A survey on the recent development of securing the networked control systems

Qinyi Wang and Hongjiu Yang

ABSTRACT

Recent years witness an ever-increasing research interest in the study of securing the Networked Control Systems due mainly to the trend of integrating the advanced communication technology into the traditional control system. As a result, the control system becomes prone to the cyber attacks and a number of serious security incidents of the industrial control system are reported. Firstly, we recall the most recent occurred security incident of control system, and various types of control-system-oriented cyber attacks are introduced. Then, a wealth of resilient control methodologies are presented which aim to securing the control system. Finally, the applications of the resilient control method to the power system is introduced.

1. Background

In recent years, networks have been received considerable attentions with the rapid development of network technologies. It has become an inevitable trend for combining networks with control systems. At present, Networked Control System (NCSs) have been widely applied in strategic and significant industrial fields such as electrical power systems, chemical industry, manufacturing industry, natural gas systems, etc. (Hespanha, Naghshtabrizi, & Xu, 2007; Yuan, Guo, & Wang, 2017; Yuan, Wang, & Guo, 2018; Yuan, Yuan, Wang, Guo, & Yang, 2017; Zhang, Gao, & Kaynak, 2013). Equipped with networks, control systems have more advantages in mobility and flexibility. However, the introduced networks also bring some new challenging problems on control systems. Although, it reduces costs to transmit control commands or measurement signals via public networks, the inherent closeness of control systems is inevitably broken. Traditional control systems adopted ignores signal transmission protocols. At present, standard transmission protocols and commercial operation systems are used for control systems, which will seriously increase attacked possibilities. Although control systems have high requirements for real time and availability, a lot of control systems ignore or even deliberately decrease security protection from security protection perspective. From external environment perspective, a variety of attack strategies are developed. Attacks aiming at industry control systems are emerging in an endless stream now (Wu, Ota, Dong, & Li, 2016; Zhu, Rieger, & Başar, 2011).

Very recently, the following security incidents occur:

- In 2010, the first nuclear power station in Iran was attacked by Stuxnet which was a malicious computer worm targeting industrial computer systems. The nuclear program of Iran was delayed seriously by the Stuxnet attack (Langner, 2011).
- In April 2016, a nuclear power plant in Germany was attacked by ‘Conficke’ and ‘W32.Ramnit’ viruses which were discovered at the nuclear power plant’s Block B Information Technology (IT) networks that handled the fuel handling system.
- In November 2016, San Francisco’s Municipal Railway was hacked, which seriously resulted in the unavailability of the railway fare system.
- In December 2016, Ukraine Electric Grid was attacked simultaneously at three regional power firms, which led to electricity black-out for 225,000 Ukrainian power customers. Before attacks, adversaries prepared for six months of reconnaissance, then they broke into the utility’s networks via attack.

Among the aforementioned control system security events, the Stuxnet viruses specifically target at industrial control systems by infecting Programmable Logic Controllers (PLCs). According to statistics, personal computers at least 60% have been affected with Stuxnet viruses.
Moreover, Stuxnet has generated a lot of homeotic viruses such as Duqu viruses, Flame viruses and so on (Virvilis & Gritzalis, 2013). It is shown from Figure 1 that the numbers of security events have increased, which is reported by the industrial control systems cyber emergency response team. From Figure 1, it is seen that security events in industrial control systems are increasing year after year. Due to the fact that industrial control systems play key roles in national infrastructure, the poor security of control systems seriously threatens republic lives. Therefore, many countries have adopted essential steps to enhance the security of industrial control systems. In America, the Department of Energy has established the national Supervisory Control And Data Acquisition (SCADA) test bed program and a 10-year outline for the protection of industrial control systems (Cárdenas, Amin, & Sastry, 2008). Oak Ridge National Laboratory, Edward National Laboratory and some other universities have investigated the security of control systems. In 2012, Japan has also established the centre of industrial control systems for the purpose of enhancing the network security for key infrastructures. In 2013, the European union agency for network and information security has published the white paper on industrial control system network security. IEEE Transactions on Cybernetics, IEEE Transactions on Automatic Control and IEEE Transactions on Industrial Informatics have held special issues on industrial control system security. At present, industrial control system securities have received significant attentions in the world.

In the following, we present some typical examples of control systems which are vulnerable to cyberattacks.

An Unmanned Aerial Vehicle (UAV) communication and control system is shown in Figure 2. It consists of UAV, navigation satellite, mobile ground control station, ground control station and so on. Among the aforementioned portions, there exist communication links. Network adversaries are able to attack the communication links to affect UAV control. For example, in the ‘RQ-170 Sentinel Event’ of the United States, an UAV was captured for the reason that the navigation communication networks were attacked. In addition, since the UAVs can communicate with each other, if an UAV is attacked, then the other UAVs will also get affected.

Figure 3 is an SCADA system architecture diagram which generally includes a data acquisition and a control terminal equipment which are also named the slave computer and the host computer, respectively. The slave computer usually consists of Remote Terminal Cells and PLCs. On the other hand, the typical host computer system comprises workstation, data server, web server, SCADA server and so on. Due to the wide deployments of SCADA systems, it is easy for adversaries to get access to the SCADA systems. They are capable of directly attacking actuators or sensors in the slave computer.

2. Form of attacks in NCSs

This section presents potential attack forms in NCSs, and some typical attack forms are illustrated emphatically in the following.
Attacks against physical objects (Peng et al., 2012): Attacks against physical objects are a kind of attack form which targets at physical structures such as controllers, actuators, sensors, or plants. The attack model of attacks against physical objects is shown in Figure 4.

Integrity attacks (Mo, Chabukswar, & Sinopoli, 2014): For integrity attacks, attackers intentionally modify control commands or measurement data to compromise the NCSs. The NCSs are affected by wrong operations for the reason that wrong external information is launched. Moreover, the integrity attack can be further subdivided into deception attack, cover attack, replay attack and data injection attack (Zhu & Martinez, 2014). Among the attacks, deception attacks compromise the NCSs via fault detection and isolation systems. In a fault detection and isolation system, filtering algorithms are usually used to calculate an estimated value of sensor measurement. If the difference between the measured value and estimated value is larger than a given threshold, then the fault detection and isolation system will trigger alarm. Deception attacks are to interfere with control or measurement processes of the NCSs without triggering an alarm. The attack model of integrity attacks is shown in Figure 5.

