

Hindawi Publishing Corporation
Abstract and Applied Analysis
Volume 2014, Article ID 461261, 10 pages
<http://dx.doi.org/10.1155/2014/461261>



Review Article

Performance Analysis with Network-Enhanced Complexities: On Fading Measurements, Event-Triggered Mechanisms, and Cyber Attacks

Derui Ding,¹ Zidong Wang,^{2,3} Hongli Dong,^{4,5} Yurong Liu,^{6,7} and Bashir Ahmad³

¹ School of Information Science and Technology, Donghua University, Shanghai 200051, China

² Department of Computer Science, Brunel University, Uxbridge, Middlesex, UB8 3PH, UK

³ NAAM Research Group, Department of Mathematics, King Abdulaziz University, Jeddah 21589, Saudi Arabia

⁴ Research Institute of Intelligent Control and Systems, Harbin Institute of Technology, Harbin 150001, China

⁵ College of Electrical and Information Engineering, Northeast Petroleum University, Daqing 163318, China

⁶ Department of Mathematics, Yangzhou University, Yangzhou 225002, China

⁷ Faculty of Engineering, King Abdulaziz University, Jeddah 21589, Saudi Arabia

Correspondence should be addressed to Derui Ding; deruiding2010@gmail.com

Received 27 April 2014; Accepted 6 May 2014; Published 25 May 2014

Academic Editor: Bo Shen

Copyright © 2014 Derui Ding et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Nowadays, the real-world systems are usually subject to various complexities such as parameter uncertainties, time-delays, and nonlinear disturbances. For networked systems, especially large-scale systems such as multiagent systems and systems over sensor networks, the complexities are inevitably enhanced in terms of their degrees or intensities because of the usage of the communication networks. Therefore, it would be interesting to (1) examine how this kind of network-enhanced complexities affects the control or filtering performance; and (2) develop some suitable approaches for controller/filter design problems. In this paper, we aim to survey some recent advances on the performance analysis and synthesis with three sorts of fashionable network-enhanced complexities, namely, fading measurements, event-triggered mechanisms, and attack behaviors of adversaries. First, these three kinds of complexities are introduced in detail according to their engineering backgrounds, dynamical characteristic, and modelling techniques. Then, the developments of the performance analysis and synthesis issues for various networked systems are systematically reviewed. Furthermore, some challenges are illustrated by using a thorough literature review and some possible future research directions are highlighted.

1. Introduction

In the past few years, the research on networked systems has been gaining momentum due to the advantages of using networked media in many aspects such as the ease of maintenance and installation, the large flexibility, and the low cost [1]. However, the inherently limited bandwidth of the communication channel inevitably brings in some network-related issues which include, but are not limited to, network-induced communication delays [2], missing data [3], signal quantizations [4, 5], and channel fading [6]. Therefore, it is of great importance to understand how these challenging issues

affect the closed-loop stability and performance properties of a controlled system or a filtering process. Fortunately, up to now, these network-related problems have gained much research effort and a wealth of literature has appeared on the related topics; see for example, [7–17] and the references therein. Roughly speaking, the published results have been concerned with the robust control and filtering problems of networked systems, \mathcal{H}_∞ control and filtering problems, Kalman and extended Kalman filtering problems, optimal control problems, synchronization and consensus problems of complex networks, consensus and cooperative control problems of multiagent systems, and so on [18, 19].

It is worth mentioning that what a network induces are much more than those already studied. Nowadays, the large-scale general systems are usually subject to various sorts of complexities such as parameter uncertainties, time-delays, fading measurements, signal quantization, nonlinear disturbances [20], network attacks [21], event-triggered communication mechanism [22], and time-varying network topology [23]. Such complexities, which do exist under nonnetworked circumstances, are becoming even severer in networked environments by means of their degrees or intensities. In other words, these kinds of complexities have been greatly *enhanced* because of the usage of the communication networks. In this case, it would be interesting to examine (1) how the networks enhance the complexity; (2) how to describe the complexity so as to reflect the reality more closely in practical engineering; and (3) how to establish a general analysis framework to handle or reduce such kind of network-enhanced complexity. Recently, three kinds of complexities, namely, fading measurements, event-triggered mechanisms, and attack behaviors of adversaries, have been gaining particular research attention due to their extensive application potentials in various engineering practices. As such, the performance analysis and synthesis issues for systems with such network-enhanced complexities serve as interesting, imperative yet challenging topics. To this end, the focus of this paper is to provide a timely review on the recent advances on performance analysis and synthesis issues with network-enhanced complexities. The aforementioned three kinds of fashionable complexities are summarized from their engineering backgrounds, dynamical characteristics, and modeling aspects. Subsequently, the recent advances on the performance analysis and synthesis problems with network-enhanced complexities are reviewed systematically. Furthermore, some challenging issues are highlighted by summarizing the latest results. Finally, some concluding remarks are drawn and some possible future research directions are pointed out.

The remainder of this paper is organized as follows. In Section 2, three kinds of complexities, that is, fading measurements, event-triggered mechanisms, and attack behavior of adversaries, are introduced in detail from their engineering backgrounds, dynamical characteristics, and modeling techniques. Section 3 reviews the developments of the performance analysis and synthesis for various networked systems. Furthermore, some challenges are highlighted. In Section 4, the conclusions and future work are given in Section 5.

2. Network-Enhanced Complexities

Because of the ever-increasing popularity of communication networks, more and more control and signal process algorithms are executed over communication links. As a result, inherent complexities with networked systems have been inevitably enhanced. In this section, three latest research focuses (i.e., fading measurements, event-triggered mechanisms, and attack behaviors of adversaries) are introduced, respectively.

2.1. Fading Measurements. Fading measurements are now well known to be one of the most frequently occurred phenomena in networked systems. To be more specific, on one hand, measurement signals in the digital communication are usually subject to probabilistic information missing (also called data dropouts or packet losses) due to a variety of reasons such as the high maneuverability of a tracked target, the faults in measurement outputs, intermittent sensor failures, and network congestions. On the other hand, for the signal transmitted over a wireless channel, some special physical phenomena are unavoidable which mainly include reflection, refraction, and diffraction. These phenomena typically result in the multipath induced fading or the shadow fading, which could drastically degrade the system performances. In the published results, fading is often modeled in time-domain by some time-varying stochastic mathematical models such as the memoryless multiplicative channel model and the ℓ th order Rice model (also called the autoregressive model); see [6, 24–27] and the references therein. In such models, the stochastic variables obeying the given probability distribution are employed to describe the transmitted signal's changes in the amplitude and/or phase. Recently, some preliminary results about the stability analysis, LQG (linear quadratic Gaussian) control, and Kalman filtering problems have been reported by many researchers in the area.

