SCIENCE CHINA
Technological Sciences

• News & Views •

December 2017 Vol.60 No.12:1975–1977
doi: 10.1007/s11431-017-9174-3

Analysis of security in cyber-physical systems

CHEN Jie[1,2], ZHANG Fan[1,2] & SUN Jian[1,2]*

[1] *School of Automation, Beijing Institute of Technology, Beijing 100081, China;*
[2] *State Key Laboratory of Intelligent Control and Decision of Complex Systems, Beijing Institute of Technology, Beijing 100081, China*

Received October 25, 2017; accepted October 31, 2017; published online November 14, 2017

Citation: Chen J, Zhang F, Sun J. Analysis of security in cyber-physical systems . Sci China Tech Sci, 2017, 60: 1975–1977, https://doi.org/10.1007/s11431-017-9174-3

In recent years, cyber-physical systems (CPSs) have received much attention from both the academic world and the industrial world, which refer to a deep integration and coordination of physical and computational resources [1,2]. Typical examples of CPSs can be found in smart grids, smart transportation systems, industrial control systems, water supply systems, and so on. Furthermore, many military systems are also CPSs. The key characteristic of CPSs is the integration of computing, control and communication. The increased interconnection between the cyber and physical spaces make CPSs vulnerable to various malicious attacks. A well-known example of an attack of CPSs is the Stuxnet which infected the control system of nuclear-fuel centrifuges of Bushehr nuclear power plant in Iran. Stuxnet makes people beware of the grave consequences of a cyber-attack on a CPS. Since many national critical infrastructures are applications of CPS, ensuring security and safety of such systems is of great importance.

In traditional information technology (IT) systems, three security objectives are confidentiality, integrity and availability, where confidentiality is in the first place. While in CPSs, availability ranks the first. Besides, there are some differences between IT systems and CPSs. For examples, in CPSs, a long-term safe and reliable operation is necessary. In CPSs, components are rarely replaced and difficult to upgrade. In CPSs, the control performance of the system should be taken into account. The traditional IT security methods such as data encryption and authentication can protect the confidentiality of data and keep from unauthorized access to some extent [3,4]. However, these protection measures will cease to be effective for malicious internal staff or a powerful hacker who can decipher the code. Furthermore, applying authentication and encryption is often resource consumed and hence hard to implement at some resource constrained devices. Meanwhile, additional time delay usually goes with applying authentication and encryption, which may have a negative effect on real-time responses of the CPS. In addition, traditional IT security approaches usually pay attention to the security of an individual component of CPSs but seldom investigate interactions among different components. Traditional IT security approaches do not use the information about the model of the physical system and thus fail to predict the response of the system under the attack and design some targeted anti-strategies. In conclusion, the traditional IT security approaches cannot completely solve the security problems emerging in CPSs. Some new security methods should be studied taking the main properties of CPSs into consideration.

Security and safety are two terms having some similarities. In Chinese, the same word is used for these two terms. The biggest similarity between security and safety lies that both of them deal with risks and hence some approaches in one field may be applicable to the other [5]. However, there are substantial differences between security and safety. Safety usually considers faults but security addresses attacks. Due to some physical reasons, such as aging of equipment, faults happen. However, attacks are often launched by attackers with a malicious intent. Attacks are usually covert and difficult to detect. Therefore, fault-tolerant methods cannot solve the security problem completely and new methods should be

* Corresponding author (email: sunjian@bit.edu.cn)

© Science China Press and Springer-Verlag GmbH Germany 2017

put forward.

It is easy to see that attack detection is very important in CPSs. Generally speaking, attack/intrusion detection methods for CPSs can be classified into three categories, that is, knowledge-based attack/intrusion detection also known as misuse-based detection, behavior-based attack/intrusion detection also known as anomaly-based detection, and behavior-specification-based attack/intrusion detection [6]. Misuse-based detection assumes that abnormal behaviors′ patterns are known and stored in a database. It compares the pattern of the attack with the ones in the database to identify the attack. The major advantage of misuse-based detection is a low false positive rate. The major disadvantage of misuse-based detection is its inability to recognize an unknown attack. The basic idea of behavior-based detection is that any anomalies will cause the deviation of the system's behavior. Therefore, a model of the normal behavior of the system is necessary in behavior-based detection. The major advantage of behavior-based detection is its ability to deal with unknown attacks. The major disadvantage of behavior-based detection is a high false positive rate. Behavior-specification-based detection takes a similar rule as behavior-based detection. It has a low false negative rate. Some existing methods for the above three classes of attack/intrusion detections can be found in excellent survey papers [6,7]. Besides, existing fault detection methods may be useful for attack detection.