Availability attacks (Carl, Kesidis, Brooks, & Rai, 2006; Huang, Ahmed, & Karthik, 2011; Yuan & Sun, 2015): Availability attacks are also called denial-of-service (DoS)/jamming attacks which aim at preventing the control command or sensor measurement from being sent to intended users by interfering communication channels. When DoS attacks interfere transmission channels of NCSs, the additional time delays and packet dropout are caused. Note that the current NCSs have high requirements for real-time properties. Any additional time delays or packet dropout will have a serious impact on the performance of NCSs, even lead to instability of the NCSs. The attack model of DoS attacks is shown in Figure 6.

3. The study of attacks on NCSs

3.1. Attacks in networked control systems

In 1998, G. C. Walsh put forward a concept of NCSs for the first time at the university of Maryland. Then problems of modelling for the NCSs have been much studied deeply, such as time delays, packets dropout, data confusion and other issues. In particular, the inherently limited bandwidth of communication channels has led to a number of network-induced phenomena, which is worth exploiting. Note that the phenomena of packets dropout and communication delays have attracted much attentions for the reason that they are considered to be two of the main causes of the performance degradation or even instability of the NCSs (He, Wang, Wang, & Zhou, 2014; Yang, Wang, Hung, & Gani, 2006).

Compared with traditional point-to-point systems, NCSs have many advantages, such as fewer expenses, higher flexibility and better resource sharing, please refer to Li, Yang, Sun, and Xia (2014), Wu, Lam, Yao, and Xiong (2011), Wu et al. (2011), Niu and Ho (2014), and Caballero, Hermoso, and Linares (2015), and the references therein. Nevertheless, an ever-increasing popularity of communication networks also brings new challenges. The exposure to public networks renders control systems as targets of potential cyber attacks. As connection of information world and reality, control systems targeted by cyber attacks can lead to serious incidents, which has been verified during the past decade (Huang et al., 2009; Park, Kim, Lim, & Eun, 2014). By
targeting at different components of control systems, attackers can launch various types of attacks. Most of these control-system-oriented attacks can be categorized as deception attacks and DoS attacks which compromise data integrity and data availability, respectively. The deception attack is launched by directly modifying the control or measurement signal and it is further categorized as cover attacks (Smith, 2015), data injection attacks (Law, Alpcan, & Palaniswami, 2015), stealthy attacks (Dan & Sandberg, 2010) and replay attacks (Mo et al., 2014). While DoS attacks or jamming attacks are launched by corrupting the communication channels of NCSs. DoS attacks usually lead to congestions in communication networks, causing time delays and packets dropout. It is worth mentioning that DoS attacks, which compromise the data availability, are vital for the reason that all control systems operate in real time. For example, control systems using deadline corrective control may be driven to instability under DoS attacks (Yuan, Sun, & Liu, 2015). Unlike deception attacks, DoS attacks which require little prior knowledge on control systems are also easy to apply. Hence, the DoS attacks have been listed as the most financially expensive security incidents (Long, Wu, & Hung, 2005). Thus, securing NCSs under DoS attacks raise major concerns. In Amin, Cardenas, and Sastry (2009), a class of DoS attack models have been considered to find an optimal causal feedback controller by minimizing a given objective function subject to safety and power constraints. When NCSs with multi-tasking and central-tasking structures suffer from DoS attacks, optimal control strategies have been presented by game theory in delta domain (Yuan, Yu, Guo, Yang, and Sun (2016). In Li, Shi, Cheng, Chen, and Quevedo (2015), a game theoretic approach has been utilized to analyse a Nash equilibrium problem between sensors and attackers. Considering a Markov modulated DoS attack strategy, attackers stochastically jam control packets in NCSs with a hidden Markov model (Befekadu, Gupta, & Antsaklis, 2015). When an energy-constrained attacker jams a networks channel, the optimal DoS attack strategy is provided to degrade system performances from the attacker’s aspect (Zhang, Cheng, Shi, & Chen, 2016). Though various attack schemes have been studied, optimal DoS attack schemes which are dangerous to NCSs have not been studied in depth yet. Moreover, it is very interesting to analyse optimal attack schemes for their serious harms on NCSs. Actually, there have been a number of literatures addressing the problem on resilient control under DoS attacks (Amin et al., 2009; Li et al., 2012; Yuan & Sun, 2015; Yuan et al., 2015).

As far as we know, most of these literatures can be categorized as attack tolerant resilient control methods and attack compensation resilient control methods. For the first category, the resilient control strategies can tolerant a certain level of negative effects caused by DoS attacks. To be specific, resilient control strategies are developed such that NCSs remain within the safety zone in spite of DoS attack induced time delays or packets dropout. For example, a semi-definite programming method has been used to minimize the objective function subject to power and safety constraints in Amin et al. (2009). Stability conditions of an event trigger system under DoS attacks has been exploited in Li et al. (2012). A model predictive resilient control method has been proposed in Zhu and Martínez (2014), where predictive values are used if DoS attack occurs.

For the second category, resilient control methods are employed to compensate for the control performance degradation caused by DoS attacks. In Yuan et al. (2015), Yuan and Sun (2015), and Zhu and Başar (2015), IDss have been deployed in the cyber layer which can defend against DoS attack and improve performances of underlying control systems. Data-sending strategies to contradict the negative influence of DoS attacks have been developed in Li, Shi, Cheng, Chen, and Quevedo (2013). From the aforementioned literature, it can be concluded that game theory employed intensively in resilient control is a powerful tool in characterizing cooperation and contradiction among agents. Furthermore, some works investigate Networked Predictive Control (NPC) schemes to cope with DoS attacks on NCSs (Du, Sun, & Wang, 2014). NPC schemes have been always used to compensate random delays and consecutive packets dropout (Du et al., 2014; Pang, Liu, & Zhou, 2016; Yang, Liu, Shi, Thomas, & Basin, 2014). Based on a switched system approach, stability analysis on NPC systems has been established via an average dwell time technique in Zhang, Xia, and Shi (2013). The NPC scheme has been utilized well on NCSs under deception attacks (Pang & Liu, 2012). Unfortunately, optimal control by using NPC methods has not been adequately investigated on the security issues of NCSs yet.