2.2. Event-Triggering Mechanisms. In order to reduce the communication burden [28, 29], the event-triggering control or filtering strategies have received particular research attention for the networked control systems (NCSs) especially the distributed real-time sensing and control systems. In comparison to the time-triggering case, the signals in event-triggering schemes are updated only when certain specific event happens. The event-triggering condition, which is usually modeled by a quadratic cost function dependent on time, sampling data, or system states [30], could reflect the absolute or relative errors between current measurements (or states) and the latest information transmitted. An appropriately generated updating time instants would guarantee the stability and other performances of the closed-loop system or the estimation error dynamics. In addition, between updates of the controller or estimator inputs, the signal remains unchanged by using the zero-order hold (ZOH). It should be pointed out that the updating time is typically unknown *a priori* and therefore a naturally arising challenge is how to cope with the complexities enhanced by event-triggering mechanisms. The theoretic research interests in event-triggering control and filter problems have been initialized by the pioneering works (e.g., [31]). Nowadays, such an event-triggering control/filtering scheme has become an active research area and the idea penetrates a number of research directions from modeling, control, estimation to optimization.

2.3. The Attack Behaviors of Adversaries. With the increasing research attention on higher safety and reliability standards, the network security is of utmost importance in the real-world engineering [32, 33]. Different from the traditional

sensor/actuator faults or system faults, the attack behaviors of adversaries are fast becoming a new research focus in very recent years and some typical examples have been reported such as the Stuxnet worm threat, power and transportation network attacks, and other staged attacks in power generators [34–36]. For networked control systems, the sensors, controllers, and actuators are integrated through common network links. As such, the exchanged data without security protection can be easily exploited by adversaries (or attackers). Generally speaking, by destroying certain significant data, the goal of the adversaries is to destabilize the plant or steer the plant to the adversaries' desired operating point [37]. It is worth noting that attacks on control systems can be arguably classified into two classes, namely, the denial-of-service (DoS) attacks and the deception attacks [38].

The DoS behavior, which can be modeled by a Bernoulli process or Markov process with known statistical information, is a strategy often used by the adversaries in order to prevent the transmission of measurement or control signals by occupying the network resource [39]. Different from the missing measurements due to the physical limitation, the network attack of adversaries is malicious which will lead to unexpected system behaviors. Furthermore, for deception attacks, the attacker aims to insert a false (or distorted) signal into the controller/actuator to disrupt the normal behaviors of the controller [40]. Such an attack is typically modeled as the sum between the opposite of the current signal and any disturbance. Obviously, it is challenging to develop appropriate methodology to examine how the networks have substantial impacts on such kind of complexity induced by the attack behaviors.

3. Recent Advances on Performance Analysis with Network-Enhanced Complexities

In this section, according to three kinds of complexities mentioned above, the developments of the performance analysis and synthesis issues for various networked systems are systematically reviewed as follows.

3.1. Performance Analysis with Fading Measurements. In most published papers, a stochastic variable obeying given Bernoulli distribution has been exploited to govern the communication channel where packets can be received if the channel is of sufficiently good quality and fully dropped if the channel is poor quality. Up to now, this is the simplest important model which describes the so-called erasure channel. Based on such a model, the performance analysis and synthesis as well as the effect of channel capacity for various networked systems have been widely studied by control researchers [41]. For instance, the Kalman filtering (KF) problems have been investigated in [42] where a threshold has been obtained such that the expected error covariance is unbounded if the packet arrival rate is below this threshold. In [6], the stochastic stability of centralized Kalman filtering has been investigated for a linear time-varying system over block fading wireless channels where the variable channel gains are counteracted by power control

to alleviate the effects of packet drops. Furthermore, in [24], the remote mean-square stabilization problem has been thoroughly dealt with for different kinds of fading channels where the largest probability of erasure tolerable by the closed loop feedback control can be obtained from solving a robust control synthesis problem. Recently, the discrete-time LQG optimal control problem has been considered in [25] for MIMO (multiinput multioutput) systems where each sensor and each actuator exchange data with the control unit in an independent way. For such a framework, it has been shown that the separation principle still holds in the case where packet arrivals are acknowledged by the receiver (i.e., the case of protocols like TCP, Transmission Control Protocols) and the optimal LQG control is a linear function of the state which explicitly depends on the loss probabilities of the actuator channels. However, for the case of protocols like UDP (user datagram protocols), the optimal LQG control has not been appropriately investigated yet since the separation principle cannot be easily derived.

In real-world systems, the signal could be subject to fades/degrades in power or amplitude and therefore the wireless channel can be regarded as a continuous valued channel with time-varying channel gains. Based on such a fact, by employing some stochastic variables with nonzero mathematical expectations, a memoryless multiplicative channel model has been developed. Such a model can describe the commonly used channels such as Rayleigh and Nakagami channels [43]. Some representative works are shown here. In order to stabilize an unstable plant over an error-free digital channel, Nair and Evans [44] have provided a tight lower bound on the data rate. Furthermore, the mean square stabilization problem has been discussed in [27] for discrete-time networked control systems over fading channels, which are supposed to use a parallel transmission strategy and own a fixed overall mean square capacity of the network. In the case of state feedback, a tight lower bound on the overall mean square capacity has been presented in terms of the Mahler measure of the plant. For the case of dynamic output feedback, such a lower bound on the capacity requirement for stabilization of SISO (single-input single-output) plants has been given in terms of the antistable poles, nonminimum phase zeros, and relative degree of the plant. Without doubt, KF or the extended Kalman filtering (EKF) with memoryless multiplicative channels has also been investigated due to its recursive nature. Recently, inspired by EKF, a novel unbiased and recursive filtering algorithm has been established for a class of discrete-time nonlinear stochastic systems in [45] where the process noise and the measurement noise are one-step autocorrelated.

