Impact of Signal Delay Attack on Voltage Control for Electrified Railways

Hoang Hai Nguyen[1] Rui Tan[1] David K. Y. Yau[1,2]
[1]Advanced Digital Sciences Center, Illinois at Singapore [2]Singapore University of Technology and Design

***Abstract*—Cybernated traction power system can be an attractive leverage for attackers who aim to cause catastrophic safety incidents in electrified railways. This paper studies the cybersecurity risks of the traction power voltage control system that regulates the voltages of railway feeder substations. We derive the stability condition of the control system when it is under a *signal delay attack*, i.e., the timing information of voltage measurements is maliciously corrupted so that the system wrongly uses old measurements to make control decisions. Our analysis and simulations show a fundamental trade-off between the voltage convergence speed when trains' reactive power draw varies and the tolerable malicious time delay in terms of system stability.**

I. Introduction

Electrified railways are evolving in the direction of cyber-physical systems due to the increasing adoption of modern information and communication technologies. However, the involved cyber components can make them vulnerable to cyber-attacks, potentially leading to catastrophic consequences. Exemplified by the Dragonfly viruses [1] and Stuxnet worms [2], crafty attacks against critical infrastructures bypass the air gaps first, penetrate the corporate networks via stolen credentials and zero-day exploits, and finally disrupt the industrial control systems that directly interact with the physical plants. In this paper, we study the cybersecurity risks of the voltage control for electrified railways, which is a networked closed-loop control system that maintains the railway feeder substations' voltages at a nominal value. A voltage deviation caused by the malfunction of the control system will trigger protective actions such as traction power disconnection and may even lead to serious safety incidents. For instance, a voltage drop was precedent to the 2014 Moscow Metro derailment that caused 24 dead and 160 injured [3]. Although this incident was not caused by a cyber-attack, it strongly suggests the importance of understanding the cybersecurity of electrified railway voltage control for the design of adequate defenses.

A major fraction of railways are electrified by alternating current power systems with voltage nominals from 6.25 kV to 50 kV [4]. These railways draw power from geographically distributed feeder substations connected to utility grids or dedicated traction power networks. Trains, which can be considered motor loads, consume significantly variable reactive power depending on their velocities, leading to feeder voltage deviations from the nominal if no regulatory controls are applied [5]. In this paper, we consider the regulation of feeder voltages by controlling the voltage outputs of generating stations in a utility grid or a dedicated traction power network, which is a basic means of voltage control [6]. Specifically, the control system determines the voltage outputs of generating stations based on the measurements of voltage sensors in the railway feeder substations. These sensors, which operate autonomously without close human supervision, and their long-range communication links to the centralized voltage controller can be attractive exploits to cyber-attackers. In this paper, we consider a generic integrity attack called *signal delay attack* that corrupts timing information of sensor measurements such that the voltage controller will use old measurements to make control decisions. Such an attack can be accomplished by less effort-intensive techniques, e.g., by compromising the time synchronization of sensors. Note that the two common time synchronization systems, i.e., NTP and GPS, have been shown to be vulnerable to realistic attack methods [7], [8].

978-1-4799-8641-5/15/$31.00

In this paper, we adopt a control-theoretic approach to deriving the stability condition of the voltage control system in the presence of a signal delay attack. A destabilized system caused by the attack will experience safety-threatening voltage oscillations. We analyze the critical stability boundary defined by a key parameter of the voltage control algorithm and the time delay introduced by the attacker. The result shows a fundamental trade-off between the voltage convergence speed when trains' reactive power draw varies and the tolerable malicious time delay in terms of system stability. This result can be used by the system designer to achieve a satisfactory trade-off in practice.

II. Railway Feeder Voltage Control

This section presents a model of the railway feeder voltage control system. Notation: x' denotes the first derivative of x with respect to time t; if x is sampled with a period of T, let $x[n]$ denote the n^{th} sample and define $\dot{x}[n] = x[n] - x[n-1]$; we use $\dot{x}$ for $\dot{x}[n]$ when n is clear; $\|\cdot\|$ represents cardinality; $j = \sqrt{-1}$; $\mathbf{I}$ is an identity matrix; $\mathbf{0}$ is a zero matrix.

