Turkish Journal of Engineering

https://dergipark.org.tr/en/pub/tuje

e-ISSN 2587-1366

A brief review on attack design and detection strategies for networked cyber-physical systems

Mustafa Sinasi Ayas *[1]

[1]*Karadeniz Technical University, Engineering Faculty, Department of Electrical and Electronics Engineering, Trabzon, Turkey*

Keywords
Networked cyber-physical system
Cyber-security
Attack design
Attack detection
Control-theoretic
CPS

ABSTRACT

Networked cyber-physical systems (NCPSs) can be found in various fields such as industrial process, robotics, smart buildings, energy, healthcare systems, transportation, and surveillance. Recently accomplished real-time attacks indicate security vulnerabilities that weaken the reliability of NCPSs. Research areas on the security of NCPSs can be categorized into two groups: from the perspective of information security, from the perspective of control theory. In this paper, first possible attack locations on the control scheme of a NCPS which can be divided into three different groups namely sensor side, actuator side, and state estimator side are discussed and then a brief survey containing some recent studies on security strategies for NCPSs from the perspective of control theory is presented. After that attack detection strategies for a NCPS are briefly introduced and a general architecture utilized for attack detection on a NCPS is presented. In addition, some of recent studies on attack detection strategies for NCPSs from the perspective of control theory are discussed.

1. INTRODUCTION

Networked cyber-physical systems (NCPSs) compose of cyber (computation units and communication units) and physical (sensors and actuators) components interacting in a framework (Cárdenas et al. 2008) as shown in Fig. 1. Large-scale and distributed monitoring and control applications have led to increased interest on NCPSs in recent years. NCPSs can be found in various fields such as industrial process control (Wang et al. 2008), robotics (Meng et al. 2011), smart buildings (Kleissl and Agarwal 2010), energy (Barthels et al. 2011), healthcare systems (Lee and Sokolsky 2010), transportation (Lau et al. 2011), and surveillance (Chen et al. 2012). Although the integration of cyber and physical components in NCPSs increases system efficiency, it also exposes security vulnerabilities that weaken the reliability of critical NCPSs (Sandberg et al. 2015). Recently accomplished real-time attacks such as the Maroochy water breach (Slay and Miller 2007), multiple power blackouts in Brazil (Conti 2010), the StuxNet worm attack to Siemens' supervisory control and data acquisition (SCADA) systems (Karnouskos 2011), the SQL Slammer worm attack on the Davis-Besse nuclear plant (Kuvshinkova 2003) prove the mentioned security vulnerabilities in NCPSs. These successful attacks signify that information security mechanisms of NCPSs are insufficient to assure their healthy operation and NCPSs are prone to malfunction under attacks. Therefore, specifically designed control systems are required to complete the security mechanism (Pasqualetti et al. 2015).

Security of NCPSs is an up-to-date and challenging issue on which researchers have paid intensive attention to remedy the vulnerabilities. Basically, the research areas on the security of NCPSs can be categorized into two groups. In the first group, the researchers consider the issue from the perspective of information security, while the other group take into account the issue from the perspective of control theory.

In this paper, first, a brief survey on attack design strategies for NCPSs from the perspective of control theory is presented. Then, general architecture utilized for attack detection on a NCPSs is introduced. After that, some of recent papers on attack detection strategies for NCPSs from the perspective of control theory are

* **Corresponding Author**

*(msayas@ktu.edu.tr) ORCID ID 0000 – 0001 – 8113 – 4817

Cite this article

Ayas M S (2021). A brief review on attack design and detection strategies for networked cyber-physical systems. Turkish Journal of Engineering, 5(1), 01-07

Review Article / DOI: 10.31127/tuje.640282

Received: 30/10/2019; Accepted: 12/04/2020

discussed. In Section 2, the papers related to attack design for NCPSs are discussed. Section 3 introduces an architecture employed for attack detection on NCPSs and presents a brief literature review on attack detection strategies for NCPSs. Should be noted that the studies which is taken into account in this paper do not cover the all literature.

