Alice Wallenberg Foundation, and the Swedish Foundation for Strategic Research. The authors are with the Department of Automatic Control, School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, Stockholm, Sweden. Emails: {jezdimir, hsan, kallej} @kth.se.

Notation. For a vector $x \in \mathbb{R}^n$, $||x||_0 = |\text{support}(x)|$ where $\text{support}(x) = \{i \in \{1,\dots,n\} : x_i \neq 0\}$. For a signal $a : \mathbb{Z}_{\geq 0} \to \mathbb{R}^n$, $a \neq 0$ implies $a(k) \neq 0$ for at least one k from $\mathbb{Z}_{\geq 0}$, and $||a||_0 = |\cup_{k\in\mathbb{Z}_{\geq 0}} \text{support}(a(k))|$. Let the indices of the elements of a be $\mathcal{I} = \{1, 2, \dots, n\}$, and let $\mathcal{I}_a \subseteq \mathcal{I}$. With $a^{(\mathcal{I}_a)}(k)$, we denote the elements of a with indices from $\mathcal{I}_a$. For a transfer function matrix G with columns with indices from the set $\mathcal{I}$, $G^{(\mathcal{I}_a)}$ is a transfer function matrix that contains the columns of G from $\mathcal{I}_a \subseteq \mathcal{I}$, and the *normal rank* of G is defined as normrank $G = \max\{\text{rank}G(z) | z \in \mathbb{C}\}$.

II. Problem Formulation

In this section, we introduce models of the system and of the attacker. Based on them, we propose a security index that can be used to characterize how vulnerable actuators are.

A. Model Setup

The attacked system evolves according to the equations

$$\begin{aligned} x(k+1) &= Ax(k) + Bu(k) + B_a a(k) \\ y(k) &= Cx(k) + D_a a(k) \end{aligned} \tag{1}$$

where $x(k) \in \mathbb{R}^{n_x}$ is the state of the system, $y(k) \in \mathbb{R}^{n_y+n_e}$ is the vector of sensor readings, $u(k) \in \mathbb{R}^{n_u}$ is the control signal, and $a(k) \in \mathbb{R}^{n_u+n_y}$ is the sparse signal that models the attacks against the sensors and the actuators. We assume that all the signals are exponentially bounded, which implies that their $\mathcal{Z}$–transforms exist. For brevity of exposition, we set $x(0) = 0$ and $u = 0$. This is without loss of generality because of the system's linearity.

The first n_u elements of $a(k)$ correspond to attacks against the actuators, while the remaining n_y elements correspond to attacks against the unprotected sensors. The assumption is that the last $n_e \geq 0$ elements of the vector $y(k)$ are protected, so the attacker cannot manipulate them. This can be achieved by deploying additional physical protection and encryption/authentication schemes [15]. Therefore, matrices B_a and D_a are of the form

$$B_a = \begin{bmatrix} B & \mathbf{0}_{n_x \times n_y} \end{bmatrix} \qquad D_a = \begin{bmatrix} \mathbf{0}_{n_y \times n_u} & \mathbf{I}_{n_y} \\ \mathbf{0}_{n_e \times n_u} & \mathbf{0}_{n_e \times n_y} \end{bmatrix}$$

and B is assumed to have a full rank. Indices of elements of a are denoted by $\mathcal{I} = \{1, \dots, n_u + n_y\}$. The elements of a that correspond to attacked components can take any value, while the remaining elements are always zero. We also assume that the attacker knows the matrices A, B, C.

In the previous work on security index for dynamical systems [23], the goal was to determine if the attacker with the resources introduced above is able to conduct undetectable attacks, where undetectability is defined next [12]. In the definition, $y(k, x(0), a)$ is used to indicate that the measurement signal y at time step k is dependent on the initial state $x(0)$ and the attack signal a.

Definition 1: The attack $a \neq 0$ is *undetectable* if $y(k, 0, a) = y(k, x(0), 0)$ for every $k \in \mathbb{Z}_{\geq 0}$ and some $x(0)$.

This definition of *undetectability* implies that the attacked output y is identical to the one that comes from the initial state $x(0)$. Therefore, if the defender has some knowledge about the initial state, this attack may be detected. In this paper, we impose a more strict definition of undetectability, so called perfect undetectability [24].

Definition 2: The attack signal $a \neq 0$ is *perfectly undetectable* if $y(k, 0, a) = 0$ for every $k \in \mathbb{Z}_{\geq 0}$.

Notice that Definition 2 is more strict then Definition 1, since the attack signal a does not leave any trace in sensor measurements when it is perfectly undetectable.

B. Security Index Problem

We now introduce a security index based on the definition of perfect undetectability. The security index $\delta(i)$ is defined for every actuator $i \in \mathcal{I}$. This index may indicate to the operator which actuators are the most vulnerable in the system, and help him/her to invest resources in a cost-efficient way [15].

The value of security index $\delta(i)$ is equal to the minimal number of sensors and actuators that has to be compromised by the attacker, such as to conduct a perfectly undetectable attack. In addition, the constraint $a^{(i)} \neq 0$ is imposed, and models a goal or intent by the attacker. This ensures that actuator i is actively used in the attack. Naturally, components with small $\delta(i)$ are more vulnerable than components with high $\delta(i)$. The worst case occurs when $\delta(i) = 1$. In that case, a perfectly undetectable attack can be conducted by using only a single component, namely actuator i.