It is worth mentioning that the ℓ th order Rice model, which can be utilized to describe both network-induced transmission delay and missing measurements in a unified framework, has also received an ever-increasing research interest. A typical application of this model is about the adaptive blind equalization issue. For example, in [46], by using the optimal linearization technique, a blind-channel equalization has been investigated for the extended-Kalman-filter-based chaotic communication of chaotic communication where the chaotic transmitter system and the channel

model operate at the same time-scale. Since the fading phenomenon can seriously degrade the signal quality, an issue of crucial importance is how to design a control system whose performance is insensitive to the effects caused by the fading channels. Therefore, the networked systems with fading channels have received particular research attention. In [47], the \mathcal{H}_∞ output-feedback control problem has been investigated for a class of discrete-time fuzzy systems with randomly occurring infinite distributed delays and channel fadings. At the same time, the \mathcal{H}_∞ filtering issue has been addressed in [48] for a class of discrete-time Takagi-Sugeno (T-S) fuzzy systems with randomly occurring uncertainties, randomly occurring interval time-varying delays, and channel fadings. In the presence of the randomly occurring phenomena, sufficient conditions are derived, via stochastic analysis and Lyapunov functional approach, such that the desired filter parameters can be obtained by solving a convex optimization problem to guarantee both the exponential mean-square stability and the prescribed \mathcal{H}_∞ performance of filtering error dynamics.

3.2. Performance Analysis with Event-Triggering Mechanisms.

Event-triggering is one of the useful ways to determine when the sampling action is carried out, which guarantees that only really “necessary” signals will be transmitted to the controller or filter. As such, the amount of the sent signals is relatively little in comparison to the time-triggering sampling case. Nowadays, three arguably representative theoretical frameworks, namely, the Lyapunov stability theory [49, 50], switch system theory [51, 52], and input-to-state stability (ISS) theory [53, 54], have been widely employed to analyze the event-triggered control and state estimation issues.

The stability is most important for control systems or filtering error dynamics. One of the simplest analysis methods for networked systems with event-triggering scheme is to view the event-triggering condition as a nonlinear constraint that can be directly embedded into the calculation of Lyapunov function or functional; see for example, [49, 50, 55, 56]. Generally speaking, a desired balance between the sensor-to-estimator communication rate and the estimation quality can be achieved by selecting an appropriate event-triggering threshold. For instance, an event-based sensor data scheduler for linear systems has been proposed and the corresponding minimum squared error estimator has also been designed in [55]. It should be pointed out that the minimum squared error can be adjusted by selecting the threshold. Recently, with the development of analysis methods of time-delay systems, the event-triggering networked systems with various time-delays have been extensively investigated. For instance, in [49], a novel event-triggering transmission scheme, which does not require any special hardware for continuous measurement, has been proposed to determine whether or not the sampled-data should be transmitted. Based on such a scheme, the sampled-data control system has been modeled as a sampled-data error dependent system and its stability condition has been derived by constructing a Lyapunov-Krasovskii functional. In [50], a delay system model has been exploited to describe both the prosperities of the event trigger and

the effect of the transmission delay on the system performance. Very recently, a set-up scheme has been proposed in [56] for the interconnected agents in order to achieve output synchronization with event-driven communication in the presence of constant communication delays. In summary, the work mentioned above has been considered in the framework of the mature time-delay system and the corresponding research with multiobjective constraints is still in its early stages.

The ISS theory is another important approach to coping with the performance analysis and synthesis issues induced by event trigger. The main reason is that the addressed system can be transformed into a traditional time-triggering system with a bound input. Taking such a fact into account, the event-triggering control and filtering problems for various networked systems have attracted an ever-increasing research interest; see [39, 53, 57–61] and the references therein. For example, in [59], a simple event-triggered scheduler based on a feedback paradigm has been investigated in order to expose how to relax the more traditional periodic execution requirements. Very recently, an event-based control algorithm has been developed in [60] for trajectory tracking in nonlinear systems where the desired trajectory has been modelled as a solution of reference system with an exogenous input. In this paper, the authors have demonstrated that the event-based controller designed not only guarantees the ultimate boundedness of the tracking error but also ensures that the interexecution times for the control algorithm are uniformly bounded away from zero. It should be pointed out that the event-triggering requires a hardware event detector that may be implemented by using custom analog integrated circuits or floating point gate array (FPGA) processors [61]. In order to reduce the cost, a software realization, which is called self-triggering, has been considered in the past few years. For example, at the technical level, based on a homogeneity assumption on the continuous dynamics, some advantages of event-triggering implementations have been extended to the self-triggering framework in [57]. Furthermore, a new self-triggering control technique has been developed in [53] for two classes of nonlinear control systems, namely, state-dependent homogeneous systems and polynomial systems.

It is clear that the event-triggering scheme could result in the impulsive behavior. As such, in the past few years, the security control problem based on the impulsive system theory has received a great deal of research interest in the literature; see [29, 51, 52, 62] and the references therein. In these references, several different event-triggering mechanisms and control strategies have been provided. For instance, in [31, 62], the impulsive control action has been applied to reset the state when the state of the plant exceeds a certain threshold. In [51], the stability and \mathcal{L}_∞ -performance have been investigated and the expression for lower bounds on the minimum interevent times has been provided for dynamical output-based controllers with decentralized event-triggering mechanisms. Recently, the optimal sampling for periodic and event-based impulse control has been discussed in [63] for

a class of second order stochastic systems. In this paper, it is shown that the event-based impulse control has given smaller variances than periodic impulse control with the same control rate for higher order systems.

3.3. Recent Advances on Security Control for the Networked Systems with Attackers. As is well known, attacks to communication networks have become prevalent over the last decade [64]. Although most control systems have been safe in the past, they are currently more vulnerable to malicious attacks [21, 65] due to the extensive application of communication networks. The consequences of successful attacks on control networks can be more damaging than attacks on other networks because control systems are at the core of many critical infrastructures. In order to guarantee the security, one of the effective strategies handling the network attacks is to discard or retransmit the destroyed data when they are detected or identified by utilizing some hardware or software tools. Such a strategy could not be suitable for real-world industrial control systems. The main reasons can be summarized as follows: (1) the attacks are usually stealthy and cannot be easily detected and (2) the retransmission method inevitably increases the network burden and also reduces the real-time performance of the addressed systems. Nowadays, considering the security of networked control systems has become very urgent and therefore a good design should make detecting attacks easy, help understand the effects of an attack, make it difficult to execute an attack, and finally minimize the consequences if an attack is successful [66].

