Spring 2018

Data analytics for stochastic control and prognostics in cyber-physical systems

Shanshan Bi

Department: Electrical and Computer Engineering

DATA ANALYTICS FOR STOCHASTIC CONTROL AND PROGNOSTICS IN CYBER-PHYSICAL SYSTEMS

by

SHANSHAN BI

A DISSERTATION

Presented to the Graduate Faculty of the

MISSOURI UNIVERSITY OF SCIENCE AND TECHNOLOGY

In Partial Fulfillment of the Requirements for the Degree

DOCTOR OF PHILOSOPHY

in

ELECTRIC ENGINEERING

2018

Approved by

Dr. Maciej Zawodniok
Dr. Jagannathan Sarangapani
Dr. Egemen K. Cetinkaya
Dr. Jie Huang
Dr. Zhaozheng Yin

PUBLICATION DISSERTATION OPTION

This dissertation consists of the following five articles:

Paper I, Pages 9-42: Shanshan Bi, Lei Wang, and Maciej Zawodniok, "Effective Capacity Estimation for Routing Path Selection in Wireless Mesh Networks," to be submitted to IEEE Transactions on Instrumentation & Measurement.

Paper II, Pages 43-73: Shanshan Bi, and Maciej Zawodniok, "PDF-based Tuning of Stochastic Optimal Controller Design For Cyber-physical Systems with Uncertain De lay Dynamics," , IET Cyber-Physical Systems: Theory & Applications, Vol. 2, Issue 1, 2017, pp: 1-9.

Paper III, Pages 74-93: Shanshan Bi, and Maciej Zawodniok, "A Novel Cyber Network Fault Diagnosis Scheme for Cyber-Physical Systems," The 10th IEEE International Conference on Cyber, Physical and Social Computing.

Paper IV, Pages 94-121: Shanshan Bi, and Maciej Zawodniok, "A Novel Cyber Fault Prognosis and Resilience Control for Cyber-Physical Systems," Under Review, ACM Transactions on Cyber-Physical System.

Paper V, Pages 122-152: Shanshan Bi, and Maciej Zawodniok, "One-class SVM-based Cyber Network Fault Prognostics in Cyber-physical Systems," to be submitted to Advanced Engineering Informatics.

ABSTRACT

In this dissertation, several novel cyber fault diagnosis and prognosis and defense methodologies for cyber-physical systems have been proposed. First, a novel routing scheme for wireless mesh network is proposed. An effective capacity estimation for P2P and E2E path is designed to guarantee the vital transmission safety. This scheme can ensure a high quality of service (QoS) under imperfect network condition, even cyber attacks. Then, the imperfection, uncertainties, and dynamics in the cyberspace are considered both in system model and controller design. A PDF identifier is proposed to capture the time-varying delays and its distribution. With the modification of traditional stochastic optimal control using PDF of delays, the assumption of full knowledge of network imperfection in priori is relaxed. This proposed controller is considered a novel resilience control strategy for cyber fault diagnosis and prognosis. After that, we turn to the development of a general framework for cyber fault diagnosis and prognosis schemes for CPSs wherein the cyberspace performance affect the physical system and vice versa. A novel cyber fault diagnosis scheme is proposed. It is capable of detecting cyber fault by monitoring the probability of delays. Also, the isolation of cyber and physical system fault is achieved with cooperating with the traditional observer based physical system fault detection. Next, a novel cyber fault prognosis scheme, which can detect and estimate cyber fault and its negative effects on system performance ahead of time, is proposed. Moreover, soft and hard cyber faults are isolated depending on whether potential threats on system stability is predicted. Finally, one-class SVM is employed to classify healthy and erroneous delays. Then, another cyber fault prognosis based on OCSVM is proposed.

ACKNOWLEDGMENTS

Foremost, I would like to express my sincere gratitude to my advisor Prof. Maciej Zawodniok for the continuous support of my Ph.D. study and research, for his patience, motivation, enthusiasm, and immense knowledge. His guidance helped me in all the time of research and writing of this thesis. I could not have imagined having a better advisor and mentor for my study.

I would also like to thank Prof. Jagannathan Sarangapani, Prof. Egemen K. Cetinkaya, Prof. Jie Huang, and Prof. Zhaozheng Yin, for serving on my doctoral committee. In addition, I would like to thank the National Science Foundation (NSF) and Intelligent System Center (ISC) for providing financial support through my Ph.D. study.

Further, I am greatly thankful to my parents, Jianquan Bi, Chunmei Li, my husband Tianchen Wang, and my son Barron Wang for enlightening me my life. I would like to thank Dr. Hao Xu, who gave me many helpful discussions and suggestions concerning my work. I would like to thank my colleagues and labmates in Missouri S&T Embeded System and RFID Lab: Lei Wang, Arul Mathi Maran Chandran, Nathan Price, and Xiang Gao, for the stimulating discussions, for the sleepless nights we were working together before deadlines, and for all the fun we have had in the past.

Finally, I would like thank the staff of ECE department for their continuous assistance and also would like to thank the staff of Curtis Laws Wilson Library for providing me with the necessary literature.

TABLE OF CONTENTS

Page

LIST OF ILLUSTRATIONS

LIST OF TABLES

SECTION

1. INTRODUCTION

1.1. OVERVIEW

In the past a few decades, the term cyber-physical systems (CPSs) refers to a new generation of systems with integrated computational and physical capabilities that can interact with humans through many new modalities (Fig.1.1). Successful applications of CPSs are found in areas as diverse as vehicle industry (CAN-based data communication Johansson *et al.* (2005)), teleoperation Arcara and Melchiorri (2002), power system Wang *et al.* (2012) Sridhar *et al.* (2012), transportation systems Liu *et al.* (2011), manufacturing Lee *et al.* (2015) and high-confidence health-care system Haque *et al.* (2014). Smart industry, smart city, even smart world are made possible by the broad dissemination of mobile devices with substantial computation resources(e.g., processing and storage capacity), a variety of sensors (e.g., cameras, GPS, speakers, microphone and light and proximity sensors), and multiple communication mechanisms (e.g. cellular, Wi-Fi Bluetooth) allowing interconnection to the Internet as well as to other devices Rawat *et al.* (2015).

Embedded computers and networks monitor and control the physical processes, usually with feedback loops where physical processes affect computations and vice versa. Such a complex interconnection of a physical system, communication network, and computational component brings challenges on modeling, control, computation and security. Especially, the embedded cyberspace imposes restrictions on the exchange of information, such a limited channel capacity, traffic congestions, and malicious cyber attacks. Such network imperfections can degrade not only the communication performance, but also the performance of control systems and they can even destabilize the system. For example,

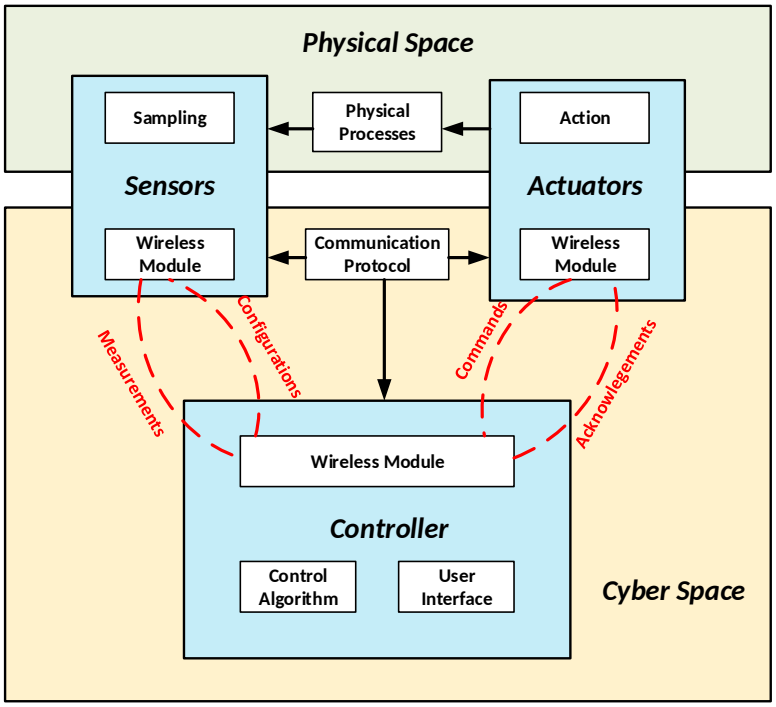


Figure 1.1. Cyber-physical system structure

self-driving cars have a large number of radars, cameras, and other various electrical components (known as electronic control units, or ECUs) connected via an internal network. If hackers manage to gain access to a vulnerable, peripheral ECU (the Bluetooth or infotainment system) from there they may be able to take control of safety critical ECUs like its brakes or engine and wreak havoc. Therefore, reliability of CPSs -particularly resilience, safety, and security - is a more complex issue than ever before.

Over the years, computer science researches have pioneered the development of new real-time computing techniques, visualization methods, embedded systems architectures, and innovative approaches to ensure computer system reliability, cyber security and fault tolerance. At the same time, systems and control researchers have made major breakthroughs in powerful engineering methods and tools to improve the resilience and reliability for industrial processes, such as system identification, filtering, prediction, optimization, robust control, stochastic control, and fault diagnosis and prognosis schemes. With respect to the

above works, cyber-physical systems research should integrate knowledge and engineering principles across the computational and engineering disciplines (network, control, software, human interaction, learning theory) to develop new CPS science and supporting technology. A high resilience CPS requires the following capabilities:

a) Detection abnormalities in the cyberspace and protection of information and network performance.

b) Detection of physical system abnormalities and protection of CPS stability.

c) Protection of system performance under cyber abnormalities.

The overall goals of the first capability (a)) include integrity (the trustworthiness of data or resources), availability (accessibility upon demand), and confidentiality (keeping information secret from unauthorized users). Many researchers addressed these issues with different technologies, such as authentication schemes, access control, and other defense scheme Pasqualetti *et al.* (2013)-Cardenas *et al.* (2008). An assumption that the adversary/attack model is fully known is often required; however, it is challenging to get. Gamage *et al.* (2010) proposed a general theory of event compensation as an information flow security enforcement mechanism for CPSs. Message scheduling methods were given to improve the security quality of wireless networks for mission-critical CPSs in Jiang *et al.* (2010). In Amin *et al.* (2009), deception and denial of service attacks had been addressed by a countermeasure based on semi-definite programming. False data injection attacks against static state estimator are studied in Liu *et al.* (2011). In a similar fashion, stealthy deception attacks against the Supervisory Control (SC) and Data Acquisition system (DAS), replay attacks, and covert attacks against control systems were investigated in Teixeira *et al.* (2010), Mo and Sinopoli (2009), and Smith (2011) respectively. With respect to the above works, Pasqualetti *et al.* (2013) proposed a mathematical framework for CPSs, attacks, and monitors, and given the fundamental limitations of monitors from system-theoretic and graph-theoretic perspectives. Finally, centralized and distributed attack detection and identification monitors were designed. Overall, the cyber attacks can be addressed on the

cyber side. However, the defense of cyber attack is still open for the further research, such as optimizing the limited channel resource for transmissions, maximizing path capacity to improve the quality of service (QoS), and so on. In addition, the effects of cyber attacks/faults on the physical system behavior are oversimplified in above existing works. Moreover, the injection time and model of the attacks/faults are difficult to learn ahead of time in practical CPSs.

Then, the second requirement (b)) has been studied by many control researchers. They focused on the conventional fault detection techniques that have successfully applied to industrial networked control systems (NCSs). They indeed took the network delay and packet loss into consideration in various ways. In Liu and Yao (2005), network delays were modeled as a constant delay (time buffer), an independent random delay, and a delay with known probability distribution governed by the Markov chain model. In Liu *et al.* (2007a), a networked predictive controller in the presence of random delay in both forward and feedback channels was proposed to minimized the effects of network failures. A robust H_∞ control for a nonlinear T-S fuzzy model system was proposed to address the network delays and packet drop in Zhang *et al.* (2007). Wang *et al.* (2008) and Zhang-qing and Xian-zhong (2007) employed a state observer-based fault detection method on the uncertain long time delay. Although, the network delays and packet drop caused by network faults/failures were considered in above works, the assumptions, such as known bounds and time invariant distribution of delays and packet loss, are always made. In addition, most of the above works aimed to detect the faults of physical components (sensors, actuators, and system plant), not the faults in the cyberspace.

However, how to meet the third requirement (c)) is still open for the further research. First of all, a full knowledge of the relation between cyber condition and system performance is crucial. That need a general model which fully present both physical system dynamics and cyberspace uncertainties. Then, the fault detection should be redesigned both on cyber and physical system side. Moreover, the isolation of cyber and physical system abnormalities is

essential. Therefore, only one observer for monitoring system states is not sufficient. Other observers for monitoring cyber condition should be proposed. At last, resilience control design should fully consider the cyber dynamics to tolerant both cyber and physical system faults/attacks.

To conclude, CPSs with an interaction of various subsystems and networks do not allow decoupling design either for system control strategy or for network security protection. Fault diagnosis and tolerant control for CPSs should be also redesigned with fully considering both cyber and physical system faults. Such a comprehensive fault detection and defense framework, which is lacking in the existing literature to the best of our knowledge, is the main objective of this dissertation.

1.2. ORGANIZATION OF THE DISSERTATION

In this dissertation, several cyber fault diagnosis and prognosis schemes and the corresponding defense schemes have been proposed. This dissertation is presented in five papers, and their relationship to the one another is illustrated in Fig. 1.2. The schemes in these five papers can be widely used to detect and defense cyber faults/attacks in CPSs.

In the first paper, the objective is to transmit packages using the path with the highest capacity. A capacity estimation based routing scheme is proposed for wireless mesh network. When a cyber attack/fault occurs, the proposed scheme can re-route the transmission based on the effective capacity estimation for each path to avoid packet losses and QoS degradation. The model of entire network is derived with considering interactions among links and paths, stochastic channel fading and noise. This scheme can be also applied in mobile network since the effective capacity is estimated in an online manner.

Next, the uncertainties in cyberspace are addressed in the second paper. We proposed a novel controller, named PDF-based tuning of stochastic optimal controller, which can manage the unknown dynamics in the embedded cyberspace, such as long time delays and packet losses. When cyber attacks occur, the proposed can be used as a resilience controller.

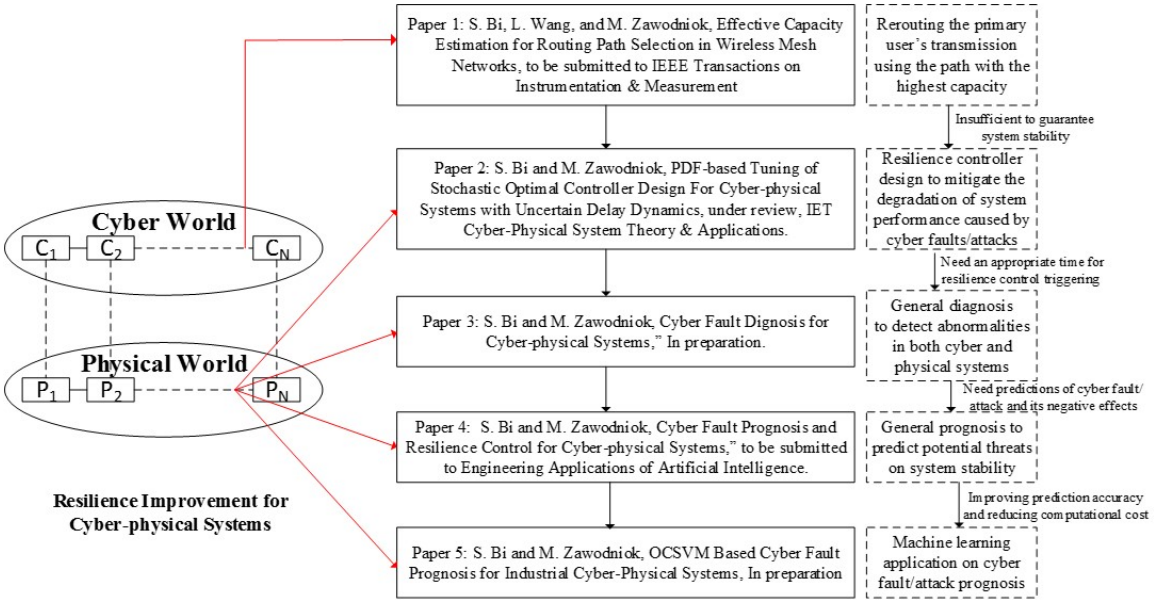


Figure 1.2. Dissertation outline

In the third paper, we proposed a novel cyber fault diagnosis scheme. Cyber fault/attack can be captured by monitoring PDF profile of network delays. Combining with the physical states observer proposed in existing works, cyber and physical system faults can be isolated. Such that the appropriate resilience control for cyber or physical fault mitigation can be accurately triggered. The controller proposed in the second paper is consider the resilience controller for cyber fault tolerance.

Subsequently, in the fourth paper, the proposed cyber diagnosis scheme in the third paper is improved to optimizing the computational cost and cyber detection accuracy. We proposed a novel cyber fault prognosis scheme to predict potential threats on CPS performance and stability. A cyber fault isolation scheme is designed to classify soft and hard cyber faults using system state prediction. For hard faults which potentially degrade CPS performance, the proposed prognosis scheme can predict them and take appropriate control action ahead of time before the system failure happening. Such that the resilience control can be effectively triggered when necessary. Moreover, the computational cost is significantly reduced.

Finally, in the last paper, we proposed another cyber fault prognosis scheme which applied one class kernel based support vector machine (OCSVM) to detect cyber faults/attacks. OCSVM can accurately separate healthy and erroneous delays. The classification results can be used to isolate soft and hard cyber faults. Moreover, the proposed scheme significantly reduce the unnecessary resilience control triggering.

1.3. CONTRIBUTIONS OF THE DISSERTATION

This dissertation provides contributions to the area of cyber fault detection and defense methodologies for CPSs. As a consequence, proposed designs can not only render reliable cyber abnormalities detection in terms of isolation but also maintain the CPS stability in the mean in the presence of unknown cyber dynamics, imperfections, and attacks. Traditionally, the fault diagnosis and prognosis in the existing works oversimplify network dynamics and its effects on system behavior. The proposed schemes, on the other hand, fully consider above dynamics and modify the defense techniques to adapt to above uncertainties. Overall, the proposed effort overcomes the mentioned deficiencies.

The main contributions of Paper I include: a) the matrix model with fully considering stochastic channel fading, interaction among links or paths are derived; b) an effective capacity estimation based on RBF neural network is proposed; c) routing schemes for peer-to-peer and end-to-end communication are proposed respectively. Overall, with full knowledge of achievable capacity for each path, the vital messages can be forwarded safely and effectively.

The main contribution of the second paper is a novel stochastic optimal controller is designed with fully considering uncertainties and dynamics. The PDF of delays is used to tune controller parameters. Such that the controller can adapt to the delays and its distribution variation. For the case of linear CPS, uniformly ultimately bounded (UUB) stability is demonstrated by using Lyapunov analysis. In addition, the proposed controller can be used as the resilience control in the reset papers.

The contributions of Paper III include the cyber fault diagnosis using PDF monitoring of delays and cyber and physical system fault isolation. Kernel density estimation is used in an online manner to update the probability of delays.

The contributions of the fourth paper include: a) a novel cyber prognosis scheme is proposed; b) a time series analysis based distribution estimation is derived to predict the future delay distribution; c) system state prediction is proposed based on the above distribution estimation. Such that soft and hard cyber fault can be accurately separated. Moreover, the convergence of this prediction is presented.

Finally, for the last paper, the main contribution is that OCSVM is designed and applied to detect cyber faults/attacks. Then a multi-class classification machine is proposed based on OCSVM. Such delay classification finally provide the health, soft fault, and hard fault range for future cyber fault isolation. The computational cost for fault prognosis is significantly reduced.

PAPER

I. EFFECTIVE CAPACITY ESTIMATION FOR ROUTING PATH SELECTION IN WIRELESS MESH NETWORKS

Shanshan Bi, Maciej Zawodniok

Department of Electrical & Computer Engineering

Missouri University of Science and Technology

Rolla, Missouri 65409–0050

Tel: 573–341–6622, Fax: 573–341–4115

Email: sbn65@mst.edu

ABSTRACT

Cyber physical system (CPS) is playing an important role in the smart industry, which connects diverse systems leading to an inter-networked system of systems spanning wide geographic areas. Wireless ad-hoc network (WANET) and mobile ad-hoc network (MANET) are reliable and suitable candidates which can take an enormous amount of communications in CPSs without requiring extra infrastructures. Moreover, each node/device such as cellphone, and laptop, in WANET/MANET can participate in routing by forwarding data for other nodes/device. The existing communication routing schemes are designed to improve the performance of network without considering the interference, data collision and cyber attacks issues. This negligence likely leads to the unexpected degradation of network performance and more power consumption. Therefore, a full knowledge on interaction among communicating links is necessary for improving the quality of communications in CPSs. In this paper, a novel signal-to-interference-and-noise ratio (SINR) model is

proposed, which includes explicit interaction among adjacent links within the entire network. A novel RBF neural network prediction based capacity estimator is proposed to do routing selection. The simulation results show that the path with the maximum available capacity/SINR is selected accurately and the reliability of transmission is improved.

Keywords: cyber physical system, capacity estimation, routing scheme, RBF neural network

1. INTRODUCTION

In the past several decades, cyber physical systems (CPSs) has attracted a great deal of attention because they are likely to emerge through such network environments to connect both humans and machines Lien *et al.* (2012)-Qu *et al.* (2010). However, it is difficult to establish adequate network infrastructures anywhere and anytime Kawamoto *et al.* (2013). Therefore, how to select an effective network to take an enormous amount of communications with a high quality is a big challenge for composing CPSs. Wireless ad-hoc network (WANET) and mobile ad-hoc network (MANET) based CPSs are flexible and reliable because all nodes in CPS participate in routing by forwarding data for other nodes. Such a WANET/MANET based CPS utilizes existing infrastructures and mobile devices to do transmissions, such as laptops, cellphones, vehicles, and other networked devices, instead of requiring extra infrastructures.

