Adaptive Compensation Control under Constant False Data Injection Attack

Xiaohang Li*, Chunlin Songa, Shaokun Liub, Jinlong Lic

Northern Information Control Research Institute Group Co., Ltd. of China North Industries Group Corporation Limited, The department of general information, Nanjing, China

*Corresponding author e-mail: 1002179508@qq.com, *songchunlinscl@163.com, 
b1789654292@qq.com, \( ^e \)274773233@qq.com

Abstract. In view of the false data injection attack of cyber physical systems (CPS), this paper aims to study the designing method of adaptive compensation controller for system executor when the system executor suffers from constant false data injection attack. The application of the adaptive compensation control algorithm to the false data injection attack shows that the designed adaptive law has the advantages of fast convergence speed and accurate parameter estimation. The compensation control algorithm can substantially compensate for the effects of false data injection attacks, and we can prove that all signals of the final closed-loop system are bounded and the state of the system can asymptotically converge to zero. Finally, we provide simulation examples to verify the effectiveness of the state feedback adaptive compensation controller proposed in this paper.

1. Introduction

With the development of the Internet, sensor networks, embedded systems, and computing intelligence, the interaction, collaboration, and integration of the information world and the physical world are constantly strengthened. As a new type of intelligent system, cyber physical system has emerged.

With the controllers, actuators, sensors and controlled objects which are distributed in different locations connected through a network, CPS is a kind of feedback control system. Its structure is shown in Figure 1. The research on CPS has been continuously paid attention to, and a series of significant research results have been obtained. CPS has gradually become a research hotspot in the field of international control [1].
In recent years, CPS has developed rapidly, and the resulting safety issues have caused great harm to society. For example, the German government announced the "High-tech Strategy 2020" in November 2011. One of its important strategies is Industry 4.0, and one of its cores is to realize "smart factories" through innovative manufacturing methods of cyber-physical systems. In the 2012 Report of the Eighteenth National Congress of the PRC, China highlighted the importance of the information physics system and pointed out the development direction of "promoting the deep integration of informatization and industrialization and accelerating the transformation and upgrading of traditional industries." In addition, in 2012, the "Flame" virus, which was extremely destructive, was widely spread in the Middle East, which caused a severe impact on the normal operation of important control systems such as the petroleum industry [2]. False data injection attack is a special type of attack and was initially applied to smart grids [3]. We will study this attack and propose a systematic quantitative analysis method.

False data injection attack is a type of attack that is intended to disrupt system stability and remain invisible to detection mechanisms. A series of researches have been done in literature [4-6] to deal with false data injection attack in smart grids. Based on the eigenvalues of the system model, Mo et al. designed a false data injection attack against the sensors in the control system, destroying the stability of the system and avoiding the detection of the chi-square detector [7]. Literature [8] studied the situation of several types of sensors and actuators false data injection attacks, and designed a method to completely eliminate the perturbation of the detector in the case of actuators and sensors under attack.

In this paper, we study the dynamic analysis of the system when an attacker launches a constant-value false data injection attack when the system has an adaptive compensation controller.

2. Problem description
The system structure of the network attack considered in this paper is shown in Figure 2. It consists of several processes as shown in the figure below. The data packet is sent to the executing agency through the wireless network. In the wireless network, the attacker can intercept and modify the sent data. The detailed model is described below.

![Figure 2. The structure of the system under false data injection](image-url)
2.1. System model

\[ \dot{x}(t) = Ax(t) + Bu(t) \]  
\[ y(t) = Cx(t) + \nu(t) \]

Where \( x(t) \in \mathbb{R}^n \) is the state vector, \( u(t) \in \mathbb{R}^n \) is the input vector, \( y(t) \in \mathbb{R}^n \) is the measurement vector measured by sensors, \( \nu(t) \in \mathbb{R}^n \) is the outer noise measured by sensors, the initial state is \( x_0 = 0 \), \( A \) and \( B \) are the matrix of appropriate dimensions. We assume that the system satisfied the following assumptions:

Assumption 1: \( (A, B) \) is completely controllable.

Assumption 2: \( (A, C) \) is completely observable.

Notation 1: The notation \( \dot{X} \) mentioned in this paper suggests the derivative of \( X \), which is also \( \frac{dX(t)}{dt} \).

When receiving the paper, we assume that the corresponding authors grant us the copyright to use the paper for the book or journal in question. Should authors use tables or figures from other Publications, they must ask the corresponding publishers to grant them the right to publish this material in their paper.

2.2. False data injection attack model for actuators

In order to research the adaptive compensation control problem, we need to establish the fake data injection attack model for the actuator:

\[ \dot{x}(t) = Ax(t) + B(u(t) + a(t)) \]  
\[ y(t) = Cx(t) + \nu(t) \]

We define that \( \hat{a}(t) \) is the estimation value of \( a(t) \), \( \tilde{a}(t) = \hat{a}(t) - a(t) \) is the error of attack signal. Because \( a(t) \) is the constant attack signal, \( \hat{a}(t) = 0 \) and \( \tilde{a}(t) = \hat{a}(t) \) are valid.

2.3. Researched problem

Use the compensator of the adaptive control method to ensure that the system can run stably after the attacker successfully injects false data and has good dynamic characteristics.

