International Journal of Information Technology and Management

Vol. IX, Issue No. XIV, November-2015, ISSN 2249-4510

AN ANALYSIS UPON TOWARD CYBER SECURE AND RELIABLE NETWORKED CONTROL SYSTEMS: CONCEPTS AND RESEARCH TRENDS

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

International Journal of Information Technology and Management
Vol. IX, Issue No. XIV, November-2015, ISSN 2249-4510

An Analysis Upon Toward Cyber Secure and Reliable Networked Control Systems: Concepts and Research Trends

Hemant Kumar Narayanbhai Patel[1] Dr. Jigar Patel[2]

[1]Research Scholar, Mewar University, Chhitorgrah. India

[2]Associate Professor, Kalol Institute of Management, GTU, Gujarat, India

Abstract – Over the past decade, many concerns have been raised about the vulnerabilities of infrastructure systems to both random failures and security attacks. Cyber-security of Supervisory Control and Data Acquisition (SCADA) systems is especially important, because these systems are employed for sensing and control of large physical infrastructures. So far, the existing research in robust and fault-tolerant control does not account for cyber-attacks on networked control system (NCS) components.

The trend towards using pervasive information technology systems, such as the Internet, results in control systems becoming increasingly vulnerable to cyber threats. Traditional cyber security does not consider the interdependencies between the physical components and the cyber systems. On the other hand, control-theoretic approaches typically deal with independent disturbances and faults, thus they are not tailored to handle cyber threats.

Security and reliability are essential properties in Networked Control Systems (NCS), which are increasingly relevant in several important applications such as the process industry and electric power networks. The trend towards using non-proprietary and pervasive communication and information technology (IT) systems, such as the Internet and wireless communications, may result in NCS being vulnerable to cyber-attacks. Traditional IT security does not consider the interdependencies between the physical components and the cyber realm of IT systems. Moreover, the control theoretic approach is not tailored to handle IT threats, focusing instead on nature-driven events. This paper addresses the security and reliability of NCS, with a particular focus on power system control and supervision, contributing towards establishing a framework capable of analyzing and building NCS security.

----------X----------

INTRODUCTION

The wide application of network brings in a lot of convenience for industrial control systems, as well as many security vulnerabilities, and more and more incidents at critical infrastructures have been reported. So how to effectively secure NCSs has gone 'mainstream' in terms of public awareness of the threat to them from hackers, cyber spies and terrorists. Consequently, many researchers have shown great concern for the security solutions for NCSs.

When A traditional feedback control system is closed via a communication channel (such as a network), which may be shared with other nodes outside the control system, then the control system is classified as a networked control system (NCS). All definitions found in literature for an NCS have one key feature in common. This defining feature is that information (reference input, plant output, control input, etc.) is exchanged among control system components (sensor, controller, actuator, etc.) using a *shared network* (Fig. 1).

The root of control systems can be traced back to 1868 when dynamics analysis of the centrifugal governor was conducted by the famous physicist J. C. Maxwell. The most significant achievement in conventional control systems occurred when the Wright brothers made their first successful test flight in 1903. The next significant achievement was the fly-bywire flight control system that was designed to eliminate the complexity, fragility, and weight of the mechanical circuit of hydromechanical flight control systems using an electrical circuit. The simplest and earliest configuration of analog fly-bywire flight control systems was first fitted to the Avro Vulcan in the

1950s. This can be called as the first form of analog NCSs.

Digital computers became powerful tools in control system design, and microprocessors added a new dimension to the capability of control systems. A modified National Aeronautics and Space Administration F-8C Crusader was the first digital fly-by-wire aircraft in 1972. The next step in evolution was the distributed control system (DCS) that was introduced in 1975. Both Honeywell and Japanese electrical engineering firm Yokogawa introduced their own independently produced DCSs at around the same time, with the TDC 2000 and CENTUM systems, respectively. As the expanding needs of industrial applications pushed the limit of point-to-point control, it became obvious that the NCS was the solution to achieve remote control operations. Research in teleoperation was initiated with the concern for safety and convenience in hazardous environments, such as space projects and nuclear reactor power plants, and was made feasible only after further development of the NCS.