A challenge of WANET/MANET based CPSs is how to defense the interference and channel fading induced by a large number of communications so that the critical messages can be delivered with a high quality. This issue can be addressed by applying an optimized transmission routing scheme. Typical routing schemes in WANET/MANETs, e.g. gradient-based routing (GBR), and energy-aware routing (EAR) Al-Karaki and Kamal (2004), select paths for an ideal case without any uncertainties. However, once a new routing path carries traffic, it interacts and interferes with links in the entire network. This often results in

a degraded performance during the routing path setup. Therefore, it is crucial that both individual the link's and the entire path's performance must be determined and estimated before selecting the path.

A transmission between the source and destination nodes has several alternative paths. Each path consists of multiple links. Before transmitting the message, the source node broadcasts a "Hello" message to find who can be the next relay of it so that the message can be delivered safely and efficiently. Therefore, the performance of each possible path or link should be evaluated accurately before the principal message sending out. Capacity is a principal metrics for evaluating the performance of path or link. Therefore, the achievable capacities of each alternative path or link should be known for the most optimal route searching. The existing approaches Chen and Gerla (1998), Royer and Toh (1999), Shah and Rabaey (2002) dealt with this challenge by posing assumptions: (a) knowing the information (e.g., the achievable channel capacity and fading model parameter a priori), (b) knowing the static (non-dynamic) network features, or (c) ignoring certain interactions, including the explicit interlink interference in the routing schemes. However, in practical network, the channel fading is stochastic and time-varying as well as the locations of nodes or relays. The effectively achievable capacity is unknown, and it varies over time. Consequently, the selected route is suboptimal due to these uncertainties. The primary challenge in estimating the effective capacity is that the interactions among adjacent links are complex and nonlinear. In addition, a full channel state between each pair of transmitter and receiver is unknown and challenging to measure. Therefore, the capacity estimation is not trivial for even a single link. The complexity of the estimation increases further when we consider the establishment of a new, multi-hop path.

In this paper, a novel routing scheme is proposed for WANET/MANET based CPSs, which guarantees the highest quality of communications with the lowest power consumption. With considering interactions and interference among different path or link, we also consider a stochastic channel fading. Meanwhile, the real time estimates of capacity

and power are updated as the dynamic changes of topology /node location. For the prediction of capacity and power, a RBF neural network predictor is designed, which is trained by a few training data taken from "Hello" message. The training data is provided by the signal-to-interference-and-noise ratio (SINR) model, which includes explicit interaction among adjacent links within the entire network, so that the training process takes uncertainties of channel into account. With a full knowledge of available maximum capacity, the vital message can be forwarded safely and effectively.

The following part is organized into five sections. Section 2 summarized the related works on capacity estimation. An example is presented to indicate our motivation in Section 3. The proposed routing scheme is illustrated in Section 4. The evaluation of the proposed scheme by simulations is presented in Section 5. Section 6 gives some conclusions.

2. RELATED WORKS ON CAPACITY ESTIMATION

Many researchers have studied both the network capacity and the techniques used to maximize the capacity of path Asgeirsson and Mitra (2011); Chen *et al.* (2009); Gao *et al.* (2006); Gastpar and Vetterli (2002); Gupta and Kumar (2000); Li *et al.* (2011); Li (2009); Liang and Guo (2006); Wang and Wu (2009); Xue *et al.* (2005). Most of these works on capacity analysis were focused on average performance in single-hop (P2P) networks. Multi-hop routing (end-to-end) cases however, were not completely understood. Gupta and Kumar (2000) collected landmark results for a P2P case that revealed the throughput attainable by each of the n randomly located nodes is under a noninterference protocol. This protocol is capable of transmitting W bits per second to a randomly chosen destination. This destination is of the order of $(W/\sqrt{n\log n})$ bits per second. Gao *et al.* (2006) discussed the channel capacity of networks with different sizes. Few studies, however, have been focused on end-to-end capacity throughput.

A number of studies have comprehensively addressed how to maximize capacity. Gupta and Kumar (2000) discussed the interaction of 802.11 MAC with ad-hoc forwarding and its affects on the network's channel capacity. They concluded that the average distance between the source and the destination nodes must remain small as the network grows to ensure an adequate and available total capacity in a larger network. Xue *et al.* (2005) studied the effects of different types of fading on capacity throughput. They made several assumptions. For example, the assumed that the channel fading type is known. They also assumed that the fading is time invariant. Measuring such information in real communication networks, however, is challenging. Other researchers Gastpar and Vetterli (2002); Li *et al.* (2011); Li (2009) examined the throughput capacity in random networks, the transport capacity in arbitrary networks. They sought to scale the network with antennas under the known boundary conditions of capacity. They did not, however, predict the actual, achievable capacity once the new traffic was introduced.

Several researchers have attempted to use either optimization techniques Liang and Guo (2006), power allocation schemes Wang and Wu (2009), or game theory Asgeirsson and Mitra (2011) to maximize link and network capacities. Liang and Guo (2006) proposed an energy-efficient online algorithm to maximize the network capacity for online disjoint path connections and online multi-casting. They indicated that the network's capacity is proportional to its lifetime. Therefore, the proposed algorithm seeks to prolong the lifetime and reduce the transmission energy consumption, so that the network's capacity can be maximized. Asgeirsson and Mitra (2011) applied a low-regret algorithm to reformulate the capacity maximization problem into a power assignment domain. Overall, these schemes maximizes capacity without understanding either the maximum achievable capacity or the corresponding power requirements.

In general, most of the work previously conducted was completed in an attempt to maximize performance and capacity without understanding what the maximum is for the particular network topology and traffic patterns. The routing decisions will often be suboptimal when the maximum capacity along the route is unknown. Hence, the goal is to predict capacity before the routing decision is made.

Jagannathan *et al.* (2006) based the power controls on a known, desired signal to interference ratio (SIR). Determining such desired desired and achievable SIR values in an ad-hoc wireless network without information on the network's non-preexisting infrastructure and dynamic topology, however, is difficult. The capacity-based performance cannot be evaluated either without an optimal SIR. Hence, either the desired SIR or the capacity should be reevaluated based on the existing information and data for the power control issue.

3. MOTIVATION

The traditional routing schemes focus on optimizing the networks performance for its current known state. This state includes channel capacities, topology, available energy, service demand, and performance metrics. However, these schemes often ignore both the interference and the interactions among the adjacent links. Interference is particularly important for multi-path routing because it aggravates the issue of a bottleneck link, which determines the entire path's performance, illustrated in Fig. 1. Interference among the links may also cause increased interference from strong links to the bottlenecks, thus further weakening each link's performance. Therefore, the maximum capacity of the entire path should be obtained when all the links maintain the same capacity. No single bottleneck link exists in such an ideal situation. The mutual interference is also reduced, thereby improving both the average signal-to-interference-noise ratio (SINR) and the overall throughput.

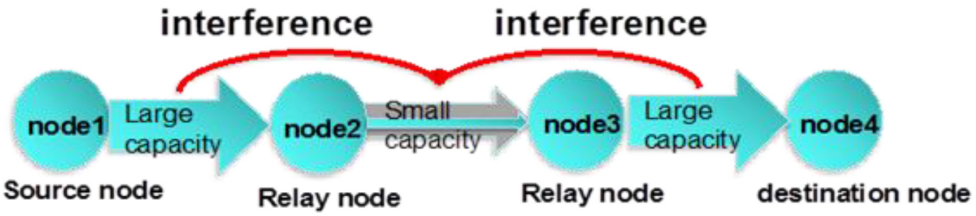


Figure 1. Bottleneck link with interfered by other links

This example illustrates how the interference affect the maximum capacity of path. Nash equilibrium control designed by Gastpar and Vetterli (2002) is applied to guarantee consistency of each link's capacity.

The simulated network topology is shown in Fig. 2. Four nodes establish six links. These links opportunistically set their target performance in terms of SINR. In the first scenario, we studied the maximum capacity achievable on link 1 while the remaining links maintained their desired performance. In second scenario, we studied the performance of an entire routing path, from the source node 1 to the destination node 3. The results included a comparison between the maximum path capacities.

The topology with four nodes and six links was considered the distance relation. It was satisfied as $d_{12} = d_{23} = d_{34} = d_{43} = d_{32} = d_{21} = d$

We examined the relationship between the power and the capacity for the single link case first. The knowledge of this relationship could make one link achieve the capacity as high as possible. The maximum capacity of link 1 (between nodes 1 and 2) was evaluated. The transmission power p_i, was controlled by Nash equilibrium power control. It was allowed to vary between $0dBm(1mW)$ and $5dBm(3.1623mW)$. The SINR of link 1 was iteratively increased by $\beta = 0.1$ ratio. The power control scheme was allowed to converge for 1 second, between SINR increases. The initial target SINR for all links was set to $\gamma_i^{tar}(0) = -7dB$. The power was set to $p_i(0) = 0mW(0dBm)$.

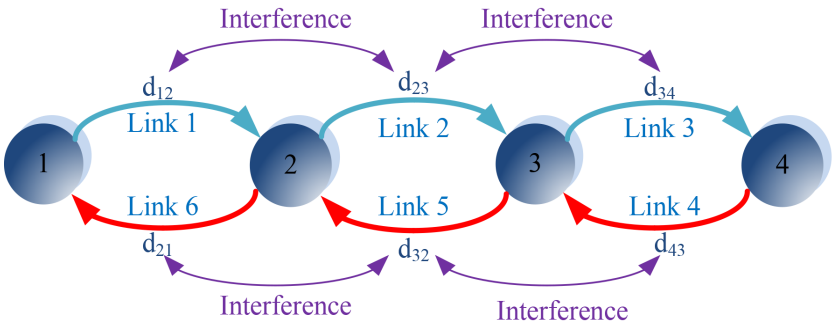


Figure 2. Diagram of the simulated network model

The maximum capacity value for an entire path, between source node 1 and destination node 3, was evaluated next. The SINRs of link 1 and link 2 were iteratively increased by $\beta = 0.1$ in multiple link case. The remaining initial conditions were the same as those in the single link case.

The capacity variation with the transmission power for the two cases (single and multi-hop) is illustrated in Fig. 3. The maximum capacity points for the single link and the multi-hop path cases were ($3.135mW$, $20.24Mbps$) and ($1.079mW$, $15.34Mbps$) respectively. Note that, in this simulation, we have allowed to saturate transmission power into $0dbm$ to $5dbm$. This saturation led to the actual SINR not reaching the target value. Hence, the capacity was reduced if the power increased beyond the maximum point. Overall, the capacity decreased by 6.57% and 21.58% for the single link and multi-hop path cases respectively, because the power was saturated at the upper bound of the power limitation ($3.1623mW$) and without feasibility to achieve the capacity targets. Consequently, the increased interference led to not only congestion but also a reduction in the capacity.

The maximum capacity for a single link was 24.21% larger than it was for a multi-hop scenario because increasing the entire path's targets required that all links be included to increase target SINR. This situation led to a power race among neighboring nodes. The resulting increase in interference was higher here than it was in the single link case, thus reaching the maximum transmission power for a lower SINR.

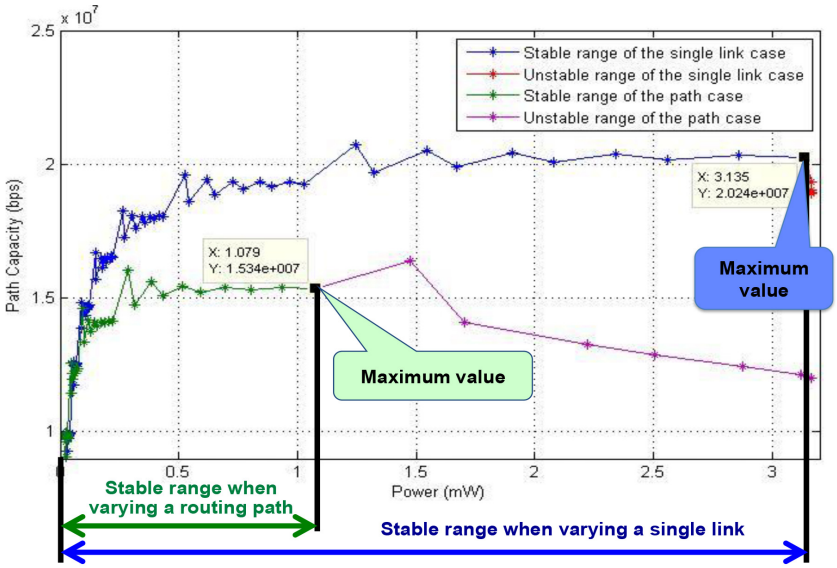


Figure 3. Comparison of maximum capacity for both scenarios

According to this example, the topology (e.g., the density of nodes' distribution, operating states of each node, and the routing decision) determined the maximum achievable link capacity. A routing decision should take into account not only the initial state (in which both links appear to be the same) but also the actual available capacity on the link. Otherwise, the selected path might underperform.

Overall, the maximum SINR (capacity) is a function of the topology, including density of the nodes and the path selection, the path loss gain (G), and the target SINR of other links representing the operating states of nodes.

$$SINR_{Max-Tar}(i) = f\big(G, [SINR_{Tar}(1), \ldots, SINR_{Tar}(i-1), SINR_{Tar}(i+1), .., SINR_{Tar}(M)]\big) \quad (1)$$

The dependency is not linear. Moreover, it is necessary to properly estimate available capacities, particularly for multi-hop routing paths. The insight gained can be used as part of a future routing scheme development to completely evaluate trade-offs among alternative routing paths.

4. CAPACITY ESTIMATION BASED ROUTING SCHEME

Dynamic routing is essential for communication in WANET/MANET based CPSs due to the uncertainties and dynamics of locations of nodes, diverse devices participation and interference from environment. Centralized routing and distributed routing schemes are critical methods to realize dynamic routing in modern communication network. Distributed routing typically allow nodes to make decisions locally. Each node gathers all needed information, and bases routing decisions on this information. Centralized routing algorithms provide a clean interface for policy specification. Global network state, including topology, is obtained from network nodes and maintained at a centralized controller Al-Karaki and Kamal (2004).

Inspiring by the above motivation, our goal is proposing a routing scheme which can applied to both distributed and centralized dynamic routing in WANET/MANET CPSs.

In next part, the primary steps of the proposed scheme are illustrated. The first subsection shows how to model the simulated network with consideration of interference among links/paths, noises from environment, and stochastic channel fading. The following assumptions on the simulated network are needed:

a) All transmissions in subnetwork are unidirectional. Although some bidirectional propagations have been set, the target transmission is unidirectional.

b) Rayleigh channel fading is applied over time. Therefore, the gain matrix of path loss is dynamical and time-varying.

c) The noise caused by environment factor is considered as a Gaussian white noise that is multiplied by path loss gain matrix.

d) Only a subnetwork in a large scale network is considered. The remaining nodes, which doesn't participate the target transmission in the subnetwork, are conducting stable transmissions all the time. The interference caused by those transmissions are included into the noise in c).

Next, RBF neural network is designed to do capacity estimation which is a principal guidance of route selection. At last, we separately illustrate how the proposed routing scheme deals with the best path selection for both distributed and centralized routing scenarios.

4.1. Modeling of Routing Path

We first introduce a traditional network-wide model of the radio links performance in terms of signal-to-interference-and-noise ratio (SINR). The equation is rewritten with a matrix form to calculate the required transmission power for each link when a desired SINR is given for all links. This model will be used for generating the training data in routing scheme design.

Certain assumptions are given here to simplify modeling and describe the network situation that is the focus of this study.

a) The network model is a non-time varying model with stable link gains and knowledge of the radio channel state.

b) We assume that the data transmissions are bidirectional when modeling an entire network. If we set a network with either N nodes or hops, then $M = 2(N - 1)$ links will be available for communication.

The traditional approach to describing the dynamics of a wireless channel in terms of per-link channel capacity and power usage considers a signal-to-interference-and-noise ratio (SINR) on the particular i^{th} link Chang *et al.* (2001); Chang and Yang (1997); Leung *et al.* (2002); Pindoriya *et al.* (2008); Yun *et al.* (2008):

$$r_i(t) = \frac{g_{ii}(t)p_i(t)}{\sum_{j=i}[g_{ij}(t)p_j(t)] + \eta_i(t)} \tag{2}$$

where $g_{ij}(t)$ is a attenuation from transmitter of j^{th} link to receiver of the i^{th} link, $p_i(t)$ is transmission power on i^{th} link, and$_i(t)$ is the channel noise on the i^{th} link. In order to represent the SINR equations for an entire network as matrix equation, we need to transform 2 into following form:

$$[\sum_{j \neq i}[g_{ij}(t)p_j(t)] + \eta_i(t)]r_i(t) = g_{ii}(t)p_i(t) \tag{3}$$

Now, we can represent the SINR for entire network as:

$$R[(G - G_L)P_T + H] = G_L P_T \tag{4}$$

where $R = det(r_i(t))$ is a diagonal matrix with SINR values for all links, $G = [g_{ij}]_{M*M}$ is the channel gain matrix among all M links (from j^{th} link transmitter to i^{th} link receiver), $G_L = [g_{ii}]$ is a matrix of gains on all the active links, $P_T = [p_i]_{M*1}$ is transmission power vector for all M links, and $H = [\eta_i(t)]_{M*1}$ is vector of noise values for each link.

From network control perspective, it is more interesting to determine the necessary transmission powers to achieved a desired, target SINR values one each link. In such a case, we solve (3) for P_T vector:

$$[G_L(I - R) - GR]P_T = RH \tag{5}$$

$$AP_T = RH \tag{6}$$

where R_d is diagonal matrix with the desired, target SINR values for all M links, and matrix $A = [G_L(I - R) - GR]$ determines the existence and uniqueness of the solution. Assuming that the inverse of A exists, the required transmission power is equal to:

$$P_T = A^{-1}RH \tag{7}$$

To understand the relation between the SINR variation and power variation, the following formulation is derived by taking first partial differential of (4). ∂R (∂P) can be considered as ΔR (ΔP). Then, series of partial differential equations are rewritten in a matrix formulation as (8).

$$\Delta R = ((G - G_L) * diag(P))^{-1}(G_L \Delta P - ((G - G_L)\Delta P. * R) \tag{8}$$

where ΔR is SINR variation with power variation ΔP . The goal of RBF network is to estimate such function for a particular link.

Without loss of generality, Rayleigh channel fading is considered here. Rayleigh model is commonly used in wireless communication system to describe the statistical time varying nature of the received envelope of a flat fading signal, or the envelope of an individual multi-path component. The Rayleigh distribution has a probability density function (PDF) as:

$$p(x) = \begin{cases} \frac{x}{\sigma^2} exp(-\frac{x^2}{\sigma^2}) & (0 \leq x \leq \infty) \\ 0 & (x < 0) \end{cases} \tag{9}$$

where x is a random variable, and σ^2 is the fading envelope of the Rayleigh distribution. The channel uncertainties distort the transmitted signals, therefore, the uncertain effect is represented via a channel loss gain Jagannathan *et al.* (2006) as:

$$g = f(d, n, x) = d^{-n} x^2 \tag{10}$$

where d^{-n} is the effect of path loss. n is path loss exponent, usually, $n = 2$ 8 in typical propagation. For Rayleigh fading, it is typical to model the power attenuation as x^2 , where x is a random variable with Rayleigh distribution. Typically the channel gain g is a function of time.

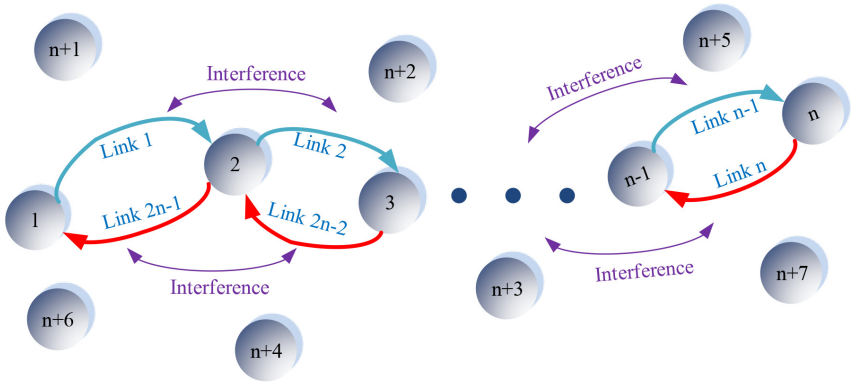


Figure 4. Interference along a multi-hop path

To study the interference among different links, we derived a matrix model for single path transmission first. Based on such a model, a multi path model is presented to describe the interactions among different paths.

Modeling for a Single Path

A signal path with N nodes is shown in Fig. 4. In more general case, there are $(N-1)$ bidirectional hops in a path. Hence, there are $M = 2N$ links with M transmitters. The corresponding transmit power vector P_T for (4) is defined as:

$$P_T = [p_{1*}, p_{2*}, .., p_{M*}]^T = [P_1, P_2, .., P_{N-1}, P_N, P_{N-1}, .., P_2] \tag{11}$$

where M is the total number of links in the path, N is the total number of nodes in the path.

In order to evaluate the performance along the multi-hop routing path, the multi-path model (8) is simulated, which is employed to abstain numerical results and not essential for the capacity analysis itself.