In practice, all real-time NCSs operate in the presence of disturbances caused by a number of factors (Guo & Cao, 2014), including the fluctuation of communication environment (Yang, Fan, & Zhang, 2015), channel fading (Xiao, Xie, & Qiu, 2012), quantization effects (Tsumura, Ishii, & Hoshina, 2009), load variation (Ginoya, Shendge, & Phadke, 2015), friction (Zhao, Yang, Xia, & Liu, 2015) and measurement noises (Yao & Guo, 2013). Therefore, the study on NCSs with external disturbances is of great importance from both theoretical and engineering points of view (Guo & Chen, 2005; Wei, Chen, Deng, Liu, & Tang, 2012; Yang, Li, Sun, & Guo, 2013). So far, a number of advanced control approaches have
been developed to deal with the optimal control problem on NCSs. It is worth mentioning that the disturbances acting on the underlying dynamics will exert impact on the optimum of cost functions. Nevertheless, it has been implicitly assumed that no disturbance exists or all the disturbances have been fully estimated and compensated in most literature concerning the optimal control of NCSs. It has been shown that the influence from the disturbances on the optimum is largely neglected (Tan & Jose, 2010; Wang, Liu, Wei, Zhao, & Jin, 2012; Xu, Jagannathan, & Lewis, 2012).

Summarizing the above results, we arrive at the conclusion that several challenges still remain despite all the reported literature on securing NCSs. One of such challenges is to develop optimal control strategies subject to DoS attacks in delta-domain and provide optimal defense and attack strategies for the designed NCSs. The second challenging problem is how to quantify the influence from the disturbances and packets dropout in terms of the concept of \( \epsilon \)-level, which are equally important for the NCSs. Another challenge is to find a defense strategy based on NPC to cope with DoS attacks under optimal schemes.

### 3.2. Resilient control of WNCSs

In recent years, Wireless Networked Control Systems (WNCSs) have experienced an ever-increasing development in fields of theory and practice. In WNCSs, the sensor and actuator communicate with the controller through wireless networks. Compared with traditional NCSs, WNCSs have considerable advantages, such as reduced wires and low installation and maintenance cost. However, the wireless networks are more vulnerable than wired networks, which may be caused by weather changing, multi-path propagation, doppler shift, networked attacks and so on. Considering the dynamic wireless networks which result in poor communication performance are vital in the design of WNCSs (Chorppath, Alpcan, & Boche, 2016). Additionally, utilizing the inherent nature of ‘openness’ of WNCSs, malicious attackers can destroy communication facilities and control systems (Yang, Xue, Zhang, Richa, & Fang, 2013). Thus, a deal of literature focusing on the security of WNCSs have been found as (Li, Quevedo, Dey, & Shi, 2016; Li et al., 2015; Yang, Ren, Yang, Shi, & Shi, 2015; Zhang et al., 2016), and the references therein. Some advanced results have been presented on the security problem of NCSs during the latest years. In Teixeira, Perez, Sandberg, and Johansson (2012), attack scenarios have been modeled and analysed according to a three-dimensional resource framework. In Pang, Liu, Zhou, Hou, and Sun (2016), two-channel false data injection attacks against output tracking problem of NCSs have been investigated. To detect integrity attacks, the probability of detection has been optimized by conceding system performance (Mo et al., 2014).

On the other hand, the security issues for remote state estimation connected by wireless channels have been studied in Li et al. (2015) and Li et al. (2016), and Markov game theoretic approaches have been used to obtain the optimal attack and defense strategies with energy constrained sensor and attacker. Then, multiple power levels have been available for sensor and attacker in remote state estimation system, and the mixed Nash equilibrium strategies have been obtained under the framework of Signal-to-Interference-plus-Noise Ratio (SINR)-based game (Li et al., 2015). In Yuan et al. (2016), the closed-loop system performance degradation caused by DoS attacks has been compensated by inverse game pricing method. The optimal attack and defense strategies have been obtained by modelling the attacker and defender as a Stackelberg game (Yuan et al., 2016). It makes practical sense to investigate SINR-based attack scheme for enhancing resilience of the closed-loop WNCSs. To analyse jamming attacks on the cyber-layer of WNCSs, game theory which also acts as a powerful tool has been employed to model interactions between legitimate users and malicious jammers (Chen, Song, Xin, & Backens, 2013). A stochastic game framework for anti-jamming defense design is proposed with time-varying spectrum environment in a cognitive radio network (Wang, Wu, Liu, & Clancy, 2011). In Sagduyu, Berry, and Ephremides (2011), a Bayesian jamming game between a legitimate transmitter and a smart jammer is discussed when there exists incomplete information for every network user. In Xiao, Chen, Liu, and Dai (2015), a power control strategy of a legitimate user against a smart jammer under power constraints is handled as a Stackelberg game with observation errors. The jammer which acts as a follower chooses a jamming power according to an observed ongoing transmission, while the user as a leader determines its transmitting power based on an estimated jamming power. The Stackelberg game is a well-developed and appropriate method to cope with hierarchical interactions among players in anti-jamming field (Yang et al., 2013). Furthermore, an anti-jamming Bayesian Stackelberg game with incomplete information is proposed in Jia, Yao, Sun, Niu, and Zhu (2016).