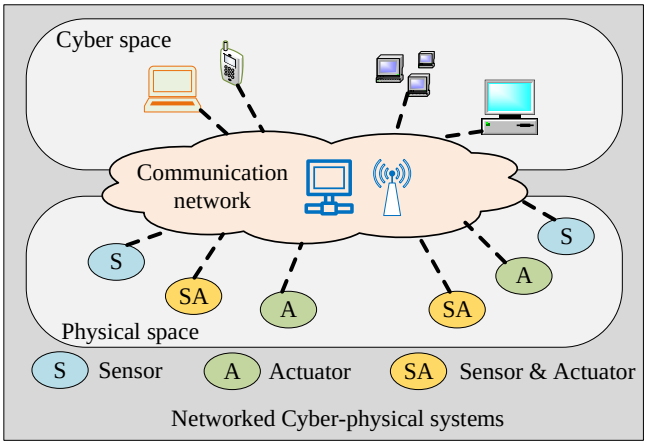

Figure 1. Holistic view of NCPSs

2. ATTACK DESIGN STRATEGIES FOR A NCPS

Possible attack locations on the control scheme of a NCPS can be categorized into three different groups: sensor side, actuator side, and state estimator side. Sensor side attacks are performed by spoofing measured sensor signals, i.e. the real time sensor data are modified by the attacker. Similarly, in the actuator side attacks, the attacker spoof the produced control signals required for actuators. State estimator side attacks can be either at the output or input of the estimator, i.e. attacker can modify either estimated state values or control signals provided as input to the estimator. These mentioned attacks are actually performed at the input-output of the main blocks such as controller, system and estimator in a closed loop system. Note that this paper does not cover attacks performed on cyber-side to change parameters of the controller.

Assume that physical plant is modelled in continuous-time state-space form given in Eq. (1) and a controller based observer has the form presented in Eq. (2).

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t) \\ y(t) &= Cx(t) + Du(t) \end{aligned} \tag{1}$$

$$\begin{aligned} \dot{\hat{x}}(t) &= A\hat{x}(t) + Bu(t) + L(y(t) - C\hat{x}(t) + Du(t)) \\ u(t) &= -K\hat{x}(t) + Gr(t) \end{aligned} \tag{2}$$

where *r(t)* is reference input signal, *(A,C)* is observable, *(A,B)* is controllable, $\hat{x}(t)$ represents state vector of the observer, *u(t)* is the produced control signal, G is a prefilter matrix determined considering steady-state error, *L* and *K* matrices are chosen such that $(A-LC)$ and $(A-BK)$ are Hurwitz.

The block diagram of the physical plant model and controller based observer given in Eqs. (1 and 2) is shown in Fig. 2.

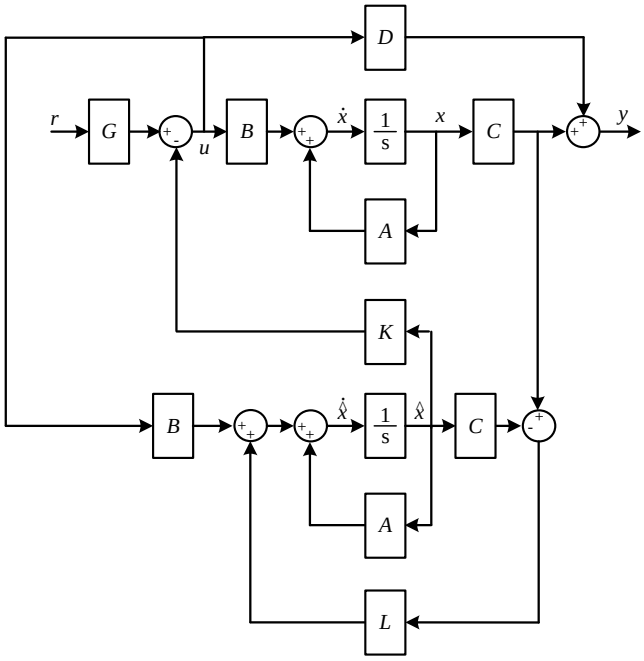

Figure 2. The block diagram of the physical plant model and controller based observer

2.1. Sensor Side Attacks

A sensor side attack can be represented by a time varying $\Delta y(t)$ signal which is added to measured sensor data by the attacker (Djouadi et al. 2014). By spoofing sensor data, the output of the system represented by *y(t)* is modified and general state-space model is written as in Eq. (3).

$$\begin{aligned} \dot{x}(t) &= Ax(t) + Bu(t) \\ y_a(t) &= Cx(t) + Du(t) + \Delta y(t) \end{aligned} \tag{3}$$

where $y_a(t)$ corresponds system output under attack.