The distance between links i^* and j^* are corresponding to the distance from the transmitter of link i^* to the receiver of link j^*. Therefore, the distance matrix denoted by link index as:

$$D^{*}=\begin{bmatrix} d_{1,1^{*}} & d_{2,1^{*}} & \cdots & d_{(M-1),1^{*}} & d_{M,1^{*}} \\ d_{1,2^{*}} & d_{2,2^{*}} & \cdots & d_{(M-1),2^{*}} & d_{M,2^{*}} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ d_{1,(M-1)^{*}} & d_{2,(M-1)^{*}} & \cdots & d_{(M-1),(M-1)^{*}} & d_{M,(M-1)^{*}} \\ d_{1,M^{*}} & d_{2,M^{*}} & \cdots & d_{(M-1),M^{*}} & d_{M,M^{*}} \end{bmatrix}_{M*M} \tag{12}$$

where $d_{i,j}$ denotes the distance between link i^{*} and j^{*} (from the position of transmitter in $i^{*}th$ link to that of the receiver in $j^{*}th$ link). Combining with (10), the corresponding path loss gain matrix is equal to:

$$G = f(D^{*}, n, x) \tag{13}$$

where $f(.)$ denotes per-element operation to apply path loss model that is the Friis transmission equation.

Modeling of Multiple Paths

The presented model for a single path can be easily extended to support multiple paths by expanding the gain matrix to include all paths.

The gain matrix for multiple paths is:

$$G=\begin{bmatrix} G_{path_1} & G_{path_2,path_1} & \cdots & G_{path_n,path_1} & G_{cross,path_1} \\ G_{path_1,path_2} & G_{path_2} & \cdots & G_{path_n,path_2} & G_{cross,path_2} \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ G_{path_1,path_n} & G_{path_2,path_n} & \cdots & G_{path_n} & G_{cross,path_n} \\ G_{path_2,cross} & G_{path_2,cross} & \cdots & G_{path_n,cross} & G_{cross} \end{bmatrix} \tag{14}$$

where n denotes the number of paths. $G_{path_i,path_j}$ denotes the gain matrix between path i and j. $G_{cross,path_j}$ is the gain matrix between path the cross paths and path j.

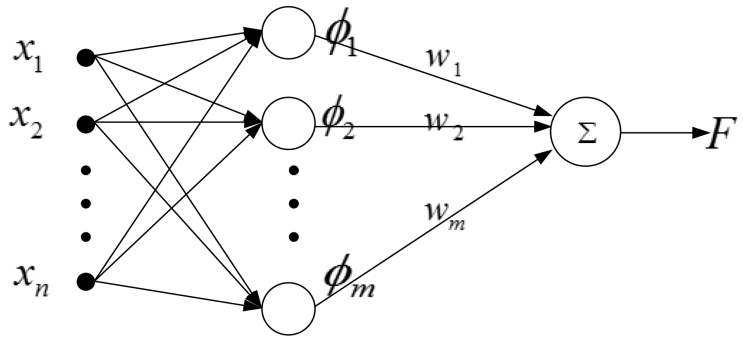


Figure 5. Schematic diagram of RBF neural network

Remark: This step of network modeling is not essential for proposing the routing scheme. The network model is only used to provide the data of SINR and power to train the RBF neural network and do maximum capacity prediction in next subsection. If the data can be taken from a real network, this step can be skipped.

4.2. RBF Based Capacity Estimation

The capacity estimation is hindered by many external and often unpredictable factors, including environmental noise, interference, measurement errors, and channel fading. These factors can be considered either an uncertainty or noise for a function estimator. Hence, the RBF neural network, which is robust in presence of uncertainties and noise, is employed for estimating the achievable capacity curve as a function of transmission power. The limited measured data and available information also make the RBF network more suitable than a traditional multi-layer neural network because it is easily and quickly trained.

RBF Network Design:

The RBF neural network typically consists of three layers: an input layer, a hidden layer, and an output layer. A radial activated function is adopted by each hidden layer node, and the output is computed by adding together the weighted hidden unit outputs. The structure of multi-input-single-output (MISO) RBF neural networks is depicted in Fig. 5.

Theoretically, RBF neural networks can approximate any nonlinear function and the feasibility of neural network to eliminate the effects of the non-target parameters on the target parameters. With this scheme, the parameters of hidden layer kernel functions and the output connection weights are adjusted simultaneously to minimize the output errors. The output is a linear combination of the activation functions computed by hidden layer weights.

The output of the j^{th} hidden neuron can be written as

$$h_j(x_i) = e^{-\frac{\|x_i - c_j\|^2}{2{\sigma_j}^2}}, \begin{cases} i = 1, 2, \ldots, n \\ j = 1, 2, \ldots, n \end{cases} \tag{15}$$

where h_j is the output of the j^{th} neuron, $x_i \in R^n$ is the input vector, c_j is the kernel centers selection using random vector, and σ_j is the center spread parameter.

Gaussian transfer function is used for the hidden neurons. The neurons of the output layer have a linear transfer function. It is the weighted summation of the outputs of all hidden neurons connected to that output neuron. Then, the output $F(x_i)$ can be obtained by

$$F(x_i) = \sum_{j=1}^{m} W_{kj} h_j \tag{16}$$

where W_{kj} is the synaptic weight connecting hidden neuron j to output neuron k and m is the number of the hidden layer neurons.

When the maximum capacity according to (8) needs to be calculated, the path loss gain matrix G should be known.

For capacity/SINR estimation, we assume the topology information of WANET are known. The channel fading and other channel dynamics and uncertainties are considered, and the main factors for estimation are the density of nodes and path selection, path loss gain G, and target SINR of other links.

We employ a RBF neural network to estimate function relating the used transmission power with the resulting (achievable) capacity. The input is power of the target link since any power changes in the network will interfere the capacity of the target link. The output is the capacity. RBF network is trained offline first and then updated online. It has to process a sufficient number of diverse datasets to converge to the estimated function in offline training process. The online prediction is ready to analyze the relation of achievable SINR (capacity) versus transmission power.

From (1) , it is clear that capacity of one link depends on all powers, not only the power of itself. Hence, we first assume the capacity of the target link C_i is a nonlinear function of power of each link as (17).

$$C_i = f(p_1, p_2, ..., p_m,) \tag{17}$$

The function f will be estimated by RBF neural network. From (15), we define the input is power vector $x = [p_1, p_2, ..., p_m]^T$ (m is number of links), and the output is $SINR_i$ (i is the target link). From (16) , the estimated capacity is

$$\widehat{C_i} = \sum_{i=1}^{m} \widehat{W_{ki}} exp\big(- \frac{\|p_i - c_j\|}{2\sigma_i^2}\big) \tag{18}$$

Then, the weights w_{kj} can be updated by

$$\widehat{w}_{ki}(k+1) = \widehat{w}_{ki}(k) + \alpha(C_i(k) - \widehat{C_i}(k))\phi(k) \tag{19}$$

When the weights converge, the future capacities versus power can be analyzed to identify the desired operating points - the most energy efficient setting or the highest achievable capacity - and the corresponding power values.

Theorem: With trained by a sufficient number of measured data, the RBF neural network using the weight update law (19) to estimate the relationship between the transmission power and the actual achievable capacity. The persistent excitation condition Gorinevsky (1995) is satisfied Jagannathan *et al.* (2006).

Proof of weights convergence:

We denote $\tilde{w}(k) = w - \hat{w}(k)$, then the estimation error can be defined as $e(k) = C_i(k) - \hat{C}_i(k) = \tilde{w}(k)\phi(k)$. $\phi(k)$ is the output vector from neurons.

According to PE condition, (20) can be obtained.

$$1 - \alpha\|\phi(k)\|^2 \geq 0 \tag{20}$$

We select the Lyapunov function candidate as

$$L = \tilde{w}^T(k)\tilde{w}(k) \tag{21}$$

Substitute the update law (19) into Lyapunov function candidate, we have (22).

$$\begin{aligned}
\Delta L &= \tilde{w}^T(k+1)\tilde{w}(k+1) - \tilde{w}^T(k)\tilde{w}(k) \\
&= (w^T - \tilde{w}^T(k+1))(w - \tilde{w}(k+1)) - \tilde{w}^T(k)\tilde{w}(k) \\
&= (\tilde{w}^T(k) - \alpha\phi^T(k)e^T(k))(\tilde{w}(k) - \alpha e(k)\phi(k)) - \tilde{w}^T(k)\tilde{w}(k) \\
&= \tilde{w}^T(k)\tilde{w}(k) - \alpha\phi^T(k)e^T(k)\tilde{w}(k) \\
&\quad - \alpha\tilde{w}^T(k)e(k)\phi(k) + \alpha^2\phi^T(k)e^T(k)e(k)\phi(k) - \tilde{w}^T(k)\tilde{w}(k) \\
&\leq -2\alpha\|\phi(k)\|\|e(k)\|\|\tilde{w}(k)\| + \alpha^2\|\phi(k)\|^2\|e(k)\|^2 \\
&\leq -2\alpha\|\phi(k)\|^2\|\tilde{w}(k)\|^2 + \alpha^2\|\phi(k)\|^4\|\tilde{w}(k)\|^2 \\
&\leq -\alpha\|\phi(k)\|^2\|\tilde{w}(k)\|^2(2 - \alpha\|\phi(k)\|^2)
\end{aligned} \tag{22}$$

Combining with PE condition and α is positive definite, ΔL is negative semi-definite. The weights are bounded.

4.3. Route Decision

The proposed routing scheme can be applied to both distributed and centralized dynamic routing in WANET/MANET CPSs. The achievable capacity is estimated for single link in distributed routing and entire path in centralized routing respectively. The following part separately illustrate how the proposed routing scheme deals with the best path selection for both distributed and centralized routing scenarios.

Distributed Dynamic Routing Scenario

In distributed dynamic routing scenario, the proposed scheme is applied to a peer-to-peer communication case. Nodes located between source and destination can be considered as multi-point relays (MPR) which can select the next MPR individually. The next relay candidate has to be achievable and within the communication range of the current relay. When the "Hello" message is send out by the current relay, the maximum capacity for each alternative link is essentially estimated with the RBF neural network. Then, a table about the achievable capacity for each alternative link is generated at the current relay. The routing decision is made and the principal message is transmitted through the link with the highest capacity.

Centralized Dynamic Routing Scenario

An end-to-end routing example is taken. The source node have to know all of alternative paths, then make the routing decision properly. Capacity prediction for end-to-end transmission is more complicated than peer-to-peer case since the "bottleneck" link is able to put down the capacity of the entire path. Therefore, keeping all capacity of each link at a same level is a big challenge for power control and capacity estimation.

To deal with this challenge, a capacity synchronization combining a Nash equilibrium power control is proposed (Fig. 6). The capacity of the first link named C_1, which is conducted by the source node and the next relay candidate, is estimated by a RBF neural network. Then, it is the desired value of other links' capacities ($C_2, C_3, ...C_N$, N is the number of link in this path). The power controller force the $C_2, C_3, ...C_N$ reach C_1. Such a

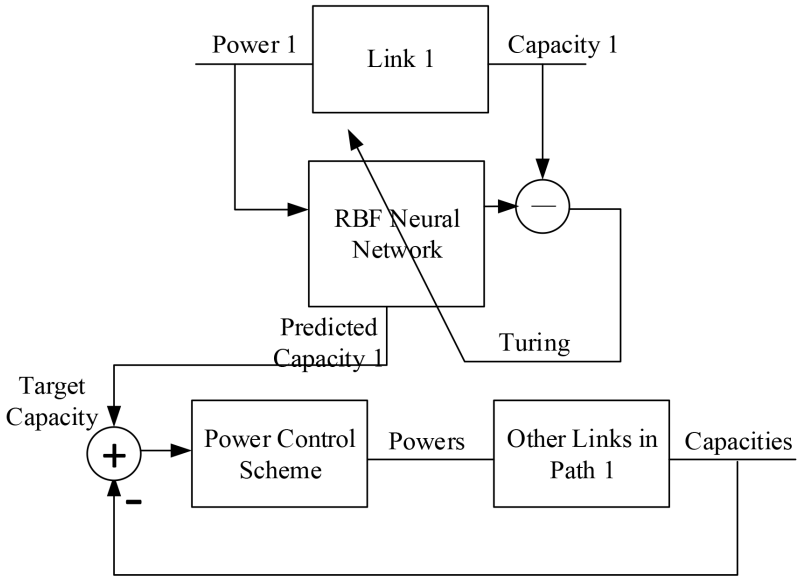


Figure 6. Control schematic

scheme can ensure the capacity consistency in a path and effectively avoid the “bottleneck” situation. A table is only generated at the source node. The routing decision is made, and the path with the best achievable capacity will take the message transmission.

5. SIMULATIONS AND DISCUSSION

In this section, the proposed routing scheme is evaluated by two scenarios with considering a Rayleigh channel fading and noise from environment. The training data are collected when the source node broadcast the "Hello" message. The simulated network is shown in Fig. 7. Twenty nodes with different transmission ranges are randomly scattered in the plate. The power limitation is $0.01mW$ $3.1623mW(0\ 5dBm)$. The initial powers are $1mW$.

Node 1 is the source and Node 4 is the destination. For this particular communication, we can extract a subnetwork that only has six nodes conducting sixteen links shown as Fig. 8. Node 2, 5 and Node 3, 6 are considered as second and third relays respectively.

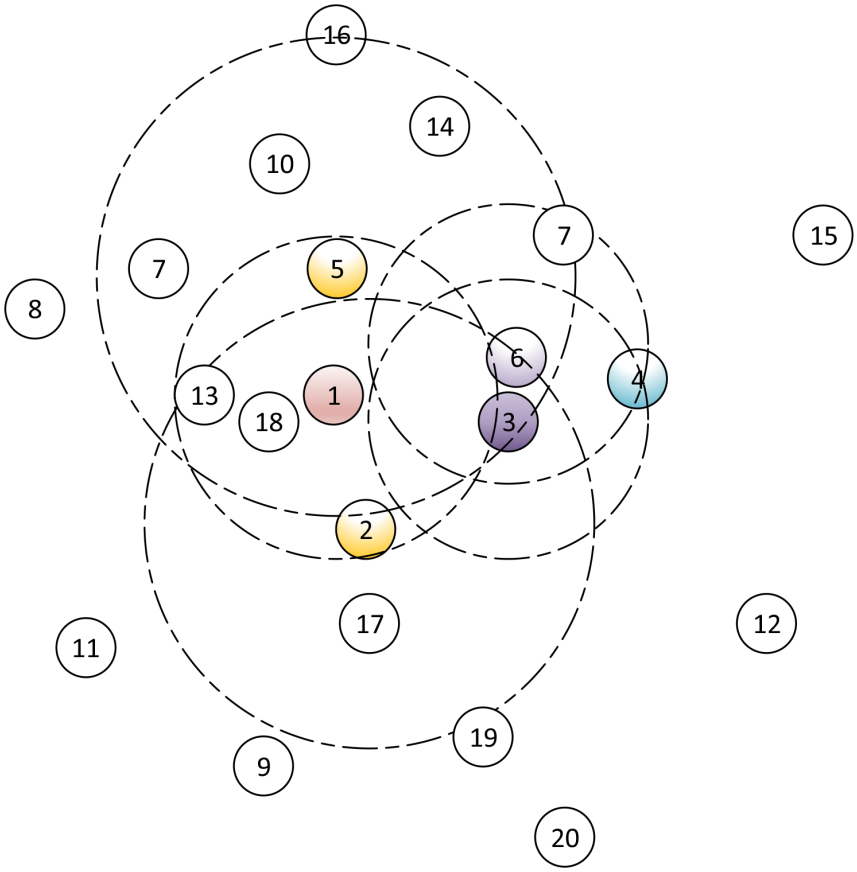


Figure 7. Network topology

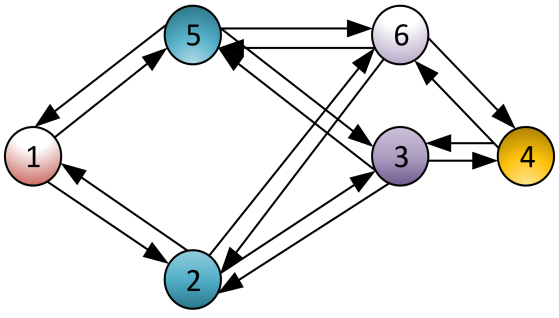


Figure 8. Sub-network topology schematic

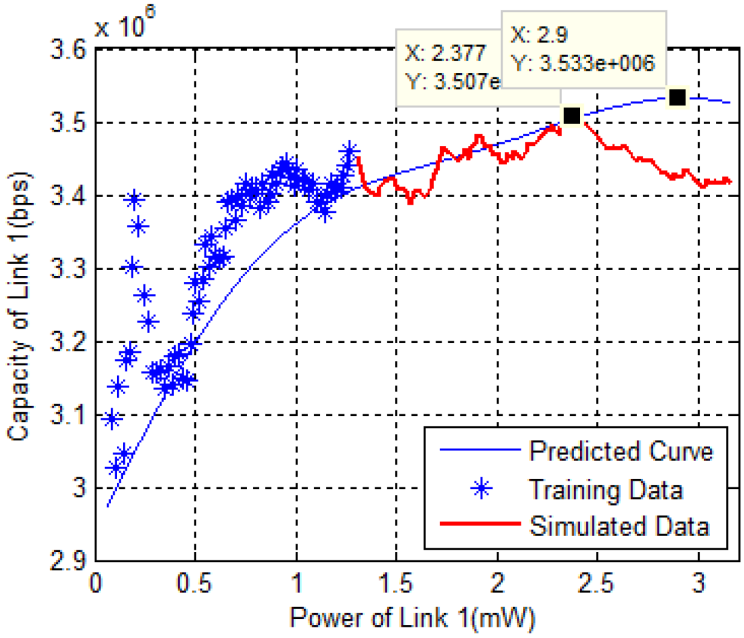


Figure 9. RBF network prediction for Link 1

Each node is free to choose the next relay in its transmission range. Therefore, it is possible that some of links will conduct cross routing. In Fig. 8, there are four paths from Node 1 to Node 4 including Path 1 : 1, 2, 3, 4; Path 2 : 1, 2, 6, 4, Path 3 : 1, 5, 3, 4; Path 4 : 1, 5, 3, 4.

5.1. Routing for Peer-to-Peer Transmission

The channel fading and environmental factors lead to a fluctuation on the capacity shown as Fig. 9. Moreover, in order to do accurate estimation, the averaged value for each variable is taken. After excluding the wrong data point, the existing data provides the capacity values corresponding to power value from $0.01mW$ to $1.4mW$.

Fig. 9 show the predicted curve (the blue curve) comparing with the collected (the green curve) and simulated curve (the red curve). The green curve has covered a part of power series, then we also need to obtain the rest curve by increasing power manually so

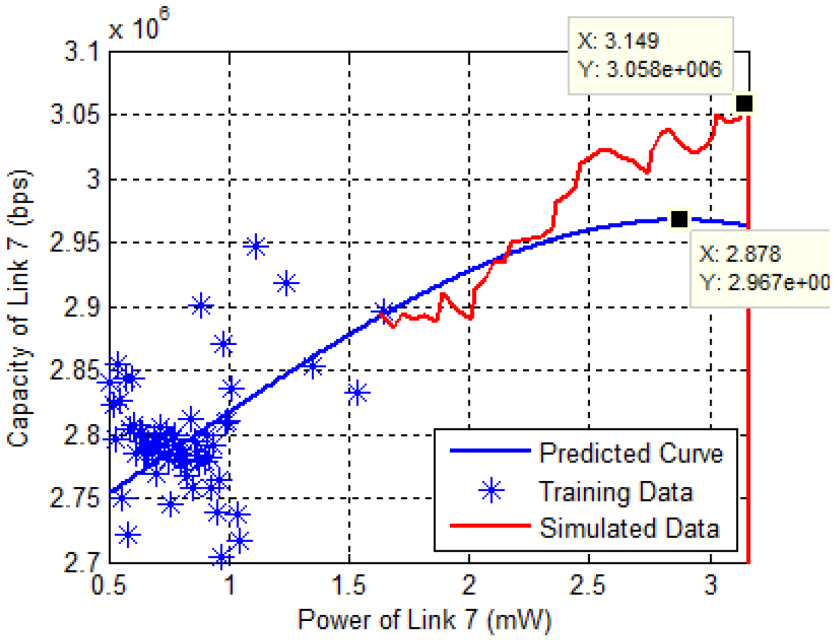


Figure 10. RBF network prediction for Link 7

that we can check if the predicted curve can catch the simulated curve. In Fig. 9, it can be seen that the actual maximum capacity $3.507 * 10^6 bps$ occur at $P_1 = 2.377mW$. Likewise, the maximum capacity is $3.533 * 10^6 bps$ at $2.9mW$ estimated by RBF neural network.

As shown in the results, it concludes that the RBF neural network can predict the capacity vs. the corresponding power curves. Therefore, the source learns how many powers should be putted in so that the best communication performance can be achieved. It also reduce the control input as well as improve the efficiency of the power usage.

