2019 12th Asian Control Conference (ASCC)
Kitakyusyu International Conference Center
Japan, June 9-12, 2019

Stealthiness of Attacks and Vulnerability of Stochastic Linear Systems

Tianju Sui, Damian Marelli, Ximing Sun, Minyue Fu

***Abstract*—The security of Cyber-physical systems has been a hot topic in recent years. There are two main focuses in this area: Firstly, what kind of attacks can avoid detection, i.e., the stealthiness of attacks. Secondly, what kind of systems can stay stable under stealthy attacks, i.e., the invulnerability of systems. In this paper, we will give a detailed characterization for stealthy attacks and detection criterion for such attacks. We will also study conditions for the vulnerability of a stochastic linear system under stealthy attacks.**

***Index Terms*—Stochastic Linear Systems, Stealthy Attacks, Vulnerability, Cyber-security.**

I. Introduction

With the fast development of intelligent manufacturing, more and more Cyber-Physical Systems (CPSs) are deployed, such as sensor networks, transportation systems and smart grids[1]. A CPS mainly consists of two components [2], a physical process and a cyber system, see Figure 1.

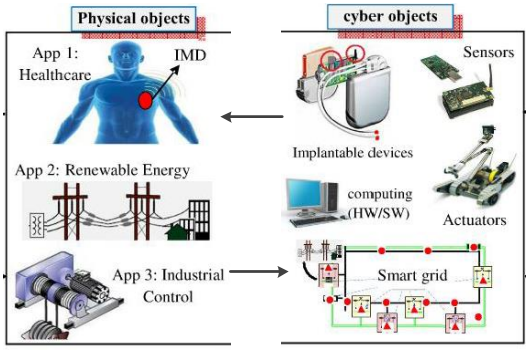

Fig. 1. The configuration of CPSs.

In a CPS, the physical process is controlled and monitored by network devices, which are small devices with basic wireless capabilities [3]. Better interaction between physical and cyber system results in better performance and stability. CPS plays a major role in many applications including, medical devices, traffic control and safety measures, automotive systems, energy efficiency[4] and environmental controls, instrumentation, critical infrastructures and many defense and smart systems. Such a system combines a physical system with network technology to greatly improve the efficiency of the system. But at the same time, this combination gives the probability for attacker to tamper the security [5], [6], [7].

The Stunex attack is one of the highlighted CPS attacks [8]. It is reported that an exquisitely designed virus was injected into the Bushehr nuclear power plant through a USB flash disk. The virus injected a stealthy input signals to accelerate the centrifuges to self destruction, whereas the traditional fault detection algorithm embedded in the nuclear power plant failed to detect it. This incident was reported to have caused a series of disastrous effects and destroyed over 3000 centrifuges [8]. It should be aware that CPS attacks like Stunex attack can not be guarded by the traditional information protection framework. Classical fault detection methods are ineffective as well [9].

Other examples of CPS attacks include: the Maroochy water breach [10], the blackout in brazil power grid [11], the SQL Slammer attack in Davis-Besse nuclear power plant [12], and many other industry security incidents [13]. According to the statistics from ICS-CERT (see https://ics-cert.us-cert.gov), there were 245 CPS attacks confirmed in 2014 and the number increased to 295 in 2015.

The CPS security has attracted many researchers [14]. The traditional fault detection method, such as robust statistics [15] and robust control [16], are designed to withstand certain types of failures. The popular Fault Detection and Isolation (FDI) method assumes that the failure is spontaneous [17]. But CPS attacks are usually purposely designed to be stealthy and destructive, and are often done with the full or partial knowledge of the system's dynamic model. Thus, it is insufficient to rely on robust control or FDI against CPS attacks.

A lot of studies have also been done on different types of attacks. Mo and Sinopoli studied the performance of Kalman Filter under attacks[18]. They further studied the attack strategy and calculated the miss/false alarm rates of a χ^2 attack detector in [19]. Zhang *et. al.* focused on the energy-constrained attack scheduling problem for Denial-of-Service (DoS)

Tianju Sui and Ximing Sun are with the School of Control Science and Engineering, Dalian University of Technology, China (email:suitj@mail.dlut.edu.cn; sunxm@dlut.edu.cn). Damian Marelli is with the School of Automation, Guangdong University of Technology, China, and with the French Argentine International Center for Information and Systems Sciences, National Scientific and Technical Research Council, Argentina (email: Damian.Marelli@newcastle.edu.au). Minyue Fu is with School of EE&CS, University of Newcastle, Australia. He also holds an Bairen Professorship at the School of Automation, Guangdong University of Technology, China (email: minyue.fu@newcastle.edu.au).