Virtually, all the WNCSs operate in the presence of disturbances which are caused by many factors such as load variation (Ginoya et al., 2015), friction (Zhao et al., 2015) and measurement noise (Yao & Guo, 2013). Therefore, considering the influence of disturbances on WNCSs is of great importance (Guo & Cao, 2014). The \( H_\infty \) minmax control theory (Basar & Olsder, 1995) which addresses the worst case controller design for plants makes systems...
achieve the optimal performance under disturbances. The $H_\infty$ minimax control has advantages comparing with the traditional observer-based disturbance control method when it is difficult to model the disturbances. A number of advanced results for NCSs or WNCSs have been presented, e.g. (Li, Yang, Sun, & Xia, 2013; Yuan & Sun, 2015; Yuan et al., 2015) and the references therein. Furthermore, a resilient control problem is investigated when WNCSs suffer malicious DoS or jamming attacks in cyber-layers with $H_\infty$ minimax control theory.

Summarizing the above discussions, although the security of WNCSs has been widely investigated in a deal of literature, several urgent issues still exist. The first one is to analyse the interaction between defender and attacker via a hierarchical game approach and design an $H_\infty$ minimax controller in delta-domain to guarantee the optimal system performance for high frequency sampled WNCS under disturbance. The second one is that comprehensively analysing interconnections between the cyber layer and physical layer, how to design cross layer control strategies such that the studied WNCS can remain stability in spite of the DoS attacks. The last one is that how to establish a Bayesian Stackelberg game framework between a malicious jammer and a legitimate user due to the incomplete information, and how to design an $H_\infty$ minimax controller to guarantee the optimal WNCS performance under disturbances.

### 3.3. Coupled design of CPS under attacks

In recent decades, the coupled design of Cyber-Physical Systems (CPSs) under attacks has been paid widely attention, since a number of critical infrastructures have been compromised by DoS attacks, as reported in Huang et al. (2009), Kisner et al. (1995), and Geer (2006). Design of such systems requires a system perspective towards cyber-physical systems against threats and malicious behaviour. Note that state awareness of ICSs under attacks has been discussed in Melin, Kisner, Fugate, and McIntyre (2012). A passivity combined with an adaptive sampling approach to design a control architecture is proposed in Eyisi, Koutsoukos, and Kottenstette (2012), and the method shows certain robustness to network uncertainties. As mentioned in Zhu et al. (2011), the Siemens SCADA systems have been compromised by Stuxnet which is a computer worm. It has also been reported in Matusitsa and Mineib (2009) that a hacker intruded and shut down a traffic air control system tower at Worcester Regional Airport USA.

Assumptions become much smarter at present. The traditional separate design of cyber layers and physical layers appears weaker than before. CPSs are a combination of physical systems and cyber systems, where the cyber systems receive real-time data from the physical systems. CPSs integrate networked computational resources into physical processes in order to add new capabilities into an original system. Due to the development of networks, the concept of resilient control emphasizing controller design in adversarial cyber environment has been proposed in Rieger, Gertman, and McQueen (2009). The aim of resilient control is to maintain an accepted level of operational normalcy in response to both external disturbances in the physical layer and malicious attacks in the cyber layer. Thus, Resilient Control Systems (RCSs), which have fully coupled cyber module and control module, require a holistic view and cooperation between IT expert and control expert. RCSs have been studied under replay attacks in Zhu and Sonia (2011), and a class of competitive resource allocation problems are characterized as convex games. RCSs have been modelled as a two-level receding-horizon dynamic Stackelberg game, in which the coupled decision-making process between control system operator and jammer has been considered (Zhu & Sonia, 2011).

In order to reduce the loss of DoS attack, many approaches have been proposed for CPSs. A game-theoretical method, which is a powerful tool to model the interactions among agents, has been also used to model the cyber attack and defense (Alpcan & Başar, 2010). Attack-resilient control built within a framework of game theory, has been tackled in recent years. Hybrid models have been proposed for RCSs, in which stochastic switching is governed by a Markov security game (Yuan, Zhu, Sun, Wang, & Başar, 2013; Zhu & Başar, 2011). It is worth mentioning that the application of game theory to cyber security issue have background in the configuration of IDSs (Alpcan & Başar, 2010; Yuan et al., 2013; Zhu & Başar, 2009). IDSs are used to raise alarms once an anomaly behaviour, such as packets dropout or overlong time delays, are detected so that malicious attacks can be removed automatically. In the attack model, game theory has been used to describe interaction between the IDSSs and DoS attacks, and to get the best delivery package rate. By Nash Equilibrium (NE) strategies, the IDSSs obtain an appropriate tradeoff between system performances and security enforcement levels (Zhu & Başar, 2009). Some critical issues on cyber security in IDSSs require a holistic and cross layer design approach for controller design of integrated cyber-physical systems. In Giorgi, Saleheen, Ferrese, and Won (2012), an adaptive neural control architecture is used for NCSs within a resilient control framework. Parameters of an attacked plant are changed to match a reference model. However, few efforts have been made to consider integrated design of defense mechanisms in the cyber layers and controller design in the physical layers.
Summarizing current situation, coupled designs of the cyber layers and physical layers meet the following challenges. Firstly, some methodologies and principles are needed for integrated design for the reason of that the cyber systems of the IDSs are not isolated from the physical systems for defense against malicious adversaries in practical situations. Secondly, how to establish a game-in-game structure for the coupled design of RCS with the aim at obtaining the tradeoff between an outcome of inner game and a solution of out game. Thirdly, practical control systems are subject to actuator saturations which bring challenging problems for the coupled design of CPSs.

Summarizing the above discussion, it is of great urgency and necessity to develop the research on the security of NCSs.

### 4. Application of resilient control to power system

In recent years, NCSs have received an increasing research interest due to their wide applicabilities to smart grids (Lee, Clark, Bushnell, & Poovendran, 2014), intelligent transportation (Zhang et al., 2016), industrial control systems, navigation systems (Kilinc, Ozger, & Akan, 2015), teleoperation or remote systems (Truong & Ahn, 2015) and so on. For the NCSs, sensors, actuators, control processing units and communication devices are connected via networks (Han, Xie, Chen, & Ling, 2014), which renders several challenging problems such as time delays (Qiu, Li, Xu, & Xu, 2015; Zhang, Feng, Yan, & Chen, 2016), packets dropout (Li, Chow, & Sun, 2009), packets disorder (Liu, Zhang, Yu, Liu, & Chen, 2015), quantization (Peters, Quevedo, & Ostergaard, 2016; Yan, Xia, & Li, 2014), cyber attacks (Yuan et al., 2015) and so on.