Following the proposed prediction, all maximum capacity values of all links can be known. In this scenario, we first estimate the capacity of both Link 1 (from Node 1 to Node 2) shown in Fig. 9 and Link 7 (from Node 1 to Node 5) shown in Fig. 10. Then which node is the next relay can be decided by comparing the maximum achievable capacities. It can be seen that the predicted value of Link 1 ($3.533 * 10^6 bps$) is $0.546 * 10^6 bps$ bigger than

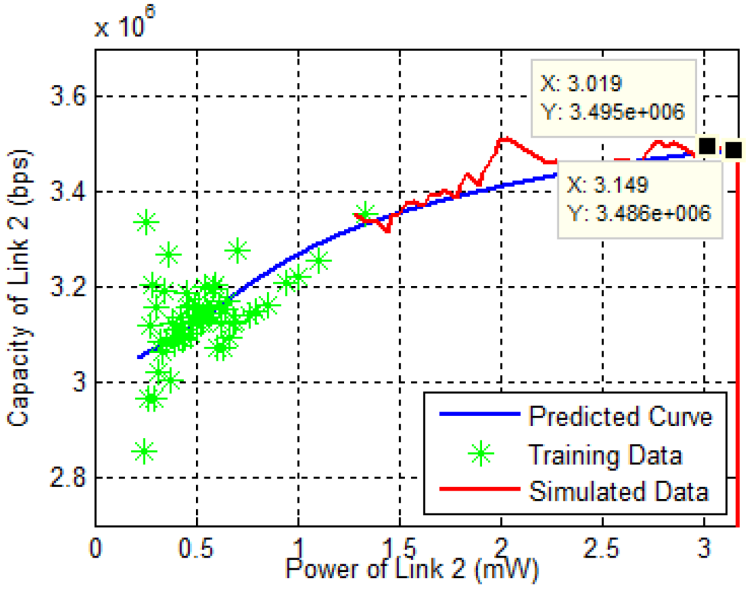


Figure 11. RBF network prediction for Link 2

Link 7's. Therefore, Link 1 is the better route to handle the communications. If Node 2 is the second relay, Node 3 will continuous to do the evaluation for the third relay selection shown as Fig. 11 that is for Link 2.

Following the proposed procedure, the each relay node can gather the local information shown in Table. 1. The simulated values are calculated based on the complete information about system dynamics including path loss gain, Rayleigh channel fading, and disturbance. However, the predicted values are estimated based on typically available measurement data. For instance, the traffic from Node 1 to Node 4 could select several alternative paths. The RBF neural network predictor allows us to identify the best path is $1-2-3-4$ which is same as simulated result.

Table. 1 shows the capacities with the upper bound power. The maximum power does not correspond to the actual maximum achievable capacity for every link. Therefore the accurate approximation of the relationship between power and capacity can be employed to maximize performance while minimize energy consumption.

Table 1. Maximum capacity comparison of predicted and simulated values

Links		**Maximum Capacity ($\times 10^6$bps) (Power(mW))**		**Prediction Error**	**Capacity with Max. Power (3.1623mW)**	**Power Saving**
Source Node	***Destination Node***	***Predicted Value***	***Simulated Value***			
1	2	3.533(2.9)	3.507(2.377)	0.74%	3.414	8.29%
	5	2.987(2.878)	3.058(3.149)	2.32%	3.055	5.53%
2	3	3.495(3.149)	3.487(3.109)	0.33%	3.467	0.42%
	6	1.783(3.155)	1.718(3.162)	3.78%	1.700	0.23%
3	4	3.268(2.229)	3.363(2.120	2.82%	3.252	32.35%
5	3	2.880(3.162)	2.893(3.109)	0.45%	2.880	0
	6	4.722(3.157)	4.642(2.673)	1.72%	4.618	0.17%
6	4	2.234(3.154)	2.005(3.151)	0.55%	2.160	0.26%

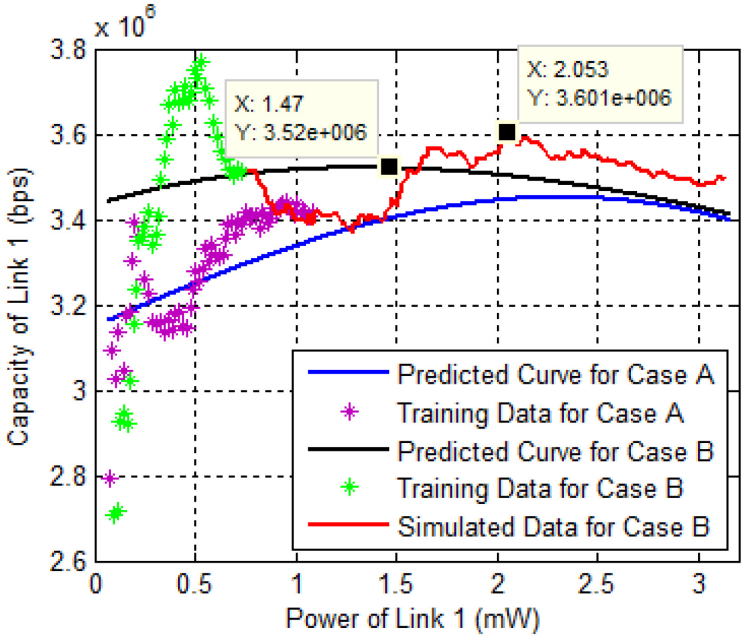


Figure 12. Pre-training RBF network prediction for Link 1

Remark: The initial values of the weights and kernel centers are random vectors in the above simulations. Consequently, more samples should be used to turn the parameters of RBF neural network. Therefore, if the neural network can use a pre-trained initial parameter instead of random one, the training time will be reduced as well as number of samples.

Fig. 12 shows the pre-training performance. The data taken from network is changed over time since the channel fading and random noise are time varying. We assume Case A is the estimation of time k, and Case B is for time $k+1$. The trained parameter of Case A is considered as the initial condition for Case B. The network is re-trained with small number of samples in Case B. Table.2 shows the parameters of neural network are slightly turned and the prediction is accurate with a small prediction error 2.25%. In addition, pretraining of RBF network with simulated data improved convergence of the function estimation by 70.31%. Therefore, pretraining is a good way to fast turning process and reduces sampling times.

Table 2. Turned parameters for Case A and B

Parameter	**Case A**	**Case B**
Weights	[-0.0648, 0.2517, 0.0642, -0.0011, 0.0566, 0.1225]	[-0.0792, 0.2384, 0.0482,-0.0127, 0.0430, 0.1115]
Centers	[-2.4405,-12.6408, -0.4779, 4.1909, -6.5563, 3.0526]	[-2.4405,-12.6408, -0.4461, 4.1909, -6.5563, 3.0526]

Table 3. Maximum capacity for all alternative paths

Distance between Origin and Node 1	Predicted Max Capacity ($\times 10^6$bps)	Simulated Max Capacity ($\times 10^6$bps)	Prediction Error (%)
0.05	8.597	8.195	4.91
0.1	8.399	8.095	3.76
0.15	8.292	7.877	5.29
0.2	8.214	7.719	6.41
0.25	8.111	7.563	7.25
0.3	7.944	7.421	7.05
0.35	7.907	7.243	9.17
0.4	7.836	7.197	8.88
0.45	7.725	7.057	9.47
0.5	7.468	6.998	6.72

By using pre-training, we extended RBF neural network prediction to do routing in mobile ad-hoc network (MANET) scenario. Fig. 12 shows the prediction performance when Node 1 was departing from origin. The data collected at Node 1 locating at origin are used to pre-train the RBF neural network. The converged weights were recorded and applied as the initial values at the next time turning. The tendency of actual and predicted curve are identical. The prediction errors shown in Table. 3 do not exceed 9.47%. Moreover, the number of the returning samples is decreased 45% at least.

5.2. Routing for End-to-End Transmission

In next simulations, we apply the proposed estimation for Path $1-2-6-4$. Due to the all capacity in the path should be same, a Nash equilibrium controller is used.

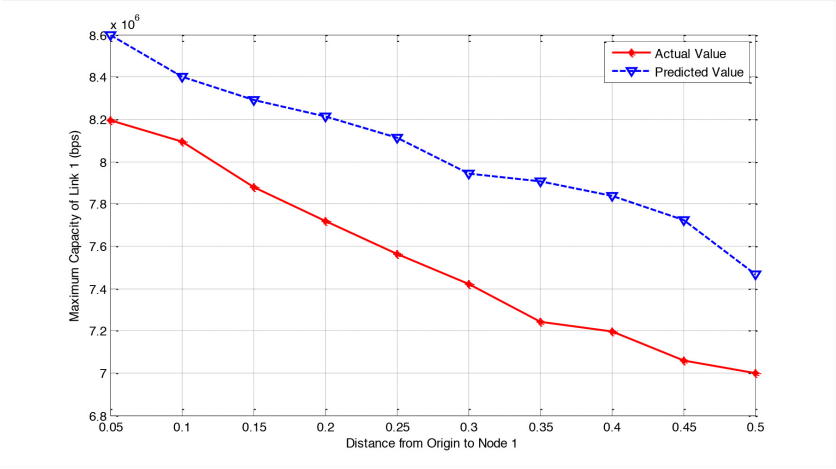


Figure 13. RBF neural network prediction for Link 1

The first link of each path is the leader link whose capacity should be followed by other links. With the proposed capacity synchronization scheme, the predicted Capacity 1 is the desired capacity of other capacities, then inputted into power controller to calculate control inputs.

Three RBF neural networks are used for function prediction for each link. Comparing three capacities at each power value, the maximum capacity is taken as the final capacity of the path.

Although the prediction error of each link cannot be avoided, the path capacity prediction is accurate with only 4.73% ($0.126 * 10^6 bps$) error.

Table. 4 shows the achievable capacities of all alternative paths from Node 1 to Node 4. The RBF neural network predictor allows us to identify the best path is Path $1-2-3-4$ which is same as simulated result.

We also conducted the same experiments as peer-to-peer scenario to test the performance of the proposed routing scheme in MANET based CPSs. Fig. 15 shows that the accuracy of the prediction for MANET scenario have the prediction errors without exceeding 3.07% shown in Table. 5.

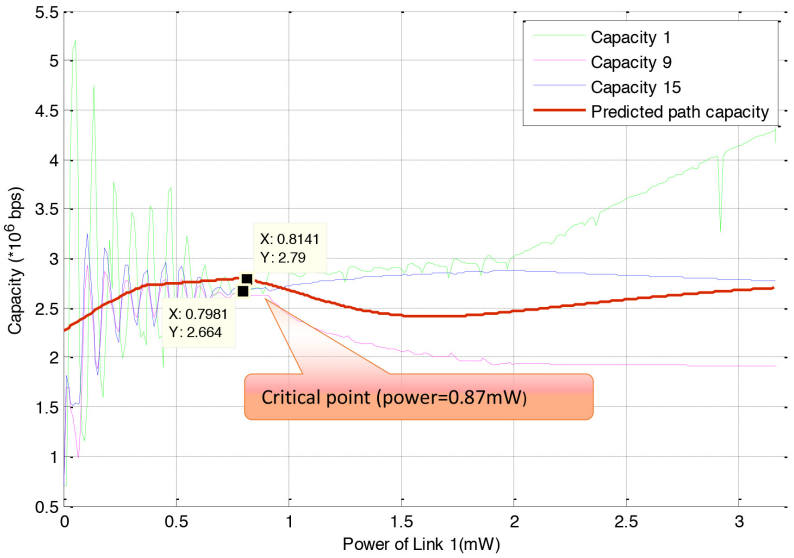


Figure 14. RBF neural network prediction for Path 1 – 2 – 6 – 4

Table 4. Maximum capacity for all alternative paths

Path	Predicted Max Capacity ($\times 10^6$bps)	Simulated Max Capacity ($\times 10^6$bps)	Prediction Error (%)
1-2-3-4	5.28	5.239	0.78
1-2-6-4	2.79	2.644	4.73
1-5-6-4	3.92	4.07	3.67
1-5-3-4	3.34	3.325	0.42

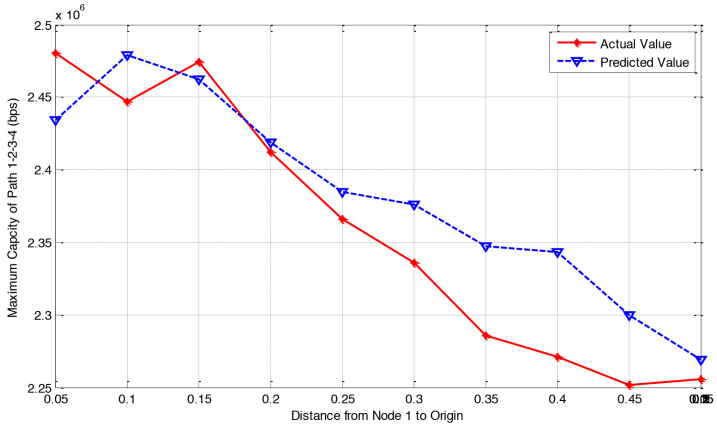


Figure 15. RBF neural network prediction for mobile network

Table 5. Maximum capacity for all alternative paths

Distance between Origin and Node 1	Predicted Max Capacity ($\times 10^6$bps)	Simulated Max Capacity ($\times 10^6$bps)	Prediction Error (%)
0.05	2.434	2.488	2.22
0.1	2.479	2.477	1.29
0.15	2.462	2.474	0.49
0.2	2.419	2.412	0.29
0.25	2.385	2.366	0.80
0.3	2.376	2.336	1.68
0.35	2.347	2.286	2.60
0.4	2.343	2.271	3.07
0.45	2.300	2.252	2.09
0.5	2.269	2.256	0.57

6. CONCLUSION

In this paper, a novel capacity estimation based routing scheme is proposed for optimizing communication performance in WANET/MANET based CPSs. The simulation results show that the proposed capacity estimation routing scheme can select the most optimal path/link with the highest capacity to ensure the vital message can be delivered safely, effectively, and high-quality. In addition, the proposed scheme is flexible to apply for distributed and centralized routing problems.

For peer-to-peer scenario, which is a typical distributed routing example, the RBF NN based capacity prediction can accurately estimate the maximum achievable capacity based on local measurements. The observed error in estimation is less than 4% of predicted throughput. The power setting that maximizes capacity and energy-efficiency can be identified using the RBF estimated function of capacity with transmission power. Comparing with simulated data, the selected route matches the expected one. Moreover, with the pre-training technique, the convergence of the RBF neural network is improved by 70.31%. Such an improvement can also adapt to topology changes caused by some moving nodes in MANET based CPSs, and its prediction error does not exceed 10%.

For end-to-end scenario, the proposed scheme combining with a novel capacity synchronization technique (Fig. 6) is used to deal with a centralized routing problem. The simulation results illustrate that the maximum capacity of multi-hop paths is accurately predicted with avoidance of "bottleneck" situation. The route selections based on the predicted and simulated data are identical and the prediction errors are lower than 4.73%. Furthermore, the proposed scheme can be applied to routing selection in MANET based CPSs. The prediction errors is lower than 3.07%.

In summary, the proposed routing scheme is a flexible and adaptive method to be applied on diverse dynamic routing issues in WANET/MANET base CPSs. Meanwhile, it is robust to against interference, interactions and environmental noises in a large scale CPS. Taking the advantage of advanced routing schemes is a vital part for improving the robustness, reliability, safety, and security of communication in WANET/MANET based CPSs. For future work, the security issues during transmission will be addressed by improving the proposed routing scheme.

REFERENCES

Al-Karaki, J. N. and Kamal, A. E., 'Routing techniques in wireless sensor networks: a survey,' IEEE wireless communications, 2004, **11**(6), pp. 6–28.

Asgeirsson, E. I. and Mitra, P., 'On a game theoretic approach to capacity maximization in wireless networks,' in 'INFOCOM, 2011 Proceedings IEEE,' IEEE, 2011 pp. 3029–3037.

Chang, F.-J., Liang, J.-M., and Chen, Y.-C., 'Flood forecasting using radial basis function neural networks,' IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 2001, **31**(4), pp. 530–535.

Chang, P.-R. and Yang, W.-H., 'Environment-adaptation mobile radio propagation prediction using radial basis function neural networks,' IEEE transactions on vehicular technology, 1997, **46**(1), pp. 155–160.

Chen, M., Chiang, M., Chou, P., Li, J., Liu, S., and Sengupta, S., 'P2p streaming capacity: Survey and recent results,' in 'Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on,' IEEE, 2009 pp. 378–387.

Chen, T.-W. and Gerla, M., 'Global state routing: A new routing scheme for ad-hoc wireless networks,' in 'Communications, 1998. ICC 98. Conference Record. 1998 IEEE International Conference on,' volume 1, IEEE, 1998 pp. 171–175.

Gao, Y., Chiu, D.-M., and Lui, J., 'Determining the end-to-end throughput capacity in multi-hop networks: methodology and applications,' in 'ACM SIGMETRICS Performance Evaluation Review,' volume 34, ACM, 2006 pp. 39–50.

Gastpar, M. and Vetterli, M., 'On the capacity of wireless networks: The relay case,' in 'INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE,' volume 3, IEEE, 2002 pp. 1577–1586.

Gorinevsky, D., 'On the persistency of excitation in radial basis function network identification of nonlinear systems,' IEEE Transactions on Neural Networks, 1995, **6**(5), pp. 1237–1244.

Gupta, P. and Kumar, P. R., 'The capacity of wireless networks,' IEEE Transactions on information theory, 2000, **46**(2), pp. 388–404.

Jagannathan, S., Zawodniok, M., and Shang, Q., 'Distributed power control for cellular networks in the presence of channel uncertainties,' IEEE Transactions on Wireless Communications, 2006, **5**(3), pp. 540–549.

Kawamoto, Y., Nishiyama, H., and Kato, N., 'Ma-ltrt: A novel method to improve network connectivity and power consumption in mobile ad-hoc based cyber-physical systems,' IEEE Transactions on Emerging Topics in Computing, 2013, **1**(2), pp. 366–374.

Leung, H., Dubash, N., and Xie, N., 'Detection of small objects in clutter using a ga-rbf neural network,' IEEE Transactions on Aerospace and Electronic systems, 2002, **38**(1), pp. 98–118.

Li, P., Zhang, C., and Fang, Y., 'The capacity of wireless ad hoc networks using directional antennas,' IEEE Transactions on Mobile Computing, 2011, **10**(10), pp. 1374–1387.

Li, X.-Y., 'Multicast capacity of wireless ad hoc networks,' IEEE/ACM Transactions on Networking (TON), 2009, **17**(3), pp. 950–961.

Liang, W. and Guo, X., 'Online multicasting for network capacity maximization in energy-constrained ad hoc networks,' IEEE Transactions on Mobile Computing, 2006, **5**(9), pp. 1215–1227.

Lien, S.-Y., Cheng, S.-M., Shih, S.-Y., and Chen, K.-C., 'Radio resource management for qos guarantees in cyber-physical systems,' IEEE Transactions on Parallel and Distributed Systems, 2012, **23**(9), pp. 1752–1761.

Pindoriya, N., Singh, S., and Singh, S., 'An adaptive wavelet neural network-based energy price forecasting in electricity markets,' IEEE Transactions on Power Systems, 2008, **23**(3), pp. 1423–1432.

Qu, F., Wang, F.-Y., and Yang, L., 'Intelligent transportation spaces: vehicles, traffic, communications, and beyond,' IEEE Communications Magazine, 2010, **48**(11).

Royer, E. M. and Toh, C.-K., 'A review of current routing protocols for ad hoc mobile wireless networks,' IEEE personal communications, 1999, **6**(2), pp. 46–55.

Shah, R. C. and Rabaey, J. M., 'Energy aware routing for low energy ad hoc sensor networks,' in 'Wireless Communications and Networking Conference, 2002. WCNC2002. 2002 IEEE,' volume 1, IEEE, 2002 pp. 350–355.

Wang, W. and Wu, R., 'Capacity maximization for ofdm two-hop relay system with separate power constraints,' IEEE Transactions on Vehicular Technology, 2009, **58**(9), pp. 4943–4954.

Xue, F., Xie, L.-L., and Kumar, P. R., 'The transport capacity of wireless networks over fading channels,' IEEE Transactions on Information Theory, 2005, **51**(3), pp. 834–847.

Yun, Z., Quan, Z., Caixin, S., Shaolan, L., Yuming, L., and Yang, S., 'Rbf neural network and anfis-based short-term load forecasting approach in real-time price environment,' IEEE Transactions on power systems, 2008, **23**(3), pp. 853–858.

II. PDF-BASED TUNING OF STOCHASTIC OPTIMAL CONTROLLER DESIGN FOR CYBER-PHYSICAL SYSTEMS WITH UNCERTAIN DE LAY DYNAMICS

Shanshan Bi, Maciej Zawodniok

Department of Electrical & Computer Engineering

Missouri University of Science and Technology

Rolla, Missouri 65409–0050

Tel: 573–341–6622, Fax: 573–341–4115

Email: sbn65@mst.edu

ABSTRACT

Cyber-physical systems (CPSs) refer to systems with integrated computational, network, and physical components. With the increasing connectivity among computational cyber connected elements and the physical entities, capturing the interrelationship between the cyber and the physical systems becomes increasingly important. Especially, this intimate coupling between the cyber and physical systems will result in fault propagation from the embedded cyberspace to the physical system. In this paper, a novel cyber network fault diagnosis scheme is proposed to detect and isolate cyber and physical system faults. Additionally, a fault resilience control is designed to mitigate the degradation of system performance when cyber network faults occur and propagate over physical components.

Keywords: cyber physical system, fault diagnosis, network fault, resilience

1. INTRODUCTION

Modern industrial systems, such as smart grid, healthcare, automotive control systems are implemented as distributed event-triggered control systems wherein the control loops are connected by a real-time communication network with limited resources. Such systems are referred to Cyber-physical Systems (CPSs) which offer many advantages: the ease of maintenance and installation, flexibility, and low cost. However, limited resources and constraints of the embedded communication network create challenges for a control system stability. For example, changing topology or background traffic result in varied delays, packet losses, and quantization over time. In addition, cyber attacks including denial-of-service, spoofing, and eavesdropping, can degrade the system performance. For example, delays exceeding the range assumed for the controller due to jamming cyber attack lead to the control signal arriving too late for the actuator to take appropriate actions. Consequently, system outputs deviate from the desired trajectory and the entire CPS becomes unstable. Therefore, an optimal networked resilience controller design for CPSs is needed. It has to mitigate the negative effects of the network uncertainties and dynamics on the CPS performance.