This work was supported by National Natural Science Foundation of China(61803068) and China Postdoctoral Science Foundation (2017M621134).

attacks [20]. Zhao *et. al.* studied the effect of stealthy attacks on consensus-based distributed economic dispatch [21]. Kung *et. al.* defined an ϵ-stealthy attack and analyzed its effect for scalar systems [22]. In [23], the authors worked on the multi-channel transmission schedule problem for remote state estimation under DoS attacks.

In this paper, we will first describe the dynamic model of a CPS under attacks and give a definition for stealthy attacks. Then, an equivalent but simpler criterion for stealthy attacks is derived. Under the constraint of stealthiness assumption, we study the stability of a control system under attacks, i.e., the invulnerability of system, and show that the boundness of the estimation error bias between the healthy and the attacked system is necessary and sufficient condition for the invulnerability.

The rest of this paper is organized as follows. In Section II, we describe the models of system, attacks and detector. In Section III, the system dynamic under attacks is expressed and a simple equivalent stealthiness definition is derived. Under the stealthy attacks, we show that the stability of a control system only depends on the boundness of the estimation error bias between the healthy system and the attacked system. In Section IV, the simulations on different systems characterize the invulnerability and vulnerability under stealthy attacks. Concluding remarks are stated in Section V.

II. Problem Formulation

A. System Description

In this paper, the linear stochastic system to be considered is modeled in the state-space form

$$x_{t+1} = Ax_t + Bu_t + w_t, \tag{1}$$
$$y_t = Cx_t + v_t. \tag{2}$$

The measurement y_t is a m-dimensional random vector, $x_0 \sim \mathcal{N}(0, \Sigma)$, $w_t \sim \mathcal{N}(0, Q)$, $v_t \sim \mathcal{N}(0, R)$, and $\{x_0, w_t, v_t : t \in \mathbb{N}\}$ are jointly independent. We assume that

$$\Sigma = A\Sigma A^\top + Q,$$

so that the system is in steady state.

Moreover, the control input u_t is assumed to be generated by the linear quadratic Gaussian (LQG) controller [24]. More specifically, the LQG controller is assumed to be

$$u_t = L\hat{x}_t, \tag{3}$$

where $\hat{x}_t$ is generated by Kalman filter as the optimal state estimate without attacks at time t and L is the steady-state control gain matrix.

Since we assume that the Kalman filter is in steady state, and the formula of Kalman filter is simplified as

$$\hat{x}_{t+1} = A\hat{x}_t + Bu_t + K[y_{t+1} - C(A\hat{x}_t + Bu_t)], \tag{4}$$

where $K = \Sigma C^T(C\Sigma C^T + R)^{-1}$ is the steady-state Kalman gain.

Remark 1. Since the design of LQG controller and Kalman filter should firstly guarantee the stability of system, the control gain L and Kalman gain K should satisfy that $A + BL$ and $A - KCA$ are both stable.

To facilitate the analysis, we define the innovation vector z_{t+1} as

$$z_{t+1} = y_{t+1} - C(A\hat{x}_t + Bu_t). \tag{5}$$

The estimation error e_t at time t is defined as

$$e_t = x_t - \hat{x}_t.$$

Following (1) and (4), we get following error dynamics

$$e_{t+1} = (A - KCA)e_t + (I - KC)w_t - Kv_{t+1}. \tag{6}$$

B. Attack Description

We firstly give the attack model

$$x'_{t+1} = Ax'_t + Bu'_t + B^a u^a_t + w_t, \tag{7}$$
$$y'_t = Cx'_t + \Gamma^a y^a_t + v_t, \tag{8}$$

where $(\bullet)'$ is the variable $\bullet$ under attack.

Then, under an attack, the Kalman estimator and LQG controller are given by

$$\hat{x}'_{t+1} = A\hat{x}'_t + Bu'_t + K[y'_{t+1} - C(A\hat{x}'_t + Bu'_t)],$$
$$u'_t = L\hat{x}'_t. \tag{9}$$

Comparing with the healthy system (1) and (2), the attacker injects a state attack $B^a u^a_t$ and a measurement attack $\Gamma^a y^a_t$ into the actuator and sensor, respectively. The matrices B^a and Γ^a are the state attack matrix and the sensor selection matrix, respectively.

