Katz Centrality-based Security in Large-Scale Networks

Anh Tung Nguyen, Sribalji C. Anand, André M. H. Teixeira

***Abstract*— This paper investigates the security challenges of continuous-time networked control systems represented by digraphs under stealthy data injection attacks. More specifically, the adversary injects false data into the information sent from these specific nodes to their neighbors. Meanwhile, a defender monitors several nodes to impose stealthiness constraints on the adversary's actions, thereby minimizing the network performance loss. We analyze the worst-case network performance loss of these stealthy attacks and show its direct connection to the Katz centrality measure of networks. The connection provides an intuitive security analysis based on the Katz centrality without solving optimization problems, suiting large-scale networks.**

I. Introduction

Control systems are deeply integrated into various critical infrastructures, such as power grids, transportation systems, and water distribution networks. Due to their large supply to society, they are divided into smaller parts to be managed efficiently. These parts often rely on open communication technologies to share their operating information, including public Internet and wireless networks, which leave them vulnerable to cyber threats. The potential consequences of such vulnerabilities are both significant and far-reaching, impacting finances and public safety. Notable examples include the devastating effects of the Stuxnet malware on an Iranian industrial system in 2010, the Havex Trojan malware on European infrastructure utilities in 2014, the Industroyer attack on Ukraine's power grid in 2016, and the thwarted Triton-like malware on Israeli water distribution network in 2020. More reported attacks can be found in [1]. As a result, ensuring the security of control systems has become a matter of critical importance.

In this paper, we consider a continuous-time networked control system, associated with a strongly connected digraph, under stealthy attacks. The system consists of several interconnected one-dimensional subsystems, known as nodes in the digraph. The adversary aims to degrade the network performance maximally by selecting several specific nodes to carry out stealthy data injection attacks, targeting the information transmitted from these nodes to their neighbors. In contrast, a defender monitors the outputs of some nodes, which imposes a stealthiness condition on the adversary's actions, aiming to minimize the network performance loss. The security problem outlined above is illustrated in Figure 1.

This work is supported by the Swedish Research Council under the grant 2021-06316, 2024-00185 and by the Swedish Foundation for Strategic Research.

Anh Tung Nguyen and André M. H. Teixeira are with the Department of Information Technology, Uppsala University, Sweden. Sribalaji C. Anand is with the School of Electrical Engineering and Computer Science, KTH Royal Institute of Technology, Sweden.

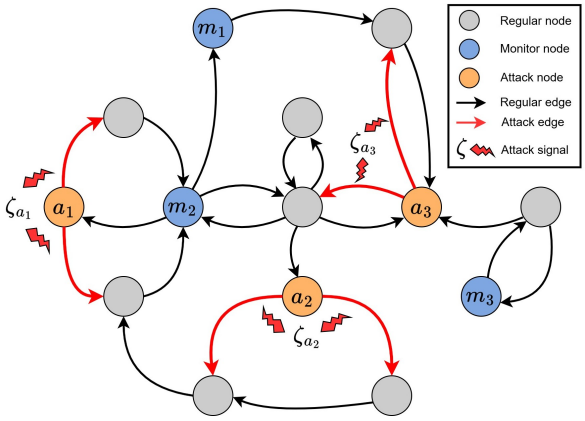

Fig. 1: A networked control system under stealthy data injection attacks. An adversary injects attack signals into the information sent from orange nodes to their neighbors while a defender monitors the outputs of blue nodes.

In the following section, We study the network performance loss of stealthy positive data injection attacks and show its direct connection to the Katz centrality measure of the network [2].

II. Problem Formulation

A. Adversary model

The adversary selects exactly α ($\alpha \leq N$) nodes on which to conduct false data injection attacks on the information sent from these α attack nodes to their neighbors (the orange nodes in Figure 1). More specifically, these α nodes are not directly affected by attacks, but their neighboring nodes are. Henceforth, these α nodes are called attack nodes which are defined in the following.