The DoS attack is the most typical security problem. In the mathematics including both modeling and performance analysis, it is similar to the traditional data loss and therefore a lot of work on this topic has been published in recent years. For example, a security constrained optimal control for discrete-time linear dynamical systems has been considered in [64], the purpose of which is to find the (optimal) causal feedback controller in order to minimize a given objective function subject to safety and power constraints. Furthermore, in terms of the level of attacks in [67], DoS attacks have been further classified into two types: weak attacks and strong attacks. For the weak DoS attacks case with the network communication constraints (random delay, packet disorder, and packet loss), a recursive networked predictive control (RNPC) method has been proposed to compensate for the adverse effects by using the switched system theory. In addition, for the strong DoS attacks on the controller side, a multicontroller switching scheme has been presented, in which each controller has been designed based on the RNPC. Note that, compared with the generally applied Bernoulli distribution, a Markov process can be also utilized to govern the attacks. In [68], a risk-sensitive stochastic control issue has been discussed for a class of discrete-time partially observed system with an exponential running cost function. In this paper, the optimal control policy, which satisfies a separation principle, has been derived by applying a chain of measure transformation techniques and dynamic programming.

It is noteworthy that the complexities should be intensified for distributed networked systems with attackers. However, the corresponding researches just receive a preliminary attention. It should be pointed out that in [69], the security decisions issue where the security is interdependent due to network induced risks has been investigated for identical plant-controller systems. By using a noncooperative game (the game between the individually optimal security and the socially optimal security), the problem of security choices has been divided into a two-stage game: on the first stage the players decide whether to invest in security or not and on the second stage they apply control inputs to minimize the average operational costs. In [70], the authors have considered the resilient consensus problem for an operator-vehicle network in which each operator-vehicle pair is attacked by an adversary who is able to maliciously replay the control commands sent from the operator. By means of the receding-horizon control strategy, a novel replay resilient consensus algorithm has been proposed such that the vehicles can be steered to a consensus point within a given constraint set.

Deception attacks (or false data injection attacks) are more general attack behavior which includes DoS as a special case. In the past few years, the problem of secure estimation and control in networked systems under false-data attacks has attracted significant attention; see [71] for more details. In [72], attack scenarios corresponding to replay, zero-dynamics, and bias injection attacks have been analyzed by using a new adversary model, and then the maximum impact of stealthy bias injection attacks has been derived which does not require perfect model knowledge. In [40], the estimation schemes have been studied in power grids and the results show how the attacker could potentially modify state estimates without being detected. Furthermore, based on the work of [40], KF under false data injection attacks has been investigated for general dynamical systems [73]. In this paper, the authors have provided a necessary and sufficient condition under which the attacker could make the estimation error unbounded if without being detected. Recently, secure networked predictive control system architecture has been presented in [74]. In order to guarantee the control system performance when suffering from deception attacks, according to round-trip time delays, the recursive networked predictive control method has been proposed to compensate the adverse effects induced by the deception attacks as well as the network communication constraints (such as time-varying network delay, packet disorder, and packet dropout). In [71], the classical notion of reachability has been extended to the security domain, and some novel results on such a notion have been established within a secure control theoretic framework. In addition, in the case that the attack and disturbance sets are ellipsoidal, the desired controller can be obtained by using ellipsoidal calculus for linear time-varying systems.

4. Some Challenging Issues on Network-Enhanced Complexities

In the past few years, we have witnessed significant progress on the performance analysis and synthesis issues with various

types of network-enhanced complexities, and a large amount of literature has appeared on the topics. Obviously, as the scale of networked systems increases, these complexities will have greater and greater effects on the desired performance and will also lead to some unexpected obstacles for system modeling, performance analysis, and parameter design.

4.1. Distributed and Networked Event-Triggering Mechanism.

It is well known that it is hard to be sticky to the time-triggering paradigm for distributed systems (e.g., sensor networks and multiagent systems) since the sample times of all sensors or the update times of controller input are very difficult to remain synchronized. Recently, a novel control strategy with event-triggering broadcasting has been provided in [75] for continuous-time first-order multiagent systems, where each agent's measurement error is bounded by a time-dependent threshold. By utilizing the convergence analysis, an iterative event-triggering algorithm has been proposed in [30] where the continuous measurement of the neighbor states is avoided. Furthermore, the distributed rendezvous phenomenon has been addressed to account for the switching issues of control inputs. Following the ideas of Tabuada [59], a decentralized event-based strategy has been presented in [76] to determine the control updates such that the overall system reaches average consensus asymptotically. The authors have shown that all agents continuously monitor their neighbors' states and each agent updates its control law not only at its own event-times but also whenever one of its neighbors triggers an event. It should be pointed out that, up to now, the corresponding results concerning control and state estimation problems are very scattered for distributed systems with event-triggering communication protocol due primarily to the difficulty in both the mathematical analysis and the design of suitable event-triggering mechanisms.

4.2. Distributed and Networked Cyber Attacks.

The distributed and networked nature of the system often makes it vulnerable to a deliberate attack since such systems are more open [77]. Different from the traditional networked systems, each node in distributed systems could suffer the impact from the behavior of the adversaries or the fault node dynamics due to proliferation of malicious attacks or fault through the network topology. Based on such a fact, the resilient asymptotic consensus problem in [78] has been investigated for discrete-time multiagent systems in the presence of adversaries and transmission delays. In this paper, an improved form of local filtering strategy has been provided for the loyal agents to resist adversaries. In [79], considering two types of agents (Byzantine agents and malicious agents), the adversarial robust consensus protocol, which combines ideas from distributed computing and cooperative control, has been established to guarantee the agreement and safety conditions in static and switching network topologies, whenever the number of adversaries in the network is bounded by a constant. It is worth pointing out that the secure and fault-tolerant consensus algorithms usually assume knowledge of nonlocal information. However, such an assumption could be not suitable for large-scale distributed dynamic networks. In

order to overcome this drawback, a necessary and sufficient condition has been proposed in [80] for the normal nodes to reach asymptotic consensus in the presence of the influence of the misbehaving nodes under different threat assumptions. In summary, these issues have not been addressed yet and still remain challenging.