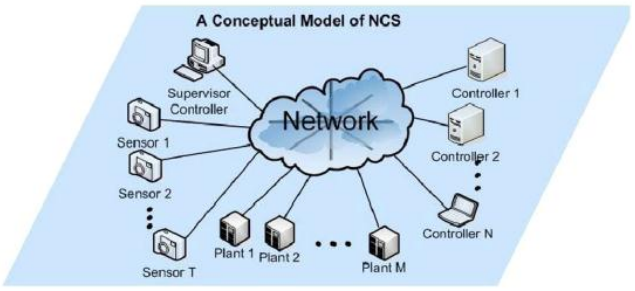

Fig. 1. Typical structure of an NCS.

The basis capabilities of any NCS are information acquisition (sensors/users), command (controllers/users), communication, and network and control (actuators). In broader terms, NCS research is categorized into the following two parts.

1) *Control of network*. Study and research on communications and networks to make them suitable for realtime NCSs, e.g., routing control, congestion reduction, efficient data communication, networking protocol, etc.

2) *Control over network*. This deals more with control strategies and control system design over the network to minimize the effect of adverse network parameters on NCS performance such as network delay.

Any network medium, particularly wireless medium, is susceptible to easy intercepting. Research in NCS was initiated from the concern for safety and convenience in hazardous environments such as nuclear reactor power plants, space projects, nursing homes, military applications, etc. In all these applications, security is of the utmost concern. The British Columbia Institute of Technology Industrial Security Incident Database contains information regarding security-related attacks on process control and industrial networked systems. Dzung *et al.* gave an overview of IT security issues in industrial automation based on open communication systems and also explained various countermeasures. Most NCSs are vulnerable to network attacks nowadays, so there is a growing demand of efficient and scalable intrusion detection systems (IDS).

Attacks to computer networks have become prevalent over the last decade.While most control networks have been safe in the past, they are currently more vulnerable to malicious attacks. The consequences of a successful attack on control networks can be more damaging than attacks on other networks because control systems are at the core of many critical infrastructures. Therefore, analyzing the security of control systems is a growing concern.

In the control and verification community there is a significant body of work on networked control, stochastic system verification, robust control, and fault-tolerant control. We argue that several major security concerns for control systems are not addressed by the current literature. For example, fault analysis of control systems usually assumes independent modes of failure, while during an attack, the modes of failure will be highly correlated.

On the other hand, most networked control work assumes that the failure modes follow a given class of probability distributions; however, a real attacker has no incentives to follow this assumed distribution, and may attack in a nondeterministic manner. Finally, the work in stochastic system verification has addressed safety and reachability problems for fairly general systems; however, the potential applicability of these results for securing control systems has not been studied.

In this article, we formulate and analyze the problem of secure control for discrete-time linear dynamical systems. Our work is based on two ideas: (1) the introduction of safety-constraints as one of the top security requirements of a control system, and (2) the introduction of new adversary models—we generalize traditional uncertainty classes for control systems to incorporate more realistic attacks. The goal in our model is to minimize a performance function such that a safety specification is satisfied with high probability and power limitations are obeyed in expectation when the sensor and control packets can be dropped by a random or a resource-constrained attacker. Our analysis uses tools from optimal control theory such as dynamic and convex programming.

The technological development during the digital era since the 1960s has led to the increased use of digital controllers and communication networks in many control applications, effectively transforming them into networked control systems (NCS). The digital revolution led to several opportunities to

increase the overall efficiency of control systems, as well as their successful use in many domains (Samad and Annaswamy, 2011). Using information technology (IT) infrastructures, digital controllers, sensors, and actuators from the low-level control layer could now be integrated with high-level supervisory layers, giving birth to supervisory control and data acquisition (SCADA) systems. the lower layers of SCADA systems consist of sensors and actuators interfaced with programmable logic computers (PLC) at local stations, or with remote terminal units (RTU) imbued with extended communication capabilities at remote locations. Measurement data are collected by RTUs and PLCs and transmitted to the higher layers of the SCADA system through heterogeneous communication networks. Low-level control may be implemented in the PLCs or RTUs, which receive supervisory commands and set-points from the higher levels.