Many existing works on cyber security Xie *et al.* (2014) - Mitchell and Chen (2016) proposed network schemes to defend against the cyber attacks without modification to the controller design. In contrast, other researchers focused on fault tolerant controller design to improve resilience against physical component faults Gao and Chen (2008)-Tiberi *et al.* (2013). In these works, the network dynamics and uncertainties are often oversimplified under strong assumptions: a) the delays are bounded within a specific range; b) the distribution of delays and package losses are known and time-invariant. However, in realistic CPSs, the delay can easily exceed such restrictive bounds and lead to unstable system. The unexpected variation in delay leads to the malfunction or overreaction on the controller and actuator, and eventually instability of the entire CPSs. Therefore, relaxing these assumptions should be addressed to improve the resilience of CPSs.

In this paper, a PDF-based tuning of stochastic optimal controller (PTSOC) is developed to address the degraded system performance induced by network uncertainties including attacks, transmission faults, and channel dynamics. This relaxes the earlier mentioned strong assumptions a) and b) made in existing works. A stochastic system model, which includes stochastic parameters that represents network dynamics, is employed. A KDE-based online PDF identifier is proposed to capture the variation of network dynamics. The probabilities of delays provided by the PDF identifier are used to tune the control law. In addition, the system stability is mathematically analysed using Lyapunov approach. Overall, the proposed approach improves the robustness, optimizes cost of regulation, prevents the physical components from unrepairable damages, and keeps the CPS working within the desired operating condition.

This paper is organized as follows. In Section 2, the related works and motivation are briefly discussed. The proposed controller design in terms of PDF identifier and stability analysis are presented in Section 3. Section 5 illustrates the effectiveness of the proposed controller through simulations in MATLAB. Section 6 gives the conclusion.

2. MOTIVATION AND RELATED WORKS

The embedded cyberspace imposes restrictions on the exchange of information in CPSs, such a limited channel capacity and traffic congestions. Malicious cyber attacks further restrict the information delivery. The delay and packet loss caused by the above restrictions are stochastic with unknown bounds and difficult to predict. Importantly, they have a potentially negative effect on the performance and stability of CPSs. For example, inappropriate control actions caused by increasing delay lead to a big overshoot as well as more actuation cost to manage such overshoot.

A following example shows that the network dynamics significantly affect the performance of CPS and the existing control approaches may fail to guarantee its stability.

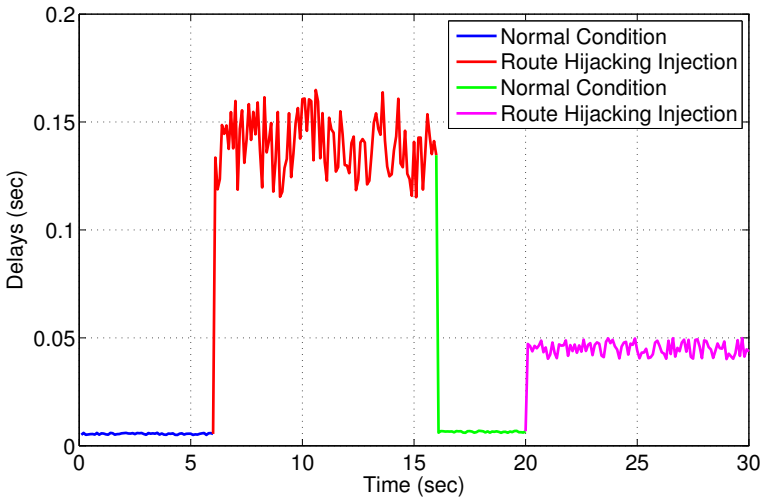


Figure 1. Delays

This scenario emulates a route hijacking by an attacker to eavesdrop control information (data integrity). Such a route hijacking increases delay and delay variation on the longer path. A network is simulated using Network Simulator 2 (NS2) with a random topology of 11 nodes. Ad hoc On-Demand Distance Vector (AODV) routing scheme is adopted. The route through the topology is altered during the simulation such that the packet delays vary for the controller loop, as shown in Fig. 1. Note, that similar network performance could be a result of topology or traffic pattern changes.

The results show the disturbance in CPS introduced by the network dynamics. With these delays, a PID controller is simulated for a simple 2I4O (two input four output) system Xu *et al.* (2012). Fig. 2 shows PID make the system states converge when delay bound is low before $6s$. Then, the sudden changes of delay at $k = 6s$, $16s$, and $20s$ make the system states vibrate. Consequently, the CPS becomes unstable due to such dynamics of delay.

The attack changes the delay distribution. This stochastic disturbance increases the probability that the system becomes uncontrollable and unstable. Therefore, it is necessary to include such dynamics both in system model and controller design.

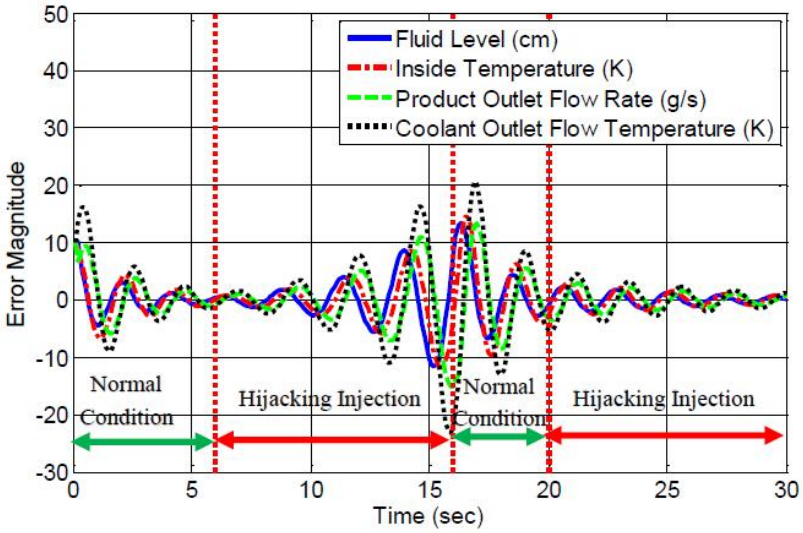


Figure 2. System performance with a PID controller

2.1. Literature Review

The following literature review discusses the existing approaches that address the uncertain dynamics of network, especially long time delays and packet losses, either in network or physical system.

Many researchers developed network protocols and tools Xie *et al.* (2014) - Mitchell and Chen (2016) to keep delays and packet losses within traditional controller constraints. The controller design of physical systems is not modified in these works. Such approaches can maintain system stability if the network configuration is simple and fixed. Designing more complicated networks and systems under cyber attacks becomes challenging if not impossible due to restrictive constraints dictated by the physical controller. Xie *et al.* (2014) proposed a channel estimation approach to calculate the packet success rate, the worst-case packet delay and average energy consumption based on acknowledgement (ACK) information. However, the worst-case delay has a upper bound known a priori while the system model is linear time invariant and not stochastic. Lee *et al.* (2005) proposed a quality-of-service based remote control scheme for CPSs via the Profibus token passing protocol. They

used the time delay data provided by transmitting the real-time messages to approximate the delays for high-priority and low-priority messages. They assumed a strong condition that the network delay has time invariant lower and upper bounds. The control schemes in above literature are valid if the delays are bounded within the acceptable range. However, if the configuration of the embedded network becomes complicated, dynamic, and stochastic, the bound constraints cannot be met. For instant, in intelligent transportation systems (ITS), moving vehicles exchange their information with other vehicles, transportation management system, and users. Such a complicated and dynamic network results in delays and packet losses exceeding their bounds because of interference from the environment and network topology changes. Thus the controller cannot guarantee the stability of CPSs. Overall, a more robust approach should consider network dynamics in controller design to relax the constraints.

Simultaneously, other researchers had designed several controllers to address stochastic network dynamics under strong constrains. Gao and Chen (2008), Gao *et al.* (2008) modelled a CPS as a sampled-data system and solved a set of linear matrix inequalities to derive the feedback gain of a memory-less controller. The dynamics in the cyberspace are simplified as known bounded delays. Similarly, Hao and Zhao (2010), Tian *et al.* (2010), Liu *et al.* (2007) proposed networked controllers by using Lyapunov stability analysis with a priori knowledge of the delay bounds. Moreover, Tiberi *et al.* (2013) proposed a self-triggered sampling for achieving substantial reduction of communication traffic. The system stability can be guaranteed under certain assumptions: a) the measurements are sent to the central node within a bounded time delay; b) The system states have to converge initially. All these works considered the network delay issues in various perspective. However, they commonly assumed the network delay had a known bound and the distribution of delay was fixed. Such schemes would fail in realistic CPSs where delay bound is unknown before

hand. For instance, new communication nodes generating new traffics will increase the upper bound which cannot be known ahead of time. Furthermore, dynamics of the delay distribution make the entire system unstable.

2.2. Explicit Modeling of Delay and Packet Losses

Xu *et al.* (2012) made a significant progress when they included the random parameters representing network dynamics in system model. All of system matrices and control input calculation concurrently change as network delays and packet losses randomly change. This model is the prototype we used in the proposed PTSOC design.

The conventional discrete time model was described as following Blundell and Duncan (1998):

$$\begin{aligned} x_{k+1} &= A_s x_k + B_0^k u_k^a + B_1^k u_{k-1}^a + \ldots + B_d^k u_{k-d}^a \\ u_{k-i}^a &= \gamma_{k-i} u_{k-i} \end{aligned} \tag{1}$$

where $x_k = x(kT)$ denotes system states; $A_s = e^{AT}$, $B_0^k = \int_{d_0^k}^{T_s} e^{A(T_s - t)} dt$, and $B_i^k = \int_{d_i^k - iT_s}^{d_{i-1}^k - (i-1)T_s} e^{A(T_s - t)} dt \ \forall i = 1, 2, \ldots, d$ are the system matrices.

Xu *et al.* (2012) derived the stochastic model expressed as

$$z_{k+1} = A_{zk} z_k + B_{zk} u_k, \tag{2}$$

where $z_k = [x_k^T \ u_{k-1}^T \ \cdots \ u_{k-d}^T]^T$ is the state variables vector; and A_{zk}, B_{zk} are the time-varying system matrices, shown as

$$A_{zk} = \begin{bmatrix} A_z & \gamma_1^k B_1^k & \cdots & \gamma_i^k B_i^k & \cdots & \gamma_d^k B_d^k \\ 0 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & I_m & \cdots & \cdots & 0 & 0 \\ \vdots & 0 & I_m & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & I_m & 0 \end{bmatrix}, B_{zk} = \begin{bmatrix} \gamma_0^k B_0^k \\ I_m \\ 0 \\ 0 \\ \vdots \\ 0 \end{bmatrix}$$

u_k is the control input; γ_i^k and γ_{k-i} are binary random variables representing the package reception status. (if the package is received, $\gamma = 1$, otherwise, $\gamma = 0$)

Then, the stochastic optimal control (SOC) law can be obtained by optimized the following cost function.

$$J = E[\sum_{m=k}^{\infty}(z_m^T Q_z z_m + u_m^T R_z u_m)] \quad k = 0, 1, 2, \cdots \tag{3}$$

where $Q_z = diag\{Q, R/d, \cdots\}$, and $R_z = R/d$ are symmetric positive semi-definite and symmetric positive definite respectively. $E(\bullet)$ is the expected operator of $\sum_{m=k}^{\infty}(z_m^T Q_z z_m + u_m^T R_z u_m)$.

Although the above model included the terms of network dynamics, the SOC only indirectly considers such dynamics through the stochastic model. It also has a strong assumption that the delay distribution is fixed. System performance becomes suboptimal when the above assumptions are invalidated by changes in bounds or distribution as observed in simulations for cases B and C in Section 5.

2.3. Capturing Network Dynamics

To relax the bounds and distribution constraints, the system model and the control law should be tuned based on current probabilities of delays. Therefore, a PDF estimation is needed.

For estimation of delay probabilities, several PDF identification methods exist in literature, such as histogram, KDE, and Maximum likelihood estimation Silverman (1986). The advantage of KDE is more accurate estimation with fewer samples than other methods. Offline KDE has been used in various applications, including computer graphics Hurter *et al.* (2012), image processing Bors and Nasios (2009), Calabrese and Zenga (2010), Blundell and Duncan (1998), and Elgammal *et al.* (2003), and industrial process He *et al.* (2015), Chen *et al.* (2014). He *et al.* (2015) introduced a novel KDE based framework for nonlinear metric learning, Kernel density metric learning (KDML). This method has been successfully applied in face recognition. Elgammal *et al.* (2003) investigated the use of Fast Gauss Transform for efficient computation of KDE techniques for computer vision applications. Chen *et al.* (2014) proposed a KDE based method to estimate the spatial intensity of false alarms for multi-target tracking system. Additionally, KDE Silverman (1986) is suitable for PDF identification in CPS because it can handle different types of distributions, such as mixture distribution and Poisson distribution. In contrast, the other approaches only work for normal distributions. In Section 3.2, an online KDE estimator is introduced. It can estimate unknown PDF with a good accuracy and adapt to the dynamic changes of delay distribution. Then, the provided PDF information is used to tune the PTSOC control law. Hence, the controller adapts to the given network dynamics.

The proposed PTSOC relaxes the bounds and distribution constraints through including PDF information in controller design. Next, the details of the proposed PTSOC are presented.

3. PROPOSED PDF-BASED TUNING OF STOCHASTIC OPTIMAL CONTROL (PTSOC) DESIGN

In this section, the overview of the proposed control scheme is given. The PDF-based tuning of stochastic optimal control (PTSOC) scheme with an online PDF estimator is introduced. The online KDE based PDF identifier is introduced in Section 3.2. Then, PTSOC is derived from the proposed cost function 4 in Section 3.3.

3.1. Overview

PTSOC takes into account uncertain network dynamics by applying online KDE to capture PDF variation of delays and tuning its control law based on the PDF information. The overall architecture of the proposed control system is shown in Fig. 3.

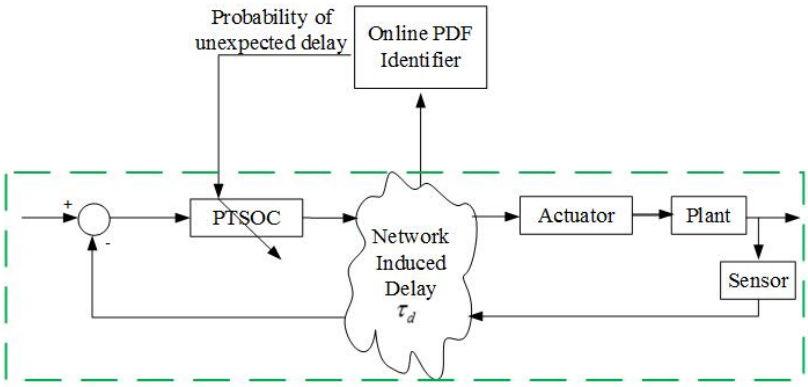


Figure 3. Overall architecture of stochastic CPS with PDF identifier

The proposed PTSOC includes three main steps that are continuous repeated:

a) Data collection of delays. n delays ($[d_{k-n+1}, \cdots, d_k]$) in the sliding window are used to do the PDF estimation at time k (PDF_k). When new delay is measured, the data in the sliding window is updated.

b) PDF estimation. The PDF of these n delays is obtained. The probability for each delay interval is calculated.

c) PTSOC law calculation. For each delay interval, the cost function (5) and the optimal control law (8) are derived from (3). The cost function of PTSOC defined by (4) is a probability weighted sum of the cost functions for all delay intervals. Similarly, the PTSOC law derived in Section. 3.3 is the summation of the weighted SOC laws of delay intervals. These weights are probabilities from the delay PDF. The final cost function is:

$$J^k = \sum_{i=1}^{n} P_i J_i^k = \sum_{i=1}^{n} P_i (E[\sum_{m=k}^{\infty} z_{mi}^{kT} Q_i z_{mi}^k + u_i^{kT} R_i u_i^k]) \tag{4}$$

where d_{int} represents the delay interval that we take $0.1s$ in the simulation section. If $d_{int} < d^k < d_{int}(i+1)$, d^k is classified in i^{th} delay case; n is the total number of delay cases; k represents sampling interval; P_i is probability of delay within $d_{int}i$ to $d_{int}(i+1)$ provided by the KDE-based PDF identifier; x is states vector; u_i is control inputs vector; Q_i and R_i are weighted constants of states and control inputs, respectively.

Remark 1: The cost function of PTSOC is more generalized than that of SOC. SOC only considers the worst delay case that is $d_{int} < d^k < d_{int}(i+1)$, $P_i = 1$, and $P_j = 0, j \neq i$. In such a case, the PTSOC cost function (7) becomes SOC (3).

As the probabilities of each possible delay changes, PTSOC continuously tracks the network dynamics with a PDF identifier and updates its parameters based on PDF information of delay to adapt to the given system situation.

3.2. PDF Identifier

To capture the dynamics of network delays, an online KDE-based PDF identifier is proposed to iteratively estimate the distribution. The data used to do identification is updated every sampling interval for a window of n last packet delays. The main steps of online PDF identification are shown in Table. 1. Here, a normal kernel smoother is selected for PDF estimation.

Table 1. Online PDF identification algorithm

1. Determining the data in the sliding window for time k:
   a) Choosing a kernel function K centered on τ with a bandwidth h;
   b) Each observation τ_i receives a specific weight proportional to the scaled distance from the observation τ_i to τ, which is $u = (\tau - \tau_i)/h$;
   c) At a given τ, the estimate is found by vertically summing up over the k shapes.
      This can be synthesized as:
      $$\widehat{f}(\tau) = \frac{1}{nh}\tau_i \in [\tau - \frac{h}{2}, \tau + \frac{h}{2}]$$
      The general formula for KDE will be given by
      $$\widehat{f_k}(\tau) = \frac{1}{nh}\sum_{i=1}^{n} K(\frac{\tau - \tau_i}{h})$$
      where the dependence of the estimate on the kernel function $K(.)$ is denoted as $\widehat{f_k}$.
2. Updating the new data for time $k + 1$ in the sliding window and go back to Step 1;

Remark 2: With a large window size, KDE provides an accurate estimation of PDF with neglectable bias Gisbert (2003). In this paper, we estimate PDF of n samples in the sliding window. Such that the estimation error is guaranteed to converge to a small value denoted as d_{KDE}. The effect of d_{KDE} on the regulation error convergence is shown in **Theorem 3**.

3.3. Optimal Controller Design with Consideration of Dynamics of Delay Distribution

In this subsection, PDF identification is employed to develop a novel stochastic optimal controller for CPSs while considering stochastic dynamics of network. First, we derived a time-varying system matrices that explicitly include probability information of delays. Each element of the matrices is derived. Then, PTSOC is proposed based on the time-driven sensing and event-driven actuating controller framework. The maximum number of control input that effects system matrices is d. Only the latest control input is allowed to act on the controlled plant when several control inputs are received at the same time Xu *et al.* (2012).

In the stochastic model (2), all of the candidate models (dynamic matrices A_{zki} and B_{zki}) and their corresponding probabilities depend on the γ_i^k values and their probabilities. γ_0^k corresponds to control input with the delay less than sampling period (T_s). γ_i^k ($k = 1, 2, d$) is determined by γ_{i-1}^{k-1}. Therefore, γ_i^k depends on γ_0^{k-1} and γ_i^{k-} . The probability $P_{\gamma_i^k}$ can be determined by $P_{d^k > T_s}$. (5) denotes the probability for each γ_i.

$$
\gamma_0^k = \begin{cases} 0 \quad if\ d^k > T_s,\ the\ corresponding\ probability\ P_{\gamma_0^k=0} = P_{d^k>T_s} \\ 1 \quad if\ d^k < T_s,\ the\ corresponding\ probability\ P_{\gamma_0^k=1} = P_{d^k<T_s} \end{cases}
$$

$$
\gamma_1^k = \begin{cases} 0\ if\ d^k < T_s,\ d^k < d^{k-1} - T_s,\ P_{\gamma_1^k} = P_{d^k>T_s} P_{d^{k-1}<T_s} P_{d^k<d^{k-1}-T_s} \\ 1 \begin{cases} if\ d^k > T_s,\ d^{k-1} > T_s \begin{cases} d^k < d^{k-1} - T_s, \\ \quad P_{\gamma_1^k=1} = P_{d^k>T_s} P_{d^{k-1}<T_s} P_{d^k<d^{k-1}-T_s} \\ d^k > d^{k-1} - T_s, \\ \quad P_{\gamma_1^k=1} = P_{d^k>T_s} P_{d^{k-1}<T_s} P_{d^k>d^{k-1}-T_s} \end{cases} \\ if\ d^k < T_s, \begin{cases} d^{k-1} > T_s,\ d^k > d^{k-1} - T_s, \\ \quad P_{\gamma_1^k=1} = P_{d^k<T_s} P_{d^{k-1}>T_s} P_{d^k>d^{k-1}-T_s} \\ d^{k-1} < T_s,\ P_{\gamma_1^k=1} = P_{d^k>T_s} \end{cases} \end{cases} \end{cases}
$$

$$
\vdots
$$

$$
\gamma_d^k = \begin{cases} 0\ P_{\gamma_d^k=0} \\ 1\ P_{\gamma_d^k=1} \end{cases}
$$

(5)

where $P_{d_{int}i<d^k<d_{int}(i+a)} = \int_{d_{int}i}^{d_{int}(i+a)} f(x)dx$, d_{int} is delay bandwidth.