4.3. The Time-Varying Characteristics in Network-Enhanced Complexities.

It should be pointed out that all models for real-time systems should be time varying since the system parameters could be changeable with the time, temperature, operating point, and so forth. As such, the finite-horizon control and filtering problem is of practical significance and therefore has received extensive research attention in the past few years [3, 81–91]. For instance, the recursive linear matrix inequality (RLMI) method has been proposed in [3] to effectively solve finite-horizon filtering \mathcal{H}_∞ problems for a class of nonlinear systems with quantization effects, and the backward recursive Riccati difference equation (RDE) approach has been developed in [82] to deal with a distributed \mathcal{H}_∞ state estimation problem over sensor networks. Furthermore, in [84], the distributed finite-horizon filtering problem has been concerned for a class of time-varying systems over lossy sensor networks which suffer from quantization errors and successive packet dropouts that are described in a unified framework. Through available output measurements from not only the individual sensor but also its neighboring sensors according to the given topology, a sufficient condition has been provided for the desired distributed filter to guarantee that the prescribed average filtering performance constraint is achieved. Unfortunately, to the best of our knowledge, there have been very few results for time-varying systems with the fading measurements, the event-triggering mechanisms, and the attack behavior of adversaries.

5. Conclusions and Future Work

In this paper, we have surveyed some recent advances on performance analysis and synthesis issues with network-enhanced complexities involving the fading measurements, the event-triggering mechanisms, and the attack behavior of adversaries. At the same time, these three kinds of complexities have been introduced from their engineering background, characteristic, and modelling. Furthermore, we have paid particular attention to some challenging issues. The related topics for the future research work are listed below.

- (1) The problems of distributed control and filtering with network-enhanced complexities are of engineering significance, especially when the system is time varying. Hence, the analysis of dynamical behaviors for time-varying system would be new research topic.
- (2) Because of the proliferation of malicious attacks or fault through the network topology, it would be interesting to further investigate how the malicious attacks or faults affect the consensus performance for multiagent systems or the filtering performance for sensor networks.

- (3) Taking the energy efficiency and communication burden into consideration, the distributed control and filtering problems with event-triggering mechanism are of significant engineering importance. The main difficulty is how to select a suitable method to model the system dynamics and analyze the desired performance for large-scale networked systems.
- (4) Since the security is a “hard” performance index, the analysis in mean-square sense is more conservative for practical engineering. As such, it would be interesting to investigate the security problems with probabilistic performance index in the presence of network attacks.
- (5) No doubt, the computation burden of proposed control and filtering schemes will increase as the scale of network nodes increases and the corresponding strategies are not especially suitable for online application. Hence, it leads to a particularly attractive area for developing some new approaches or improving the established schemes to satisfy the requirement of real-world engineering systems.
- (6) Another future research direction is to discuss the applications of the established theories and methodologies to some practical engineering problems such as power systems and mobile robots.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

This work was supported in part by the National Natural Science Foundation of China under Grants 61134009, 61329301, 61203139, 61374127, and 61374010, the Royal Society of the UK, and the Alexander von Humboldt Foundation of Germany.

References

- [1] H. Dong, Z. Wang, and H. Gao, *Filtering, Control and Fault Detection with Randomly Occurring Incomplete Information*, Wiley, Chichester, UK, 2013.
- [2] H. Gao, T. Chen, and J. Lam, “A new delay system approach to network-based control,” *Automatica*, vol. 44, no. 1, pp. 39–52, 2008.
- [3] B. Shen, Z. Wang, and Y. S. Hung, “Distributed H_∞ -consensus filtering in sensor networks with multiple missing measurements: the finite-horizon case,” *Automatica*, vol. 46, no. 10, pp. 1682–1688, 2010.
- [4] X. Su, L. Wu, and P. Shi, “Sensor networks with random link failures: distributed filtering for T-S fuzzy systems,” *IEEE Transactions on Industrial Informatics*, vol. 9, no. 3, pp. 1739–1750, 2013.
- [5] Z. Wang, Y. Wen, and X. Luo, “Quantized \mathcal{H}_∞ fault-tolerant control for networked control systems,” *International Journal of Automation and Computing*, vol. 9, no. 4, pp. 352–357, 2012.
- [6] D. E. Quevedo, A. Ahlén, A. S. Leong, and S. Dey, “On Kalman filtering over fading wireless channels with controlled transmission powers,” *Automatica*, vol. 48, no. 7, pp. 1306–1316, 2012.
- [7] J. Bhattacharyya and S. Pal, “Dynamics of a stage-structured system with harvesting and discrete time delays,” *Systems Science and Control Engineering*, vol. 2, no. 1, pp. 192–215, 2014.
- [8] R. Caballero-Águila, A. Hermoso-Carazo, and J. Linares-Pérez, “A new estimation algorithm from measurements with multiple-step random delays and packet dropouts,” *Mathematical Problems in Engineering*, vol. 2010, Article ID 258065, 18 pages, 2010.
- [9] H. Gao and T. Chen, “ H_∞ estimation for uncertain systems with limited communication capacity,” *IEEE Transactions on Automatic Control*, vol. 52, no. 11, pp. 2070–2084, 2007.
- [10] X. He, Z. Wang, and D. Zhou, “Robust H_∞ filtering for networked systems with multiple state delays,” *International Journal of Control*, vol. 80, no. 8, pp. 1217–1232, 2007.
- [11] H. R. Karimi, “Robust delay-dependent H_∞ control of uncertain time-delay systems with mixed neutral, discrete, and distributed time-delays and Markovian switching parameters,” *IEEE Transactions on Circuits and Systems I*, vol. 58, no. 8, pp. 1910–1923, 2011.
- [12] M. Kermani and A. Sakly, “Stability analysis for a class of switched nonlinear time-delay systems,” *Systems Science and Control Engineering*, vol. 2, no. 1, pp. 80–89, 2014.
- [13] J. Liang, Z. Wang, and X. Liu, “Distributed state estimation for uncertain Markov-type sensor networks with mode-dependent distributed delays,” *International Journal of Robust and Nonlinear Control*, vol. 22, no. 3, pp. 331–346, 2012.
- [14] J. Liang, Z. Wang, B. Shen, and X. Liu, “Distributed state estimation in sensor networks with randomly occurring nonlinearities subject to time-delays,” *ACM Transactions on Sensor Networks*, vol. 9, no. 1, article 4, 2012.
- [15] G. Wei, L. Wang, and F. Han, “A gain-scheduled approach to fault-tolerant control for discrete-time stochastic delayed systems with randomly occurring actuator faults,” *Systems Science and Control Engineering*, vol. 1, no. 1, pp. 82–90, 2013.
- [16] J. Xiong and J. Lam, “Stabilization of networked control systems with a logic ZOH,” *IEEE Transactions on Automatic Control*, vol. 54, no. 2, pp. 358–363, 2009.
- [17] X. Zhang and L. Yang, “A fiber Bragg grating quasi-distributed sensing network with a wavelength-tunable chaotic fiber laser,” *Systems Science and Control Engineering*, vol. 2, no. 1, pp. 268–274, 2014.
- [18] L. Qin, X. He, and D. H. Zhou, “A survey of fault diagnosis for swarm systems,” *Systems Science and Control Engineering*, vol. 2, no. 1, pp. 13–23, 2014.
- [19] Q. Wang, H. Gao, F. Alsaadi, and T. Hayat, “An overview of consensus problems in constrained multi-agent coordination,” *Systems Science and Control Engineering*, vol. 2, no. 1, pp. 275–284, 2014.
- [20] J. Liang, F. Sun, and X. Liu, “Finite-horizon H_∞ filtering for time-varying delay systems with randomly varying nonlinearities and sensor saturations,” *Systems Science and Control Engineering*, vol. 2, no. 1, pp. 108–118, 2014.
- [21] A. A. Cárdenas, S. Amin, and S. S. Sastry, “Research challenges for the security of control systems,” in *Proceedings of the 3rd USENIX Workshop on Hot Topics in Security (HotSec '08)*, vol. 6, San Jose, Calif, USA, 2008.