NETWORKED CONTROL SYSTEMS

The technological developments in computer and communication technologies triggered several paradigm shifts in control systems over the last decades. Until the 1960s, feedback controllers were mostly comprised of mechanical or analog electronic devices that exchanged analog measurements and control signals with the plant through dedicated wired media (Astrom and Kumar, 2014). At the time, many control challenges dealt with stability and regulation problems. The digital revolu- tion was already ongoing, and it soon reached a level of maturity that led to the use of digital computers and communication networks in many control applications.

The use of digital technologies enabled the integration of multiple sensors and actuators, which communicated with the controller through shared wired media. This new paradigm raised several novel challenges, such as digital controller design, data sampling, and state estimation, which were addressed by the modern control theory.

During the 1970s, digital controllers and communication infrastructures were developed for spatially-distributed systems, which are now an integral part of SCADA systems. Initially, these systems used proprietary hardware, software, and wired communication technologies, making them closed to external networks and hard to interface with solutions from other vendors. Therefore, given the natural “security through obscurity” of these systems, cyber security was not a main concern (Samad et al., 2007).

The further technological advances since the 1970s prompted a pervasive use of IT infrastructures in many engineered systems. Communication technologies were be standardized (Galloway and Hancke, 2013), leading to the proliferation of protocols such as FieldBus and CAN, commonly used in SCADA and automotive systems, respectively. “Security through obscurity” became outdated, as details of communication protocols became openly available. In parallel, wireless technologies, such as cellular communications, were under active development in the 1970s. Devices with wireless communication capabilities are suitable for operating in remote locations, given their reduced installation cost compared to wired solutions. Therefore, wireless devices became an integral component of SCADA solutions for large-scale spatially-distributed systems, such as electric power networks.

On the other hand, wireless communications are naturally more vulnerable to external adversaries than wired technologies, since the communication medium is easily accessible.

These recent technological developments led to two main research directions within the controls community, which are revisited below. The first deals with the effects of unreliable communication technologies in systems controlled over communication networks, while the second leverages on communication networks to distributedly control and monitor large-scale systems.

Later, we give an overview also on a third research direction that is currently emerging, namely, to address the increased exposure to cyber threats that stems from the use of pervasive and open IT infrastructures.

Control over Communication Networks - Digital controllers and digital communication networks, through which measurements and control signals are transmitted, have been present in industrial systems for several decades. Initially, the digital devices were connected through reliable wired communication networks, with few or no data losses. Due to the high wiring costs, the communication medium was shared between all the devices in the network, which caused delays in the data exchange. As such, the main concern until the early 1990s was the effect of varying delays on the control system performance.

As the computational and communication hardware cost is reduced, wireless devices with low-cost computational capabilities become an appealing choice for spatially-distributed control systems. However, wireless communication networks have characteristics and inherent limitations that may hinder the control performance.

The design of control systems have recently addressed several of these issues, for instance, packet losses, limited data-rate (Ishii and Francis, 2002), and out-of-order packets. However,

approaches focusing solely on controller design may prove insufficient, when the time-scales of control systems and communication networks become closer. In such cases, the inter-play between the control system's sampling time and the communication networks parameters becomes more significant and cannot be neglected. Different approaches have been put forward to tackle this challenge, such as the use of event-triggered sampling (Wang and Lemmon, 2011), co-design of controller and communication network (Demirel et al., 2014), and wireless medium access mechanisms (Ramesh et al., 2013), to name a few examples.

Control of Networked Systems - The challenge of controlling large-scale interconnected systems has been addressed since the 1970s, such as the hierarchical and decentralized control frameworks. These frameworks considered spatially distributed physical systems with a sparse structure, e.g., electric power networks. A typical approach is to decompose the global system into a set of smaller interconnected systems, for which local controllers are designed. Apart from decomposing the system, one of the main challenges of decentralized control is to design the local controllers so that the stability and performance of the overall system are guaranteed.

The use of wireless communication networks in control systems led to new possibilities and problems. By using communication networks, the local controllers became able to communicate and exchange information with each other, triggering a shift towards the distributed control framework.

Some of the challenges have been addressed, such as the design of distributed controllers, distributed state estimation, and distributed fault detection, among others.