From the previous discussion, the security index problem based on perfect undetectability can be defined as follows.

Problem 1: Calculating security index

$$\begin{aligned} \underset{a}{\text{minimize}} \quad & \delta(i) \triangleq ||a||_0 \\ \text{subject to} \quad & x(k+1) = Ax(k) + B_a a(k) && \text{(C1)} \\ & 0 = Cx(k) + D_a a(k) && \text{(C2)} \\ & x(0) = 0 && \text{(C3)} \\ & a^{(i)} \neq 0 && \text{(C4)} \end{aligned}$$

The objective function reflects our desire to find the minimal number of attacked components to conduct a perfectly undetectable attack (sparsest signal $a : \mathbb{Z}_{\geq 0} \to \mathbb{R}^n$). The constraints (C1) and (C2) ensure that the attack signal satisfies the physical dynamics of the system. The constraints (C2) and (C3) guarantee the attack to be perfectly undetectable, while the constraint (C4) ensures that the component i is actively used in the attack.

Remark 1: Problem 1 is not necessarily feasible. If a solution does not exist, we define the index to be ∞.

Remark 2: The previous problem can also be used for finding the security index of sensor i. However, in the case of perfectly undetectable attacks, at least one actuator must be attacked in order to make the attack signal against sensor i active. Therefore, the problem of finding $\delta(i)$ of sensor i can in general be reduced to the problem of finding an actuator with minimal security index that excites sensor i.

In the remainder of the paper, we are interested in analyzing and solving Problem 1.

III. Security Index for Small Scale and Large Scale Systems

In this section, we investigate properties of the security index. We first derive a sufficient and necessary condition that a solution of Problem 1 needs to satisfy. This condition can help us to find a security index for networks that have a relatively small number of sensors and actuators. We then outline difficulties with the index once the system is large, which motivate our further study in Section IV.

A. Calculating Security Index for Small Scale Systems

We now derive the sufficient and necessary condition that a solution to the security index problem needs to satisfy. We first revisit necessary and sufficient condition for existence of perfectly undetectable attacks [24, Theorem 1]. In the following, a transfer matrix from a to y is defined by

$$G(z) = C(z\mathbf{I}_{n_x} - A)^{-1}B_a + D_a.$$

Lemma 1: Assume that the set of attacked sensors and actuators is $\mathcal{I}_a \subseteq \mathcal{I}$. Then there exists a perfectly undetectable attack if and only if the transfer function $G^{(\mathcal{I}_a)}$ has normal rank less than $|\mathcal{I}_a|$.

To ensure that the i-th attack signal is used in the perfectly undetectable attack, the following condition must hold.

Theorem 1: Assume that the set of attacked components is $\mathcal{I}_a \subseteq \mathcal{I}$. There is a perfectly undetectable attack involving component $i \in \mathcal{I}_a$ if and only if

$$\text{normrank } G^{(\mathcal{I}_a)} = \text{normrank } G^{(\mathcal{I}_a \setminus i)}. \tag{2}$$

Proof: ($\Rightarrow$) Assume (2) does not hold, but there exists a perfectly undetectable attack with $\mathcal{Z}$ transform $\mathcal{A}$, $\mathcal{A}^{(i)} \neq 0$, such that $G^{(\mathcal{I}_a \setminus i)}\mathcal{A}^{(\mathcal{I}_a \setminus i)} + G^{(i)}\mathcal{A}^{(i)} = 0$. We split the proof into two cases:

(I) normrank $G^{(\mathcal{I}_a \setminus i)} = |\mathcal{I}_a| - 1$;

(II) normrank $G^{(\mathcal{I}_a \setminus i)} = |\mathcal{I}_b| < |\mathcal{I}_a| - 1$.

Case (I). Since undetectable attacks are possible, transfer function $[G^{(\mathcal{I}_a \setminus i)}\ G^{(i)}]$ needs to have normal rank lower than $|\mathcal{I}_a|$ according to Lemma 1. Therefore, it follows

$$|\mathcal{I}_a| > \text{normrank} G^{(\mathcal{I}_a)} = \text{normrank}[G^{(\mathcal{I}_a \setminus i)} G^{(i)}] \geq |\mathcal{I}_a| - 1$$

which implies that (2) holds and contradicts the assumption.

Case (II). Let the set $\mathcal{I}_b \subseteq \mathcal{I}_a \setminus i$ be chosen such that normrank $G^{(\mathcal{I}_b)} = |\mathcal{I}_b|$ and the columns of $G^{(\mathcal{I}_b)}$ span columns $G^{(j)}$, where $j \in \mathcal{I}_a \setminus (\mathcal{I}_b \cup i)$. We can then find $\mathcal{A}'$ such that $G^{(\mathcal{I}_a \setminus i)}\mathcal{A}^{(\mathcal{I}_a \setminus i)} = G^{(\mathcal{I}_b)}\mathcal{A}'^{(\mathcal{I}_b)}$. Thus, it follows $G^{(\mathcal{I}_b)}\mathcal{A}'^{(\mathcal{I}_b)} + G^{(i)}\mathcal{A}^{(i)} = 0$. From the proof of Case (I), we have normrank $[G^{(\mathcal{I}_b)}\ G^{(i)}] =$ normrank $G^{(\mathcal{I}_b)}$. However, in that case it follows

$$\begin{aligned} \text{normrank } [G^{(\mathcal{I}_a \setminus i)}\ G^{(i)}] &= \text{normrank } [G^{(\mathcal{I}_b)}\ G^{(i)}] \\ &= \text{normrank } G^{(\mathcal{I}_b)} \\ &= \text{normrank } G^{(\mathcal{I}_a \setminus i)}. \end{aligned}$$

Therefore, (2) holds, so we again have a contradiction.