All of the probabilities in (5) can be obtained from the PDF identifier. The data in the sliding window maps the PDF and provide the probabilities of delays in different ranges $P(d_i^k),\ P(d_i^{k-1}),\ \cdots,\ P(d_i^{k-d})$. The probability of delays can be denoted as $P(\gamma_0^k = i)$ and

$P(\gamma_i^k = i)$. Then, it is easy to obtain the probabilities of each possible B_i^k based on the above information. Finally, a set of candidate stochastic models A_{zki} and B_{zki} are defined. The corresponding control law (candidate control law) for each candidate model (6) is obtained by optimizing its corresponding cost function (7). Each candidate cost function has its optimal parameters Q_{zi} and R_{zi} for the corresponding control law derivation. The final proposed control law (8) is a weighted sum of these candidate control laws, with weights that are equal to the corresponding probabilities from the PDF identifier.

$$
\begin{aligned}
& d_{int} i < d_k < d_{int}(i+1) \\
= & \begin{cases}
i = 1 & u_{1k} = -K_{1k} z_{1k},\ K_{1k} = (B_{zk1}^T z_{1k} B_{zk1} + R_{zk})^{-1} (B_{zk1}^T z_{1k} A_{zk1} + S_{z1k}) \\
i = 2 & u_{2k} = -K_{2k} z_{2k},\ K_{2k} = (B_{zk2}^T z_{2k} B_{zk2} + R_{zk})^{-1} (B_{zk2}^T z_{2k} A_{zk2} + S_{z2k}) \\
\vdots & \\
i = n_d & u_{n_d k} = -K_{n_d k} z_{n_d k},\ K_{n_d k} = (B_{zkn_d}^T z_{n_d k} B_{zkn_d} + R_{zk})^{-1} (B_{zkn_d}^T z_{n_d k} A_{zkn_d} + S_{zn_d k})
\end{cases}
\end{aligned}
\tag{6}
$$

$$
\begin{aligned}
J_1 &= E[\sum_{m=k}^{\infty} z_{1m}^T (Q_{z1} - K_{1m}^T R_z K_{1m}) z_{1m}] \\
J_2 &= E[\sum_{m=k}^{\infty} z_{2m}^T (Q_{z2} - K_{2m}^T R_z K_{2m}) z_{2m}] \\
&\vdots \\
J_{n_d} &= E[\sum_{m=k}^{\infty} z_{n_d m}^T (Q_{zn_d} - K_{n_d m}^T R_z K_{n_d m}) z_{n_d m}]
\end{aligned}
\tag{7}
$$

where K_{ik} is the optimal gain when $d_{int}i < d^k < d_{int}(i+1)$ at k, J_i is the corresponding cost function.

$$
\begin{aligned}
u_k &= -K_k z_k \\
K_k &= \sum_{i=1}^{n_d} P_{ki}(B_{zki}^T z_{mi} B_{zki} + R_{zk})^{-1}(B_{zki}^T z_{mi} A_{zki} + S_{zki}) = \sum_{j=1}^{n_d} P_{kj} K_j
\end{aligned}
\tag{8}
$$

where K_k is the optimal gain and u_k is the control input. $S_{zik} \geq 0$ is the solution to the ARE. $n_d = d_{upper}/d_{int}$, d_{upper} is the maximum delay in the sliding window; P_{ki} is the probability of $d_{int}i < d^k < d_{int}(i+1)$.

PTSOC, which considers PDF of delays, is able to optimize the trade-off between system state error and cost of regulation. Its control law is more accurate for the given network situation than that of SOC because the weights of each candidate control law are continuously updated to reflect the actual PDF of delays. In contrast, SOC considers only one of delay cases in 7 in optimization.

4. STABILITY ANALYSIS

Three theorems and their corresponding proofs are presented to demonstrate stability of the proposed PTSOC. Lyapunov based stability analysis is used. Theorems **1** and **2** demonstrate asymptotic convergence of regulation error and estimation error of the control gain. **Theorem 3** shows uniformly ultimately bounded (UUB) stability of the regulation error when the irremovable bias of PDF estimation exists.

In **Theorem 1**, the control law tuned by probability information guarantees the asymptotic convergence for regulation error with an assumption that delay PDFs are accurately estimated without bias. **Theorem 2** relaxes the assumption in **Theorem 1**. It shows the control gain estimation asymptotically converges even if PDF estimation has an error provided it asymptotically converges to zero. **Theorem 3** considers the irremovable bias of PDF estimation as a bounded disturbance. However, an UUB stability is guaranteed.

Theorem 1: (Asymptotic stability of regulation error with a perfect PDF estimation). Given the initial conditions as the system state z_0 and system matrices A_{z0}, and B_{z0}, let $u_0(z_k)$ be an initial admissible control policy for the CPS (1). Let the control update law be given by (8) with properly selected Q_{zm} and R_{zm}. Let the PDF estimation be a no error estimation. Then, there exists a constant K_{max} satisfying $K_{max} \leq (1-a)/b$ such that the regulation error of system states converge to zero asymptotically in the mean.

Proof

Consider the following positive definite Lyapunov function candidate: $V_{zk} = z_k^T z_k$. z_k is the state vector of k.

The system matrices are time varying and stochastic, therefore, we consider $\Delta V_{z_{km}} = V_{z_{k+1}m} - V_{z_k m}$ for each possible system matrices (A_{zkm} and B_{zkm}). m represents the number of the candidate systems. If the maximum value of $\Delta V_{z_k m}$ is negative definite, the convergence of system states is proved.

$$
\begin{aligned}
\Delta V_{z_k m} &= V_{z_{k+1}m} - V_{z_k} \\
&= (A_{zkm} z_k + B_{zkm} u_k)^T (A_{zkm} z_k + B_{zkm} u_k) - z_k^T z_k \\
&= \| A_{zkm} z_k + B_{zkm} u_k \|^2 - \| z_k \|^2 \\
&= \| A_{zkm} z_k - B_{zkm} \sum_{i=1}^{n_d} P_{ik} K_{ik} z_k \|^2 - \| z_k \|^2 \\
&= \left(\| A_{zkm} z_k - B_{zkm} \sum_{i=1}^{n_d} P_{ik} K_{ik} \|^2 - 1 \right) \| z_k \|^2
\end{aligned}
$$

With Cauchy-Schwarz inequality,

$$
\begin{aligned}
\Delta V_{z_k m} &\leq \left\{ (\parallel A_{zkm} \parallel + \parallel B_{zkm} \parallel \parallel K_k \parallel)^2 - 1 \right\} \parallel z_k \parallel^2 \\
&\leq \left\{ (\parallel A_{zkm} \parallel + \parallel B_{zkm} \parallel K_{max})^2 - 1 \right\} \parallel z_k \parallel^2 \\
&\leq \left\{ (a_{max} + b_{max} K_{max})^2 - 1 \right\} \parallel z_k \parallel^2 \\
\forall k &= 1, 2, \cdots \\
\forall m &= 1, 2, \cdots, n_d \\
K_{max} &= max\{ \parallel K_1 \parallel, \parallel K_2 \parallel, \cdots, \parallel K_{n_d} \parallel \} \\
&= max\{ \parallel (B_{zki}^T z_{mi} B_{zki} + R_{zk})^{-1} (B_{zki}^T z_{mi} A_{zki} + S_{zk}) \parallel \}, \\
\forall i &= 1, 2, \cdots, n_d,
\end{aligned}
$$

where A_{zj} and B_{zj} are the system matrices of j. K_j is the control gain of j. K_{max} is the maximum control gain of k. n_d is the number of system matrices case. $a_{max} = max\{ \parallel A_{zk1} \parallel, \parallel A_{zk2} \parallel, \cdots, \parallel A_{zkm} \parallel \}$ is the upper bound of $\parallel A_{zkm} \parallel$, and $b_{max} = max\{ \parallel B_{zk1} \parallel, \parallel B_{zk2} \parallel, \cdots, \parallel B_{zkm} \parallel \}$ is the upper bound of $\parallel B_{zkm} \parallel$.

We define $a = maxa_1, a_2, \cdots, a_{n_d}$ and $b = maxb_1, b_2, \cdots, b_{n_d}$. Q_{zm} and R_{zm} are selected properly Carnevale *et al.* (2007). Since $V_{z_k m}$ is positive definite and $\Delta V_{z_k m}$ is negative definite provided K_{max} is selected as above. Therefore, the regulation error converges to zero asymptotically. ■

Next, the assumption that PDF estimation has no bias is relaxed with **Theorem 2**. The control gain estimation error still has an asymptotic convergence.

Theorem 2 (Control gain estimation error convergence): As the delay data keeps updating PDF identifier and $\left(\parallel \sum_{j=1}^{n} \widetilde{P}_{(k+1)j} \parallel - \parallel \sum_{j=1}^{n} \widetilde{P}_{kj} \parallel \right) < 0$ is satisfied, then the estimation error for control gain $\parallel \widetilde{K}_k \parallel$ asymptotically converges to zero.

Proof

First, we define the estimation error of control gain K as $\widetilde{K}_k = K_k - \widehat{K}_k = \sum_{j=1}^{n} P_{kj}K_j - \sum_{j=1}^{n} \widehat{P}_{kj}K_j$. P_{ij} is the actual probability at k. Then, Lyapunov function candidate is $V_{K_k} = \widetilde{K}_k^T \widetilde{K}_k$.

$$
\begin{aligned}
\Delta V_{K_k} &= V_{K_{k+1}} - V_{K_k} \\
&= \widetilde{K}_{k+1}^T \widetilde{K}_{k+1} - \widetilde{K}_k^T \widetilde{K}_k \\
&= (K_{k+1} - \widehat{K}_{k+1})^T (K_{k+1} - \widehat{K}_{k+1}) - (K_k - \widehat{K}_k)^T (K_k - \widehat{K}_k) \\
&= (\sum_{j=1}^{n_d} P_{(k+1)j}K_j - \sum_{j=1}^{n_d} \widehat{P}_{(k+1)j}K_j)^T (\sum_{j=1}^{n_d} P_{(k+1)j}K_j - \sum_{j=1}^{n_d} \widehat{P}_{(k+1)j}K_j) \\
&\quad - (\sum_{j=1}^{n_d} P_{kj}K_j - \sum_{j=1}^{n_d} \widehat{P}_{kj}K_j)^T (\sum_{j=1}^{n_d} P_{kj}K_j - \sum_{j=1}^{n_d} \widehat{P}_{kj}K_j) \\
&= \| \sum_{j=1}^{n_d} (P_{(k+1)j} - \widehat{P}_{(k+1)j})K_j \|^2 - \| \sum_{j=1}^{n_d} (P_{kj} - \widehat{P}_{kj})K_j \|^2 \\
&= \| \sum_{j=1}^{n_d} \widetilde{P}_{(k+1)j}K_j \|^2 - \| \sum_{j=1}^{n_d} \widetilde{P}_{kj}K_j \|^2 \\
&= \underbrace{\left(\| \sum_{j=1}^{n_d} \widetilde{P}_{(k+1)j}K_j \| + \| \sum_{j=1}^{n_d} \widetilde{P}_{kj}K_j \| \right)}_{\Delta_1} \left(\| \sum_{j=1}^{n_d} \widetilde{P}_{(k+1)j}K_j \| - \| \sum_{j=1}^{n_d} \widetilde{P}_{kj}K_j \| \right) \\
&= \Delta_1 \left(\| \sum_{j=1}^{n_d} \widetilde{P}_{(k+1)j}K_j \| - \| \sum_{j=1}^{n_d} \widetilde{P}_{kj}K_j \| \right) \\
&= \Delta_1 [(\| \widetilde{P}_{(k+1)1} \| - \| \widetilde{P}_{k_1} \|) \| K_1 \| + \| \widetilde{P}_{(k+1)2} \| - \| \widetilde{P}_{k_2} \|) \| K_2 \| + \cdots \\
&\quad + \| \widetilde{P}_{(k+1)n_d} \| - \| \widetilde{P}_{k_{n_d}} \|) \| K_{n_d} \|] \\
&\leq \Delta_1 \left(\| \sum_{j=1}^{n} \widetilde{P}_{(k+1)j} \| - \| \sum_{j=1}^{n} \widetilde{P}_{kj} \| \right) \| K_{max} \|
\end{aligned}
$$

$\Delta_1 > 0, K_{max} = max\{K_1, K_2, \cdots, K_{n_d}\}$

Since V_{K_k} is positive definite and ΔV_{K_k} is negative definite provided $\widetilde{K}_k = K_k - \widehat{K}_k = \sum_{j=1}^{n} P_{kj}K_j - \sum_{j=1}^{n} \widehat{P}_{kj}K_j$. Therefore, the estimation error of control gain asymptotically converge to zero. ■

Remark 3: Monotonically decreased estimation error for each delay range ($\| \widetilde{P}_{(k+1)j} \| - \| \widetilde{P}_{kj} \| < 0$) is not a necessary condition. The convergence only requires the estimation error of the entire PDF ($\left(\| \sum_{j=1}^{n} \widetilde{P}_{(k+1)j} \| - \| \sum_{j=1}^{n} \widetilde{P}_{kj} \| \right) < 0$) monotonically decreasing over time. The maximum error occurs when the first sample of the new distribution comes in the sliding window. Then the accuracy of PDF estimation improves as the sliding window includes more and more new samples from the new distribution after the PDF change occurs. Therefore, $\left(\| \sum_{j=1}^{n} \widetilde{P}_{(k+1)j} \| - \| \sum_{j=1}^{n} \widetilde{P}_{kj} \| \right) < 0$ holds.

Theorem 2 considers an ideal case where the PDF estimation error converge to zero. In realistic case, there is an irremovable bias due to the finite sliding window size. **Theorem 3** shows the UUB convergence of the regulation error in such a case.

Theorem 3: (UUB Stability of the Regulation Error). Given the initial conditions as the system state z_0 and system matrices A_{z0}, and B_{z0}, let $u_0(z_k)$ be an initial admissible control policy for the CPS (1). Let the control update law be given by (8) and if the disturbance induced by the irremovable bias of PDF estimation has a bound $\| d_{KDE} \|$ and $K_{min} < 1/b_{min}$ such that the regulation error of system states has an uniformly ultimate bounded convergence in the mean.

Proof

Consider the following positive definite Lyapunov function candidate: $V_{z_k} = z_K^T z_k$. z_k is the state vector of k. The corresponding estimated Lyapunov is $\widehat{V}_{z_k}$, therefore, $\Delta\widehat{V}_{z_k} = \widehat{V}_{z_{k+1}} - \widehat{V}_{z_k}$. Similar to proof of **Theorem 1**, we consider $\Delta\widehat{V}_{z_{km}} = \widehat{V}_{z_{(k+1)m}} - \widehat{V}_{z_k}$ for each possible system matrices (A_{zkm} and B_{zkm}). m represents one of the possible cases. If the maximum value of $\Delta\widehat{V}_{z_k m}$ is negative definite, the system convergence is proved. The irremovable bias of PDF estimation is considered the system state disturbance d_k bounded by d_M.

$$
\begin{aligned}
\Delta\widehat{V}_{z_k m} &= \widehat{V}_{z_{k+1} m} - \widehat{V}_{z_k m} \\
&= \| A_{zkm} - B_{zkm} K_k z_k + d_k \|^2 - \| z_k \|^2 \\
&= \underbrace{\left(\| A_{zkm} - B_{zkm} K_k z_k + d_k \| + \| z_k \| \right)}_{\Delta_2} \left(\| A_{zkm} - B_{zkm} K_k z_k + d_k \| - \| z_k \| \right) \\
&= \Delta_2 \left(\| A_{zkm} - B_{zkm} K_k z_k + d_k \| - \| z_k \| \right) \\
&\leq \Delta_2 \left(\| a_{max} - b_{min} K_{min} z_k + d_M \| - \| z_k \| \right) \\
&\leq \Delta_2 \left(a_{max} + b_{min} K_{min} \| z_k \| + \| d_M \| - \| z_k \| \right) \\
&\forall k = 1, 2, \cdots \\
&\forall m = 1, 2, \cdots, n_d
\end{aligned}
$$

where Δ_2 is positive definite, $b_{min} = min\{ \| B_{zk1} \|, \| B_{zk2} \|, \cdots, \| B_{zkm} \| \}$, $K_{min} = min\{ \| K_1 \|, \| K_2 \|, \cdots, \| K_{n_d} \| \}$.

Since $\widehat{V}_{z_k}$ is positive definite and $\Delta\widehat{V}_{K_k}$ is negative definite provided the system state $\| z_k \| \geq \frac{\|d_M\| + A_{max}}{1 - b_{min} K_{min}}$ and $K_{min} < 1/b_{min}$. Therefore, UUB stability of the regulation error is proved.

5. SIMULATIONS

In this section, the proposed PTSOC is evaluated and shown to be better than SOC Xu *et al.* (2012). The metrics of regulation performance are overshoot and convergence time when the delays of network randomly changes. Three scenarios A, B, C are simulated. In Case A, the delays satisfy the bound constrains Xu *et al.* (2012). It illustrates that PTSOC can obtain as good performance as that of SOC. Case B illustrates that the system performance are significantly improved by employing PTSOC, even though the bound changes over time due to network changes or cyber attacks. In realistic CPSs, topology variation and cyber attacks bring more dynamics and uncertainties to the embedded network and entire CPS.

Therefore, the bounds and constrains of delays made in ideal case are relaxed in Case C. This illustrates that PTSOC has a better performance in terms of overshoot, convergence time, and cost of regulation than that of the conventional SOC when the delay bound and PDF are time-varying.

Simulated benchmark example:

The simulations employ the continuous-time model of a batch reactor system Xu *et al.* (2012), Silverman (1986), Hurter *et al.* (2012) whose dynamic are given by:

$$\dot{x} = \begin{bmatrix} 1.38 & -0.2077 & 6.715 & -5.676 \\ -0.5814 & -4.29 & 0 & 0.675 \\ 1.067 & 4.273 & -6.654 & 5.893 \\ 0.048 & 4.273 & 1.343 & -2.104 \end{bmatrix} x + \begin{bmatrix} 0 & 0 \\ 5.679 & 0 \\ 1.136 & -3.146 \\ 1.136 & 0 \end{bmatrix} u \tag{9}$$

where $x \in \Re^{4\times1}$ and $u \in \Re^{2\times1}$

The parameters of this CPS are selected as a) the sampling time $T_s = 100ms$; b) $d = 2$, while the delays are not bounded. The continuous-time model is converted to a discrete time model with stochastic parameters representing network dynamics.

Case A: Bounded Random Delays with a Fixed PDF

PTSOC is evaluated for an ideal case with delays that satisfy the a priori set bound constrains of SOC Xu *et al.* (2012). The delays follow a normal distribution $d{\sim}N(0.15, 0.05^2)$. The upper bound is 0.2 sec. Overshoot, convergence time, and cost of regulation are the primary metrics to evaluate SOC and PTSOC. The tests are repeated 50 times for the statistical validation.

In Figs. 4, 5 and Table 2, the performance of SOC and PTSOC are compared. Both of these controllers make the errors converge. PTSOC presents an opposite improvement with high percentages but closed values. This illustrates that SOC is optimal when the bounds and distribution of delays are satisfied the assumed constraints. Similarly, a longer

convergence time of PTSOC is induced because the sliding window needs several iterations to converge the PDF estimation. Importantly, a significantly reduced cost by 92.1% is conspicuous. It demonstrates that PTSOC tuned by PDF of delays can optimize the trade-off between regulation error and cost. Overall, SOC and PTSOC have good and comparable performance when the delays are less than 0.2 sec.

Remark 4: Tuning the Q and R of PTSOC cost function can improve its performance in terms of overshoot and convergence time at the expense of a higher actuation cost. However, increasing the cost can lead to inefficient actuation and operating the actuators beyond its preferred range which leads to excessive wear and damages to actuators and the system.

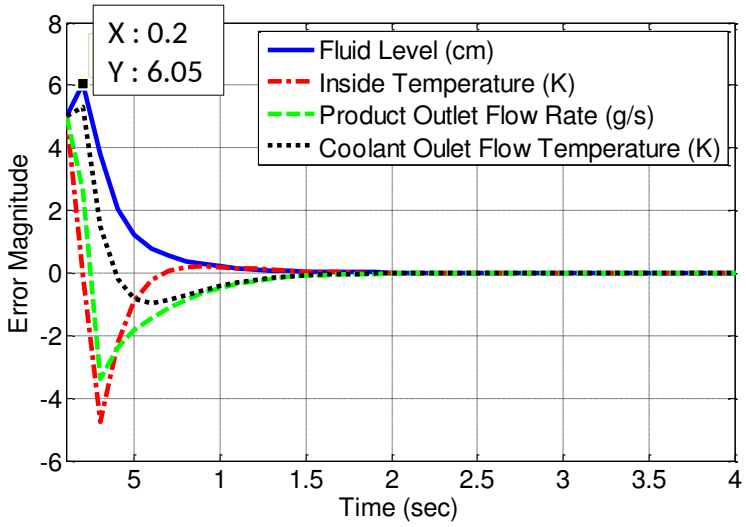


Figure 4. Case A: Performance evaluation of SOC (tracking errors)

Case B: Increased Random Delays with a Fixed PDF

In this case, the delays increase beyond the initially set bounds of SOC while maintaining a fixed PDF distribution $d \sim (0.3, 0.1^2)$. Such a case aims to demonstrate PTSOC still guarantee a good performance with delays with *an unknown bound*, while SOC performance degrades in terms of overshoot, convergence time, and the cost of regulation.