In addition to the challenges from the decentralized control, new opportunities came to light with the distributed control approach. Once physically-decoupled systems become coupled through controllers and communication networks, the structure of the network plays an important role in the behavior of the global system. Such observation contributed to a large body of research with direct application to the behavior of complex networks (Barrat et al., 2008), motion of animal groups, and multi-agent systems and cooperative robotics, among others.

Cyber Security in Networked Control Systems - The recent developments in control over communication networks and control of networked systems may be considered as initial steps towards future systems, where cyber and physical components are tightly coupled and intertwined. A particular example is the Internet-of-Things vision (Atzori et al., 2010), where multiple heterogeneous devices are able to communicate and interact with each other to achieve common goals. This vision builds on the maturity of wireless technologies and embedded computational hardware platforms. By embedding low-cost hardware in sensors, actuators, and other devices in the physical environment, they can be used to take automatic decisions based on information exchanged locally through communication networks.

However, as illustrated in Figure 2, each communication link and device with communication capabilities may be vulnerable to cyber-attacks from malicious and knowledgeable adversaries. Therefore, the use of IT platforms increases the exposure of networked control systems to vulnerabilities and cyber threats, which leads to several challenges regarding cyber security and resilience.

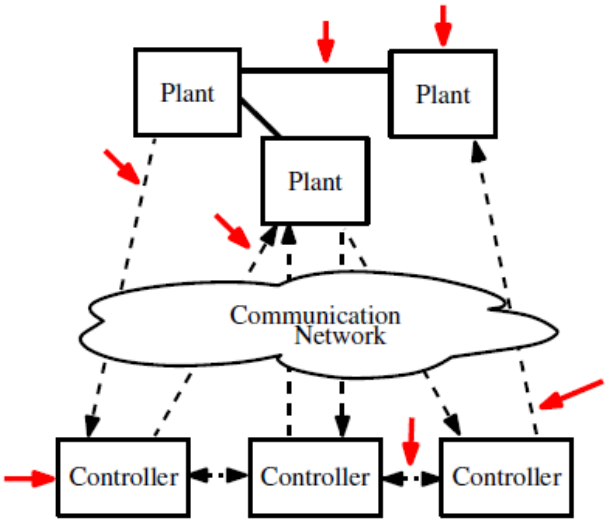

Figure 2: Schematic of a distributed control architecture under cyber and physical threats.

SECURE AND RELIABLE NETWORKED CONTROL SYSTEMS

Secure NCS have received increasing attention recently. An overview of existing cyber threats and vulnerabilities in NCS is presented in, where the authors also mention some of the new challenges arising from the interconnection of IT and control systems. Particularly, realistic and rational adversary models are mentioned as one of the key items in security for NCS.

In the framework of security, however, such faults are rational and are endowed with intelligence and intent. Therefore these faults may exploit vulnerabilities ex- isting in the traditional fault detection mechanisms and remain undetected. In fact, Amin et al. (2010) reported experimental stealthy data deception attacks on water irrigation canals controlled by SCADA systems. Smith (2011) characterized stealthy attack policies for scenarios where the attacker is able to perform disclosure and deception attacks on all the sensors, illustrating it on the same water irrigation system.

Rational attackers performing stealthy deception attacks were also considered for sensor networks distributively computing linear functions, where each node is modeled as a first-order system. The class of stealthy deception attacks was characterized in a system-theoretic fashion in terms of the number of compromised nodes and the network connectivity. Other work also considering rational attack-

ers analyzes Denial-of-service attacks, where the optimal attack policy under finite resources is characterized considered replay attacks on wireless networks performing state estimation, which are a particular class of deceptions attacks, and proposed a novel detection scheme tailored to this class of attacks. The safety of Automatic Generation Control for power system under deception attacks was considered in and the authors showed that the cyber-attacks could violate the system safety constraints. Although the attackers were not assumed to be rational in these papers, the former illustrates that tailored detection mechanisms can increase the attack detection rate, while the latter identified existing safety vulnerabilities.

Benchmark examples for NCS security were described and numerical experiments on a benchmark process plant were reported in (Cardenas et al., 2011). In the latter, although a mathematical formulation for the effects of cyber-attacks was given, as well as attack objectives, the attack policies presented did not make use of the full attacker resources.