2.2. Actuator Side Attacks

Actuator side attacks are employed to spoof control signals directly utilized in state-space models. Assume that a time varying $\Delta u(t)$ signal is added to the produced control signal. Then, the state-space model of the plant is written as in Eq. (4) (Ayas and Djouadi 2016).

$$\begin{aligned} \dot{x}(t) &= Ax(t) + B(u_a(t)) \\ y(t) &= Cx(t) + D(u_a(t)) \end{aligned} \tag{4}$$

where $u_a(t) = u(t) + \Delta u(t)$ represent modified control signal.

2.3. State Estimator Side Attacks

In this case, the attacker is able to spoof either the input of the estimator, i.e. control signals provided as input to the estimator, or the output of the estimator, i.e. estimated state vector. If the attacker modify only the input control signal of the estimator then controller based observer has the following form in Eq. (5).

On the other hand, the attacker can directly modify the output of the estimator by adding a $\Delta\hat{x}(t)$ signal to the

estimated state vector. In this case, the model of the controller based observer is written as in Eq. (6).

A general closed loop system containing state estimator for a NCPS is demonstrated in Fig. 3. In the figure, possible attack locations for the mentioned three category are emphasized with red icons.

$$\dot{\hat{x}}_a(t) = A\hat{x}(t) + B(u(t) + \Delta u_o(t)) + L(y(t) - C\hat{x}(t) + D(u(t) + \Delta u_o(t)))$$
$$u(t) = -K\hat{x}_a(t) + Gr(t) \quad (5)$$

$$\dot{\hat{x}}_a(t) = A(\hat{x}(t) + \Delta\hat{x}(t)) + Bu(t) + L(y(t) - C(\hat{x}_a(t) + \Delta\hat{x}(t)) + Du(t))$$
$$u(t) = -K(\hat{x}(t) + \Delta\hat{x}(t)) + Gr(t) \quad (6)$$

where $\hat{x}_a(t)$ represent the attacked state vector.

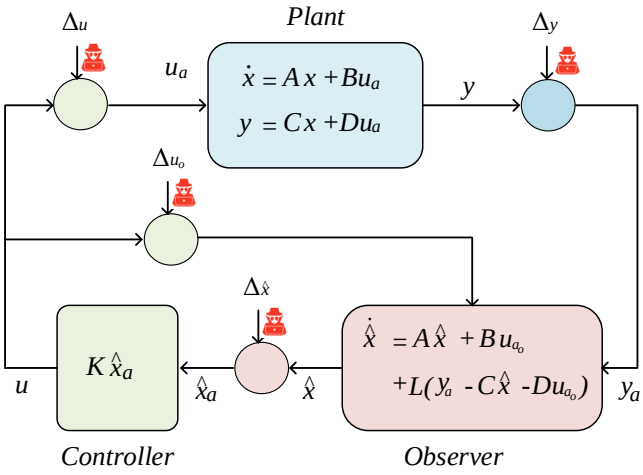

Figure 3. Possible actuator, sensor, and state attacks on a general closed loop system

Unlike traditional IT systems, where security is based on the advocacy of data-related features and services, cyber attacks on NCPS can affect physical processes due to their feedback structure. Hence, NCPS security should take into account threats on both the cyber and physical layers. Within this scope three dimensional attack-scenario space seen in Fig. 4. was presented in (Teixeira et al. 2015) by considering control systems perspective. Commonly used specific attack types such as replay attack, denial-of-service (DoS) attack, bias-injection attack, zero dynamics attack, eavesdropping attack and covert attack are positioned in the attack space considering axes which are system knowledge, disruption resources and disclosure resources. For example, DoS and eavesdropping attacks require only disruption and disclosure resources, respectively, whereas replay attack utilizes both of the resources. On the other hand, for a covert attack model knowledge is necessary in addition to disruption and disclosure resources.

The general approach in attack design for a NCPS has been to focus on the effect of specific attacks against the NCPS. (Amin et al. 2009) have studied the effect of deception and DoS attacks on discrete-time linear dynamical systems. Deception attacks aim to compromise the trustworthiness of some data of sensors and actuators by changing their values. On the other hand, DoS attacks compromise availability of sensor and actuator data by jamming the communication channel. As a result legitimate users are unable to get a respond to their requests, i.e. a lack of accessibility of sensor and actuator components occurs.