We consider a traction power network with N buses. Let $\mathbb{F}$ and $\mathbb{G}$ denote the sets of feeder buses and generator buses, respectively. Assume that the $(i,k)^{\text{th}}$ element of the nodal admittance matrix of the traction power network is $Y_{ik} = G_{ik} + jB_{ik}$. For bus i, let V_i, V_{i0}, and θ_i denote its voltage magnitude, voltage nominal value, and voltage angle, respectively. Define $\theta_{ik} = \theta_i - \theta_k$. The net reactive power entering the network at bus i is $Q_i = \sum_{k=1}^{N} V_i V_k (G_{ik}\sin\theta_{ik} - B_{ik}\cos\theta_{ik})$ [9, p. 330]. By assuming that θ_{ik} is fixed, the first derivative of the above model around the nominals can be approximated by $Q_i' \simeq \sum_{k=1}^{N} C_{ik}\,(V_i' V_k + V_i V_k')$, where $C_{ik} = G_{ik}\sin\theta_{ik} - B_{ik}\cos\theta_{ik}$. Discretizing the above equation by $Q_i' \simeq \dot{Q}_i/T$, $V_i' \simeq \dot{V}_i/T$, and $V_k' \simeq \dot{V}_k/T$ yields $\dot{Q}_i \simeq \sum_{k=1}^{N} C_{ik}V_{k0}\dot{V}_i + C_{ik}V_{i0}\dot{V}_k$. Thus, for all the feeder buses, $\dot{\mathbf{q}}_F \simeq \mathbf{A}\dot{\mathbf{v}}_F + \mathbf{B}\dot{\mathbf{v}}_G$, where $\mathbf{A} \in \mathbb{R}^{\|\mathbb{F}\|\times\|\mathbb{F}\|}$ and $\mathbf{B} \in \mathbb{R}^{\|\mathbb{F}\|\times\|\mathbb{G}\|}$ are constant matrices, $\dot{\mathbf{q}}_F$ is a column vector

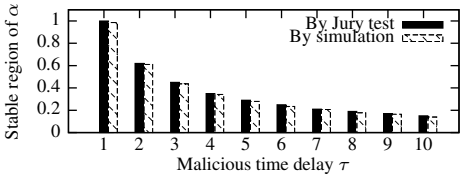

Fig. 1. Stable region of α vs. malicious time delay τ.

of $\dot{Q}_i$ where $i \in \mathbb{F}$, $\dot{\mathbf{v}}_F$ is a column vector of $\dot{V}_i$ when $i \in \mathbb{F}$, and $\dot{\mathbf{v}}_G$ is a column vector of $\dot{V}_i$ when $i \in \mathbb{G}$. By denoting the control variable $\mathbf{u} = \dot{\mathbf{v}}_G$ and the state variable $\mathbf{x} = \mathbf{v}_F$, we have $\dot{\mathbf{x}} \simeq -\mathbf{A}^{-1}\mathbf{B}\mathbf{u} + \mathbf{A}^{-1}\dot{\mathbf{q}}_F$. The term $\mathbf{A}^{-1}\dot{\mathbf{q}}_F$ captures the varying reactive power draw of trains, which can be considered a natural disturbance to the system. In other words, voltage control aims to maintain $\mathbf{x}$ at the nominal value $\mathbf{x}_0$ in the presence of changing $\mathbf{q}_F$. Thus, the system dynamics is

$$\dot{\mathbf{x}}[n] \simeq \mathbf{C}\mathbf{u}[n], \tag{1}$$

where $\mathbf{C} = -\mathbf{A}^{-1}\mathbf{B} \in \mathbb{R}^{\|\mathbb{F}\| \times \|\mathbb{G}\|}$ is a constant matrix. To simplify the discussion, we choose $\mathbb{G}$ such that $\|\mathbb{G}\| = \|\mathbb{F}\|$ and $\mathbf{C}$ has full rank. It is easy to prove by control theory [10] that the following control algorithm stabilizes the system:

$$\mathbf{u}[n] = \alpha\mathbf{C}^{-1}(\mathbf{x}_0 - \mathbf{x}[n]), \text{ where } 0 < \alpha < 2. \tag{2}$$

This algorithm has been widely used in practice [11], [6].