($\Leftarrow$) If (2) holds, then there exist real rational functions P and $Q \neq 0$ such that $G^{(\mathcal{I}_a \setminus i)}P + G^{(i)}Q = 0$. Thus, an attack signal $\mathcal{A}^{(i)}$ can be masked by applying the attack signal $\mathcal{A}^{(\mathcal{I}_a \setminus i)} = \frac{P}{Q}\mathcal{A}^{(i)}$ on the remaining components. ■

The condition from Theorem 1 can be used for calculating δ when the number of sensors and actuators is relatively small. We can search all the subsets $\mathcal{I}_a \subseteq \mathcal{I}$, $i \in \mathcal{I}_a$, and check if (2) holds. This condition can be checked efficiently, since the normal rank is equal to the rank of the transfer matrix for almost all z. The value of $\delta(i)$ is then $|\mathcal{I}_a|$, where $\mathcal{I}_a$ is the subset of smallest cardinality that satisfies (2).

B. Issues with Large Scale Systems

We now outline the two issues that appear once the network is of a large scale. Firstly, Problem 1 is combinatorial in nature, and therefore, NP–hard in general. Thus, the brute force search cannot be used to find a security index once the network is large. In fact, even in the static case, the security index problem is proved to be NP–hard [17].

Secondly, as we show in the next example, the security index can be quite fragile with respect to changes in the system matrix A. Therefore, an actuator may appear to be more important than the other for one realization of the system, but for the other, that may not be the case. Given the complexity of large scale systems, it is reasonable to assume that they change configuration over time.

Example 1: Let the realization of a system be

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & -1 & 0 \end{bmatrix} \quad B = \begin{bmatrix} 1 \\ 0 \\ 0 \\ 0 \end{bmatrix} \quad C = \begin{bmatrix} 0 & 0 & 0 & 1 \end{bmatrix}.$$

and assume that the sensor is protected. It can be shown that the transfer function from the actuator to the sensor is equal to 0. Therefore, the security index $\delta(1) = 1$. However, if $A(3,1)$ changes from 1 to 0, than any non-zero input influences the output that is protected, so $\delta(1) = +\infty$.

Motivated by these shortcomings, we introduce a robust and fast-to-calculate upper bound for δ.

IV. Upper Bound on Security Index

In this section, we introduce a robust structural model of the system [26], and based on it, we derive an upper bound for the security index. In contrast to the original security index, the bound is robust to system variations and the exact value of the bound can be obtained in polynomial time. Preliminaries from graph theory and the minimum s–t cut problem are introduced first.

A. Preliminaries

Let $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ be a *directed graph*, with the set of *nodes* $\mathcal{V} = \{v_1, \ldots, v_n\}$, and the set of *edges* $\mathcal{E} \subseteq \mathcal{V} \times \mathcal{V}$. We say that two nodes v_j and v_k are *non-adjacent* if there exists no edge between them, and they are said to be *adjacent* otherwise. A *directed path* from node v_{j_1} to node v_{j_l} is a sequence of nodes $v_{j_1}, v_{j_2}, \ldots, v_{j_l}$, where $(v_{j_k}, v_{j_{k+1}}) \in \mathcal{E}$ for $1 \leq k \leq l$. A directed path that does not contain repeated nodes is called a *simple directed path*. The *vertex separator* is defined as follows.

Definition 3: Let $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ be a directed graph, and $v_a \in \mathcal{V}$ and $v_b \in \mathcal{V}$ be non-adjacent nodes. A vertex separator

for v_a and v_b is a subset of nodes $\mathcal{V}' \subseteq \mathcal{V} \setminus (v_a \cup v_b)$ whose removal deletes all directed paths from v_a to v_b.

We now briefly revisit the min s–t cut problem. Assume that a weight w_{ij} is associated to each edge $(v_i, v_j) \in \mathcal{E}$ of the graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$. The node set $\mathcal{V}$ contains two nodes of special importance: source s and sink t. A partition of the nodes into disjoint sets $\mathcal{V}_s$ and $\mathcal{V} \setminus \mathcal{V}_s$ that satisfies $s \in \mathcal{V}_s$ and $t \in \mathcal{V} \setminus \mathcal{V}_s$ is called an s–t cut, while the cut capacity is

$$C(\mathcal{V}_s) \triangleq \sum_{\{(i,j) \in \mathcal{E} | i \in \mathcal{V}_s, j \notin \mathcal{V}_s\}} w_{ij}.$$

The minimum cut problem can then be defined as the problem of finding a cut of minimum capacity:

$$\begin{aligned} \underset{\mathcal{V}_s}{\text{minimize}} \quad & C(\mathcal{V}_s) \\ \text{subject to} \quad & \mathcal{V}_s \text{ and } \mathcal{V} \setminus \mathcal{V}_s \text{ is an } s-t \text{ cut} \end{aligned}$$

Algorithms for finding the *exact* solution of this problem efficiently are well known. For instance, the algorithm from [27] solves the problem with running time $\mathcal{O}(|\mathcal{V}||\mathcal{E}|+|\mathcal{V}|^2 \log|\mathcal{V}|)$.

