On Actuator Security Indices

Jezdimir Milošević, Sebin Gracy, and Henrik Sandberg

KTH Royal Institute of Technology, 10044 Stockholm, Sweden
{jezdimir,gracy,hsan}@kth.se

Abstract. Actuator security indices are developed for risk assessment purposes. Particularly, these indices can tell a system operator which of the actuators in a critical infrastructure network are the most vulnerable to cyber-attacks. Once the operator has this information, he/she can focus the security budget to protect these actuators. In this short paper, we first revisit one existing definition of an actuator security index, and then discuss possible directions for future research.

Keywords: Risk Assessment · Cyber-Attacks · Cyber-Physical Systems.

1 Introduction

Actuators are one of the crucial components in controlling critical infrastructure networks. For example, generators in a power grid enable us to use electricity, and pumps in a water distribution network ensure that we have a stable supply of drinkable water. Due to their importance, one should ensure that actuators are secured. Namely, the problem of security of critical infrastructure networks is well recognized [1], and attacks against these networks have already been documented [2, 5]. Hence, one should be able to characterize if the actuators are vulnerable, and if they are, build an effective defence strategy to protect them.

A possible way to characterize the security level of network components is by using security indices. The first security index was introduced to characterize the vulnerability of sensors monitoring a power network [7]. This sensor security index was further analyzed in [4, 10], where it was discussed how to calculate it efficiently. Motivated by the research on sensor security indices, the work [6] proposed a security index that can be used to characterize vulnerability of actuators in a network. In this short paper, we first revisit the actuator security index from [6] in some detail, and illustrate with an example how the index can be used to characterize vulnerability of actuators. We then outline some open problems suitable for future work.

2 Actuator Security Index δ

In this section, we start off by listing the notations, then introduce the model setup, define an actuator security index, and finally conclude by illustrating on an example how to use the index for risk assessment purposes.

Notations

$\mathbb{R}$, $\mathbb{Z}$, $\mathbb{Z}_+$ and $\mathbb{Z}_{\geq 0}$ denote the set of real numbers, integers, positive integers, and non-negative integers, respectively. I_N indicates an identity matrix of size N. $|\mathcal{X}|$ indicates cardinality of a set $\mathcal{X}$. Given two matrices A and B, let $A \odot B$ denote the entrywise product. $[A]_{ij}$ denotes the element corresponding to the i^{th} row and j^{th} column of matrix A.

Model Setup

We first model dynamics of a critical infrastructure network. We use the linear time-invariant model

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

where: $k \in \mathbb{Z}_{\geq 0}$ is a time step; $x(k) \in \mathbb{R}^{n_x}$ is the vector of physical states of the network (such as pressures, temperatures, or power flows); $y(k) \in \mathbb{R}^{n_y}$ is the vector containing measurements collected from the process; $a(k) \in \mathbb{R}^{n_u+n_y}$ is the attack vector. The first n_u elements of a model attacks against the actuators, while the last n_y model attacks against the sensors. Hence, the matrices B_a and D_a have the form $B_a = [B\ \mathbf{0}_{n_x \times n_y}]$, $D_a = [\mathbf{0}_{n_y \times n_u}\ \mathbf{I}_{n_y}]$, where $B \in \mathbb{R}^{n_x \times n_u}$ is assumed to have a full column rank. Note that the matrix W models interaction in between the system states and that the matrix C maps the system states to the sensor measurements.

Let $\mathcal{I} = \{1, \ldots, n_u + n_y\}$ be the set of sensors and actuators, and $\mathcal{I}_a \subseteq \mathcal{I}$ be the set of sensors and actuators controlled by the attacker. The attacker can arbitrarily select the values of the elements of a with the indices from $\mathcal{I}_a$. The elements of a that correspond to non-attacked components $\mathcal{I} \setminus \mathcal{I}_a$ are always equal to zero. Additionally, the attacker possesses full model knowledge, that is, knows the matrices W, B, C. Finally, we assume that the attacker wants to: (i) Attack one of the actuators; (ii) Remain undetected by the operator. To model the second goal, we need a suitable definition of undetectability. In this work, we use the definition of perfect undetectability [13].

Definition 1. *Let $x(0)$=0. The attack $a \neq 0$ is perfectly undetectable if y=0.*

In simple words, the measurements under the attack appear to be the same as in the steady state $x(0) = 0$, that is, $y = 0$. For this reason, perfectly undetectable attacks are potentially very dangerous.