Definition 1 (Attack nodes): Given a digraph $\mathcal{G} \triangleq (\mathcal{V}, \mathcal{E}, A, \Theta)$, a node $a \in \mathcal{V}$ is called an attack node if the information sent from this node to all their neighbors is maliciously manipulated by the same attack signal. $\triangleleft$

Let us denote a set of α attack nodes as follows: $\mathcal{A} \triangleq \{a_1, a_2, \ldots, a_\alpha\} \subset \mathcal{V}$. For each attack node $a_i \in \mathcal{A}$, the adversary designs an additive attack signal $\zeta_{a_i}(t)$ into the information sent from the attack node a_i to all its neighbors, which is assumed to be positive and have bounded energy: $\|\zeta_{a_i}\|^2_{\mathcal{L}_2[0,\infty]} \leq E^2 < \infty$, $\forall a_i \in \mathcal{A}$. where the maximum attack energy E is given.

B. Defender model

To get prepared for facing malicious activities, the defender selects a subset of the node set $\mathcal{V}$ as a set of monitor nodes, denoted as $\mathcal{M} = \{m_1, m_2, \ldots, m_{|\mathcal{M}|}\} \subset \mathcal{V}$. More specifically, the defender monitors the following output

measurements: $y_m(t) = e_m^\top x(t), \quad \forall\, m \in \mathcal{M}$. At each monitor node $m \in \mathcal{M}$, a corresponding alarm threshold $\delta_m \in \mathbb{R}_{>0}$ is assigned. The defender detects the presence of the adversary if the output energy for a given time horizon $[0, H]$ of at least one monitor node crosses its corresponding alarm threshold, i.e., $\|y_m\|^2_{\mathcal{L}_2[0,H]} > \delta_m^2$.

C. Networks under attack

The network under false positive data injection attacks can be described as follows:

$$\dot{x}^a(t) = -Lx^a(t) + B_{\mathcal{A}}\zeta(t), \tag{1}$$
$$p^a(t) = Wx^a(t), \tag{2}$$
$$y_m^a(t) = e_m^\top x^a(t),\ \forall m \in \mathcal{M}, \tag{3}$$

where p^a is the performance output of the network. The main purpose of the adversary is to maximally disrupt this performance output while remaining stealthy to the defender, which is formulated as follows:

$$\begin{aligned} Q(\mathcal{M}, \mathcal{A}) \triangleq \sup_{\zeta}\ & \|p^a\|^2_{\mathcal{L}_2} \\ \text{s.t. } & (1)-(3),\ x^a(0) = 0,\ x^a(\infty) = 0, \\ & \|y_m^a\|^2_{\mathcal{L}_2} \le \delta_m^2,\ \forall\, m \in \mathcal{M}, \\ & \left\|e_j^\top \zeta\right\|^2_{\mathcal{L}_2} \le E^2,\ \forall\, j \in \{1, 2, \ldots, \alpha\}. \end{aligned} \tag{4}$$

In the next section, we study the worst-case disruption (4) and address the following problem

Problem 1: Given a digraph $\mathcal{G}$ describing the system under attacks (1)-(3), the worst-case disruption (4), provide a graph-theoretic selection of an optimal pair $(\mathcal{M}, \mathcal{A})$. ◁

III. Katz Centrality-based Security Assessment

Let us introduce a modified version of the Katz centrality measure [2] in the following:

Definition 2 (Katz-like centrality measure): Given a digraph $\mathcal{G}$ with an adjacency matrix A and an in-degree matrix D_{in}, the monitor Katz-like centrality matrix K_δ and the performance Katz-like centrality matrix K_W are defined as:

$$K_\delta \triangleq \mathbf{diag}(E^{-1}\delta)^{-1} \sum_{i=1}^{\infty} (D_{in}^{-1}A)^i, \tag{5}$$

$$K_W \triangleq W \sum_{i=1}^{\infty} (D_{in}^{-1}A)^i. \tag{6}$$

Now, we are ready to present the Katz centrality-based security assessment with the help of [3, Lemmas 2-3] and [4, Theorem 1] in the following theorem for the single node selection.