B. Structural Upper Bound

To derive a robust upper bound for the security index, we first introduce the structural model $[A], [B], [C]$ for the system (1) [26]. The structural matrix $[A]$ has only binary elements. If $[A](i,j) = 0$, then $A(i,j) = 0$ for any realization A of the system. In case that $[A](i,j) = 1$, then $A(i,j)$ can take values different from 0. Same holds for $[B]$ and $[C]$. On one hand, this model is less informative, since it does not use the exact values of the coefficients from A, B, C. However, this also makes it robust to system changes, which are to be expected in large systems.

We restrict our attention to matrices $[B]$ and $[C]$ with a special structure. It is assumed that each of the actuators influences directly only one of the states, and each of the sensors measures only one of the states for any realization. This is a commonly adopted simplifying assumption in actuator and sensor placement problems [3], [4], [28]. We also exclude realizations where an actuator (a sensor) is idle, that is, it does not influence (measure) any state.

Assumption 1: The matrices $[B]$ and $[C]$ are given by

$$[B] = \begin{bmatrix} e_{i_1} & \dots & e_{i_{n_u}} \end{bmatrix} \qquad [C] = \begin{bmatrix} e_{j_1} & \dots & e_{j_{n_y+n_e}} \end{bmatrix}^T$$

where e_i is the i-th vector of the canonical basis of appropriate size. Moreover, if $[B](i,j) = 1$ ($[C](i,j) = 1$), then $B(i,j) \neq 0$ ($C(i,j) \neq 0$) for any realization of the system.

We now introduce a graph $\mathcal{G} = \{\mathcal{V}, \mathcal{E}\}$ for the structural model $[A], [B], [C]$. The set of nodes is $\mathcal{V} = \mathcal{X} \cup \mathcal{U} \cup \mathcal{Y}$ where $\mathcal{X} = \{x_1, \dots, x_{n_x}\}$ is the set of states, $\mathcal{U} = \{u_1, \dots, u_{n_u}\}$ is the set of actuators, $\mathcal{Y} = \{y_1, \dots, y_{n_y+n_e}\}$ is the set of sensors. The set of edges is $\mathcal{E} = \mathcal{E}_{ux} \cup \mathcal{E}_{xx} \cup \mathcal{E}_{xy}$, where $\mathcal{E}_{ux} = \{(u_j, x_i) : [B](i,j) \neq 0\}$ are edges from the actuators to the states, $\mathcal{E}_{xx} = \{(x_j, x_i) : [A](i,j) \neq 0\}$ are edges between the states, and $\mathcal{E}_{xy} = \{(x_j, y_i) : [C](i,j) \neq 0\}$ are the edges from the states to the sensors. The extended graph of the system is $\mathcal{G}_t = \{\mathcal{V}_t, \mathcal{E}_t\}$, where $\mathcal{V}_t = \mathcal{V} \cup t$ and $\mathcal{E}_t = \mathcal{E} \cup \{(y_i, t) : \forall y_i \in \mathcal{Y}\}$.

In [25], the authors considered the problem of designing a system such that perfectly undetectable attacks with p components are not possible. In their framework, every state can be attacked. They derived a graph theoretical condition that states that if minimal vertex separator in between each of the nodes x_i and sink node t is greater than p, then perfectly undetectable attacks using p components cannot be conducted for almost every realization of the system. In what follows, we show use vertex separators to upper bound the security index.

Theorem 2: Let $\mathcal{G}_t$ be the extended graph of the system, $\mathcal{U}_a \subseteq \mathcal{U}$ ($\mathcal{Y}_a \subseteq \mathcal{Y}$) be subsets of actuators (sensors) under the attacker's control, and $u_i \in \mathcal{U}_a$ an actuator for which we want to estimate the security index. Let $\mathcal{X}_a$ be defined as

$$\mathcal{X}_a = \{x_j | (u_j, x_j) \in \mathcal{E}_t, u_j \in \mathcal{U}_a \setminus u_i\}.$$

If $\mathcal{X}_a \cup \mathcal{Y}_a$ is a vertex separator for u_i and t in $\mathcal{G}_t$, then $\delta(u_i) \leq |\mathcal{U}_a| + |\mathcal{Y}_a|$ for *any* realization A, B, C of the structural matrices $[A], [B], [C]$.

Proof: To prove the claim, we first introduce an attack strategy. We then prove that this attack strategy is using actuator u_i, and it is perfectly undetectable.

For actuator u_i, the attacker injects an arbitrary persistent signal $a^{(u_i)} \neq 0$, which ensures that the actuator is used in the attack actively. For other actuators $u_j \in \mathcal{U}_a \setminus u_i$, the attack is $a^{(u_j)}(k) = -A^{(u_j)}/b^{(u_j)} x(k)$, where $A^{(u_j)}$ is the row of matrix A corresponding to attacked actuator u_j, and $b^{(u_j)}$ is the element of B multiplying $a^{(u_j)}(k)$. Thus, we have $x_p(k) = A^{(u_j)} x(k) - A^{(u_j)} x(k) = 0$, where $x_p \in \mathcal{X}_a$ is the state adjacent to u_j. Therefore, we conclude that all the states from the set $\mathcal{X}_a$ are always equal to 0, since $x(0) = 0$. For the attacked sensor $y_j \in \mathcal{Y}_a$, the attack signal is given by $a^{(y_j)}(k) = -C^{(y_j)} x(k)$, where $C^{(y_j)}$ represents the row of the matrix C corresponding to attacked measurement y_j.