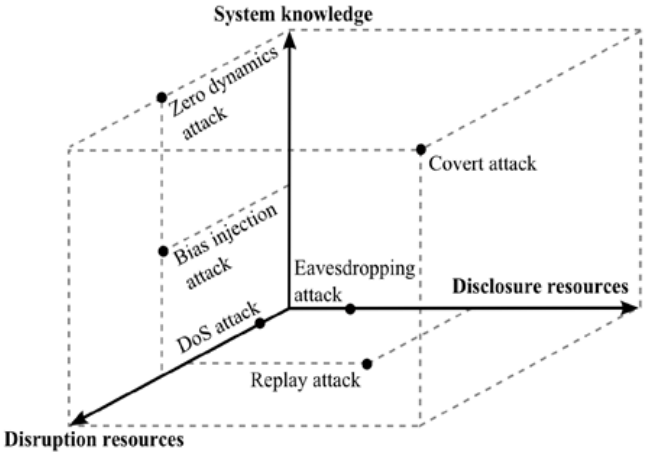

Figure 4. Three dimensional attack-scenario space (Teixeira et al. 2015)

(Mo et al. 2010) presented specific deception attacks named false data injection attacks against state estimator used in a discrete-time linear time-invariant Gaussian system. A Kalman filter was used as state estimator in the study. The false data injection attack scenario designed as a constrained control problem and the solution of this problem is provided using ellipsoidal approximation approach to show the solution space of the control problem.

(Liu et al. 2011) studied the effect of false data injection attacks against state estimators in electric power systems. The researchers successfully launched the false data injection attacks to state estimator and injected arbitrary errors into the certain state variables without being detected. The study indicates that design of undetectable false data injection attacks is possible even the adversary has limited resources.

(Teixeira et al. 2010) introduced stealthy deception attacks against state estimators in SCADA system operating in power grids. The researchers indicated that widely used bad data detection hypothesis tests, i.e. the performance index test and the largest normalized residual test, do not guarantee detection of cyber-attacks.

(Djouadi et al. 2014) studied on sensor signal attacks on observer-based controlled systems and formulate optimal sensor attack for both finite and infinite horizon linear quadratic (LQ) control. Then, the researchers considered actuator signal attack case and introduce optimal actuator attack for both finite and

infinite horizon LQ control on observer-based controlled systems (Djouadi et al. 2015).

(Ayas and Djouadi 2016) focused on theoretical analysis of undetectable sensor and actuator attacks on observer-based controlled systems. The researchers formulated explicit equations of both undetectable sensor and actuator signal attacks. Furthermore, they showed that the actuator signal attack is optimal in the sense of minimal energy attack signal.

(Hao et al. 2015) introduced stealthy attack design strategies for state estimators in power grid. The researchers indicated that the proposed random attack construction algorithm is able to launch exceptionally sparse attack vectors and these attacks successfully compromise certain state variables.

(Feng et al. 2017) presented a deep learning-based framework to launch stealthy attacks on industrial control systems with minimal a-priori knowledge of system. The researchers also showed that the proposed framework contains an adversarial learning method providing bypass the employed anomaly detector. In addition, the framework determined the optimal amount of bias injection at each time step.

(Wu et al. 2018) studied on the effect of optimal data injection attack which is characterized considering optimal control theory. Two different design problem were considered by the researchers who emphasized that the proposed optimal attack strategies have a high possibility to be launched. The impressive side of this study is that the adversaries can analyze the worst case impact of the applied attack according to the attack location.

(Lu and Yang 2020) examined the effects of false data injection attacks on power networks under sensor failures. A bad data detector and a state estimator were used in the power networks. They design a class of sparse undetectable attack (SUA) to decrease state estimation performance without being detected. The effectiveness of the proposed SUA design was demonstrated using IEEE 5, 9, and 30-bus systems. The proposed SUA disrupt the state estimator and as a result, the bad data detector fails to detect both sensor failures and the designed attacks.

(Song et al. 2019) studied on problem of state estimation problem for multi-sensor systems subjected to undetectable attacks. First, a sufficient condition was derived for the undetectable attack. Then, an undetectable attack design method was presented. The researchers showed the performance of the proposed attack scheme and estimator under by carrying out a simulation example.