Theorem 1 (Katz centrality-based disruption comparison): Consider the worst-case disruption (4) with a fixed single attack node $\mathcal{A} = \{a_i\}$, two monitor sets $\mathcal{M}_i = \{m_i\}$ and $\mathcal{M}_j = \{m_j\}$, and the monitor Katz-like centrality matrix K_δ defined in (5). If,

$$e_{m_i}^\top K_\delta e_{a_i} \ge e_{m_j}^\top K_\delta e_{a_i}, \tag{7}$$

then,

$$Q(m_i, a_i) \le Q(m_j, a_i). \tag{8}$$

Algorithm 1 Sub-optimal monitor nodes

Output: Optimal monitor nodes $\{m_1^\star, m_2^\star, \ldots, m_\alpha^\star\}$.
Input: Set of attack nodes $\mathcal{A} = \{a_1, a_2, \ldots, a_\alpha\}$, in-degree Laplacian matrix L, weighting factor W, alarm threshold δ, maximum attack energy E.

1: Compute K_δ in (5)
2: **for** $a_i \in \mathcal{A}$ **do**
3: Find $m_i^\star$ such that $e_{m_i^\star}^\top K_\delta e_{a_i}$ is minimized.
4: **end for**

By using the following relation

$$Q(\mathcal{M}, \mathcal{A}) \le \sum_{(a_i, m_i) \in \mathcal{A} \times \mathcal{M}} Q(m_i, a_i). \tag{9}$$

we leverage the result of Theorem 1 to introduce Algorithm 1 to find the sub-optimal selection of nodes for the defender and the adversary.

IV. Simulation Results

We validate the obtained results through the Nordic490 transmission power grid (see Fig. 2 left). To validate theoretical results, we compute the optimal nodes by using Theorem 1 and Algorithm 1, which are compared to solving SDP in [3]. The numerical results are reported in the right-hand side of Fig. 2 where the top plot shows the comparisons of single-node cases and the bottom plot depicts the comparisons of multi-node scenarios. These numerical results show us that the optimal single monitor node can be found exactly while only sub-optimal monitor nodes are found using Algorithm 1.

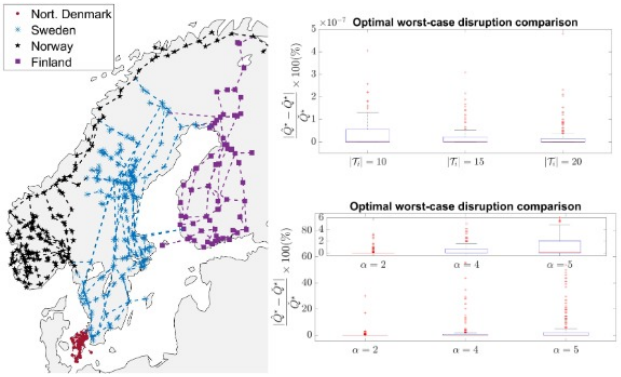

Fig. 2: Nordic490 power transmission grid (left) and simulation results (right)

References

[1] T. Miller, A. Staves, S. Maesschalck, M. Sturdee, and B. Green, "Looking back to look forward: Lessons learnt from cyber-attacks on industrial control systems," *International Journal of Critical Infrastructure Protection*, vol. 35, p. 100464, 2021.

[2] L. Katz, "A new status index derived from sociometric analysis," *Psychometrika*, vol. 18, no. 1, pp. 39–43, 1953.

[3] A. T. Nguyen, S. C. Anand, and A. Teixeira, "Scalable and optimal security allocation in networks against stealthy injection attacks," *arXiv preprint arXiv:2411.15319*, 2024.

[4] A. Rantzer, "On the Kalman-Yakubovich-Popov lemma for positive systems," *IEEE Trans. Automat. Contr.*, vol. 61, no. 5, pp. 1346–1349, 2015.