We now prove that the strategy is perfectly undetectable. From the strategy, we have $y_j(k) = C^{(y_j)} x(k) + a^{(y_j)}(k) = 0$ for arbitrary $y_j \in \mathcal{Y}_a$. Thus, attacked measurements are always equal to zero. It remains to be proven that under the condition stated in the theorem, non-attacked sensor measurements $\mathcal{Y} \setminus \mathcal{Y}_a$ remain 0 as well. Let $\mathcal{X}_b$ be the set of states for which there exists a directed path from actuator u_i that does not contain the states $\mathcal{X}_a$, and let $\mathcal{X}_c = \mathcal{X} \setminus (\mathcal{X}_b \cup \mathcal{X}_a)$. Note that the states $\mathcal{X}_b$ cannot be measured using non attacked sensors $\mathcal{Y} \setminus \mathcal{Y}_a$, since that would imply that there exists a path in between u_i and sink t, which would contradict the assumption that $\mathcal{X}_a \cup \mathcal{Y}_a$ is a vertex separator. Additionally, edges (x_b, x_c) where $x_b \in \mathcal{X}_b$ and $x_c \in \mathcal{X}_c$ cannot exist, since that would imply that there exists directed path from u_i to x_c. Since $x(0) = 0$ and the states $\mathcal{X}_a$ are equal to zero, we conclude that any state $x_c \in \mathcal{X}_c$ remains 0 during the attack. Thus, non-attacked sensor measurements $\mathcal{Y} \setminus \mathcal{Y}_a$ are equal to 0. It follows that perfectly undetectable attacks with $a^{(u_i)} \neq 0$ can be conducted using $\mathcal{U}_a \cup \mathcal{Y}_a$, which concludes the proof. ■

Based on the previous result, we can formulate the problem of finding an upper bound for the security index. The idea is to find minimal number of attacked components

$\mathcal{U}_a, \mathcal{Y}_a$ such that the condition stated in Theorem 2 holds. We then analyze this bound in the next section.

Problem 2: Calculating structural upper bound

$$\begin{aligned} \underset{\mathcal{U}_a, \mathcal{Y}_a}{\text{minimize}} \quad & \bar{\delta}(u_i) := |\mathcal{U}_a \cup \mathcal{Y}_a| \\ \text{subject to} \quad & \mathcal{X}_a = \{x_j | (u_j, x_j) \in \mathcal{E}_t, u_j \in \mathcal{U}_a \setminus u_i\} \\ & \mathcal{Y}_a \text{ are not protected} \\ & \mathcal{X}_a \cup \mathcal{Y}_a \text{ is a vertex separator for } u_i \text{ and } t \\ & u_i \in \mathcal{U}_a \end{aligned}$$

Remark 3: Problem 2 does not have to be solvable, in which case we define the bound to be equal to ∞.

V. Properties of Upper Bound

We now outline two important properties of $\bar{\delta}$.

A. Robustness

The first important property of $\bar{\delta}$ is its robustness to system variations. Since it is derived based on a structural model of the system $[A], [B], [C]$, which does not use the exact values of model parameters, the bound has the same value for any realization of the system A, B, C. Therefore, the bound can help us to find extremely vulnerable actuators in the system. Namely, having a small value of the bound $\bar{\delta}(u_i)$ is far more serious than having a small value of $\delta(u_i)$. In case that $\bar{\delta}(u_i)$ is small, the attacker can conduct the attack involving actuator u_i for *any* realization A, B, C of the system using a small number of components.

On the other hand, the bound does not necessarily have to be tight, as shown later in the simulations. Therefore, in case that we obtain a large value of the bound for some actuator, we do not know whether or not the attack can be conducted using a smaller number of components. Tightness of the bound will be addressed in the future research.

B. The Bound can be Computed Efficiently

In what follows, we show that Problem 2 can be converted to a minimum s–t cut problem. Thus, the exact value of the bound can be obtained efficiently, using well established algorithms such as [27]. The main step is to transform $\mathcal{G}_t$ to a convenient graph $\mathcal{G}_{u_i} = \{\mathcal{V}_{u_i}, \mathcal{E}_{u_i}\}$, with an additional set of weights W_{u_i} for each edge in $\mathcal{E}_{u_i}$. In what follows, we refer to node $x_j \in \mathcal{X}$ as a node of Type 1 if it is adjacent to actuator $u_k \neq u_i$. Otherwise, we say the node is of Type 2.

Remark 4: In [25], it was explained how to construct a graph for finding a minimal vertex separator. However, in our case, not all the states are controllable by the actuators and protected sensors are possible, so the graph needs to be adjusted accordingly.