Among these network-induced factors, two significant challenges are time delays and packet dropout, which lead to degradation of the control performance or even destabilize the whole controlled system (Qiu, Yu, & Zhang, 2015). For instance, deterministic time delays in NCSs have been considered in Zhang et al. (2013), Zhang et al. (2016), Chen and Han (2016), Guo, Lu, and Han (2012), and Guo (2010), and the time delays in the stochastic setting have been addressed in Dong, Wang, and Gao (2016), Chen, Gao, Shi, and Lu (2016), and Zhang, Lu, Xie, and Dong (2016). Specifically, the time delayed control system which can only accommodate a subset of actuators at any time has been exploited in Guo et al. (2012). In Chen et al. (2016), an $H_{\infty}$ control problem has been addressed for NCSs with stochastic time delays subjected to Markovian distributions. On the other hand, the NCSs with packet dropout have been exploited in Maass, Vargas, and Silva (2016), Lin, Su, Shi, Lu, and Wu (2015), Yin, Yue, Hu, Peng, and Xue (2016), Schenato, Sinopoli, Franceschetti, Poolla, and Sastry (2007), Guo and Jin (2010), and Guo et al. (2012). For instance, in Schenato et al. (2007), an optimal Linear Quadratic (LQ) gaussian control problem has been addressed with signal estimation subjected to packet dropout. In Guo and Jin (2010), a stochastic optimal control problem of nonlinear NCSs with packets dropout and long time delays has been studied. In simultaneous presence of time delays, packets dropout and measurement quantization effects, a coupled design of networked controller has been addressed in Guo et al. (2012).

Since control systems can be regarded as a connection of information world and physical world, any successful attacks on NCSs may lead to significant loss of properties or even human lives. Actually, it has already been reported in Li et al. (2016) and Pang and Liu (2012) that systems in a number of critical infrastructures are compromised by a series of attacks. Hence, many researchers have exploited the security of NCSs from both control and communication communities, please refer to Teixeira et al. (2012), Sandberg, Amin, and Johansson (2015), Li et al. (2015), Zhang et al. (2016), and Guo, Shi, Johansson, and Shi (2017) and the references therein. To avoid attacks, some IDSs are deployed in a cyber layer to raise alarms once an anomaly behaviour is detected such that it can be removed automatically. Thus, DoS attackers have to go through the IDSs firstly before they compromise a control system.

Owing to the rapid development of sensing techniques, sampling intervals of modern industrial control systems are normally quite small, and a sampled-data problem becomes very critical in system design. The delta operator approach has been well recognized in addressing sampling issues for NCSs (Yang, Xia, Shi, & Fu, 2012). Numerical-stiffness problems resulting from the fast sampling protocol can be circumvented by using the delta operator approach (Yang, Xia, Shi, & Zhao, 2012). Furthermore, some related results for both discrete-and continuous-time systems can be unified in the delta operator systems. As such, it is of vital importance to develop delta-domain results for discrete-time systems with a high sampling rate. Due to its theoretical significance and practical importance, the delta operator approach has been extensively exploited in NCSs (see, e.g. Hirano, Mukai, Azuma, & Fujiata, 2005; Li, Li, Yang, Zhang, & Sun, 2015; Yang et al., 2012; Yang, Xia, Shi, & Liu, 2013; Yang, Yan, Xia, & Zhang, 2016). Specifically, some inspiring results have been reported for some control and filtering problems of NCSs (Yang et al., 2012), a control problem on Markovian jump systems, and some robust control problems with actuator saturation (Yang et al., 2016). It has been shown in Yang et al. (2013)
that the delta-domain results can not only deal with the inherent numerical stiffness caused by the fast sampling protocol in the discrete-time NCSs, but can also adapt to dynamic network environment. In comparison with reported literatures, the delta-domain results for dynamic games have been scattered, especially within the framework of Riccati recursions (Yang et al., 2012).

Summarizing the above results, we arrive at the conclusion that, several challenges still remain despite all the reported literatures on securing NCSs. One of such challenges is to estimate the attack-induced performance degradation such that the loss does not exceed the limitation of designed NCSs. This is of vital importance for the reason that one can verify whether a system remains within safety regions with applied securities or control strategies by assessing the security level before adversarial incidents occur. The second challenging problem is that how to quantify the influences of disturbances, long delays and packets dropout on NE, which is equally important for the NCSs. Another challenge is to find a tradeoff between system performances and security enforcement levels under the coupled design of the IDSSs and controllers for the reason that higher security level IDSSs lead to control performance degradation. Electric Power Systems (EPSs) are a kind of typical NCS in national basic industry. In this part, we will mainly investigate the aforementioned issues on the EPSs.

5. Conclusion

In this paper, we have reviewed the most recent research papers on securing the NCS methodologies. A variety of control-system-oriented cyber attacks have been introduced. Furthermore, in the presence of various types of cyber attacks, the corresponding resilient control methods have been represented. Among the reported resilient control methods, it is worth mentioning that the coupled design scheme has required a holistic view towards the NCS under cyber attacks. Finally, the resilient control of power systems has been introduced because power system is a typical CPS.

Disclosure statement

No potential conflict of interest was reported by the authors.