In order to consider general cyber-attacks, the attacker is assumed to have the following features:

1) The prior knowledge of the attacker includes all measurements and system parameters.
2) The state attack $B^a u^a_t$ is only constrained by[1]
$$\|B^a u^a_t\| \leq \alpha. \tag{10}$$
3) The attack starts at time 0 and there is no attack prior to it.

Under the attack defined above, the innovation vector and estimation error are updated as

$$z'_{t+1} = y'_{t+1} - C(A\hat{x}'_t + Bu'_t), \tag{11}$$
$$e'_t = x'_t - \hat{x}'_t. \tag{12}$$

Then, the difference between attacked system and healthy system are characterized by

$$\triangle x_t := x'_t - x_t, \triangle\hat{x}_t := \hat{x}'_t - \hat{x}_t,$$
$$\triangle u_t := u'_t - u_t, \triangle y_t := y'_t - y_t,$$
$$\triangle z_t := z'_t - z_t, \triangle e_t := e'_t - e_t. \tag{13}$$

[1]Since the state change requires real energy input and the maximum power is constrained by the actuator property.

C. Detector Description

To detect various attacks as described above, the system is equipped with an attack detector, which generates an alarm when attack is believed to be found. To make the discussion more general, the attack detector triggers an alarm at time t based on following event:

$$g_t > X_g, \tag{14}$$

where X_g is the alarm threshold and g_t is the general case of trigger variable at time t, i.e.,

$$g_t := g(y_t, y_{t-1}, \ldots, y_0). \tag{15}$$

We have an assumption for the function $g(\cdot)$.

Assumption 1. *The function $g(\cdot)$ is continuous and let $\triangle g_t = g'_t - g_t$, for any $\varsigma > 0$ and $t \in \mathbb{N}$, there exists $\tilde{\varsigma} > 0$ such that*

$$|\triangle g_t| > \varsigma$$

if

$$\|\triangle y_t\| > \tilde{\varsigma}.$$

Remark 2. Since the only information available is the measurements history, (15) is a general attack detector. For example, the popular χ^2 detector [19] is a special case of (15) for that $\hat{x}_t, u_t$ depend on $\{y_t, y_{t-1}, \ldots, y_0\}$ as in (9) and that

$$\begin{aligned} g_{t+1} &= z_{t+1}^T P_z^{-1} z_{t+1} \\ &= (y_{t+1} - C(A\hat{x}_k + Bu_k))^T P_z^{-1} \\ &\quad \cdot (y_{t+1} - C(A\hat{x}_k + Bu_k)), \end{aligned}$$

where P_z is the steady-state covariance matrix of z_k without attacks. In this case, it is easy to verify that, for any $\varsigma > 0,\ t \in \mathbb{N}$, there exists $\tilde{\varsigma} > 0$ such that $\|\triangle y_k\| > \tilde{\varsigma}$ implies $|\triangle g_t| > \varsigma$.

Then, the probability of alarm(i.e., alarm rate) is given by

$$\beta_t := \mathbb{P}(g_t > X_g). \tag{16}$$

If the attack happens, then the attack detector follows

$$\begin{aligned} g'_t &:= g(y'_t, y'_{t-1}, \ldots, y'_0), \\ \beta'_t &:= \mathbb{P}(g'_t > X_g). \end{aligned} \tag{17}$$

And the corresponding difference between attacked and healthy systems is

$$\triangle \beta_t := \beta'_t - \beta_t. \tag{18}$$

Theoretically, the attack detector could can trigger an alarm if $\triangle \beta_t \neq 0$. But it is not realistic for a detector to find out the real β'_t based on the available measurements up to time t. Therefore we assume that an attack is not detected at time t if

$$|\triangle \beta_t| \leq \delta, \tag{19}$$

where δ is the designed threshold.

The definition for stealthy attacks is then proposed.

Definition 1. An attack is called *stealthy* if (19) holds for all $t \in \mathbb{N}$.

III. The Stealthy Attacks and Vulnerable Systems

The purpose of this section is to study stealthy attacks. Recall from its definition, stealthy attacks are difficult to detect, thus having great potential to cause serious damages (including instability) to the physical system. Due to this, we will also study in this section the vulnerability of the physical system to such attacks.

Our first task is to provide an alternative characterization for stealthy attacks. This is due to the fact that the variable $\triangle \beta_t$ is difficult to analyze. We have the following result.