The set of nodes $\mathcal{V}_{u_i}$ contains actuator u_i for which we are calculating the bound (source node), a dummy node t (sink node), the nodes x_{j1} and x_{j2} for every node $x_j \in \mathcal{X}$ of Type 1, the nodes $x_j \in \mathcal{X}$ of Type 2, and the sensors $\mathcal{Y}$. The set of edges $\mathcal{E}_{u_i}$ is constructed according to the following five rules. (1) The edge $(u_i, x_j) \in \mathcal{E}_{ux}$ is contained in $\mathcal{E}_{u_i}$, and its weight is ∞. (2) If $x_j \neq x_k$ are of Type 1, and if $(x_j, x_k) \in \mathcal{E}_{xx}$, then $(x_{j_2}, x_{k_1}) \in \mathcal{E}_{u_i}$. If x_j is of Type 1 and x_k is of Type 2, and if $(x_j, x_k) \in \mathcal{E}_{xx}$, then $(x_{j_2}, x_k) \in \mathcal{E}_{u_i}$. If x_j is of Type 2 and x_k is of Type 1, and if $(x_j, x_k) \in \mathcal{E}_{xx}$, then $(x_j, x_{k_1}) \in \mathcal{E}_{u_i}$. If $x_j \neq x_k$ are of Type 2, and if $(x_j, x_k) \in \mathcal{E}_{xx}$, then $(x_j, x_k) \in \mathcal{E}_{u_i}$. The weights of all the aforementioned edges are ∞. (3) For every pair of nodes x_{j_1} and x_{j_2} that correspond to a node x_j of Type 1, we add an edge (x_{j_1}, x_{j_2}) of weight 1 to $\mathcal{E}_{u_i}$. (4) For every edge $(x_j, y_k) \in \mathcal{E}_{xy}$ where x_j is of Type 1, we add an edge (x_{j_2}, y_k) to $\mathcal{E}_{u_i}$. If y_k is protected, the edge weight is ∞. Otherwise, the weight is 1. Similarly, for every edge $(x_j, y_k) \in \mathcal{E}_{xy}$ where x_j is of Type 2, we add an edge (x_j, y_k) to $\mathcal{E}_{u_i}$. The weight of the edge is determined in the same way as for the state of Type 1. (5) There exists an edge between every measurement $\mathcal{Y}$ and sink t. The weights of these edges are ∞. We now introduce an example to clarify the differences between G_t and $\mathcal{G}_{u_i}$.

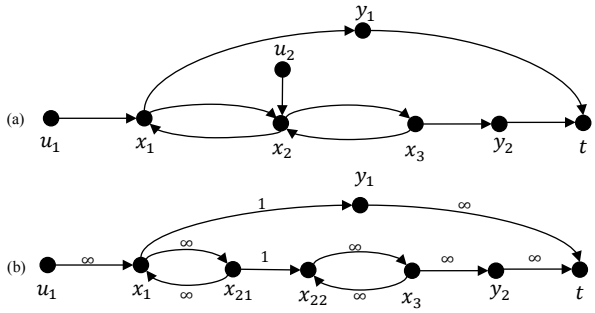

Fig. 1. (a) The extended graph of the system $\mathcal{G}_t$. (b) The graph $\mathcal{G}_{u_1}$ constructed for the purpose of solving Problem 2 for u_1.

Example 2: Let the structural matrices be given by

$$[A] = \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \quad [B] = \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 0 \end{bmatrix} \quad [C] = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix}.$$

Assume that the first sensor can be attacked, while the second one is protected. The extended graph of the system $\mathcal{G}_t$ is shown on Figure 1 (a), and the graph $\mathcal{G}_{u_1}$ constructed for the purpose of solving Problem 2 for u_1 on Figure 1 (b).

We now show that Problem 2 can be reduced to solving a minimum s–t cut problem on $\mathcal{G}_{u_i}$. As we mentioned in the introduction, this result extends the previous finding for the static security index derived in [18], which also used min-cut to find an upper bound on the static security index.

Proposition 1: Assume that the Problem 2 is solvable, and let $\bar{\delta}(u_i)$ be the optimal value. Let δ^* be the value of minimal u_i–t cut on graph $\mathcal{G}_{u_i}$. The equality $\bar{\delta}(u_i) = \delta^* + 1$ then holds. In case that $\bar{\delta}(u_i) = +\infty$, then $\delta^* = +\infty$.

Proof: By construction, for every simple directed path $u_i, x_i, \ldots, t$ in $\mathcal{G}_t$ there exists exactly one simple path in $\mathcal{G}_{u_i}$ which is either the same, or obtained by replacing every state x_k of Type 1 that belongs to the path by a pair x_{k1},x_{k2}. Similarly, for every simple directed path $u_i, x_i, \ldots, t$ in $\mathcal{G}_{u_i}$, there is exactly one simple directed path in $\mathcal{G}_t$ which is the same, or obtained by replacing every pair x_{k1},x_{k2} by x_k. Note now that selecting $u_j \neq u_i$ to belong to a solution of Problem 2 implies that we select the state x_k adjacent to u_j to belong to a vertex separator in graph $\mathcal{G}_t$. This action is

equivalent to cutting an edge in between the states x_{k_1}, x_{k_2} in the graph $\mathcal{G}_{u_i}$. Adding a non-protected sensor y_j measuring the state x_k to a vertex separator implies that we delete all the directed paths from x_i to t passing through the y_j. This action is equivalent to cutting an edge in between x_k (or x_{k_2}) and y_j in the graph $\mathcal{G}_{u_i}$. Therefore, finding a vertex separator from u_i to t for graph $\mathcal{G}_t$ is equivalent to finding a minimum u_i–t cut in the graph $\mathcal{G}_{u_i}$. Given that the cut capacity δ^* does not take into consideration actuator u_i, we need to increase δ^* by 1 to obtain the value $\bar{\delta}(u_i)$.