References

Alpcan, T., & Başar, T. (2010). Network security: A decision and game theoretic approach. Cambridge: Cambridge Univ. Press. Amin, S., Cardenas, A. A., & Sastry, S. S. (2009). Hybrid systems: Computation and control. Berlin: Springer-Verlag. Basar, T., & Olsder, G. J. (1995). Dynamic noncooperative game theory. London: Academic Press. Befekadu, G. K., Gupta, V., & Antsaklis, P. J. (2015). Risk-sensitive control under markov modulated denial-of-service (dos) attack strategies. IEEE Transactions on Automatic Control, 60(12), 3299–3304. Caballero, R., Hermoso, A., & Linares, J. (2015). Optimal state estimation for networked systems with random parameter matrices, correlated noises and delayed measurements. Automatica, 44(2), 142–154. Cárdenas, A., Amin, S., & Sastry, S. (2008). Research challenges for the security of control systems. In Usenix Workshop on Hot Topics in Security (pp. 629–633). San Jose, CA. Carl, G., Kesidis, G., Brooks, R. R., & Rai, S. (2006). Denial-of-service attack-detection techniques. IEEE Internet Computing Magazine, 10(1), 82–89. Chen, H., Gao, J., Shi, T., & Lu, R. (2016). H∞ control for networked control systems with time delay, data packet dropout and disorder. Neurocomputing, 179, 211–218. Chen, P., & Han, Q. (2016). On designing a novel self-triggered sampling scheme for networked control systems with data losses and communication delays. IEEE Transactions on Industrial Electronics, 63(2), 1239–1248. Chen, C., Song, M., Xin, C., & Backens, J. (2013). A game-theoretical anti-jamming scheme for cognitive radio networks. IEEE Network, 27(3), 22–27. Chorpopath, A. K., Alpcan, T., & Boche, H. (2016). Bayesian mechanisms and detection methods for wireless network with malicious users. IEEE Transactions on Mobile Computing, 15(10), 2452–2465. Dan, G., & Sandberg, H. (2010). Stealth attacks and protection schemes for state estimators in power systems. In Proceedings of IEEE international conference on smart grid communications (pp. 214–219), Gaithersburg, MD, USA. Dong, H., Wang, Z., & Gao, H. (2016). Distributed hinfinity filtering for a class of Markovian jump nonlinear time-delay systems over lossy sensor networks. IEEE Transactions on Industrial Electronics, 60(10), 4665–4672. Du, S., Sun, X., & Wang, W. (2014). Guaranteed cost control for uncertain networked control systems with predictive scheme. IEEE Transactions on Automation and Engineering, 11(3), 740–748. Eyiš, E., Koutsoukos, X., & Kottenstette, N. (2012). Passivity-based trajectory tracking control with adaptive sampling over a wireless network. In Proceedings of the 5th international symposium on resilient control systems (pp. 130–136). Salt Lake, UT. Geer, D. (2006). Security of critical control systems sparks concern. Computer, 39(1), 20–26. Ginoya, D., Shendge, P. D., & Phadke, S. B. (2015). Disturbance observer based sliding mode control of nonlinear mismatched uncertain systems. Communications in Nonlinear Science and Numerical Simulation, 26(1), 98–107. Giorgi, S., Saleheen, F., Ferrese, F., & Won, C. H. (2012). Adaptive neural replication and resilient control despite malicious attacks. In Proceedings of the 5th international symposium on resilient control systems (pp. 112–117). Salt Lake, UT. Guo, G. (2010). Linear system with medium-access constraint and markov actuator assignment. IEEE Transactions on Circuits and Systems-I: Regular Papers, 57(11), 2999–3010. Guo, L., & Cao, S. (2014). Anti-disturbance control theory for systems with multiple disturbances: A survey. ISA Transactions, 53(4), 846–849.
Li, L., Hu, B., & Lemmon, M. D. (2010). A switching system approach to actuator assignment with limited channels. *International Journal of Robust and Nonlinear Control, 20*(12), 1407–1426.

Guo, G., & Jin, H. (2010). A switching system approach to actuator assignment with limited channels. *International Journal of Robust and Nonlinear Control, 20*(12), 1407–1426.

Guo, L., & Chen, W. (2005). Disturbance attenuation and rejection for systems with nonlinearity via dobc approach. *International Journal of Robust and Nonlinear Control, 15*, 109–125.

Guo, Z., Shi, D., Johansson, K. H., & Shi, L. (2017). Optimal linear cyber-attack on remote state estimation. *IEEE Transactions on Control of Network Systems, 4*(1), 4–13.

Han, S., Xie, M., Chen, H., & Ling, Y. (2014). Intrusion detection in cyber-physical systems: Techniques and challenges. *IEEE Systems Journal, 8*(4), 1049–1059.

He, X., Wang, Z., Wang, X., & Zhou, D. (2014). Networked strong tracking filtering with multiple packet dropouts: Algorithms and applications. *IEEE Transactions on Industrial Electronics, 61*(3), 1454–1463.

Hespanha, J. P., Naghshtabrizi, P., & Xu, Y. (2007). A survey of recent results in networked control systems. *Proceedings of the IEEE, 95*(1), 138–162.

Hirano, H., Mukai, M., Azuma, T., & Fujiyata, M. (2005). Optimal control of discrete-time linear systems with network-induced varying delay. In *Proceedings of American control conference* (pp. 1419–1424). Portland.

Huang, H., Ahmed, N., & Karthik, P. (2011). On a new type of denial of service attack in wireless networks: The distributed jammer network. *IEEE Transactions on Wireless Communications, 10*(7), 2316–2324.

Huang, Y., Cardenas, A. A., Amin, S., Lin, Z. S., Tsai, H. Y., & Sastry, S. (2009). Denial-of-service attack-detection techniques. *IEEE Internet Computing Magazine, 2*(3), 73–83.

Jia, L., Yao, F., Sun, Y., Niu, Y., & Zhu, Y. (2016). Bayesian Stackelberg game for anti-jamming transmission with incomplete information. *IEEE Communication Letters, 20*(10), 1991–1994.

Kilinc, D., Ozger, M., & Akan, O. B. (2015). On the maximum coverage area of wireless networked control systems with maximum cost-efficiency under convergence constraint. *IEEE Transactions on Automatic Control, 60*(7), 1910–1914.