Security of NCS is a recent research field, full of broad open questions. Further-more recent work within the control community, this paper included, only consider how the possible threats affect the control system dynamics, while the IT system and respective security mechanisms are neglected. Although this approach is interesting and valid, looking more closely at the IT framework and tools may help to design better protective schemes.

LITERATURE REVIEW

DACFEY DZUNG (2005) gives an overview of IT security issues in industrial automation systems, analyses the industrial communication systems' security-relevant characteristics distinct from the general IT systems in detail.

Xu *et al.* (2005) developed a core architecture to address the collaborative control issues of distributed device networks under open and dynamic environments by adopting policy-based network security technologies and XML processing technologies.

Swaminathan P (2006), analysis and compare several typical encryption algorithms, then introduce DES is the fastest one of them and enough to guarantee the security of the data transmitted in NCSs. Ke-Ya

Alvaro A. C´ardenas and Saurabh Amin (2008) identify and define the problem of secure control, then propose a set of challenges that need to be addressed to improve the survivability of cyber-physical systems.

Gupta *et al. (*2008) characterized the WNCS application on the basis of security effect on NCS performance to show this tradeoff for an NCS path-tracking application. However, NCS with security from the control system's perspective is in infancy. There is a large scope of research considering the practicality of NCS in any critical application. The same goes for integration of components. This is another issue when it comes to actual implementation of NCSs on broader scale.

Yuan (2009) describes the advantages of DES algorithm, the hardware and software design of the DES encryption algorithm. So, in this paper we also use the DES algorithm for data encryption and decryption.

Jianfeng Dong (2010) presents a network security situation evaluation and prediction model based on grey theory, and the model includes two parts: current situation evaluation and future situation prediction. Given the above, in this paper, we use grey theory to predict legal data of the next moment.

Wente Zeng (2011) propose the impact of the security policy on system performance, and then present a trade-off model for system dynamic performance and system security.

Alvaro A. Cárdenas (2011) explore security mechanisms that detect attacks by monitoring the physical system under control, and the sensor and actuator values, then develop a new attack detection algorithm and study the methodology on how to evaluate anomaly detection algorithms and their possible response strategies. While most of the research efforts focus on prevention (authentication, access controls, cryptography etc) or detection (intrusion detection systems), in practice there are quite a few response mechanisms.

Zhong-Hua Pang and Guo-Ping Liu (2012) design and implement a secure transmission mechanism, which integrates the Data Encryption Standard (DES) algorithm, Message Digest (MD5) algorithm and timestamp strategy.

CYBERPHYSICAL SECURITY IN NCS

This special issue provides an introduction to cyberphysical security of networked control systems (NCSs) and summarizes recent progress in applying

fundamentals of systems theory and decision sciences to this new and increasingly promising area. NCS applications range from large-scale industrial applications to critical infrastructures such as water, transportation, and electricity networks. The security of NCSs naturally depends on the integration of cyber and physical dynamics and on different ways in which they are affected by the actions of human decision makers.

Thus, problems in this area lie at the intersection of control systems and computer security. The six articles that constitute this special issue approach cyberphysical security from a variety of perspectives, including control theory, optimization, and game theory. They cover a range of topics such as models of attack and defense, risk assessment, attack detection and identification, and secure control design.

A common theme among these contributions is an emphasis on the development of a principled approach to cyberphysical security of NCS. A justified first question for this special issue is whether NCS security can be handled simply with information technology (IT) and network security solutions. After all, NCSs are applications typically built on Internet Protocol (IP)-based networks. However, feedback loops inherent to NCSs and the coupling to the physical environment impose fundamentally new challenges for cybersecurity tools.

NCSs highlight special feedback characteristics of control systems that have implications on the underlying physical dynamics. On one hand, the traditional IT security focuses on the protection of information in the cyberworld. On the other hand, classical control theory focuses on the attenuation of disturbances and uncertainties in the physical world. This separation was natural for many practical applications, such as traditionally hard-wired supervisory control and data acquisition (SCADA) systems. However, the separation at the design stages of IT security tools and control-theoretic implementations is no longer permissible.

Indeed, NCSs are vulnerable to remote access over IP-based communication networks, software flaws and hardware malfunctions of off-the-shelf IT devices, and the presence of a large number of field devices used for sensing and actuation. In such a networked environment, the cyber and physical components become interconnected and hence, their security is interdependent.