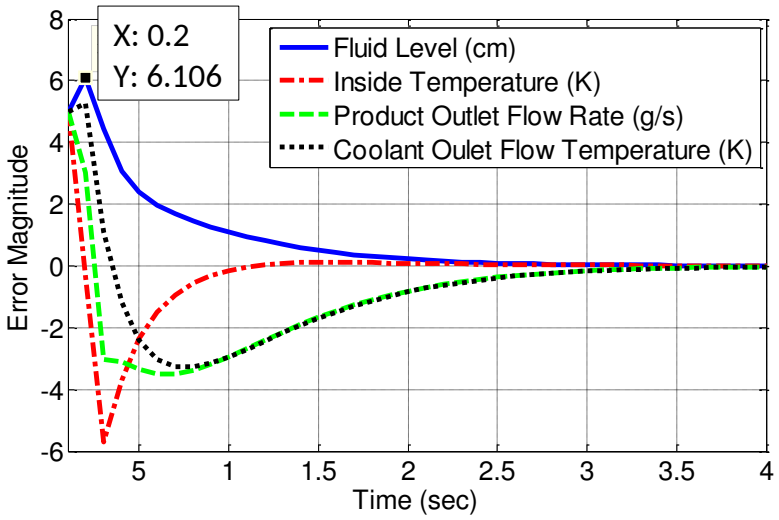


Figure 5. Case A: Performance evaluation of PTSOC (tracking errors)

The performance of SOC and PTSOC are presented in Figs. 6 and 7. PTSOC has a significant improved performance when compared with SOC, as shown in Table 3. Its overshoot is reduced at least by 36.4%. The convergence time is reduced by 7.1%. Moreover, the cost of regulation is reduced by 94.9% thus the control inputs implemented by the actuators are within their preferred ranges. Such that the physical components are prevented from excessive wear and damages. Overall, SOC no longer guarantees the stability if the delay is over its upper bound. In contrast, PTSOC uses PDF information to tune the control law such that the performance and stability of the entire CPS is guaranteed.

Remark 5: In this case, the initial conditions are same as that in Case A. The initial control law of SOC is pre-tuned for the smaller delay bound. Consequently, SOC control law is selected inappropriately for the case with longer delays. Hence, for the first second, the system states have large deviations and overshoots as shown in Fig. 6. Over time, SOC updates the system model and allows it to converge. In contrast, PTSOC can tune its control laws based on both dynamic model changes and the drift of PDF of delays. Such that PTSOC quicker adapts to the uncertainties on system model and network delay.

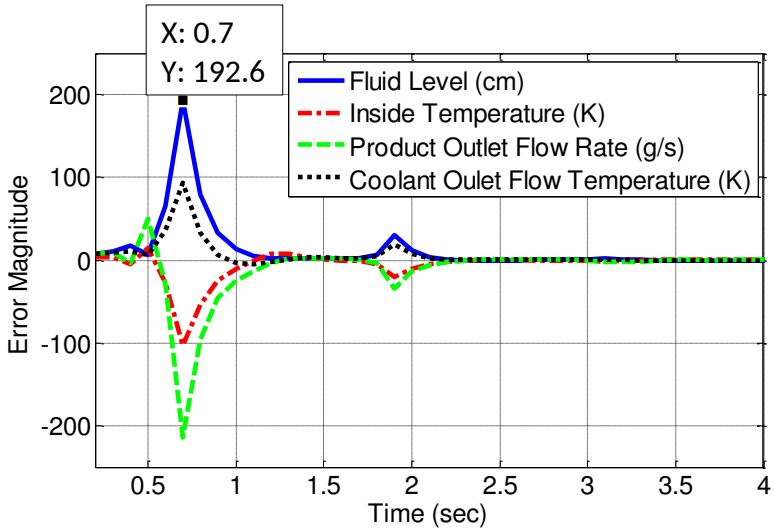


Figure 6. Case B: Performance of SOC (tracking errors)

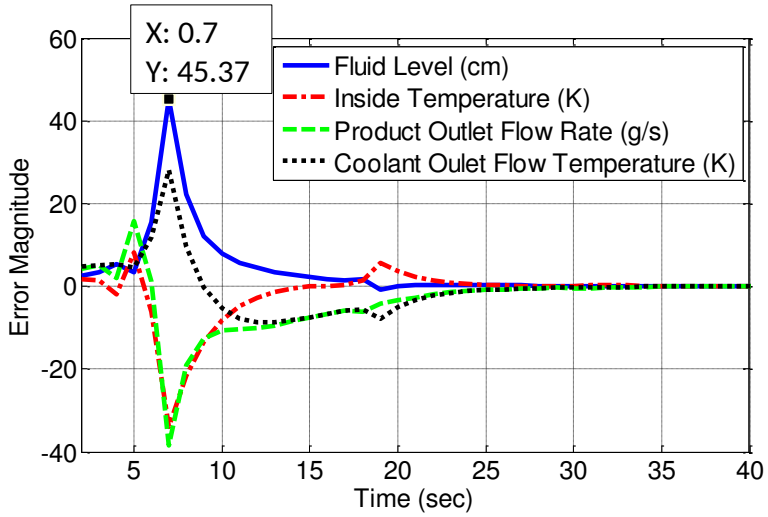


Figure 7. Case B: Performance of PTSOC (tracking errors)

Table 2. Performance comparison (statistical average values for 50 times tests)

Performance Metrics		SOC	PTSOC	Improvements(Ave (min,max)) ((SOC-PTSOC)/SOC)(%)
Overshoot	Fluid Level (cm)	9.1	9.3	-1.5% (-3.6%, -0.2%)
	Inside Temperature (K)	8.6	9.7	-14.9% (-41.7%, -0.1%)
	Product Outlet Flow Rate (g/s)	9.8	9.9	-3.3% (-20.2%, 7.6%)
	Coolant Outlet Flow Temperature (K)	7.3	8.2	-12.0% (-42.9%, 1.4%)
Convergence Time (s)		3.7	4.0	-40.4% (-55.6%, 7.8%)
Cost of the first 20 sec		28531.3	2248.4	92.1% (91.4%, 93.2%)

Table 3. Performance comparison (statistical average values for 50 times tests)

Performance Metrics		SOC	PTSOC	Improvements(Ave (min,max)) ((SOC-PTSOC)/SOC)(%)
Overshoot	Fluid Level (cm)	101.6	42.6	55.6% (10.5%, 83.0%)
	Inside Temperature (K)	54	32	36.4 (-26.1%, 67.0%)
	Product Outlet Flow Rate (g/s)	133.4	53.7	52.4% (15.2%, 86.3%)
	Coolant Outlet Flow Temperature (K)	48.9	25.1	42.7% (-6.6%, 72.1%)
Convergence Time (s)		4.2	3.9	7.1% (-34.4%, 31.3%)
Cost of the first 20 sec		154530.1	7891.4	94.9% (94.2%, 95.7%)

Case C: High Variation Delay with Time-varying PDF

Next, the distribution of delays is allowed to change over time. First, it follows a normal distribution with $0.45sec$ mean value. Then, the mean value jumps to $0.2sec$ at randomly selected time within $[40s, 50s]$. The simulations are repeated to obtain statistically valid comparisons. The results firmly indicate that tracking of PDF changes is critical in both system modeling and optimal controller design.

Fig. 8 shows one specific case when the distribution changed at time $47sec$. The parameters $Q_z = 0.15 \times I^{8\times 8}$ and $R_z = I$ are set for the SOC. The simulations show that the controller can make the regulation error converge. However, the errors increase right after the change in PDF of delays. Additionally, the input command to actuator increases. Such large inputs often exceed the preferred operating range for actuators thus increasing wear and tear or saturating actuator response.

In Fig. 9, the performance of PTSOC is presented. PTSOC convergence is sped up by using the updated PDF information. Hence, a shorter convergence time and a lower cost of regulation (Table. 4) are observed.

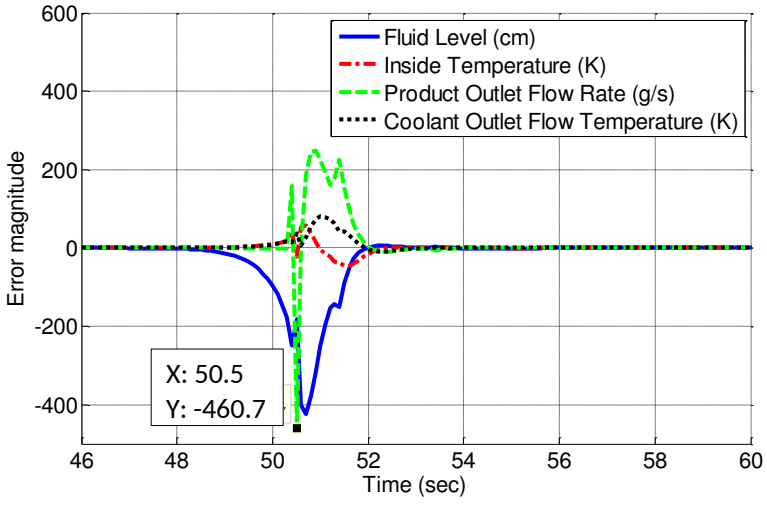


Figure 8. Case C: Performance of SOC (tracking errors) for delay change at 47 sec

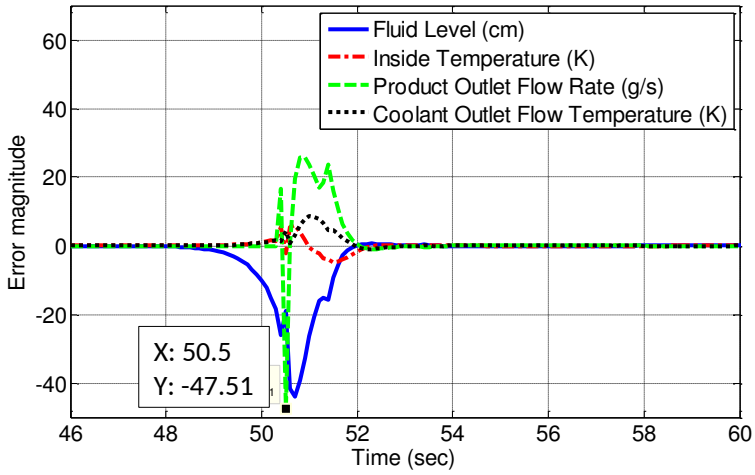


Figure 9. Case C: Performance of PTSOC (tracking errors) for delay change at 47 sec

Overall, SOC makes the error converge with a significant overshoot and a high actuation cost. Instead, the overshoot and cost of PTSOC are significantly reduced by several orders of magnitude. Table. 4 shows the average value for 50 simulations. As the weights of each control input are updated continuously in terms of cost function, PTSOC has a better performance on overshoot (reduced by 80%) and cost of regulation (reduced by 96.1%). A cost function with the optimal parameters (Q and R) selection not only guarantees that Algebraic Riccati equation (ARE) has a finite solution, but also reduces the control input cost. The convergence time of PTSOC is improved by 17.3%. Overall, PTSOC significantly improves the system performance in terms of overshoot, convergence time, and cost for every simulated scenario. Therefore, PTSOC indeed strengthens the resilience of the entire CPS.

Remark 6: In this case, the delay PDF is kept constant for at least 40 seconds to allow both PTSOC and SOC to achieve initial convergence. With such "pre-training" process, the physical system model (1) is accurately tuned. When the change of PDF occurs, only the network dynamic terms in the model (2) are updated. Thus, both SOC and PTSOC perform better on overshoots than that for Case B (Table. 3).

Table 4. Performance comparison (statistical average values for 50 times tests)

Performance Metrics		SOC	PTSOC	Improvements(Ave (min,max)) ((SOC-PTSOC)/SOC))
Overshoot	Fluid Level (cm)	187.7	34.0	82.0 % (80.6%, 85.7%)
	Inside Temperature (K)	26.1	4.8	81.7% (80.5%, 85.6%)
	Product Outlet Flow Rate (g/s)	111.9	37.6	66.4 % (62.6%, 73.4%)
	Coolant Outlet Flow Temperature (K)	36.3	6.7	81.4 % (80.1%, 85.3%)
Convergence Time (s)		9.4	7.8	17.3% (5.3%, 22.8%)
Cost after distribution changes		208299.5	8191.4	96.1% (95.9%, 96.2%)

6. CONCLUSIONS

In this work, PTSOC is proposed to address uncertainties of the embedded cyberspace, particularly delays with an unknown bound and time-varying distribution. The simulation results show that PTSOC has a reduced overshoot (by about 80%), convergence time (by 17.3%), and cost of regulation (by 96%) over that of the SOC. Continuous update of the probability weights speeds up convergence, optimizes control input selection, and make control law adapt to delays with unknown bound and time-varying distribution. It facilitates the trade-off between system states and cost of regulation. Additionally, the constrains of known bound of delays and fixed distribution in existing works are relaxed. Overall, reliability of CPSs in terms of resilience are improved.

REFERENCES

Blundell, R. and Duncan, A., 'Kernel regression in empirical microeconomics,' Journal of Human Resources, 1998, pp. 62–87.

Bors, A. G. and Nasios, N., 'Kernel bandwidth estimation for nonparametric modeling,' IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 2009, **39**(6), pp. 1543–1555.

Calabrese, R. and Zenga, M., 'Bank loan recovery rates: Measuring and nonparametric density estimation,' Journal of Banking & Finance, 2010, **34**(5), pp. 903–911.

Carnevale, D., Teel, A. R., and Nesic, D., 'A lyapunov proof of an improved maximum allowable transfer interval for networked control systems,' IEEE Transactions on Automatic Control, 2007, **52**(5), pp. 892–897.

Chen, X., Tharmarasa, R., Kirubarajan, T., and McDonald, M., 'Online clutter estimation using a gaussian kernel density estimator for multitarget tracking,' IET Radar, Sonar & Navigation, 2014, **9**(1), pp. 1–9.

Elgammal, A., Duraiswami, R., and Davis, L. S., 'Efficient kernel density estimation using the fast gauss transform with applications to color modeling and tracking,' IEEE transactions on pattern analysis and machine intelligence, 2003, **25**(11), pp. 1499–1504.

Gao, H. and Chen, T., 'Network-based $h\infty$ output tracking control,' IEEE Transactions on Automatic control, 2008, **53**(3), pp. 655–667.

Gao, H., Meng, X., and Chen, T., 'Stabilization of networked control systems with a new delay characterization,' IEEE Transactions on Automatic Control, 2008, **53**(9), pp. 2142–2148.

Gisbert, F. J. G., 'Weighted samples, kernel density estimators and convergence,' Empirical Economics, 2003, **28**(2), pp. 335–351.

Hao, F. and Zhao, X., 'Linear matrix inequality approach to static output-feedback stabilisation of discrete-time networked control systems,' IET control theory & applications, 2010, **4**(7), pp. 1211–1221.

He, Y., Mao, Y., Chen, W., and Chen, Y., 'Nonlinear metric learning with kernel density estimation,' IEEE Transactions on Knowledge and Data Engineering, 2015, **27**(6), pp. 1602–1614.

Hurter, C., Ersoy, O., and Telea, A., 'Graph bundling by kernel density estimation,' in 'Computer Graphics Forum,' volume 31, Wiley Online Library, 2012 pp. 865–874.

Lee, K. C., Lee, S., and Lee, M. H., 'Qos-based remote control of networked control systems via profibus token passing protocol,' IEEE Transactions on Industrial Informatics, 2005, **1**(3), pp. 183–191.

Liu, G.-P., Xia, Y., Rees, D., and Hu, W., 'Design and stability criteria of networked predictive control systems with random network delay in the feedback channel,' IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 2007, **37**(2), pp. 173–184.

Mitchell, R. and Chen, R., 'Modeling and analysis of attacks and counter defense mechanisms for cyber physical systems,' IEEE Transactions on Reliability, 2016, **65**(1), pp. 350–358.

Silverman, B. W., *Density estimation for statistics and data analysis*, volume 26, CRC press, 1986.

Tian, E., Yue, D., and Peng, C., 'Reliable control for networked control systems with probabilistic sensors and actuators faults,' IET Control Theory & Applications, 2010, **4**(8), pp. 1478–1488.

Tiberi, U., Fischione, C., Johansson, K. H., and Di Benedetto, M. D., 'Energy-efficient sampling of networked control systems over ieee 802.15. 4 wireless networks,' Automatica, 2013, **49**(3), pp. 712–724.

Xie, S., Low, K. S., and Gunawan, E., 'An adaptive tuning algorithm for ieee 802.15. 4-based network control system,' in 'Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2014 IEEE Ninth International Conference on,' IEEE, 2014 pp. 1–6.

Xu, H., Jagannathan, S., and Lewis, F. L., 'Stochastic optimal control of unknown linear networked control system in the presence of random delays and packet losses,' Automatica, 2012, **48**(6), pp. 1017–1030.

III. A NOVEL CYBER NETWORK FAULT DIAGNOSIS SCHEME FOR CYBER-PHYSICAL SYSTEMS

Shanshan Bi, Maciej Zawodniok

Department of Electrical & Computer Engineering

Missouri University of Science and Technology

Rolla, Missouri 65409–0050

Tel: 573–341–6622, Fax: 573–341–4115

Email: sbn65@mst.edu

ABSTRACT

Cyber-physical systems (CPSs) consists of a network, computation, and physical process. Embedded networks, which deliver control and sensing signal, can potentially affect CPSs performance. However, the degradation of physical system performance caused by the embedded networks is frequently oversimplified with strong assumptions. The proposed scheme effectively relaxes those assumptions in the existing works, that network delays are bounded in a specific range or its distribution is time invariant. Most of the existing works on fault diagnosis and prognosis addressed the physical system fault detection and isolation, and ignore cyber network faults. A novel cyber network fault prognosis scheme is proposed to detect and isolate cyber and physical device faults, then forecast the effects of cyber network faults on the performance of CPSs, and finally trigger resilience controller at an appropriate time to minimize the computational overhead. Thus, it can guarantee the stability of the entire CPS and substantially reduce computational overhead of the resilience control by triggering it if necessary.

Keywords: cyber physical system, fault prognosis, network fault, resilience

1. INTRODUCTION

Cyber-physical system (CPS) refers to a new generation of systems with integrated computation and physical capability that can interact with humans through many new modalities. As the increasing interdependence between cyber and physical subsystems, capturing the interrelationship between cyberspace and physical system becomes important Fisher *et al.* (2014). The dynamic changes in cyberspace, which are induced by stochastic channel fading, random traffics, and malicious attacks, affect the physical system states. Such connectivity is often oversimplified when designing high resilience CPS, resulting in severe system failures. In this work, we address detecting cyber network faults and mitigate its negative effects on the physical systems with the proposed resilience controller. For example, self-driving cars have a large number of radars, cameras, and other various electrical components (known as electronic control units, or ECUs) connected via an internal network. If hackers manage to gain access to a vulnerable, peripheral ECU (the Bluetooth or infotainment system) from there, they may be able to take control of safety critical ECUs like its brakes or engine and wreak havoc. Falsifying the control commands – for instance, an acceleration command is replaced by a stop one – definitely threaten users' lives. Therefore, cyber failures that possibly propagate to physical world has to be detected, isolated, and mitigated timely to avoid catastrophe failures.

In the past few years, many control and system researchers have pioneered the development of approaches and tools to model and control CPSs. Liu and Yao (2005) - Zhang-qing and Xian-zhong (2007) addressed the fault detection, isolation, and mitigation in the physical subsystem alone (e.g. actuators, sensors, and controlled components). They assumed the network performs well and satisfies their priori assumptions. Therefore, the interactions between cyberspace and physical world are ignored or simplified.

At the same time, communication and signal process researchers have made major breakthroughs in monitoring, identification, and defense of cyber attacks and other security issues on the cyber side Gamage *et al.* (2010) - Pasqualetti *et al.* (2013). Such existing ap-

proaches focus on either cyber or physical control aspects while ignoring or oversimplifying the other aspect. However, such decoupling designs will fail in practical CPS. Therefore, system control and fault prognosis must be redesigned to take full account of the interaction between cyberspace and physical systems.

Inspired by this motivation, we proposed a novel diagnosis scheme in this work. The main contributions are listed as following:

a) The proposed diagnosis scheme can timely detect the cyber network fault only based on the measured delays.

b) A fault isolation scheme is proposed to distinguish cyber network and physical system faults.

c) A resilience control triggering strategy is investigated to activate the resilience control ahead of resulting in the degradation on system performance.

The rest paper is organized as following. In Section. 2, the motivation is discussed. An example is given to illustrate the interdependence between cyberspace and physical system behavior. Next, the related works on fault diagnosis and prognosis for cyber-physical systems (CPSs) or networked control systems (NCSs) are presented in Section. 3. In Section. 4, the proposed prognosis scheme is demonstrated. The simulation results are shown in Section. 5 and the conclusions are given in Section. 6.

2. MOTIVATION

CPSs are characterized by integrating cyber and physical systems. The performance of embedded cybers significantly affect CPSs performance and vice versa. However, such an interaction between physical system behavior and network performance tends to be oversimplified by researchers. The conventional diagnosis and prognosis methods Liu and Yao (2005) - Zhang-qing and Xian-zhong (2007) are wildly used in physical system faults detection and prediction. Similarly, the existing cyber attacks detection and defense

approaches Gamage *et al.* (2010) - Pasqualetti *et al.* (2013) only addressed the security issues on the cyber/network side without considering the severe consequence of the physical system.

To address the cyber network fault issues, a full knowledge of the interactions between cyber dynamics and system performance is crucial for the first step. Next, a scheme should be proposed for detecting and isolating cyber network and physical system fault. At last, a resilience controller should be applied before physical system failure. Because resilience controller consumes a lot of computing capacity and resources, it should not always be applied when a simple controller can achieve the required physical system performance. Therefore, the novel diagnosis scheme should accurately make the decision for triggering the resilience control at an appropriate time. Such that unnecessary computational overhead is effectively reduced.

An example is given to illustrate the relation between cyber uncertainties and system behavior.

This example simulates a route hijacking by an attacker to eavesdrop control information. Such an attack increases delay and delay variation when the attacker secretly relays and possibly alters the communication between the controller and actuators. A network is simulated using Network Simulator 2 (NS2) with a random topology of 11 nodes. Ad hoc On-Demand Distance Vector (AODV) routing scheme is adopted. The route through the topology is altered because the attacker node relays the transmission such that the packet delays vary for the controller loop, as shown in Fig. 1. Note, that similar network performance could be a result of topology or traffic pattern changes. A feedback loop with the simulated delays employs an optimal controller to regulate a two input four output (2I4O) system.