If Problem 2 is not solvable, then there exists a simple directed path $u_i, x_i, \ldots, t$ in $\mathcal{G}_t$ which does not contain the states adjacent to the actuators $u_k \neq u_i$, or unprotected measurements. The same path exists in $\mathcal{G}_{u_i}$, and can be deleted only by cutting an edge with the weight $+\infty$. ■

VI. Numerical Example

We now illustrate the differences between δ and $\bar{\delta}$ on a numerical example. We consider a system with 10 states, 4 actuators, and 5 sensors. The structural system matrix is

$$[A] = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}.$$

The states x_3, x_4, x_7, x_{10} ($x_2, x_3, x_4, x_9, x_{10}$) are directly influenced by the actuators u_1–u_4, respectively (are directly measured by the sensors y_1–y_5, respectively).

A. Robustness

We first investigate how system variations influence the index and the upper bound. For this purpose, we generated 50 realizations (A, B, C) based on the structural model. The elements of A were generated as $a(i, j) = XY$, where X is a discrete random variable that takes values from the set $\{0, 1\}$ with probabilities $p_0 = 0.3$ and $p_1 = 0.7$, and $Y \sim \mathcal{N}(0, 1)$. We set $B = [B]$ and $C = [C]$ in all the realizations. For each realization, we calculated the security index and the upper bound for u_1–u_4. The results are shown in Figure 2.

Firstly, it can be seen that the security index is indeed fragile. For example, $\delta(u_2)$ can take values $\{2, 3, 4, 5\}$ depending on a realization. This confirms that defining security index based on a single realization can be misleading. Naturally, $\bar{\delta}$ was the same for all the realizations. On the other hand, we also see that δ and $\bar{\delta}$ are rarely equal, which is the weakness of the bound. For instance, for u_2, the bound is tight for only 12 out of 50 realizations. However, the bound can still help us to find extremely vulnerable actuators, such as u_3. For this actuator, the bound is tight in all the realizations, and we have $\bar{\delta}(u_3) = \delta(u_3) = 1$. Thus, it is enough for the attacker to attack this actuator in order to conduct a perfectly undetectable attack for any realization.

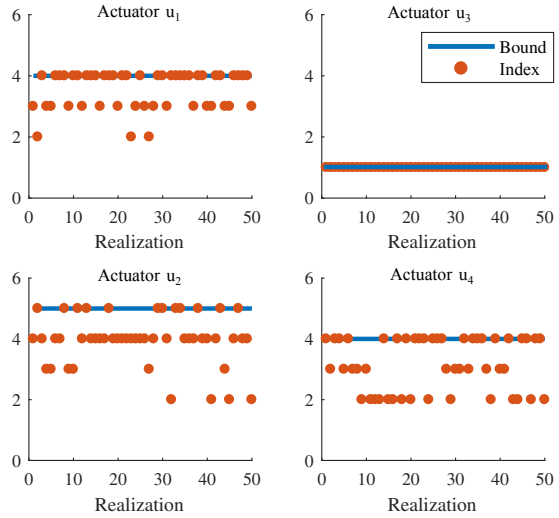

Fig. 2. The values of δ and $\bar{\delta}$ for 50 different realizations of the system.

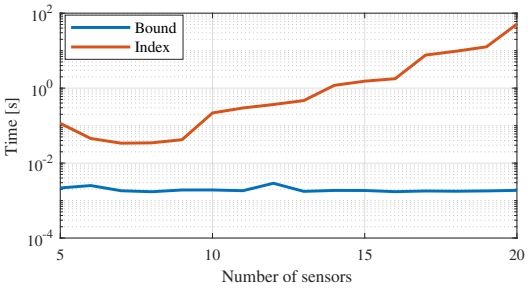

Fig. 3. Computational time required for calculating the security index and the bound for actuator u_4 with respect to the number of sensors.

B. Computational Effort

We now compare the computational efforts needed to calculate $\delta(u_4)$ and $\bar{\delta}(u_4)$. In this experiment, we kept the realization of the system fixed, and varied the number of sensors monitoring the system from 5 to 20 by placing additional sensors at random locations. To calculate $\delta(u_4)$, we performed brute force search through the power set $\mathcal{I}$. For each subset, we used the function $tzero$ implemented in Matlab to check if the condition from Theorem 1 holds. The search was stopped after finding the subset of minimal cardinality that satisfies the condition. To calculate $\bar{\delta}(u_4)$, we used the function $maxflow$, which is also available in Matlab. The results are shown in Figure 3.

As expected, the effort for calculating the security index grows exponentially with the number of components within the system. On the other hand, the effort for calculating the upper bound was almost not affected by the placement of additional sensors, and remained below 10^{-2} [s]. This illustrates that $\bar{\delta}$ can be computed efficiently using well established algorithms.

VII. Conclusion and Future Work

In this paper, we proposed a novel type of security index based on the definition of perfect undetectability. A sufficient and necessary condition that a solution of the problem has to satisfy was derived. The condition can be used to find the index once the system is small scale. Deficiencies of the index for the case of large scale systems were then outlined. Namely, the problem of calculating the index is NP-hard in general, and the index can be fragile with respect to system variations. To overcome the deficiencies, an upper bound was introduced. This bound can be obtained efficiently, by solving a graph min-cut problem. Additionally, since it is based on a structural system model, the bound is not affected by system variations. Finally, differences between the bound and the index were illustrated on a numerical example. The future work will: (1) Investigate tightness of the bound; (2) Consider the problem of placing additional sensors to improve the index, and make the system more secure.