Theorem 1. *For any $\varepsilon > 0$, there exists $\tilde{\varepsilon} > 0$ such that*

$$|\triangle \beta_t| \leq \varepsilon$$

for all $t \in \mathbb{N}$, if and only if

$$\|\triangle z_t\| \leq \tilde{\varepsilon}$$

for all $t \in \mathbb{N}$.

Proof: By substracting the equation (11) from (5) and equation (9) from (4), we have

$$\triangle \hat{x}_{t+1} = (A + BL)\triangle \hat{x}_t + K\triangle z_{t+1}, \tag{20}$$

$$\triangle y_{t+1} = \triangle z_{t+1} + C(A + BL)\triangle \hat{x}_t. \tag{21}$$

Then, we separate the proof for necessity and sufficiency respectively.

Necessity: Suppose that $|\triangle \beta_t| \leq \varepsilon$ for all $t \in \mathbb{N}$, for that $\beta_t := \mathbb{P}(g_t > thereshold)$ and $\beta'_t := \mathbb{P}(g'_t > thereshold)$, there exists a constant $\varsigma > 0$ such that $|\triangle g_t| \leq \varsigma$ for all $t \in \mathbb{N}$. Based on the Assumption 1, it follows that there also exists $\tilde{\varsigma} > 0$ such that $\|\triangle y_t\| \leq \tilde{\varsigma}$ for all $t \in \mathbb{N}$.

Then, we transform (20) and (21) into

$$\triangle \hat{x}_{t+1} = (I - KC)(A + BL)\triangle \hat{x}_t + K\triangle y_{t+1}, \tag{22}$$

$$\triangle z_{t+1} = \triangle y_{t+1} - C(A + BL)\triangle \hat{x}_t. \tag{23}$$

In equation (22), we could deduce that there exists a constant ι such that $\|\triangle \hat{x}_t\| \leq \iota$ for all $t \in \mathbb{N}$. Thus, from equation (23), there also exists a constant $\tilde{\varepsilon}$ such that $\|\triangle z_t\| \leq \tilde{\varepsilon}$ for all $t \in \mathbb{N}$.

Sufficiency: For any reasonable $\varepsilon > 0$, we are going to prove that there exists a constant $\tilde{\varepsilon}$ such that $\|\triangle z_t\| \leq \tilde{\varepsilon}$ for all $t \in \mathbb{N}$ could deduce that $\|\triangle \beta_t\| \leq \varepsilon$ for all $t \in \mathbb{N}$.

Based on the definition of $\triangle \beta_t$, there exist a constant $\varsigma > 0$ such that $|\triangle g_t| \leq \varsigma$ for all $t \in \mathbb{N}$ implies $|\triangle \beta_t| \leq \varepsilon$ for all $t \in \mathbb{N}$. Following the continuous property of function $g(\cdot)$, there exists $\tilde{\varsigma} > 0$ such that $\|\triangle y_t\| \leq \tilde{\varsigma}$ for all $t \in \mathbb{N}$ is sufficient for that $|\triangle g_t| \leq \varsigma$ for all $t \in \mathbb{N}$.

Based on the equations (20) and (21), the $\triangle z_{t+1}$ could be viewed as the only input signal. Thus, there exists a constant $\tilde{\varepsilon} > 0$ satisfying $\|\triangle z_t\| \leq \tilde{\varepsilon}$ for all $t \in \mathbb{N}$ such that $\|\triangle y_t\| \leq \tilde{\zeta}$. Following the above analysis between $\|\triangle y_t\| \leq \tilde{\zeta}$ and $|\triangle \beta_t| \leq \varepsilon$ for all $t \in \mathbb{N}$, the proof is done. ■

Following the result in Theorem 1, the *stealthy* condition (19) is equivalent to

$$\|\triangle z_t\| \leq \tilde{\delta}, \tag{24}$$

where $\tilde{\delta}$ is determined by δ from Theorem 1.

Next, we turn to study if a system can stay stable under *stealthy* attacks. The stability of a system under attacks is given from two perspectives:

1) The state difference $\triangle x_t$ between healthy system and attacked system should be bounded, i.e., $\limsup_{t\to\infty} \|\triangle x_t\| < \infty$.

2) The state estimation error e'_t under attack should be bounded, i.e., $\limsup_{t\to\infty} \|e'_t\| < \infty$.