3. ATTACK DETECTION STRATEGIES for a NCPS

Attack detection strategies for a NCPS should take both cyber and physical layers of the NCPS into consideration. In addition to traditional IT systems considering network traffic and try to keep data safe, physical plant should also be taken into account to detect attacks. Therefore, a model of the physical plant is required to predict behavior of the plant to a known control input signal. Assume that the control signal $u_a(t)$ seen in Fig. 3 is a regular control signal produced by the controller, i.e. $u_a(t)$ is not under attack, and $u_a(t)$ can be monitored meaning that it is known. Then, using the model of the physical plant, expected output signal, i.e. $\hat{y}(t)$ can be estimated. The estimated output signal is simply compared to measured sensor output signal $y(t)$ to potentially detect any sensor side attack mentioned in the previous section. If the attacker has spoofed the sensor data, an alarm is triggered at that time. The same scenario can be modified to detect actuator side attacks and state estimator side attacks. Note that there might be false alarm depending of the estimation accuracy of the considered signals, i.e. $\hat{y}(t)$, $\hat{u}_a(t)$, and $\hat{x}_a(t)$. As a result, in order to detect attacks on a physical plant, the model of the plant and a detector, i.e. anomaly detection algorithm, are required. Fig. 5. shows a general architecture utilized for attack detection on a NCPS. Should be noted that the detector part of the framework is actually the main part that the researchers focus on to detect subjected attacks summarized in Fig. 4. For instance, (Mo et al. 2014) proposed χ^2 failure detector to detect replay attack, while (Hu et al. 2019). proposed a residual based detection approach by using skewness analysis of the residual signal. In the architecture given in Fig. 5., alarm is triggered by considering both produced control signals and measured output sensor signals. In the scenario given in the figure, attackers spoof both actuator A_2 and sensor S_2 and so alarm is triggered.

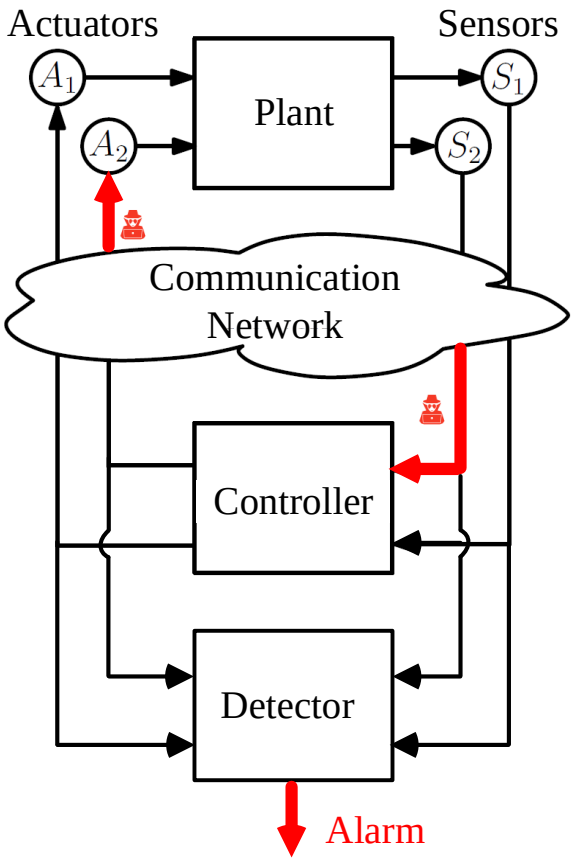

Figure 5. A general architecture utilized for attack detection

The aforementioned attack detection architecture actually based on monitoring regular behavior of the physical plant. By considering this manner, researchers have performed studies on attack detection strategies for

NCPSs from the perspective of control theory. Some of recent ones are discussed below.

(Pasqualetti et al. 2013) designed both distributed and centralized attack detection and identification monitors by considering monitoring limitations of CPSs subject to exogenous attacks. The IEEE 118 bus system and the IEEE RTS96 power network subjected to false data injection attack were utilized to show the effectiveness of the designed monitors even under noises and uncertainties. (Pasqualetti et al. 2013) showed that dynamic monitors have superiority over static monitors.