References

[1] A. Olshevsky, "Minimal controllability problems," *IEEE Transactions on Control of Network Systems*, vol. 1, no. 3, pp. 249–258, 2014.

[2] F. L. Cortesi, T. H. Summers, and J. Lygeros, "Submodularity of energy related controllability metrics," in *Proceeding of the 53rd Conference on Decision and Control*, 2014.

[3] F. Pasqualetti, S. Zampieri, and F. Bullo, "Controllability metrics, limitations and algorithms for complex networks," *IEEE Transactions on Control of Network Systems*, vol. 1, no. 1, pp. 40–52, 2014.

[4] V. Tzoumas, M. A. Rahimian, G. J. Pappas, and A. Jadbabaie, "Minimal actuator placement with bounds on control effort," *IEEE Transactions on Control of Network Systems*, vol. 3, no. 1, pp. 67–78, 2016.

[5] A. Clark, L. Bushnell, and R. Poovendran, "On leader selection for performance and controllability in multi-agent systems," in *Proceedings of the 51st Conference on Decision and Control (CDC)*, 2012.

[6] J. Slay and M. Miller, "Lessons learned from the Maroochy water breach," in *Proceedings of the International Conference on Critical Infrastructure Protection*, 2007.

[7] D. Kushner, "The real story of STUXNET," *IEEE Spectrum*, vol. 50, no. 3, pp. 48–53, 2013.

[8] "Analysis of the cyber attack on the Ukrainian power grid," *Electricity Information Sharing and Analysis Center*, 2016.

[9] A. A. Cardenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," *in Proceedings of the 28th International Conference on Distributed Computing Systems Workshops (ICDCS)*, 2008.

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

[11] Y. Mo and B. Sinopoli, "On the performance degradation of cyber-physical systems under stealthy integrity attacks," *IEEE Transactions on Automatic Control*, vol. 61, no. 9, pp. 2618–2624, Sept 2016.

[12] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, Nov 2013.

[13] S. Sundaram and C. N. Hadjicostis, "Distributed function calculation via linear iterations in the presence of malicious agents Part I: Attacking the network," in *Proceedings of the American Control Conference (ACC)*, 2008.

[14] F. Pasqualetti, A. Bicchi, and F. Bullo, "Consensus computation in unreliable networks: A system theoretic approach," *IEEE Transactions on Automatic Control*, vol. 57, no. 1, pp. 90–104, 2012.

[15] O. Vuković, K. Sou, G. Dan, and H. Sandberg, "Network-aware mitigation of data integrity attacks on power system state estimation," *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 6, pp. 1108–1118, 2012.

[16] H. Sandberg, A. Teixeira, and K. Johansson, "On security indices for state estimators in power networks," in *Proceedings of the First Workshop on Secure Control Systems (SCS)*, 2010.

[17] J. M. Hendrickx, K. H. Johansson, R. M. Jungers, H. Sandberg, and K. C. Sou, "Efficient computations of a security index for false data attacks in power networks," *IEEE Transactions on Automatic Control*, vol. 59, no. 12, pp. 3194–3208, 2014.

[18] K. C. Sou, H. Sandberg, and K. H. Johansson, "Electric power network security analysis via minimum cut relaxation," in *Proceedings of the 50th Conference on Decision and Control and European Control Conference*, 2011.

[19] ——, "Computing critical k-tuples in power networks," *IEEE Transactions on Power Systems*, vol. 27, no. 3, pp. 1511–1520, 2012.

[20] O. Kosut, "Max-flow min-cut for power system security index computation," in *Proceedings of the 8th IEEE Sensor Array and Multichannel Signal Processing Workshop (SAM)*, 2014.

[21] Y. Yamaguchi, A. Ogawa, A. Takeda, and S. Iwata, "Cyber security analysis of power networks by hypergraph cut algorithms," *IEEE Transactions on Smart Grid*, vol. 6, no. 5, pp. 2189–2199, 2015.

[22] M. S. Chong and M. Kuijper, "Characterising the vulnerability of linear control systems under sensor attacks using a system's security index," in *Proceedings of the 55th Conference on Decision and Control (CDC)*, 2016.

[23] H. Sandberg and A. M. H. Teixeira, "From control system security indices to attack identifiability," in *Proceedings of the Science of Security for Cyber-Physical Systems Workshop (SOSCYPS)*, 2016.

[24] H. Cam, P. Mouallem, Y. Mo, B. Sinopoli, and B. Nkrumah, "Modeling impact of attacks, recovery, and attackability conditions for situational awareness," in *Proceedings of the IEEE International Inter-Disciplinary Conference on Cognitive Methods in Situation Awareness and Decision Support (CogSIMA)*, 2014.

[25] S. Weerakkody, X. Liu, S. H. Son, and B. Sinopoli, "A graph-theoretic characterization of perfect attackability for secure design of distributed control systems," *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 60–70, 2017.

[26] J.-M. Dion, C. Commault, and J. Van Der Woude, "Generic properties and control of linear structured systems: a survey," *Automatica*, vol. 39, no. 7, pp. 1125–1144, 2003.

[27] M. Stoer and F. Wagner, "A simple min-cut algorithm," *Journal of the ACM (JACM)*, vol. 44, no. 4, pp. 585–591, 1997.

[28] V. Tzoumas, A. Jadbabaie, and G. J. Pappas, "Sensor placement for optimal Kalman filtering: Fundamental limits, submodularity, and algorithms," in *Proceedings of the American Control Conference (ACC)*, 2016.