The definition for invulnerability follows from the stability under attacks and given below.

Definition 2. A system (1)-(2) is said to be invulnerable if, for any attack sequence $\{y^a_t : t \in \mathbb{N}\}$ and $\{u^a_t : t \in \mathbb{N}\}$ satisfying (24), we have

$$\limsup_{t\to\infty} \|\triangle x_t\| < \infty$$

and

$$\limsup_{t\to\infty} \|e'_t\| < \infty.$$

Otherwise, the system is said to be vulnerable.

Remark 3. The vulnerability of a system means that, even equipped with any attack detector, the system may become unstable under some *stealthy* attacks. From the security point of view, this kind of system is not robust enough against stealthy attacks.

Then, we give a necessary and sufficient condition for the system's invulnerability.

Theorem 2. *Under* stealthy *attacks satisfying* (24)*, the system in* (1)-(2) *is invulnerable if and only if*

$$\limsup_{t\to\infty} \|\triangle e_t\| < \infty. \tag{25}$$

Proof: Based on the definitions in (13), we have

$$\begin{aligned} \triangle x_t &= x'_t - x_t \\ &= (\hat{x}'_t + e'_t) - (\hat{x}_t + e_t) \\ &= \triangle \hat{x}_t + \triangle e_t. \end{aligned}$$

By subtracting equation (4) from (9), it follows that

$$\triangle \hat{x}_{t+1} = (A + BL)\triangle \hat{x}_t + K\triangle z_{t+1} \tag{26}$$

Since the constrain in (19) is equivalent to that of (24), we have $\|\triangle z_t\| \leq \tilde{\delta}$ for any $t \in \mathbb{N}$. Combining with that $A + BL$ is stable, the variable $\triangle \hat{x}_t$ is bounded for any $t \in \mathbb{N}$.

Then, the condition $\limsup_{t\to\infty} \|\triangle e_t\| < \infty$ is equivalent to that $\limsup_{t\to\infty} \|\triangle x_t\| < \infty$.

Moreover, since the estimation error is unbiased, i.e., $\mathbb{E}[e_t] = 0$ for any $t \in \mathbb{N}$. Based on that

$$\triangle e_t = e'_t - e_t$$

and

$$\begin{aligned} & \triangle z_{t+1} \\ = \;& \triangle y_{t+1} - C(A + BL)\triangle \hat{x}_t \\ = \;& C\triangle x_{t+1} + \Gamma^a y^a_{t+1} - C(A + BL)\triangle \hat{x}_t \\ = \;& CA\triangle x_t + CBL\triangle \hat{x}_t + CB^a u^a_t + \Gamma^a y^a_{t+1} \\ & -C(A + BL)\triangle \hat{x}_t \\ = \;& CA\triangle e_t + CB^a u^a_t + \Gamma^a y^a_{t+1}, \end{aligned} \tag{27}$$

combining with that

$$\begin{aligned} & \triangle e_{t+1} \\ = \;& \triangle x_{t+1} - \triangle \hat{x}_{t+1} \\ = \;& [A\triangle x_t + BL\triangle \hat{x}_t + B^a u^a_t] - [(A + BL)\triangle \hat{x}_t \\ & +K\triangle z_{t+1}] \\ = \;& [A\triangle x_t + BL\triangle \hat{x}_t + B^a u^a_t] - [(A + BL)\triangle \hat{x}_t \\ & +K\{\triangle y_{t+1} - C(A + BL)\triangle \hat{x}_t\}] \\ = \;& [A\triangle x_t + BL\triangle \hat{x}_t + B^a u^a_t] - [(A + BL)\triangle \hat{x}_t \\ & +K\{C\triangle x_{t+1} + \Gamma^a y^a_{t+1} - C(A + BL)\triangle \hat{x}_t\}] \\ = \;& [A\triangle x_t + BL\triangle \hat{x}_t + B^a u^a_t] - [(A + BL)\triangle \hat{x}_t \\ & +K\{CA\triangle x_t + CBL\triangle \hat{x}_t + CB^a u^a_t + \Gamma^a y^a_{t+1} \\ & -C(A + BL)\triangle \hat{x}_t\}] \\ = \;& [A\triangle x_t + BL\triangle \hat{x}_t + B^a u^a_t] - [(A + BL)\triangle \hat{x}_t \\ & +K\{CA\triangle e_t + CB^a u^a_t + \Gamma^a y^a_{t+1}\}] \\ = \;& (I - KC)A\triangle e_t + (I - KC)B^a u^a_t - K\Gamma^a y^a_{t+1} \end{aligned} \tag{28}$$