(Manandhar et al. 2014) studied detection of false data injection attacks on smart grids. They presented a robust security framework based on the χ^2 detector and Euclidean detector, which was also proposed in the study. Kalman filter which fed these detectors was used as the estimator. The proposed framework was tested on IEEE 9-bus power systems both using χ^2 detector and Euclidean detector. The obtained results show that Euclidean detector is capable of detecting statistically derived false data injection attacks while χ^2 detector is not capable of detecting them.

(Liu et al. 2014) introduced a false data detection framework for power grids. They defined detection of false data injection attacks as a matrix separation problem. Low rank matrix factorization and nuclear norm minimization were used to solve this problem. IEEE 57 and 118-bus systems were utilized in numerical experiments to illustrate the performance of the proposed detection framework. The results indicate that malicious attacks in the power grids are detected by the framework.

(Mo et al. 2014) presented a problem containing Kalman estimator, LQG optimal controller, and χ^2 failure detector for an LTI system. They showed that replay attack is feasible and proposed countermeasures against replay attack. A zero-mean Gaussian noise signal was utilized as authentication signal. The authentication signal was added as a marking to optimal control signal produced by the LQG controller. Although this marking process improved detectability of the replay attack, the control performance of the system was decreased. Therefore, the relationship between control performance and detection rate was characterized in the study by considering maximum control performance and detection rate.

(Rawat et al. 2015) introduced the χ^2 detector and cosine similarity matching approaches in order to detect false data injection attacks on smart grids. Kalman filter was utilized to estimate expected measurement values and a comparison was performed between the estimated and measured real values for attack detection. Numerical experiments were carried out and the results indicate that cosine similarity matching approach is capable of detecting both false data injection attacks and random attacks whereas χ^2 detector is competent of detecting only random attacks.

(Deng et al. 2017) proposed a defense framework against false data injection attacks on power systems. They designed a least-budget defense framework to enhance immunity against this kind of attacks by considering the relationship of a rational attacker and defender. In addition, (Deng et al. 2017) presented solution to meter selection problem, which was considered as a mixed integer nonlinear programming problem and solved thanks to Bender's decomposition. Numerical experiments were carried out by using IEEE 9, 14, 30, 118, and 300-bus systems to verify the proposed defense framework.

(Hu et al. 2019) focused on detection of stealthy attacks on CPSs. They proposed a residual based detection approach by using skewness analysis of the residual signal. Hu et al. showed that a residual signal has a skewed distribution if an adversary perform a specific attack. Therefore, stealthy attacks on CPSs can be detected by considering residual skewness coefficients obtained from regular case, i.e. attack-free case, and under attack case of the CPSs. On two different experiments, effectiveness of the skewness analysis based approach was verified. The researchers indicated that the proposed approach has the disadvantage of parameter selection which depends on human experience. It was emphasized that the proposed approach is suitable for real-time implementation.

(Li et al. 2019) presented a cyberattack detection framework based on online learning algorithms for industrial control system. The researchers proposed adaptive regularized cost-sensitive multiclass online learning scheme to detect cyberattack in the industrial control system. They utilized power system and gas pipeline to demonstrate the performance of the proposed cyberattack detection framework. The results show that the proposed online learning scheme is effective for cyberattack detection in industrial control systems.

(Luo et al. 2019) proposed a framework for smart grids to detect bias injection attacks and isolate them. They introduced nonlinear observer-based distributed detection method, which was demonstrated to be robust against external disturbances. In addition, the researchers also presented an interval residual-based detection standard to emphasize the restrictions of the predefined threshold.

4. CONCLUSION

Some of the studies in the literature about attack design and detection strategies for NCPSs from the perspective of control theory are briefly presented in this paper. In most of the studies, researchers assume that all state variables are either accurately measurable or determined utilizing some kind of estimators. Furthermore, some of them formulate the attack strategy for either single-input and single-output (SISO) systems or multiple-input and multiple-output (MIMO) systems. However, uncertainties of system parameters and process noises should be considered. In addition, attack design strategies should be characterized for both SISO and MIMO systems. One more opinion is to focus on optimal attack strategies to inject worst case attack to NCPs instead of specific attacks based on many assumptions.

In a general manner, attack design and detection strategies for NCPSs is a difficult issue and requires

approaches from different areas such as robust control, fault-tolerant control, systems, networked control systems and big data analysis.