Problem Formulation

We now introduce an actuator security index δ from [8]. By $\delta(i)$, we denote the security index of an actuator $i \in \mathcal{I}$. We define this index to be equal to the minimum number of sensors and actuators that need to be compromised to enable the attacker to conduct a perfectly undetectable attack. Additionally, we

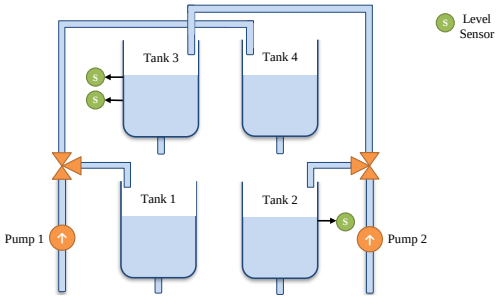

Fig. 1. Quadruple tank process.

impose the constraint that actuator i has to be used in the attack. In this way, we capture a goal or intent by the attacker.

Note that actuators that have small values of δ are considered to be more vulnerable compared to those with high values. Hence, one can use the security index in a risk assessment as a likelihood score of an actuator being attacked [12]. From the defender's perspective, the worst case that can happen is to have $\delta(i)$=1. In this case, an attacker can attack i while remaining perfectly undetectable without compromising any other component.

Let $||a||_0 = |\cup_{k\in\mathbb{Z}_{\geq 0}} \text{supp}(a(k))|$, where $\text{supp}(a(k)) = \{i \in \mathcal{I} : a^{(i)}(k) \neq 0\}$. The problem of calculating security index $\delta(i)$ for an actuator i can then be defined in the following way.

Problem 1. Calculating δ

$$\begin{aligned} \delta(i) := \underset{a}{\text{minimize}} \quad & ||a||_0 \\ \text{subject to} \quad & x(k+1) = Wx(k) + B_a a(k), \\ & 0 = Cx(k) + D_a a(k), \\ & x(0) = 0, \\ & a^{(i)} \neq 0. \end{aligned}$$

Here, we have as the objective to find the minimum number of sensors and actuators to conduct a perfectly undetectable attack. The first two constraints are introduced to ensure that the physical dynamics is according to the model we introduced. The second and the third constraint ensure that the attack signal a is perfectly undetectable. The last constraint implies that actuator i for which we are calculating the security index is actively used in the attack. We now introduce an example to clarify the index.

Example

Consider a quadruple tank process shown in Fig. 1. The plant states x_1–x_4 are the levels in four tanks. There are two actuators in the system: Pump 1 (P_1)

and Pump 2 (P_2). From [11], we know that this process can be modeled by

$$x(k+1) = \begin{bmatrix} 0.975 & 0 & 0.0042 & 0 \\ 0 & 0.977 & 0 & 0.0044 \\ 0 & 0 & 0.958 & 0 \\ 0 & 0 & 0 & 0.956 \end{bmatrix} x(k) + \begin{bmatrix} 0.05155 & 0.0016 & 0 & 0 & 0 \\ 0.0019 & 0.0447 & 0 & 0 & 0 \\ 0 & 0.0737 & 0 & 0 & 0 \\ 0.0850 & 0 & 0 & 0 & 0 \end{bmatrix} a(k),$$

$$y(k) = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} x(k) + \begin{bmatrix} 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 1 \end{bmatrix} a(k).$$

By manipulating P_1, the attacker influences levels in Tank 1, Tank 2, and Tank 4. Since the level in Tank 2 is measured, the attacker needs to attack the corresponding sensor to stay perfectly undetectable. The levels in Tank 1 and Tank 4 are not measured, so the attacker does not need to attack additional components. Hence, the attacker needs to attack only P_1 and the sensor measuring level in Tank 2, so the security index for this actuator is $\delta(P_1) = 2$.

Attacking P_2 is more complex. Namely, this pump influences the levels in Tank 1, Tank 2, and Tank 3. Since the level in Tank 2 is measured by one, and the level in Tank 3 by two sensors, the attacker needs to attack three sensor to ensure perfect undetectability. Thus, the attacker needs to attack P_2 and three sensors, so the security index for this pump is $\delta(P_2) = 4$.

We now move to the next section, where we outline possible extensions of the work on security indices.