One concrete example is an incident from 2010 that is now well known, namely when the advanced computer worm Stuxnet infected industrial control systems that supposedly had strategic value to certain nation states. While there are no confirmed reports about the actual impact of the attack, the incident highlights the potential threats to control systems. Indeed, the articles in this special issue motivate their problem formulations using Stuxnet and other known attacks to control systems by malicious insiders or external hackers.

Incorporating traditional IT security in control designs, such as encryption of certain communication channels, is important; however, it is only a partial solution to NCS security concerns. Even if certain communication channels have been encrypted, malicious data or actions can enter due to unauthorized access to NCS components, which can result in undesirable behaviors of the controlled physical plant. Furthermore, many encryption solutions will likely introduce time delay in the feedback loop, which usually deteriorates control system performance. Therefore, traditional IT security cannot completely provide the desired level of defense against malicious insiders and computer hackers who target NCSs. We therefore argue for the need to develop a new set of analysis and synthesis tools drawing on control theory, game theory, and network optimization. Below is a brief overview of the topics that are covered in this issue.

Specifically, the adversary model includes the attack policy or mechanism as well as the resources available for violating NCS security and the adversary's knowledge of the system dynamics. Next, the article presents quantitative tools for the assessment and management of security risks to static and dynamic systems, with particular focus on stealthy deception attacks. For static systems, the proposed riskassessment approach quantifies the likelihood of threats by posing the problem of finding minimum resource stealthy attacks. For dynamic systems, both impact and the likelihood of threats are considered by posing a multiobjective optimization problem that finds minimum-resource, maximum-impact stealthy attacks. Third, the applicability of these tools is explained by using examples of large-scale electric power systems and a wireless quadruple-tank test bed. Technological solutions for mitigating security risks are also discussed.

A complementary approach to assessing security NCS risks and improving their survivability in the face of strategic adversaries is to use game-theoretic tools. Two of the articles in this special issue present game-theoretic formulations to address security and resilience issues in NCS.

The article by Zhu and Bas□ ar presents a game-theoretic framework to analyze and improve the resilience of NCSs in the face of attacks. The framework builds on a hybrid dynamic model that models the evolution of the cybersystem as a discrete-time Markov model and combines it with continuous-time dynamics of the underlying controlled physical system. Two zero-sum games are introduced. First, a zero-sum differential game is used for robust control design at the physical system level. Next, a stochastic zero-sum game between attacker and network operator is used for design of security strategies at the cyber level. A security

strategy at the cyber (upper) level influences the optimal control strategy at the physical (lower) level, and in turn the design of security strategy at upper level must account for the optimal control strategy at the lower level. This two-level framework enables understanding the resilience and security aspects arising from cyberphysical interactions. Specifically, the article uses this framework to illustrate the tradeoff in allocating resources for improving the level of security of the cybersystem versus increasing control effort to ensure resilience.

CONCLUSION

In this paper, the NCS and its different forms are introduced. NCSs have been popular and widely applied for many years because of their numerous advantages and widespread applications. This paper identified some of the main research topics related to NCS. Some of them have been analyzed since the advent of NCS such as network delay compensation and resource allocation. The ones which came into focus later to improve NCS are scheduling, network security with NCS, fault tolerance, etc., which are also studied in this paper.

With increasing real-life applications for NCS, the real-time secured control is an important issue. This gives rise to a real-time optimization problem and security threat modeling requirement in NCS. Designing an FTC system for a large-scale complex NCS is still very difficult due to the large number of sensors and actuators spatially distributed on a network.