Kisner, R. A., Manges, W. W., MacIntyre, L. P., Nutaro, J. J., Munro, J. K., Ewing, P. D., & Olarna, M. M. (1995). Cybersecurity through real-time distributed control systems. Office of Scientific & Technical Information Technical Reports.

Langner, R. (2011). Stuxnet: Dissecting a cyberwarfare weapon. *IEEE Security & Privacy, 9*(3), 49–51.

Law, Y. W., Alpcan, T., & Palaniswami, M. (2015). Security games for risk minimization in automatic generation control. *IEEE Transactions on Power Systems, 30*(1), 223–232.

Lee, P., Clark, A., Bushnell, L., & Poovendran, R. (2014). A passivity framework for modeling and mitigating wormhole attacks on networked control systems. *IEEE Transactions on Automatic Control, 59*(12), 3224–3237.

Li, H., Chow, M. Y., & Sun, Z. (2009). Optimal stabilizing gain selection for networked control systems with time delays and packet losses. *IEEE Transactions on Control Systems Technology, 17*(5), 1154–1162.

Li, L., Hu, B., & Lemmon, M. D. (2012). Resilient event triggered systems with limited communication, Maui, Hawaii, USA.

Li, H., Li, Z., Yang, H., Zhang, Y., & Sun, F. (2015). Stabilisation of networked delta operator systems with uncertainty. *IET Control Theory and Applications, 8*, 2289–2296.

Li, Y., Quevedo, D. E., Dey, S., & Shi, L. (2016). SINR-based DoS attack on remote state estimation: A game-theoretic approach. *IEEE Transactions on Control of Network Systems, 4*(3), 632–642.

Li, Y., Shi, L., Cheng, P., Chen, J., & Quevedo, D. E. (2013). Jamming attack on cyber-physical systems: A game-theoretic approach. In *Proceedings of the IEEE international conference on cyber technology in automation, Control and Intelligent Systems* (pp. 252–257). Nanjing, China.

Li, Y., Shi, L., Cheng, P., Chen, J., & Quevedo, D. E. (2015). Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach. *IEEE Transactions on Automatic Control, 60*(10), 2831–2836.

Li, H., Yang, H., Sun, F., & Xia, Y. (2013). A network-bound-dependent stabilization method of networked control systems. *Automatica, 49*(8), 2561–2566.

Li, H., Yang, H., Sun, F., & Xia, Y. (2014). Sliding-mode predictive control of networked control systems under a multiple-packet transmission policy. *IEEE Transactions on Industrial Electronics, 61*(11), 6234–6243.

Lin, H., Su, H., Shi, P., Lu, R., & Wu, Z. (2015). Log control for networked control systems over packet drop links without packet acknowledgment. *Journal of the Franklin Institute, 352*(11), 5042–5060.

Liu, A., Zhang, Q., Yu, L., Liu, S., & Chen, M. (2015). New results on stabilization of networked control systems with packet disordering. *Automatica, 52*, 255–259.

Long, M., Wu, C. H., & Hung, J. Y. (2005). Denial-of-service attack-detection techniques. *IEEE Internet Computing Magazine, 1*(2), 85–96.

Maass, A., Vargas, F., & Silva, E. (2016). Optimal control over multiple erasure channels using a data dropout compensation scheme. *Automatica, 68*, 155–161.

Matusitza, J., & Mineb, E. (2009). In quest of benchmarking security risks to cyber-physical systems. *Journal of Digital Forensic Practice, 2*(4), 161–171.

Melin, A., Kisner, R., Fugate, D., & McIntyre, T. (2012). Minimum state awareness for resilient control systems under cyber-attack. In *Proceedings of future of instrumentation international workshop* (pp. 978–982). Gatlinburg, TN.

Mo, Y., Chabukswar, R., & Sinopoli, B. (2014). Detecting integrity attacks on scada systems. *IEEE Transactions on Control Systems Technology, 61*(11), 1396–1407.

Niu, Y., & Ho, D. W. C. (2014). Control strategy with adaptive quantizer’s parameters under digital communication channels. *Automatica, 50*(10), 2665–2671.

Pang, Z., & Liu, G. P. (2012). Design and implementation of secure networked predictive control systems under deception attacks. *IEEE Transactions on Control Systems Technology, 20*(5), 1334–1342.

Pang, Z., Liu, G. P., & Zhou, D. (2016). Design and performance analysis of incremental networked predictive control systems. *IEEE Transactions on Cybernetics, 46*(6), 1400–1410.

Pang, Z., Liu, G., Zhou, D., Hou, F., & Sun, D. (2016). Two-channel false data injection attacks against output tracking control of networked control systems. *IEEE Transactions on Industrial Electronics, 63*(5), 3242–3251.

Park, K., Kim, J., Lim, H., & Eun, Y. (2014). Robust path diversity for network quality of service in cyber-physical systems. *IEEE Transactions on Industrial Informatics, 10*(4), 2204–2215.
Wang, B., Wu, Y., Liu, K., & Clancy, T. (2011). Industrial control system cybersecurity research. Journal of Tsinghua University, 52(10), 1396–1408.

Peters, E., Quevedo, D., & Ostergaard, J. (2016). Shaped gaussian dictionaries for quantized networked control systems with correlated dropouts. IEEE Transactions on Signal Processing, 64(1), 203–213.

Qiu, L., Li, S., Xu, B., & Xu, G. (2015). $h_{\infty}$ control of networked control systems based on Markov jump unified model. International Journal of Robust and Nonlinear Control, 26, 2770–2786.

Qiu, X., Yu, L., & Zhang, D. (2015). Stabilization of supply networks with transportation delay and switching topology. Neurocomputing, 155, 247–252.

Rieger, C. G., Gertman, D. I., & McQueen, M. A. (2009). Resilient control systems: Next generation design research. In Conference on human system interactions (pp. 629–633). Catania, Italy.

Sagduyu, Y. E., Berry, R. A., & Ephremides, A. (2011). Jamming games in wireless networks with incomplete information. IEEE Communications Magazine, 49(8), 112–118.