- [22] W. P. M. H. Heemels, J. H. Sandee, and P. P. J. Van Den Bosch, "Analysis of event-driven controllers for linear systems," *International Journal of Control*, vol. 81, no. 4, pp. 571–590, 2008.
- [23] M. Huang and J. H. Manton, "Stochastic consensus seeking with noisy and directed inter-agent communication: fixed and randomly varying topologies," *IEEE Transactions on Automatic Control*, vol. 55, no. 1, pp. 235–241, 2010.
- [24] N. Elia, "Remote stabilization over fading channels," *Systems & Control Letters*, vol. 54, no. 3, pp. 237–249, 2005.
- [25] E. Garone, B. Sinopoli, A. Goldsmith, and A. Casavola, "LQG control for MIMO systems over multiple erasure channels with perfect acknowledgment," *IEEE Transactions on Automatic Control*, vol. 57, no. 2, pp. 450–456, 2012.
- [26] Y. Mostofi and R. M. Murray, "To drop or not to drop: design principles for Kalman filtering over wireless fading channels," *IEEE Transactions on Automatic Control*, vol. 54, no. 2, pp. 376–381, 2009.
- [27] N. Xiao, L. Xie, and L. Qiu, "Feedback stabilization of discrete-time networked systems over fading channels," *IEEE Transactions on Automatic Control*, vol. 57, no. 9, pp. 2176–2189, 2012.
- [28] Q. Liu, Z. Wang, X. He, and D. Zhou, "survey of event-based strategies on control and estimation," *Systems Science and Control Engineering*, vol. 2, no. 1, pp. 90–97, 2014.
- [29] X. Meng and T. Chen, "Event based agreement protocols for multi-agent networks," *Automatica*, vol. 49, no. 7, pp. 2125–2132, 2013.
- [30] Y. Fan, G. Feng, Y. Wang, and C. Song, "Distributed event-triggered control of multi-agent systems with combinational measurements," *Automatica*, vol. 49, no. 2, pp. 671–675, 2013.
- [31] K. J. Åström and B. M. Bernhardsson, "Comparison of Riemann and Lebesgue sampling for first order stochastic systems," in *Proceedings of the 41st IEEE Conference on Decision and Control*, pp. 2011–2016, December 2002.
- [32] D. He, C. Chen, S. Chan, J. Bu, and L. T. Yang, "Security analysis and improvement of a secure and distributed reprogramming protocol for wireless sensor networks," *IEEE Transactions on Industrial Electronics*, vol. 60, no. 11, pp. 5348–5354, 2013.
- [33] W. Zeng and M.-Y. Chow, "Optimal tradeoff between performance and security in networked control systems based on coevolutionary algorithms," *IEEE Transactions on Industrial Electronics*, vol. 59, no. 7, pp. 3016–3025, 2012.
- [34] S. Amin, X. Litrico, S. Sastry, and A. M. Bayen, "Cyber security of water SCADA systems—part I: analysis and experimentation of stealthy deception attacks," *IEEE Transactions on Control Systems Technology*, vol. 21, no. 5, pp. 1963–1970, 2013.
- [35] S. Amin, X. Litrico, S. Sastry, and A. M. Bayen, "Cyber security of water SCADA systems—part II: attack detection using enhanced hydrodynamic models," *IEEE Transactions on Control Systems Technology*, vol. 21, no. 5, pp. 1679–1693, 2013.
- [36] A. Teixeira, H. Sandberg, and K. H. Johansson, "Networked control systems under cyber attacks with applications to power networks," in *Proceedings of the American Control Conference (ACC '10)*, pp. 3690–3696, Baltimore, Md, USA, July 2010.
- [37] A. Clark, L. Bushnell, and R. Poovendran, "passivity-based framework for composing attacks on networked control systems," in *Proceedings of the 50th Annual Allerton Conference*, pp. 1814–1821, Monticello, Ill, USA, October 2012.
- [38] A. A. Cárdenas, S. Amin, and S. Sastry, "Secure control: towards survivable cyber-physical systems," in *Proceedings of the 28th International Conference on Distributed Computing Systems Workshops (ICDCS '08)*, pp. 495–500, Beijing, China, June 2008.
- [39] H. Foroush and S. Martínez, "On event-triggered control of linear systems under periodic Denial-of-Service jamming attacks," in *Proceedings of the the 51st IEEE Conference on Decision and Control*, pp. 2551–2256, Maui, Hawaii, USA, December 2012.
- [40] Y. Liu, P. Ning, and M. K. Reiter, "False data injection attacks against state estimation in electric power grids," in *Proceedings of the 16th ACM Conference on Computer and Communications Security (CCS '09)*, pp. 21–32, Chicago Ill, USA, November 2009.
- [41] J. Hu, Z. Wang, B. Shen, and H. Gao, "Quantised recursive filtering for a class of nonlinear systems with multiplicative noises and missing measurements," *International Journal of Control*, vol. 86, no. 4, pp. 650–663, 2013.
- [42] B. Sinopoli, L. Schenato, M. Franceschetti, K. Poolla, M. I. Jordan, and S. S. Sastry, "Kalman filtering with intermittent observations," *IEEE Transactions on Automatic Control*, vol. 49, no. 9, pp. 1453–1464, 2004.
- [43] A. S. Leong, S. Dey, and J. Anand, "Optimal LQG control over continuous fading channels," in *Proceedings of the 18th IFAC World Congress*, pp. 6580–6585, Milano, Italy, August 2011.
- [44] G. N. Nair and R. J. Evans, "Stabilizability of stochastic linear systems with finite feedback data rates," *SIAM Journal on Control and Optimization*, vol. 43, no. 2, pp. 413–436, 2004.
- [45] J. Hu, Z. Wang, and H. Gao, "Recursive filtering with random parameter matrices, multiple fading measurements and correlated noises," *Automatica*, vol. 49, no. 11, pp. 3440–3448, 2013.
- [46] J. S. H. Tsai, F.-C. Lu, R. S. Provence, L. S. Shieh, and Z. Han, "A new approach for adaptive blind equalization of chaotic communication: the optimal linearization technique," *Computers & Mathematics with Applications*, vol. 58, no. 9, pp. 1687–1698, 2009.
- [47] S. Zhang, Z. Wang, D. Ding, and H. Shu, " \mathcal{H}_∞ fuzzy control with randomly occurring infinite distributed delays and channel fadings," *IEEE Transactions on Fuzzy Systems*, vol. 22, no. 1, pp. 189–200, 2014.
- [48] S. Zhang, Z. Wang, D. Ding, and H. Shu, "Fuzzy filtering with randomly occurring parameter uncertainties, interval delays, and channel fadings," *IEEE Transactions on Cybernetics*, vol. 44, pp. 406–417, 2014.
- [49] C. Peng and Q.-L. Han, "A novel event-triggered transmission scheme and \mathcal{L}_2 control co-design for sampled-data control systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 10, pp. 2620–2626, 2013.
- [50] D. Yue, E. Tian, and Q.-L. Han, "A delay system method for designing event-triggered controllers of networked control systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 2, pp. 475–481, 2013.
- [51] M. C. F. Donkers and W. P. M. H. Heemels, "Output-based event-triggered control with guaranteed L_∞ -gain and improved and decentralized event-triggering," *IEEE Transactions on Automatic Control*, vol. 57, no. 6, pp. 1362–1376, 2012.
- [52] X. Wang and M. Lemmon, "On event design in event-triggered feedback systems," *Automatica*, vol. 47, no. 10, pp. 2319–2322, 2011.
- [53] A. Anta and P. Tabuada, "To sample or not to sample: self-triggered control for nonlinear systems," *IEEE Transactions on Automatic Control*, vol. 55, no. 9, pp. 2030–2042, 2010.
- [54] M. Mazo, Jr., A. Anta, and P. Tabuada, "An ISS self-triggered implementation of linear controllers," *Automatica*, vol. 46, no. 8, pp. 1310–1314, 2010.
- [55] J. Wu, Q.-S. Jia, K. H. Johansson, and L. Shi, "Event-based sensor data scheduling: trade-off between communication rate and