is deterministic and is not correlated with stochastic noise. Thus,

$$\triangle e_t = \mathbb{E}[e'_t] - \mathbb{E}[e_t] = \mathbb{E}[e'_t], \tag{29}$$

and it completes the proof. ■

Remark 4. According to the results in Theorem 1 and 2, we could use the boundness of $\limsup_{t\to\infty} \|\triangle e_t\| < \infty$ to represent the stability of system(i.e., the vulnerability) and $\|\triangle z_t\| \leq \tilde{\delta}$ to represent the stealthy constrain.

IV. Example

In this section, we choose an example to verify that attacks on different sensor channels have very different effects. Take the system parameters $A = \begin{bmatrix} 2 & 0 \\ 0 & 0.5 \end{bmatrix}, B = B^a = C = Q = R = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ and the attack is constrained by

$$\|B^a u^a_t\| \leq 1 \text{ and } \|\triangle z_t\| \leq 1$$

for any $t \in \mathbb{N}$.

Then, we use simulations to show that the system is vulnerable under the stealthy attacks on the first sensor channel while invulnerable with the second sensor channel attacked.

1) Take the sensor attack matrix $\Gamma^a = \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$:

In this case, to show that the system can be unstable under a stealthy attack, we plot the norm of $\|\triangle e_t\|$ and $\|\triangle z_t\|$.

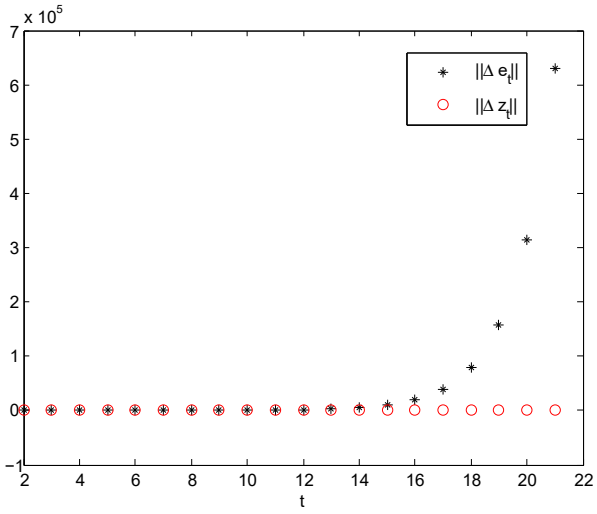

Fig. 2. The evolution of $\|\triangle e_t\|$ and $\|\triangle z_t\|$ under a stealthy attack.

From the Figure 2, the estimation error bias between the healthy and attacked systems diverges while the residual bias is kept bounded. This means that the system is unstable under a stealthy attack.

2) Take the sensor attack matrix $\Gamma^a = \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix}$:

In this case, to show that the system stays stable under any stealthy attack, we plot the reachable set of $\triangle e_t$.

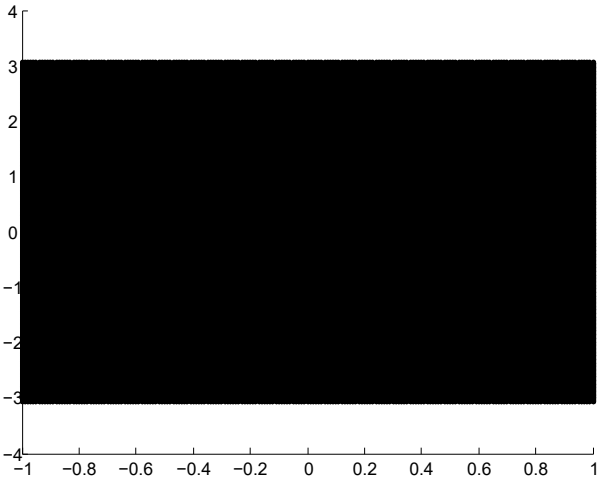

Fig. 3. The reachable set of $\triangle e_t$ under stealthy attacks.

From Figure 3, we see that the system is stable under any stealthy attacks because its reachable set is bounded.