3 Actuator Indices Independent of System Parameters

Critical infrastructure networks are complex systems that can change configuration over time. Take for example power grids. There, micro-grids can detach from the grid to form separate grid [9] or power lines may be turned of due to maintenance or due to damage [3]. Hence, the matrices W, B_a, C, and D_a can change over time. Note that changing the coefficients in the system matrices might result in a change in the value of $\delta(i)$. To overcome this limitation, one could take recourse to structured systems theory. More specifically, the objective in such a setting would be to obtain a lower bound on $\delta(i)$ that is impervious to variations in system parameters. In some sense, if this lower bound is sufficiently high, then one can be certain that the system is secure for almost all realizations. In the rest of this section, we will focus on introducing this idea.

Problem Statement

Let $\mathcal{W}$ (resp. $\mathcal{B}_a$, $\mathcal{C}$, $\mathcal{D}_a$) denote structured matrices that obey the pattern of imposed zeros of W (resp. B_a, C, D_a). That is, fixed zeros in W (resp. B_a, C, D_a) would be denoted by zeros in $\mathcal{W}$ (resp. $\mathcal{B}_a$, $\mathcal{C}$, $\mathcal{D}_a$), while positions that are not fixed to zero in W (resp. B_a, C, D_a) would be represented by a parameter in $\mathcal{W}$ (resp. $\mathcal{B}_a$, $\mathcal{C}$, $\mathcal{D}_a$). Note that all such parameters are *free* parameters (i.e.,

real-valued parameters that can be chosen arbitrarily). The interpretation is as follows: the fixed zero positions denote interactions that are prohibited, while parameters represent the intensity of existing interactions. With respect to the Example depicted in Figure 1, $\mathcal{W}$ and B_a are given by

$$\mathcal{W} = \begin{bmatrix} w_{11} & 0 & w_{13} & 0 \\ 0 & w_{22} & 0 & w_{24} \\ 0 & 0 & w_{33} & 0 \\ 0 & 0 & 0 & w_{44} \end{bmatrix}, \qquad \mathcal{B}_a = \begin{bmatrix} b_{a_{11}} & b_{a_{12}} & 0 & 0 & 0 \\ b_{a_{21}} & b_{a_{22}} & 0 & 0 & 0 \\ 0 & b_{a_{32}} & 0 & 0 & 0 \\ b_{a_{41}} & 0 & 0 & 0 & 0 \end{bmatrix}.$$

The matrices $\mathcal{C}$ and $\mathcal{D}_a$ can be written analogously.

Each numerical choice of free parameters yields a realization $\{W, B_a, C, D_a\}$. Let $\{\mathcal{W}, \mathcal{B}_a, \mathcal{C}, \mathcal{D}_a\}$ denote the family of all linear time-invariant (LTI) systems $\{W, B_a, C, D_a\}$ having dynamics as given in (1). The main objective is to provide a bound on $\delta(i)$, say γ (where $\gamma \in \mathbb{Z}_{>0}$) such that for *almost all* [1] realizations $\{W, B_a, C, D_a\} \in \{\mathcal{W}, \mathcal{B}_a, \mathcal{C}, \mathcal{D}_a\}$, $\delta(i) \geq \gamma$. A secondary objective is to seek strategies so as to increase γ. The rationale being the following: the higher the value of γ, the more secure actuator i is, since $\delta(i)$ becomes larger.

Note that addressing our main objective essentially translates to solving Problem 1 for almost all realizations $\{W, B_a, C, D_a\} \in \{\mathcal{W}, \mathcal{B}_a, \mathcal{C}, \mathcal{D}_a\}$, as opposed to a specific realization. However, this might be a rather cumbersome route towards achieving our goals, since for large-scale networks Problem 1 is NP-hard (see, Theorem 1 in [6]). This motivates us to seek alternative approaches.

Alternative Approach: Graph Theory

Structured system (1) can be described by a graph as explained in the following. Let $X = \{x_1, x_2, \ldots, x_{n_x}\}$, $Y = \{y_1, y_2, \ldots, y_{n_y}\}$, and $A = \{a_1, a_2, \ldots, a_{n_u+n_y}\}$ denote the set of state vertices, actuator vertices, output vertices, and attack vertices, respectively. We define by: $\mathcal{E}_W = \{(x_j, x_i) \mid \mathcal{W}_{ij} \neq 0\}$ the edges in between the state nodes; $\mathcal{E}_{B_a} = \{(a_j, x_i) \mid \mathcal{B}_{a_{ij}} \neq 0\}$ the edges in between the attack and state nodes; $\mathcal{E}_C = \{(x_j, y_i) \mid \mathcal{C}_{ij} \neq 0\}$ the edges in between the states and measurements; $\mathcal{E}_{D_a} = \{(a_j, y_i) \mid \mathcal{D}_{a_{ij}} \neq 0\}$ the edges in between the attack and measurement nodes. The graph associated with the system (1) can then be defined as $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where $\mathcal{V} = X \cup A \cup Y$ and $\mathcal{E} = \mathcal{E}_W \cup \mathcal{E}_{B_a} \cup \mathcal{E}_C \cup \mathcal{E}_{D_a}$.