- estimation quality," *IEEE Transactions on Automatic Control*, vol. 58, no. 4, pp. 1041–1046, 2013.
- [56] H. Yu and P. J. Antsaklis, "Output synchronization of networked passive systems with event-driven communication," *IEEE Transactions on Automatic Control*, vol. 59, no. 3, pp. 750–756, 2012.
- [57] A. Anta and P. Tabuada, "Self-triggered stabilization of homogeneous control systems," in *Proceedings of the American Control Conference (ACC '08)*, pp. 4129–4134, Washington, DC, USA, June 2008.
- [58] E. Garcia and P. J. Antsaklis, "Model-based event-triggered control for systems with quantization and time-varying network delays," *IEEE Transactions on Automatic Control*, vol. 58, no. 2, pp. 422–434, 2013.
- [59] P. Tabuada, "Event-triggered real-time scheduling of stabilizing control tasks," *IEEE Transactions on Automatic Control*, vol. 52, no. 9, pp. 1680–1685, 2007.
- [60] P. Tallapragada and N. Chopra, "On event triggered tracking for nonlinear systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 9, pp. 2343–2348, 2013.
- [61] X. Wang and M. D. Lemmon, "Event design in event-triggered feedback control systems," in *Proceedings of the 47th IEEE Conference on Decision and Control (CDC '08)*, pp. 2105–2110, Cancun, Mexico, December 2008.
- [62] T. Henningsson, E. Johansson, and A. Cervin, "Sporadic event-based control of first-order linear stochastic systems," *Automatica*, vol. 44, no. 11, pp. 2890–2895, 2008.
- [63] X. Meng and T. Chen, "Optimal sampling and performance comparison of periodic and event based impulse control," *IEEE Transactions on Automatic Control*, vol. 57, no. 12, pp. 3252–3259, 2012.
- [64] S. Amin, A. A. Cárdenas, and S. S. Sastry, "Safe and secure networked control systems under denial-of-service attacks," in *Proceedings of the 12th International Conference on Hybrid Systems: Computation and Control*, vol. 5469 of *Lecture Notes in Comput. Sci.*, pp. 31–45, Springer, San Francisco, Calif, USA, 2009.
- [65] R. J. Turk, *Cyber Incidents Involving Control Systems*, Idaho National Engineering and Environmental Laboratory, 2005.
- [66] A. Rai, D. Ward, S. Roy, and S. Warnick, "Vulnerable links and secure architectures in the stabilization of networks of controlled dynamical systems," in *Proceedings of American Control Conference*, pp. 1248–1253, Montreal, Canada, 2012.
- [67] Z. H. Pang, G. P. Liu, and Z. Dong, "Secure networked control systems under denial of service attacks," in *Proceedings of the 18th IFAC World Congress*, pp. 8908–8913, Milano, Italy, August 2011.
- [68] G. K. Befekadu, V. Gupta, and P. J. Antsaklis, "Risk-sensitive control under a class of denial-of-service attack models," in *Proceedings of the American Control Conference (ACC '11)*, pp. 643–648, San Francisco, Calif, USA, July 2011.
- [69] S. Amin, G. A. Schwartz, and S. S. Sastry, "Security of interdependent and identical networked control systems," *Automatica*, vol. 49, no. 1, pp. 186–192, 2013.
- [70] M. Zhu and S. Martínez, "On resilient consensus against replay attacks in operator-vehicle networks," in *Proceedings of the American Control Conference*, pp. 3553–3558, Montreal, Canada, June 2012.
- [71] A. N. Bishop, "A robust reachability review for control system security," in *Proceedings of the 1st Australian Control Conference (AUCC '11)*, pp. 381–385, Melbourne, Australia, November 2011.
- [72] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," 2012, <http://arxiv.org/pdf/1212.0226.pdf>.
- [73] Y. Mo, E. Garone, A. Casavola, and B. Sinopoli, "False data injection attacks against state estimation in wireless sensor networks," in *Proceedings of the 49th IEEE Conference on Decision and Control (CDC '10)*, pp. 5967–5972, Atlanta, Ga, USA, December 2010.