III. Impact of Signal Delay Attack

Under a signal delay attack, a sensor measurement vector that has been delayed for τ time periods is used to determine $\mathbf{u}$. Specifically, the control law in Eq. (2) becomes

$$\mathbf{u}[n] = \alpha\mathbf{C}^{-1}(\mathbf{x}_0 - \mathbf{x}[n-\tau]). \tag{3}$$

Such an attack can be accomplished by maliciously drifting sensors' clocks ahead, which is not impossible due to vulnerabilities of time synchronization systems [7], [8]. We now analyze the stability condition of the system controlled by Eq. (3). Define $\mathbf{y}_i[n] = \mathbf{x}[n-i] - \mathbf{x}_0$ where $i \in [0, \tau]$, and $\mathbf{y}[n] = [\mathbf{y}_0[n], \mathbf{y}_1[n], \ldots, \mathbf{y}_\tau[n]]^\intercal$. By substituting $\mathbf{y}$ into Eq. (1) and Eq. (3), we have $\mathbf{y}[n+1] = \mathbf{G}\mathbf{y}[n]$, where

$$\mathbf{G} = \begin{bmatrix} \mathbf{I} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & -\alpha\mathbf{I} \\ \mathbf{I} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} \\ \mathbf{0} & \mathbf{I} & \mathbf{0} & \cdots & \mathbf{0} & \mathbf{0} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \mathbf{0} & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{I} & \mathbf{0} \end{bmatrix} \in \mathbb{R}^{(\tau+1)\|\mathbb{F}\| \times (\tau+1)\|\mathbb{F}\|}.$$

From control theory [10], if the eigenvalues of $\mathbf{G}$ lie inside the unit circle, the system is asymptotically stable. The eigenvalues are the roots of $\det(\mathbf{G} - \lambda\mathbf{I}) = \left((1 - \lambda + \frac{-\alpha}{\lambda^\tau})(-\lambda)^\tau\right)^{\|\mathbb{F}\|} = 0$. Thus, the non-zero eigenvalues of $\mathbf{G}$ are the roots of

$$\lambda^{\tau+1} - \lambda^\tau + \alpha = 0. \tag{4}$$

However, it is difficult to derive the closed-form roots of Eq. (4). The Jury test [10, p. 185] can be applied to test the stability using Eq. (4) without explicitly solving its roots. Fig. 1 shows the region of α that ensures the system's stability under different settings of τ. We can see that the stable region of α shrinks with τ. We note that, in the absence of attack, the closed-loop system has a single eigenvalue of $(1 - \alpha)$. From control theory, the closer this eigenvalue is from the origin (i.e., the α is closer to 1), the faster the system converges. Note that the convergence speed is important for adapting to fast time-varying reactive power consumption of trains. Thus, from Fig. 1, we can see a trade-off between the voltage convergence speed when trains' reactive power draw varies and the tolerable malicious time delay in terms of system stability.

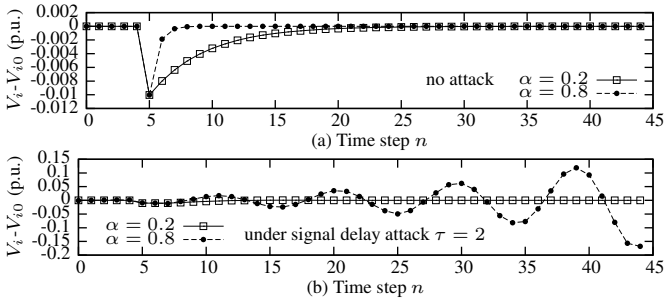

Fig. 2. Voltage deviation at a feeder when (a) no attack and (b) the system is under signal delay attack.