REFERENCES

Amin S, Cárdenas A A & Sastry S S (2009). Safe and secure networked control systems under denial-of-service attacks. In International Workshop on Hybrid Systems: Computation and Control. Springer, Berlin, Heidelberg, 5469, 31-45. ISBN 978-3-642-00602-9

Ayas M S & Djouadi S M (2016). Undetectable sensor and actuator attacks for observer based controlled Cyber-Physical Systems. IEEE Symposium Series on Computational Intelligence, 1-7. DOI: 10.1109/SSCI.2016.7849882

Barthels A, Ruf F, Walla G, Fröschl J, Michel H U & Baumgarten U (2011). A model for sequence based power management in cyber physical systems. In International Conference on Information and Communication on Technology. Springer, Berlin, Heidelberg, 87-101. ISBN 978-3-642-23447-7

Cárdenas A A, Amin S & Sastry S (2008). Secure control: Towards survivable cyber-physical systems. The 28th International Conference on Distributed Computing Systems Workshops, Beijing, China, 495-500. DOI: 10.1109/ICDCS. Workshops.2008.40

Chen J, Tan R, Xing G, Wang X & Fu X (2012). Fidelity-aware utilization control for cyber-physical surveillance systems. IEEE Transactions on Parallel and Distributed Systems, 23(9), 1739-1751. DOI: 10.1109/TPDS.2012.74

Conti J P (2010). The day the samba stopped [power blackouts]. Engineering & Technology, 5(4), 46-47. DOI: 10.1049/et.2010.0410

Deng R, Xiao G & Lu R (2017). Defending against false data injection attacks on power system state estimation. IEEE Transactions on Industrial Informatics, 13(1), 198-207. DOI: 10.1109/TII.2015.2470218

Djouadi S M, Melin A M, Ferragut E M, Laska J A & Dong J (2014). Finite energy and bounded attacks on control system sensor signals. 2014 American Control Conference, Portland, Oregon, USA, 1716-1722. DOI: 10.1109/ACC.2014.6859001

Djouadi S M, Melin A M, Ferragut E M, Laska J A, Dong J & Drira A (2015). Finite energy and bounded actuator attacks on cyber-physical systems. 2015 European Control Conference (ECC), Linz, Austria, 3659-3664. DOI: 10.1109/ECC.2015.7331099

Feng C, Li T, Zhu Z & Chana D (2017). A deep learning-based framework for conducting stealthy attacks in industrial control systems. arXiv preprint arXiv:1709.06397. Available online: https://arxiv.org/abs/1709.06397

Hao J, Piechocki R J, Kaleshi D, Chin W H & Fan Z (2015). Sparse malicious false data injection attacks and defense mechanisms in smart grids. IEEE Transactions on Industrial Informatics, 11(5), 1-12. DOI: 10.1109/TII.2015.2475695

Hu Y, Li H, Yang H, Sun Y, Sun L & Wang Z (2019). Detecting stealthy attacks against industrial control systems based on residual skewness analysis. EURASIP Journal on Wireless Communications and Networking, 74. DOI: 10.1186/s13638-019-1389-1

Karnouskos S (2011). Stuxnet worm impact on industrial cyber-physical system security. IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society, Melbourne, VIC, Australia, 4490-4494. DOI: 10.1109/IECON.2011.6120048

Kleissl J & Agarwal Y (2010). Cyber-physical energy systems: Focus on smart buildings. Design Automation Conference, Anaheim, CA, USA, 749-754. DOI: 10.1145/1837274.1837464

Kuvshinkova S (2003). SQL Slammer worm lessons learned for consideration by the electricity sector. North American Electric Reliability Council, 1(2), 5.

Lau J K S, Tham C K & Luo T (2011). Participatory cyber physical system in public transport application. 2011 Fourth IEEE International Conference on Utility and Cloud Computing, Victoria, NSW, Australia, 355-360. DOI: 10.1109/UCC.2011.59

Lee I & Sokolsky O (2010). Medical cyber physical systems. Design automation conference, Anaheim, CA, USA, 743-748.