V. Conclusion

In this paper, the dynamics of a CPS under attacks was firstly described and a definition for stealthy attacks was given. Then, we proved an equivalent but simpler criterion for stealthy attacks. Under the consideration of stealthy attacks, the vulnerability of control system under attacks was studied and it is founded that the boundness of the estimation error bias between the healthy and attacked systems is necessary and sufficient for ensuring the system stability under stealthy attacks.

References

[1] Hao Xing, Zhiyun Lin, Minyue Fu, and Benjamin F Hobbs. Distributed algorithm for dynamic economic power dispatch with energy storage in smart grids. *IET Control Theory & Applications*, 11(11):1813–1821, 2017.

[2] K. Kim and P. Kumar. Cyber-physical systems: A perspective at the centennial. *Proceedings of the IEEE*, 100(Special Centennial Issue):1287–1308, 2012.

[3] C. Liao, C. Ten, and S. Hu. Strategic future deployment considering cybersecurity in secondary distribution network. *IEEE Transactions on Smart Grid*, 4(3):1264–1274, 2013.

[4] Hao Xing, Pingliang Zeng, Yuting Mou, and Qiuwei Wu. Consensus-based distributed approach to lossy economic power dispatch of distributed energy resources. *International Transactions on Electrical Energy Systems*, 00(00):accepted for publication, 2019.

[5] C. Konstantinou, M. Maniatakos, F. Saqib, S. Hu, J. Plusquellic, and Y. Jin. Cyber-physical systems: A security perspective. In *20th IEEE European Test Symposium*, pages 1–8, 2015.

[6] L. Crossman. World war zero: How hackers fight to steal your secrets. In *Time Magazine*, 2014.

[7] C. Heres, A. Etemadieh, M. Baker, and H. Nielsen. Hack all the things: 20 devices in 45 minutes. In *DEFCON*, 2014.

[8] J. Farwell and R. Rohozinski. Stuxnet and the future of cyber war. *Survival*, 53(1):23–40, 2011.

[9] D. Dimase, Z. Collier, K. Heffner, and I. Linkov. System engineering framework for cyber physical security and resilience. *Environment Systemsand Decisions*, 35(2):291–300, 2015.

[10] J. Slay and M. Miller. Lessons learned from the maroochy water breach. *in Proceeding of Critical Infrastructure Protection*, 253:73–82, 2007.

[11] J. Conti. The day the samba stopped. *Engineering & Technology*, 5(6):46–47, 2010.

[12] S. Kuvshinkova. Sql slammer worm lessons learned for consideration by the electricity sector. *North American Electric Reliability Council*, 1(2):5, 2003.

[13] G. Richards. Hackers vs slackers. *Engineering & Technology*, 3(19):40–43, 2008.

[14] A. Cardenas, S. Amin, and S. Sastry. Research challenges for the security of control systems. In *HotSec*, 2008.

[15] P. Huber. *Robust statistics*. Springer Berlin Heidelberg, 2011.

[16] K. Zhou, J. Doyle, and K.Glover. *Robust and optimal control*. New Jersey: Prentice hall, 1996.

[17] A. Willsky. A survey of design methods for failure detection in dynamic systems. *Automatica*, 12(6):601–611, 1976.

[18] Y. Mo, E. Garone, A. Casavola, and B Sinopoli. False data injection attacks against state estimation in wireless sensor networks. In *49th IEEE Conference on Decision and Control*, pages 5967–5972, 2010.

[19] Y. Mo and B. Sinopoli. On the performance degradation of cyber-physical systems under stealthy integrity attacks. *IEEE Transactions on Automatic Control*, 61(9):2618–2624, 2016.

[20] H. Zhang, P. Cheng, L. Shi, and J. Chen. Optimal denial-of-service attack scheduling with energy constraint. *IEEE Transactions on Automatic Control*, 60(11):3023–3028, 2015.

[21] C. Zhao, J. He, P. Cheng, and J. Chen. Analysis of consensus-based distributed economic dispatch under stealthy attacks. *IEEE Transactions on Industrial Electronics*, 64(6):5107–5117, 2017.

[22] S. Dey E. Kung and L. Shi. The performance and limitations of epsilon-stealthy attacks on higher order systems. *IEEE Transactions on Automatic Control*, 62(2):941–947, 2017.

[23] K. Ding, Y. Li, D. Quevedo, S. Dey, and L. Shi. A multi-channel transmission schedule for remote state estimation under dos attacks. *Automatica*, 78:194–201, 2017.

[24] R. Kalman. On the general theory of control systems. In *Proceedings of the First International Congress on Automatic Control*, 1960.