- [74] Z.-H. Pang and G.-P. Liu, "Design and implementation of secure networked predictive control systems under deception attacks," *IEEE Transactions on Control Systems Technology*, vol. 20, no. 5, pp. 1334–1342, 2012.
- [75] G. S. Seyboth, D. V. Dimarogonas, and K. H. Johansson, "Event-based broadcasting for multi-agent average consensus," *Automatica*, vol. 49, no. 1, pp. 245–252, 2013.
- [76] D. V. Dimarogonas, E. Frazzoli, and K. H. Johansson, "Distributed event-triggered control for multi-agent systems," *IEEE Transactions on Automatic Control*, vol. 57, no. 5, pp. 1291–1297, 2012.
- [77] G. Kumar and K. Kumar, "Network security—an updated perspective," *Systems Science and Control Engineering*, vol. 2, no. 1, pp. 325–334, 2014.
- [78] Y. Wu, X. He, S. Liu, and L. Xie, "Consensus of discrete-time multi-agent systems with adversaries and time delays," *International Journal of General Systems*, vol. 43, no. 3-4, pp. 402–411, 2014.
- [79] H. J. Leblanc and X. Koutsoukos, "Low complexity resilient consensus in networked multi-agent systems with adversaries," in *Proceedings of the 15th ACM International Conference on Hybrid Systems: Computation and Control (HSCC '12)*, pp. 5–14, chn, April 2012.
- [80] H. J. LeBlanc, H. Zhang, and X. Koutsoukos, "Resilient asymptotic consensus in robust networks," *IEEE Transactions on Automatic Control*, vol. 31, no. 4, pp. 766–781, 2013.
- [81] T. Binazadeh and M. Shafiei, "A novel approach in the finite-time controller design," *Systems Science and Control Engineering*, vol. 2, no. 1, pp. 119–124, 2014.
- [82] D. Ding, Z. Wang, H. Dong, and H. Shu, "Distributed H_∞ state estimation with stochastic parameters and nonlinearities through sensor networks: the finite-horizon case," *Automatica*, vol. 48, no. 8, pp. 1575–1585, 2012.
- [83] H. Dong, Z. Wang, and H. Gao, "Distributed filtering for a class of time-varying systems over sensor networks with quantization errors and successive packet dropouts," *IEEE Transactions on Signal Processing*, vol. 60, no. 6, pp. 3164–3173, 2012.
- [84] H. Dong, Z. Wang, D. W. C. Ho, and H. Gao, "Variance-constrained H_∞ filtering for a class of nonlinear time-varying systems with multiple missing measurements: the finite-horizon case," *IEEE Transactions on Signal Processing*, vol. 58, no. 5, pp. 2534–2543, 2010.
- [85] T. Hou, W. Zhang, and H. Ma, "Finite horizon H_2/H_∞ control for discrete-time stochastic systems with Markovian jumps and multiplicative noise," *IEEE Transactions on Automatic Control*, vol. 55, no. 5, pp. 1185–1191, 2010.
- [86] Y. S. Hung and F. Yang, "Robust H_∞ filtering for discrete time-varying uncertain systems with a known deterministic input," *International Journal of Control*, vol. 75, no. 15, pp. 1159–1169, 2002.
- [87] B. Shen, Z. Wang, H. Shu, and G. Wei, "Robust H_∞ finite-horizon filtering with randomly occurred nonlinearities and quantization effects," *Automatica*, vol. 46, no. 11, pp. 1743–1751, 2010.

- [88] B. Shen, Z. Wang, and X. Liu, "Bounded H_∞ synchronization and state estimation for discrete time-varying stochastic complex networks over a finite horizon," *IEEE Transactions on Neural Networks*, vol. 22, no. 1, pp. 145–157, 2011.
- [89] Z. Wang, D. Ding, H. Dong, and H. Shu, " H_∞ consensus control for multi-agent systems with missing measurements: the finite-horizon case," *Systems & Control Letters*, vol. 62, no. 10, pp. 827–836, 2013.
- [90] Z. Wang, H. Dong, B. Shen, and H. Gao, "Finite-horizon H_∞ filtering with missing measurements and quantization effects," *IEEE Transactions on Automatic Control*, vol. 58, no. 7, pp. 1707–1718, 2013.
- [91] Y. Zhu, X. Guan, and X. Luo, "Finite-time consensus for multi-agent systems via nonlinear control protocols," *International Journal of Automation and Computing*, vol. 10, no. 5, pp. 455–462, 2013.