Li G, Shen Y, Zhao P, Lu X, Liu J, Liu Y & Hoi S C H (2019). Detecting cyberattacks in industrial control systems using online learning algorithms. Neurocomputing, 364, 338-348. DOI: 10.1016/j.neucom.2019.07.031

Liu L, Esmalifalak M, Ding Q, Emesih V A & Han Z (2014). Detecting false data injection attacks on power grid by sparse optimization. IEEE Transactions on Smart Grid, 5(2), 612-621. DOI: 10.1109/TSG.2013.2284438

Liu Y, Ning P & Reiter M K (2011). False data injection attacks against state estimation in electric power grids. ACM Transactions on Information and System Security (TISSEC), 14(1), 13. DOI: 10.1145/1952982.1952995

Lu A Y & Yang G H (2020). False data injection attacks against state estimation in the presence of sensor failures. Information Sciences, 508, 92-104. DOI: 10.1016/j.ins.2019.08.052

Luo X, Wang X, Zhang M & Guan X (2019). Distributed detection and isolation of bias injection attack in smart energy grid via interval observer. Applied Energy, 256, 113703. DOI: 10.1016/j.apenergy.2019.113703

Manandhar K, Cao X, Hu F & Liu Y (2014). Detection of faults and attacks including false data injection attack in smart grid using Kalman filter. IEEE transactions on control of network systems, 1(4), 370-379. DOI: 10.1109/TCNS.2014.2357531

Meng W, Liu Q, Xu W & Zhou Z (2011, September). A cyber-physical system for public environment perception and emergency handling. IEEE International Conference on High Performance Computing and Communications, Banff, AB, Canada, 734-738. DOI: 10.1109/HPCC.2011.104

Mo Y, Chabukswar R & Sinopoli B (2014). Detecting integrity attacks on SCADA systems. IEEE Transactions on Control Systems Technology, 22(4), 1396-1407. DOI: 10.1109/TCST.2013.2280899

Mo Y, Garone E, Casavola A & Sinopoli B (2010). False data injection attacks against state estimation in wireless sensor networks. 49th IEEE Conference on

Decision and Control (CDC), Atlanta, GA, USA, 5967-5972. DOI: 10.1109/CDC.2010.5718158

Pasqualetti F, Dörfler F & Bullo F (2013). Attack detection and identification in cyber-physical systems. IEEE transactions on automatic control, 58(11), 2715-2729. DOI: 10.1109/TAC.2013.2266831

Pasqualetti F, Dorfler F & Bullo F (2015). Control-theoretic methods for cyberphysical security: Geometric principles for optimal cross-layer resilient control systems. IEEE Control Systems Magazine, 35(1), 110-127. DOI: 10.1109/MCS.2014.2364725

Rawat D B & Bajracharya C (2015). Detection of false data injection attacks in smart grid communication systems. IEEE Signal Processing Letters, 22(10), 1652-1656. DOI: 10.1109/LSP.2015.2421935

Sandberg H, Amin S & Johansson K H (2015). Cyberphysical security in networked control systems: An introduction to the issue. IEEE Control Systems Magazine, 35(1), 20-23. DOI: 10.1109/MCS.2014.2364708

Slay J & Miller M (2007). Lessons learned from the maroochy water breach. International Conference on Critical Infrastructure Protection, Springer, Boston, MA, 73-82.

Song H, Shi P, Lim C C, Zhang W A & Yu L (2019). Attack and estimator design for multi-sensor systems with undetectable adversary. Automatica, 109, 108545. DOI: 10.1016/j.automatica.2019.108545

Teixeira A, Amin S, Sandberg H, Johansson K H & Sastry S S (2010). Cyber security analysis of state estimators in electric power systems. 49th IEEE conference on decision and control (CDC), Atlanta, GA, USA, 5991-5998. DOI: 10.1109/CDC.2010.5717318

Teixeira A, Shames I, Sandberg H & Johansson K H (2015). A secure control framework for resource-limited adversaries. Automatica, 51, 135-148. DOI: 10.1016/j.automatica.2014.10.067

Wang Y, Vuran M C & Goddard S (2008). Cyber-physical systems in industrial process control. ACM Sigbed Review, 5(1), 12. DOI: 10.1145/1366283.1366295

Wu G, Sun J & Chen J (2018). Optimal data injection attacks in cyber-physical systems. IEEE transactions on cybernetics, 48(12), 3302-3312. DOI: 10.1109/TCYB.2018.2846365