IV. Simulations

This section illustrates the trade-off discussed in Section III by simulations conducted in PowerWorld [12], a high-fidelity power system simulator. The simulated traction power network consists of 10 generators and 37 buses, in which 10 buses are railway feeder substations under voltage control. The matrix $\mathbf{C}$ in Eq. (1) is obtained by least squares. We implement the control algorithm in Eq. (2). Fig. 2(a) shows the evolution of the voltage deviation at a feeder in per unit (p.u.) when there is a step change of the reactive power consumption of all the trains at the 5^{th} time step. We can see that with a larger α, the feeder voltage converges faster. Fig. 2(b) shows the result when the sensor measurements are under a signal delay attack with $\tau = 2$. We can see that, with $\alpha = 0.2$, the feeder voltage deviation remains at around zero after the step change. However, with $\alpha = 0.8$, the feeder voltage oscillates and diverges. We note that the settings $\alpha = 0.2$ and $\alpha = 0.8$ fall into the stable and unstable regions of our numeric results in Fig. 1 when $\tau = 2$. Similar results can be observed for the other 9 feeder buses.

The approximations made in Section II to obtain the linear model in Eq. (1) may affect the accuracy of the stability analysis. We run extensive simulations to evaluate the stability conditions obtained by the Jury test. Note that a system is classified unstable if divergence is detected as in Fig. 2(b). The stability conditions obtained by simulations are shown in Fig. 1, which are consistent with the Jury test results.

V. Conclusion and Future Work

This paper studies the stability condition of railway feeder voltage control systems in the presence of a signal delay attack. The result shows a fundamental trade-off between the voltage convergence speed when trains' reactive power draw varies and the tolerable malicious time delay in terms of system stability. In our future work, we will study early attack detection and follow-up attack mitigation.

ACKNOWLEDGMENT

This work was supported in part by the National Research Foundation (NRF), Prime Minister's Office, Singapore, under its National Cybersecurity R&D Programme (Award No. NRF2014NCR-NCR001-31) and administered by the National Cybersecurity R&D Directorate, and in part by the research grant for the Human-Centered Cyber-physical Systems Programme at the Advanced Digital Sciences Center from Singapore's Agency for Science, Technology and Research (A*STAR).

REFERENCES

[1] "Hackers infiltrated power grids," http://recode.net/2014/07/01/hackers-infiltrated-power-grids-in-us-spain/.

[2] R. Langner, "Stuxnet: Dissecting a cyberwarfare weapon," *IEEE Security Privacy*, vol. 9, no. 3, pp. 49–51, 2011.

[3] "Deadly derailment in moscow metro," http://www.themoscowtimes.com/article/503479.html.

[4] "25kV AC railway electrification," https://en.wikipedia.org/wiki/25_kV_AC_railway_electrification.

[5] J. Kilter, T. Sarnet, and T. Kangro, "Modelling of high-speed electrical railway system for transmission network voltage quality analysis: Rail baltic case study," in *Electric Power Quality and Supply Reliability Conference*, 2014.

[6] P. Kundur, N. J. Balu, and M. G. Lauby, *Power system stability and control*. McGraw-hill New York, 1994.

[7] "Multiple vulnerabilities in NTP," https://blogs.oracle.com/sunsecurity/entry/multiple_vulnerabilities_in_network_time.

[8] T. Nighswander, B. Ledvina, J. Diamond, R. Brumley, and D. Brumley, "GPS software attacks," in *CCS*, 2012.

[9] J. J. Grainger and W. D. Stevenson, *Power system analysis*. McGraw-Hill New York, 1994, vol. 621.

[10] K. Ogata, *Discrete-time control systems*. Prentice-Hall, 1995.

[11] J. P. Paul and J. Y. Leost, "Improvements of the secondary voltage control in france," in *The IFAC Symposium*, 1986, pp. 83–88.

[12] "PowerWorld (version 18)," http://www.powerworld.com/.