3. Design of adaptive compensation controller

In this section, we study the dynamic performance of the system with an adaptive compensation controller under constant false data injection attack. We first define the attack strategy and then design an adaptive compensation controller.

Similar to the attack model in the existing paper, we assume that the attacker can intercept and modify the transmitted actuator-related data [6]. We define the control input as

\[ u(t) = Kx(t) - \hat{a}(t) \]

Where \( K \) is the feedback control gain matrix. Then the adaptive control law is

\[ B^T P x(t) = \hat{a}(t) \]
Theorem 1: Considering the system (3) that the actuator is under attack, when the controller (5) and the adaptive law (6) play a role, all the signals of the final closed-loop system can be guaranteed to be bounded and the state can gradually converge to zero.

Proof: In view that \((A, B)\) is completely controllable, there exists a positive matrix \(P \in \mathbb{R}^{n \times n}\), so that \(P(A + BK) + (A + BK)^TP < 0\) satisfies. We assume \(P(A + BK) + (A + BK)^TP = -Q\), where \(Q\) is a positive matrix, so

\[
\dot{x}(t) = Ax(t) + B(u(t) + a(t)) = Ax(t) + B(Kx(t) - \hat{a}(t) + a(t)) = (A + BK)x(t) - B\hat{a}(t) \tag{7}
\]

We construct the Lyapunov function as

\[
\dot{V}(t) = \dot{x}^T(t)(Px(t)) + P\dot{x}^T(t)\dot{x}(t) + 2\dot{a}^T(t)\hat{a}(t) = 2x^T(t)P[(A + BK)x(t) - B\hat{a}(t)] + 2\dot{a}^T(t)\hat{a}(t)
\]

\[
= 2x^T(t)P(A + BK)x(t) - 2x^T(t)PB\hat{a}(t) + 2\dot{a}^T(t)\hat{a}(t) \tag{8}
\]

So we can obtain the following equation

\[
B^TPx(t) = \dot{\hat{a}}(t) \tag{9}
\]

can achieve the control aim.

4. Simulation example
In order to demonstrate the effectiveness of the adaptive compensation control method against false data injection attacks, we provide a simulation example here. The dynamic model of the system we consider is as follows:

\[
\dot{X}(t) = \begin{bmatrix}
-3 & -1 \\
-1 & -2
\end{bmatrix}X(t) + \begin{bmatrix}1 \\ 1 \end{bmatrix}u(t) \quad \text{where} \quad X(t) = \begin{bmatrix} \dot{x}(t) \\ x(t) \end{bmatrix} \tag{10}
\]

We can obtain \(K = \begin{bmatrix} 2.1541 & 0.9162 \\ 0.0229 & -0.0081 \end{bmatrix}\), \(P = \begin{bmatrix} -0.0081 & 0.0081 \\ 0.0081 & 0.0175 \end{bmatrix}\) by linear matrix inequality.

When the system actuator is under attack \(a(t) = 5\) after the system runs for 5s, the simulation results are shown in Figures 3 and 4. Figure 3 shows the system's estimated attack signal value after using the adaptive compensation controller. We can see that the system can accurately estimate the attack signal value after 13s. Figure 4 shows the dynamic changes of the system state after applying the adaptive compensation controller. We can see that the system's state gradually converges to 0 after running for 13s, and the adaptive compensation control works well.

\[\text{Figure 3. The estimation of constant attack signal}\]
5. Conclusion

In this paper, we mainly study the design method of adaptive compensation controller for system actuators under constant false data injection attack. We provide a simulation example to verify the effectiveness of the state feedback adaptive compensation controller proposed in this paper.

References

[1] Wang Z, Xie L. Review of Research on Information Physics Fusion System [J]. Journal of Automation, 2011, 37(10): 1157-1166.

[2] Wang W, Lu Z. Cyber security in the smart grid: Survey and challenges [J]. Computer Networks, 2013, 57 (5): 1344-1371.

[3] Liu Y, Ning P, Reiter M K. False data injection attacks against state estimation in electric power grids [J]. ACM Transactions on Information and System Security (TISSEC), 2011, 14 (1): 13.

[4] Chaojun G, Jirutitijaroen P, Motani M. Detecting false data injection attacks in ac state estimation [J]. IEEE Transactions on Smart Grid, 2015, 6 (5): 2476-2483.

[5] Rawat D B, Bajracharya C. Detection of false data injection attacks in smart grid communication systems [J]. IEEE Signal Processing Letters, 2015, 22(10): 1652-1656.

[6] Tang B, Yan J, Kay S, et al. Detection of false data injection attacks in smart grid under colored Gaussian noise [C]/Communications and Network Security (CNS), 2016 IEEE Conference on. IEEE in Philadelphia, PA, USA, 2016: 172-179.

[7] Mo Y, Sinopoli B. False data injection attacks in cyber physical systems [C]/First Workshop on Secure Control Systems in Stockholm, Sweden. 2010.

[8] Zhang H, Qi Y, Wu J, et al. DoS attack energy management against remote state estimation [J]. IEEE Transactions on Control of Network Systems, 2018, 5 (1): 383-394