Sandberg, H., Amin, S., & Johansson, K. (2015). Cyberphysical security in networked control systems an introduction to the issue. IEEE Control Systems Magazine, 31(1), 20–23.

Schenato, L., Sinopoli, B., Franceschetti, M., Poolla, K., & Sastry, S. (2007). Foundations of control and estimation over lossy networks. Proceedings of the IEEE, 95(1), 163–187.

Smith, R. S. (2015). Covert misappropriation of networked control systems: Presenting a feedback structure. IEEE Control Systems Magazine, 35(1), 82–92.

Tan, X. H., & Jose, B. C. (2010). Adaptive noncooperative-person games with unknown general quadratic objectives. IEEE Transactions on Control Systems Technology, 18(5), 1033–1043.

Teixeira, A., Perez, D., Sandberg, H., & Johansson, K. H. (2012). Attack models and scenarios for networked control systems. In Proceedings of the 1st international conference on high confidence networked systems (pp. 55–64), Beijing, China, April 17-18, 2012.

Truong, D. Q., & Ahn, K. K. (2015). Robust variable sampling period control for networked control systems. IEEE Transactions on Industrial Electronics, 62(9), 5630–5643.

Tsumura, K., Ishii, H., & Hoshina, H. (2009). Tradeoffs between quantization and packet loss in networked control of linear systems. Automatica, 45, 2963–2970.

Virvilis, N., & Gritzalis, D. (2013). The big four-what we did wrong in advanced persistent threat detection? In International conference on availability, reliability and security, (pp. 248–254). Greece.

Wang, D., Liu, D., Wei, Q., Zhao, D., & Jin, N. (2012). Optimal control of unknown nonaffine nonlinear discrete-time systems based on adaptive dynamic programming. Automatica, 48, 1825–1832.

Wang, B., Wu, Y., Liu, K., & Clancy, T. (2011). An anti-jamming stochastic game for cognitive radio networks. IEEE Journal on Selected Areas in Communications, 29(4), 877–889.

Wei, X., Chen, N., Deng, C., Liu, X., & Tang, M. (2012). Composite stratified anti-disturbance control for a class of mimo discrete-time system with nonlinearity. International Journal of Robust and Nonlinear Control, 22, 453–472.

Wu, L., Lam, J., Yao, X., & Xiong, J. (2011). Robust guaranteed cost control of discrete-time networked control systems. Optimal Control Application and Methods, 32(1), 95–112.
Yuan, Y., & Sun, F. (2015). Data fusion-based resilient control system under dos attacks: A game theoretic approach. *International Journal of Control Automation and Systems, 13*(3), 513–520.

Yuan, Y., Sun, F., & Liu, H. (2015). Resilient control of cyber-physical systems against intelligent attacker: A hierarchical stackelberg game approach. *International Journal of Systems Science, 47*(9), 1–11.

Yuan, Y., Wang, Z., & Guo, L. (2018). Event-triggered strategy design for discrete-time nonlinear quadratic games with disturbance compensations: The noncooperative case. *IEEE Transactions on Systems, Man, and Cybernetics: Systems, 99*, 1–12.

Yuan, Y., Yuan, H., Guo, L., Yang, H., & Sun, S. (2016). Resilient control of networked control system under dos attacks: A unified game approach. *IEEE Transactions on Industrial Informatics, 12*(5), 1786–1794.

Yuan, Y., Yuan, H., Wang, Z., Guo, L., & Yang, H. (2017). Optimal control for networked control systems with disturbances: A delta operator approach. *IET Control Theory & Applications, 11*(9), 1325–1332.

Yuan, Y., Zhu, Q., Sun, F., Wang, Q., & Başar, T. (2013). Resilient control of cyber-physical systems against denial-of-service attacks. In *Proceedings of the 6th international symposium on resilient control systems* (pp. 54–59). Beijing, China.

Zhang, H., Cheng, P., Shi, L., & Chen, J. (2016). Optimal dos attack scheduling in wireless networked control system. *IEEE Transactions on Control Systems Technology, 24*(3), 843–852.

Zhang, H., Feng, G., Yan, H., & Chen, Q. (2016). Sampled-data control of nonlinear networked systems with time-delay and quantization. *International Journal of Robust and Nonlinear Control, 26*, 919–933.

Zhang, X., Lu, C., Xie, X., & Dong, Z. (2016). Stability analysis and controller design of a wide-area time-delay system based on the expectation model method. *IEEE Transactions on Smart Grid, 7*(1), 520–529.

Zhang, J., Xia, Y., & Shi, P. (2013). Design and stability analysis of networked predictive control systems. *IEEE Transactions on Control Systems Technology, 21*(4), 1495–1501.

Zhao, L., Yang, Y., Xia, Y., & Liu, Z. (2015). Active disturbance rejection position control for a magnetic rodless pneumatic cylinder. *IEEE Transactions on Industrial Electronics, 62*, 5838–5846.

Zhu, Q., & Başar, T. (2009). Dynamic policy-based ids configuration. In *IEEE conference on decision and control* (pp. 8600–8605). Atlanta, GA.

Zhu, Q., & Başar, T. (2011). Robust and resilient control design for cyber-physical systems with an application to power systems. In *IEEE conference on decision and control* (pp. 4066–4071). Nashville.

Zhu, Q., & Başar, T. (2015). Game-theoretic methods for robustness, security, and resilience of cyberphysical control systems: Games-in-games principle for optimal cross-layer resilient control systems. *IEEE Control Systems Magazine, 35*(1), 46–65.

Zhu, M., & Martínez, S. (2014). On the performance analysis of resilient networked control systems under replay attacks. *IEEE Transactions on Automatic Control, 59*(3), 804–808.

Zhu, Q., Rieger, C., & Başar, T. (2011). Stealthy deception attacks on water SCADA systems. In *Proceedings of international symposium on resilient control systems*, pp. 161–170, Stockholm, Sweden.

Zhu, M. H., & Sonia, M. (2011). Stackelberg-game analysis of correlated attacks in cyber-physical systems. In *American control conference* (pp. 4063–4068). San Francisco, CA.