To detect and mitigate an attack, it is important to understand the attack and the objective of the attacker. Therefore, modeling and analysis of the attack are necessary. There are several approaches for attack modeling, such as attack tree, attack vector, attack surface, diamond model, and kill chain [8]. However, the above approaches are proposed for cyber-security and they do not considered the interaction between the cyber layer and the physical layer in CPSs. Recently, a framework of modeling some typical attacks such as denial-of-service, replay, zero-dynamics, and bias injection attacks has been proposed in ref. [9] for CPSs.

As the saying goes, the best defense is a good offense. In recent years, how to design a high covert attack strategy from the attacker's angle has received much attention. To mention a few, Mo et al. [10] studied the covert false data injection attack against state estimation for linear Gaussian systems under the framework of constrained optimal control. Zhang et al. [11] investigated the jamming attack problem for linear systems with attacking energy constraints, and they proved theoretically that grouping the limited attacks together in every active interval is optimal. Some other attack design methods please refer the survey paper [12] and references therein.

When a malicious attack happens, the problem of mitigating damages resulting from the attack and recovering operation of CPSs is undoubtedly of great importance. Therefore, secure state estimation and control problem received much attention. Pang et al. [13] considered the security of networked control systems and proposed a secure architecture. The basic idea is that data encryption standard (DES) algorithm and message digest (MD5) algorithm are used to keep the confidentiality of data during communication and networked predictive control method is adopted to compensate for the network constraints such as time-delay and dropout. Resilient estimation for swarm systems was discussed in ref. [14].

In the above, we have analyzed the security of CPSs from several aspects such as attack detection, attack modeling, attack design, secure estimation and control. Next, we point out some research directions deserving future studies.

Recently, artificial intelligence has gained enormous momentum. Some advanced technologies in artificial intelligence such as deep learning, reinforcement learning can be applied to study security of CPSs.

Control-theoretic security methods [9–11,13] should be combined with IT security methods to deal with security of CPSs.

An assumption that the attacker is omniscient and omnipotent is commonly used in the existing literature on security of CPSs, which obviously exaggerates the ability of the attacker. When the attacker is under some constraints, the attack design and resilient estimation and control problems are challenging.

The features about the physical process and specific domain knowledge should be well considered.

This work was supported by the National Natural Science Foundation of China (Grant Nos. 61522303, U1509215 & 61621063), and Program for Changjiang Scholars and Innovative Research Team in University (Grant No. IRT1208).

1 Kim K D, Kumar P R. Cyber-physical systems: A perspective at the centennial. Proc IEEE, 2012, 100: 1287–1308

2 Yang G, Zhou X. Intelligent CPS: Features and challenges. Sci China Inf Sci, 2016, 59: 050102

3 Cao Z. New trends of information security-how to change perople's life (in Chinese)? Sci China Inf Sci, 2016, 59: 050106

4 Sun H, Wen Q, Li W. A strongly secure pairing-free certificateless authenticated key agreement protocol under the CDH assumption. Sci China Inf Sci, 2016, 59: 032109

5 Kriaa S, Pietre-Cambacedes L, Bouissou M, et al. A survey of approaches combining safety and security for industrial control systems. Reliability Eng Syst Safety, 2015, 139: 156–178

6 Mitchell R, Chen I R. A survey of intrusion detection techniques for cyber-physical systems. ACM Comput Surv, 2014, 46: 1–29

7 Han S, Xie M, Chen H H, et al. Intrusion detection in cyber-physical systems: techniques and challenges. IEEE Syst J, 2014, 8: 1052–1062

8 AL-Mohannadi H, Mirza Q, Namanya A, et al. Cyber-attack modeling analysis techniques: An overview. In: Proceedings of the 4th International Conference on Future Internet of Thing and Cloud Workshop. Vienna: IEEE, 2016. 69–76

9 Teixeira A, Shames I, Sandberg H, et al. A secure control framework for resource-limited adversaries. Automatica, 2015, 51: 135–148

10 Mo Y, Garone E, Casavola A, et al. False data injection attacks against state estimation in wireless sensor networks. In: Proceedings of the

49th IEEE Conference on Decision and Control. Atlanta: IEEE, 2010. 5967–5972

11 Zhang H, Cheng P, Shi L, et al. Optimal denial-of-service attack scheduling with energy constraint. IEEE Trans Automat Contr, 2015, 60: 3023–3028

12 Wu G, Sun J, Chen J. A survey on the security of cyber-physical systems. Control Theor Technol, 2016, 14: 2–10

13 Pang Z H, Liu G P. Design and implementation of secure networked predictive control systems under deception attacks. IEEE Trans Contr Syst Technol, 2012, 20: 1334–1342

14 Zhu B, Xie L, Han D, et al. A survey on recent progress in control of swarm systems. Sci China Inf Sci, 2017, 60: 070201