Our approach towards addressing the aforementioned problem can be crystallized as follows. Given that we have knowledge of the underlying graph $\mathcal{G}$ and also of the set of attacked actuators and sensors $\mathcal{I}$: (i) Find graph-theoretic conditions which ensure that, for actuator i, for almost all choices of edge weights in $\mathcal{G}$, $\delta(i) \geq \gamma$; (ii) If possible, modify the graph $\mathcal{G}$ (for instance, by adding or deleting suitable edges) such that γ is increased.

[1] There might exist realizations $\{W^1, B_a^1, C^1, D_a^1\} \in \{\mathcal{W}, \mathcal{B}_a, \mathcal{C}, \mathcal{D}_a\}$, for which $\delta(i) < \gamma$. However, all such realizations would lie on a set of Lebesgue measure zero in the space of free parameters in $\mathcal{W}$, $\mathcal{B}_a$, $\mathcal{C}$ and $\mathcal{D}_a$. Hence, instead of ensuring that for *every* realization $\delta(i) \geq \gamma$, we seek to ensure for almost all realizations, $\delta(i) \geq \gamma$

4 Conclusions

This work revisited the security index that can be used to measure vulnerability of actuators in a network, and illustrated in an example how this index can be used for risk assessment purposes. We then outlined possible directions for future research. Namely, since critical infrastructure networks are changing over time, and the security indices are fragile in terms of system variations, we plan to define novel security indices that are not fragile with respect to the aforementioned changes. Particularly, structured system theory seems to be a promising approach to analyze and efficiently calculate novel types of security indices.

Acknowledgments. This work was supported by the Swedish Civil Contingencies Agency through the CERCES project, the Swedish Research Council (grant 2016-0861), and the EU-project LarGo!

References

1. Guide to increased security in industrial information and control systems. Swedish Civil Contingencies Agency (MSB) (2014)
2. Analysis of the cyber attack on the Ukrainian power grid. Electricity Information Sharing and Analysis Center (2016)
3. Amin, M., Schewe, P.F.: Preventing blackouts. Scientific American **296**(5) (2007)
4. Hendrickx, J.M., Johansson, K.H., Jungers, R.M., Sandberg, H., Sou, K.C.: Efficient computations of a security index for false data attacks in power networks. IEEE Transactions on Automatic Control **59**(12), 3194–3208 (2014)
5. Kushner, D.: The real story of STUXNET. IEEE Spectrum **50**(3), 48–53 (2013)
6. Milosevic, J., Texeira, A., Johansson, K.H., Sandberg, H.: Actuator security indices based on perfect undetectability: Computation, robustness, and sensor placement. CoRR **abs/1807.04069** (2019), http://arxiv.org/abs/1807.04069
7. Sandberg, H., Teixeira, A., Johansson, K.: On security indices for state estimators in power networks. In: Proceedings of the First Workshop on Secure Control Systems (2010)
8. Sandberg, H., Teixeira, A.M.H.: From control system security indices to attack identifiability. In: Proceedings of the Science of Security for Cyber-Physical Systems Workshop (2016)
9. Simpson-Porco, J.W., Dörfler, F., Bullo, F.: Synchronization and power sharing for droop-controlled inverters in islanded microgrids. Automatica **49**(9) (2013)
10. Sou, K.C., Sandberg, H., Johansson, K.H.: Computing critical k-tuples in power networks. IEEE Transactions on Power Systems **27**(3), 1511–1520 (2012)
11. Teixeira, A.: Toward cyber-secure and resilient networked control systems. Ph.D. thesis, KTH Royal Institute of Technology (2014)
12. Teixeira, A., Sou, K.C., Sandberg, H., Johansson, K.H.: Secure control systems: A quantitative risk management approach. IEEE Control Systems Magazine **35**(1), 24–45 (2015)
13. Weerakkody, S., Liu, X., Son, S.H., Sinopoli, B.: A graph-theoretic characterization of perfect attackability for secure design of distributed control systems. IEEE Transactions on Control of Network Systems **4**(1), 60–70 (2017)