REFERENCES

- Cardenas, S. Amin, Z. Lin, Y. Huang, C. Huang, and S. Sastry. Attacks against process control systems: risk assessment, detection, and response. In *Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security*, ASIACCS '11, pages 355–366, New York, NY, USA, 2011. ACM. ISBN 978-1-4503-0564-8.
- Byres, Eric, and Justin Lowe, " The myths and facts behind cyber security risks for industrial control systems ", Proceedings of the VDE Kongress, vol. 116, 2004.
- Cárdenas, Alvaro A., et al, "Attacks against process control systems: risk assessment, detection, and response", Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security. ACM, pp. 355-366, 2011.
- Cardenas, Alvaro A., Saurabh Amin, and Shankar Sastry, " Secure control: Towards survivable cyber-physical systems", Distributed Computing Systems Workshops, 2008. ICDCS'08. 28th International Conference on IEEE, pp. 495-500, 2008.
- D. Dzung, M. Naedele, T. P. Von Hoff, and M. Crevatin, "Security for industrial communication systems," *Proc. IEEE*, vol. 93, no. 6, pp. 1152– 1177, Jun. 2005.
- Demirel, Z. Zou, P. Soldati, and M. Johansson. 2014. Modular design of jointly optimal controllers and forwarding policies for wireless control. IEEE Transactions on Automatic Control. To appear.
- Dzung, Dacfey, et al, "Security for industrial communication systems", Proceedings of the IEEE 93.6, pp. 1152-1177, 2005.
- Galloway and G. P. Hancke. 2013. Introduction to industrial control networks. IEEE Communications Surveys & Tutorials, 15(2):860–880.
- Jianfeng Dong, "The Building of Network Security Situation Evaluation and Prediction Model Based on Grey Theory", Challenges in Environmental Science and Computer Engineering (CESCE), 2010 International Conference on , vol.2, no., pp.401-404, 6-7 March 2010.
- K. J. Astrom and P. R. Kumar. 2014. Control: A perspective. Automatica, 50(1): 3–43.
- Ke-Ya Yuan; Jie Chen; Guo-Ping Liu; Jian Sun, "Design and implementation of data encryption for networked control systems", Systems, Man and Cybernetics, 2009. SMC 2009. IEEE International Conference on. IEEE, vol. no, pp.2105-2109, 11-14 Oct. 2009.
- Luigi Atzori, Antonio Iera, and Giacomo Morabito. 2010. The internet of things: A survey. Computer Networks, 54(15):2787–2805.
- Peng Jie; Liu Li, "Industrial Control System Security," *Intelligent Human-Machine Systems and Cybernetics (IHMSC), 2011 International Conference on* , vol.2, no., pp.156,158, 26-27 Aug. 2011.
- R. A. Gupta and M.-Y. Chow, "Performance assessment and compensation for secure networked control systems," in Proc. IECON, Nov. 2008, pp. 2929–2934.

- R. Smith. A decoupled feedback structure for covertly appropriating networked control systems. In *Proceedings of the 18th IFAC World Congress*, Milano, Italy, August-September 2011.
- S. Amin, X. Litrico, S. S. Sastry, and A. M. Bayen. Stealthy deception attacks on water scada systems. In *Proceedings of the 13th ACM international conference on Hybrid systems: computation and control*, HSCC '10, pages 161–170, New York, NY, USA, 2010. ACM.
- Swaminathan, P.; Padmanabhan, K.; Ananthi, S.; Pradeep, R, "The Secure Field Bus (SecFB) Protocol-Network Communication Security for secure Industrial Process control ", TENCON 2006. 2006 IEEE Region 10 Conference , vol., no, pp.1,4, 14-17, Nov. 2006.
- T. Samad, P. McLaughlin, and J. Lu. 2007. System architecture for process automation: Review and trends. Journal of Process Control, 17(3):191–201.
- Wang and M.D. Lemmon. 2011. Event-triggering in distributed networked control systems. IEEE Transactions on Automatic Control, 56(3):586–601.
- Wente Zeng; Mo-Yuen Chow, "A trade-off model for performance and security in secured Networked Control Systems", Industrial Electronics (ISIE), 2011 IEEE International Symposium on , vol., no., pp.1997-2002, 27-30 June 2011.
- Y. Xu, R. Song, L. Korba, L. Wang, W. Shen, and S. Lang, "Distributed device networks with security constraints," *IEEE Trans. Ind. Informat.*, vol. 1, no. 4, pp. 217–225, Nov. 2005.
- Zhong-Hua Pang; Guo-Ping Liu, "Design and Implementation of Secure Networked Predictive Control Systems Under Deception Attacks", Control Systems Technology, IEEE Transactions on , vol.20, no.5, pp.1334-1342, Sept. 2012.