The results show the disturbance in CPS introduced by the network dynamics. With these delays, a PID controller is simulated for a simple 2I4O (two input four output) system Xu *et al.* (2012). Fig. 2 shows that the sudden change of delay at $k = 6s$ makes the system states vibrate. Consequently, the CPS becomes unstable when the original non-networked PID controlled performed fine.

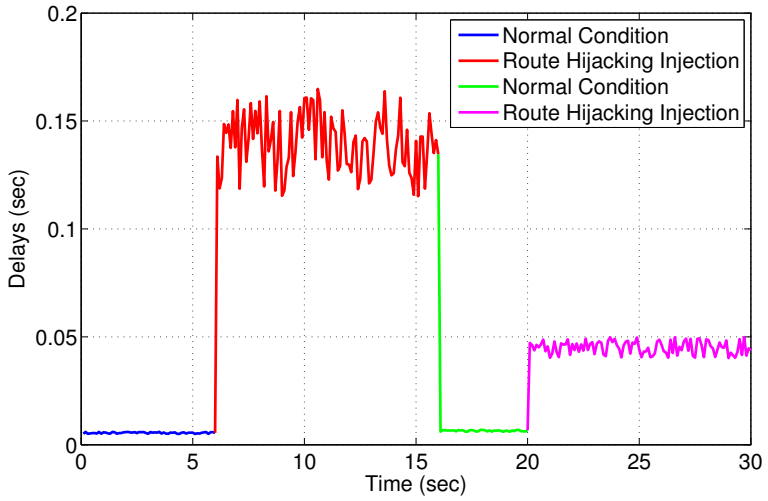


Figure 1. Delays of the simulated network

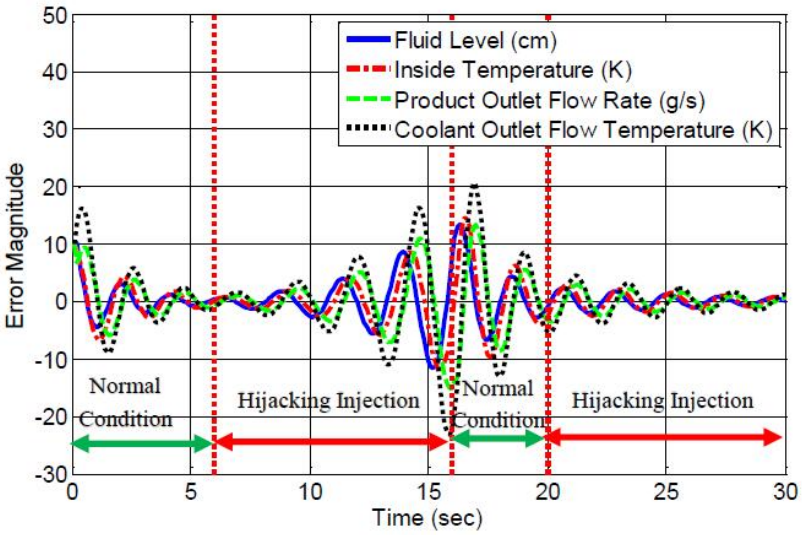


Figure 2. System performance with a PID controller

It is concluded that stochastic cyber attacks indeed affect the system performance. Cyberspace is particularly difficult to secure due to its vulnerabilities of linkages between cyber and physical systems. Of growing concern is the cyber threat to critical hardware devices. Cyber attacks could cause harm or disrupt services upon which our economy and the daily lives depend on. In light of the risk and potential consequences of cyber events, strengthening the risk awareness and resilience of CPSs has become an important mission.

3. RELATED WORKS

In this section, we first discuss the existing works on cyber security issues. Next, the works on fault diagnosis issues of the physical system are discussed.

The overall goals of cyber security include integrity (the trustworthiness of data or resources), availability (accessibility upon demand), and confidentiality (keeping information secret from unauthorized users). Many researchers addressed these issues with different technologies, such as authentication schemes, access control, and other defense scheme Gamage *et al.* (2010) - Pasqualetti *et al.* (2013). An assumption that the adversary/attack model is fully known is often required; however, it is challenging to get. Gamage *et al.* (2010) proposed a general theory of event compensation as an information flow security enforcement mechanism for CPSs. Message scheduling methods were given to improve the security quality of wireless networks for mission-critical CPSs in Jiang *et al.* (2010). In Amin *et al.* (2009), deception and denial of service attacks had been addressed by a countermeasure based on semi-definite programming. False data injection attacks against static state estimator are studied in Liu *et al.* (2011). In a similar fashion, stealthy deception attacks against the Supervisory Control (SC) and Data Acquisition system (DAS), replay attacks, and covert attacks against control systems were investigated in Teixeira *et al.* (2010), Mo and Sinopoli (2009), and Smith (2011) respectively. With respect to the above works, Pasqualetti *et al.* (2013) proposed a mathematical framework for CPSs, attacks, and monitors, and given the fundamental limitations of monitors from system-theoretic

and graph-theoretic perspectives. Finally, centralized and distributed attack detection and identification monitors were designed. Overall, many cyber attacks can be addressed on the cyber side. However, the effects of cyber attacks/faults on the physical system behavior are oversimplified in the above mentioned existing works. Moreover, the injection time and model of the attacks/faults are difficult to learn ahead of time in practical CPSs.

The control researchers focused on the conventional fault detection techniques that have successfully applied to industrial networked control systems (NCSs). They indeed considered the network delay and packet loss in various ways. In Liu and Yao (2005), network delays were modeled as a constant delay (time buffer), an independent random delay, and a delay with known probability distribution governed by the Markov chain model. In Liu *et al.* (2007), a networked predictive controller in the presence of random delay in both forward and feedback channels was proposed to minimized the effects of network failures. However, they assumed the boundary condition of delays was alway satisfied. A robust H_∞ control for a nonlinear T-S fuzzy model system was proposed to address the network delays and packet drop in Zhang *et al.* (2007). Wang *et al.* (2008) and Zhang-qing and Xian-zhong (2007) employed a state observer-based fault detection method on the uncertain long time delay. Although, the network delays and packet drop caused by network faults/failures were considered in above works, the assumptions, such as known bounds and time-invariant distribution of delays and packet loss, are always made. Such assumptions probably result in the entire system failure when the unexpected issues invalidate the assumptions. In addition, most of the above works aimed to detect the faults of physical components (sensors, actuators, and system plant), not the faults in the cyberspace.

This work is motivated to address cyber network faults detection and isolation. Meanwhile, the tolerant control schemes for cyber faults mitigation is designed.

4. CYBER FAULT DIAGNOSIS SCHEME

In this section, the overview of the proposed cyber fault diagnosis scheme is given in Section.4.1. The PDF monitoring based observer for cyber fault detection is introduced in Section.4.2. Then, the isolation of cyber and physical system fault is demonstrated in Section. 4.3. At last the resilience controller is designed in Section. 4.4.

4.1. Overview

In this work, two observers for cyber and physical system fault detection are designed respectively. The main idea of cyber fault detection (CFD) is designing a PDF identifier to capture the distribution variation of network delays. Another observer which supervises the physical system behavior in a real time manner can capture the physical system fault by pre-setting the residual for each controlled system state, which is called physical fault detection (PFD). The frame of the proposed diagnosis scheme is shown in Fig. 3.

The plant we applied in this work is a multi-input-multi-output (MIMO) stochastic model (2), which includes uncertainties (delays and packet loss) in cyber network. Such a model can be derived from the conventional discrete time model (1).

The conventional discrete time model was described as following Blundell and Duncan (1998):

$$\begin{aligned} x_{k+1} &= A_s x_k + B_0^k u_k^a + B_1^k u_{k-1}^a + \ldots + B_d^k u_{k-d}^a \\ u_{k-i}^a &= \gamma_{k-i} u_{k-i} \end{aligned} \tag{1}$$

where $x_k = x(kT)$ denotes system states; $A_s = e^{AT}$, $B_0^k = \int_{d_0^k}^{T_s} e^{A(T_s-t)}dt$, and $B_i^k = \int_{d_i^k - iT_s}^{d_{i-1}^k - (i-1)T_s} e^{A(T_s-t)}dt \ \forall i = 1, 2, ..., d$ are the system matrices. T_s is sampling interval. A is the system matrix of the continuous-time model.

Xu Xu *et al.* (2012) derived the stochastic model expressed as

$$z_{k+1} = A_{zk} z_k + B_{zk} u_k \tag{2}$$

where

$$A_{zk} = \begin{bmatrix} A_s & \gamma_1^k B_1^k & \cdots & \gamma_i^k B_i^k & \cdots & \gamma_d^k B_d^k \\ 0 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & I_m & \cdots & \cdots & 0 & 0 \\ \vdots & 0 & I_m & \cdots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & \cdots & I_m & 0 \end{bmatrix}, B_{zk} = \begin{bmatrix} \gamma_0^k B_0^k & I_m & 0 & 0 & \cdots & 0 \end{bmatrix}^T$$

$z_k = [x_k^T \; u_{k-1}^T \; \cdots \; u_{k-d}^T]^T$ is the state variables vector; A_{zk} and B_{zk} are is the time-varying system matrices; A_s and B_i^k are the system matrices calculated by (1). u_k is the control input; γ_i^k and γ_{k-i} are binary random variables representing the package reception status (if the package is received, $\gamma = 1$, otherwise, $\gamma = 0$). I_m is an identity matrix.

Such stochastic model includes the dynamics both of cyber network and physical systems. Thus, any uncertainties, changes, and faults can be observable by monitoring the outputs of this model.

4.2. Fault Detection

In this subsection, cyber fault detection are proposed first. Then, a observer-based physical system fault detection is introduced.

4.2.1. Cyber Fault Detection (CFD). For cyber fault detection, we proposed an online PDF identifier to capture the variation of delay and its distribution. We assume that the PDF profile of healthy delays is known as well as the expected value. A residual of the expected value is user designed.

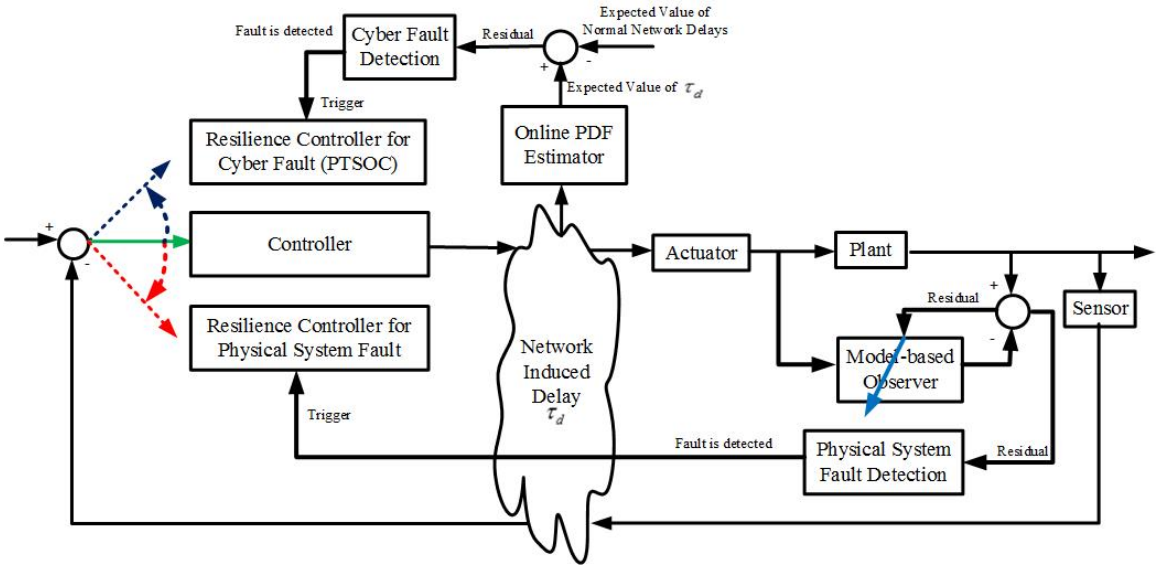


Figure 3. Frame of the proposed diagnosis scheme

The proposed fault detection includes three main steps that are continuous repeated:

a) Data collection of delays. n delays ($[d_{k-n+1}, \cdots, d_k]$) in the sliding window are used to do the PDF estimation of time k (PDF_k). The probability for each delay interval is calculated. When the new delay comes in the window at time $k+1$, the PDF is updated.

b) PDF estimation. The distribution of these n delays is obtained by using an online KDE-based PDF identifier. The main steps are shown in Table. 1. Here, a normal kernel smoother is selected for PDF estimation.

As updating the delays in the sliding window for each sampling interval, the PDF information is updated for given network situation.

Delays are divided into n_d groups based on their values. The probability for each delay group and the expected value are calculated.

c) Decision making. If the variation of the expected value exceeds the presetted residual, the cyber network fault is detected.

4.2.2. Physical System Fault Detection (PFD). An standard observer based physical system fault detection (PFD) Liang and Du (2007) is needed.

Table 1. Online PDF identification algorithm

1. Determining the data in the sliding window for time k:
   a) Choosing a kernel function K centered on x with a bandwidth h;
   b) Each observation x_i receives a specific weight proportional to the scaled distance from the observation x_i to x, which is $u = (x - x_i)/h$;
   c) At a given x, the estimate is found by vertically summing up over the k shapes.
      This can be synthesized as:
      $\widehat{f}(x) = \frac{1}{nh} x_i \in [x - \frac{h}{2}, x + \frac{h}{2}]$
      The general formula for KDE will be given by
      $\widehat{f_k}(x) = \frac{1}{nh} \sum_{i=1}^{n} K(\frac{x - x_i}{h})$
      where the dependence of the estimate on the kernel function $K(.)$ is denoted as $\widehat{f_k}$.
2. Updating the new data for time $k + 1$ in the sliding window and go back to Step 1;

Consider

$$\dot{x} = Ax + Bu, y = Cx + Du \tag{3}$$

where A, B, C, D are system matrices of appropriate dimensions. The faults are often modelled by extending (3)

$$\dot{x} = Ax + Bu + E_w w, y = Cx + Du + F_w w \tag{4}$$

where w represents the fault vector and E_w, F_w are known matrices of appropriate dimensions.

By means of a full-order observer described by

$$\dot{\widehat{x}} = A\widehat{x} + Bu + Lr, r = y - \widehat{y}, \widehat{y} = C\widehat{x} + Du \tag{5}$$

the estimate of system output is provided, which is further used to construct the residual vector $y - \widehat{y}$. The observer (5) is also called fault detection filter (FDF) with L being the gain matrix which makes the FDF stable and residual signal $r(t)$ satisfies

$$\forall u(t), x(0), \lim_{t\to\infty} r(t) = 0 \tag{6}$$

a norm of $r(t)$, typically $\mathcal{L}_2$- or $\mathcal{L}_\infty$- norm, is adopted as residual evaluation function, which is defined by

$$J = \|r(t)\| or J = \|r(t)\|_\infty \tag{7}$$

Let $J_{th} = sup_{x0,w=0} J$ be the threshold, which is interpreted as the maximum influence of $x(0) = x_0$ on the fault-free ($w(t) = 0$) residual vector $r(t)$. A simple form of detection logic is

$$\begin{cases} J > J_{th} & faulty \\ J \leq J_{th} & fault - free \end{cases} \tag{8}$$

4.3. Fault Isolation

When designing the proposed fault diagnosis scheme, CFD and PFD supervise the states of cyberspace and physical systems in real-time. Thus, the root-cause of the abnormality happening in cyber-physical system can be timely captured and accurately isolated. The primary isolation logic is illustrated in Fig. 4.

For the fault isolation, three residuals have to be monitored in an online manner:

Expected Value Residual (EVR): It is the difference of the expected value of delays at k and the last interval $k-1$ ($EVR(k) = EV(k) - EV(k-1)$). Such information is provided by the proposed PDF identifier. The corresponding threshold T_{EVR} is customizable by the users for satisfying the requirement of fault awareness capability. If $EVR(k) > T_{EVR}$, the cyber fault is detected.

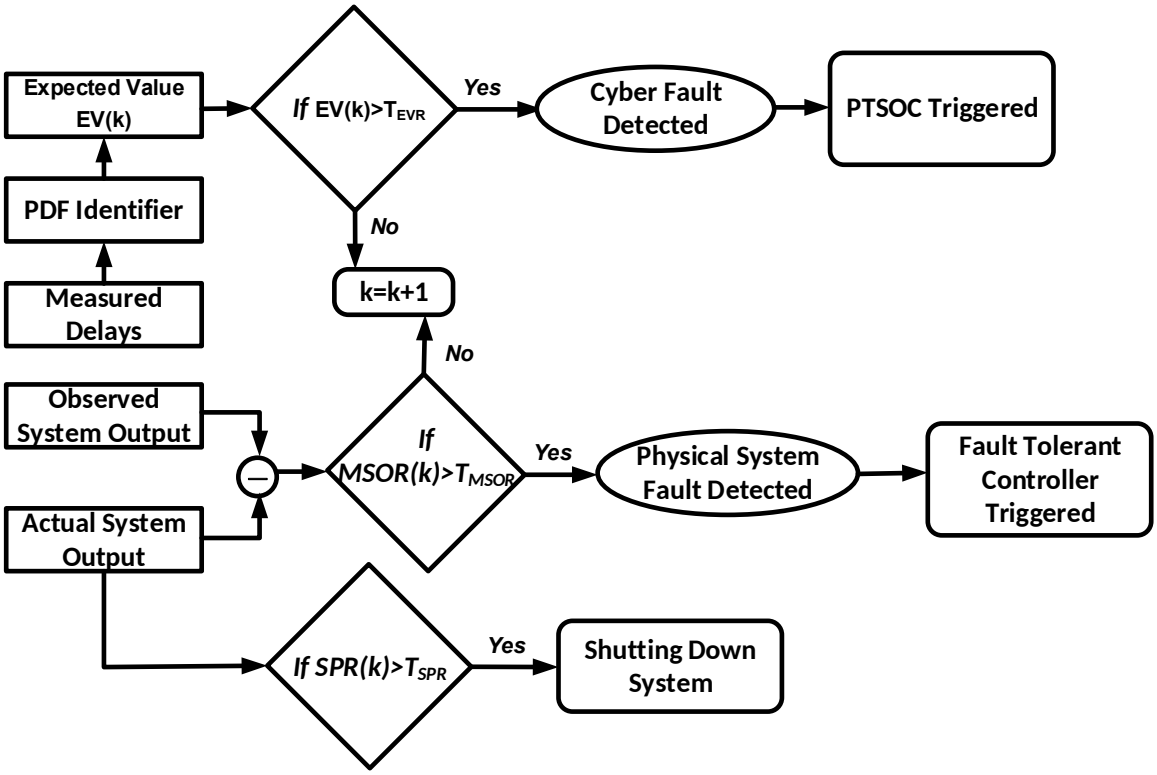


Figure 4. Fault isolation logic

Modeled system output residual ($MSOR$): It is provided by the PFD observer, which is the difference of outputs of modeled and that of actual systems: $MSOR = x(k) - \hat{x}(k)$. The corresponding threshold T_{MSOR} is selected to detect physical system faults. If $MSOR > T_{MSOR}$, the physical system fault is detected.

System performance residual (SPR): It is the difference between actual and desired system outputs: $SPR = x_d(k) - x(k)$. The threshold for each system output variable T_{SPR} is determined by the saturation of physical components. This residual is used to evaluate the system performance and determine when the system should shut down.

Also, the resilience scheme for two types of fault are different and proposed in next subsection.

4.4. Fault Tolerant Control

In this section, we proposed a resilience controller for cyber network fault mitigation. The triggering strategy is also given. The Lyapunove-based stability analysis is used to prove the convergence of the proposed controller. In addition, we briefly introduce the physical system fault tolerant control.

4.4.1. The Resilience Control for Cyber Faults. A PDF-based tuning of stochastic optimal controller (PTSOC) is designed to mitigate the adverse effects induced by the uncertainties of cyberspace and adapt to the random occurrence of cyber faults. Its control law considers the PDF of delays by optimizing a weighted summation of cost functions of different delay ranges (9). Each weight is the probability of its corresponding delay intervals from the PDF identifier.

$$J^k = E\left[\sum_{i=1}^{n} P_i J_i^k\right] = E\left[\sum_{i=1}^{n} P_i (x_i^{kT} Q_{zi} x_i^k + u_i^{kT} R_{zi} u_i^k)\right] \tag{9}$$

where i presents the delay interval ($d_{int} i < d^k < d_{int}(i+1)$); n is the total number of delay cases; k represents sampling interval; P_i is probability of delay within $d_{int} i$ to $d_{int}(i+1)$ provided by the PDF identifier; x_i is the states vector; u_i is the control inputs vector; $Q_{zi} = diag[Q_i, \frac{R_i}{d}, ...]$ and $R_{zi} = \frac{R_i}{d}$ are symmetric positive semi-definite and symmetric positive definite respectively. $E[\bullet]$ is the expectation operator.

By optimizing (9), the control input is given by:

$$u(k) = -K(k)Z(k) \tag{10}$$

$$\begin{aligned} K(k) = \sum_{i=1}^{n_d} & P_i(k)(B_{zi}(k)^T Z_i(k) B_{zi}(k) + R_z(k))^{-1} \\ & (B_{zi}(k)^T Z_i(k) A_{zi}(k) + S_{zi}(k)) \end{aligned} \tag{11}$$

where $K(k)$ is the optimal gain and $u(k)$ is the control input; $S_{zi}(k) \geq 0$ is the solution of the algebraic riccati equation (ARE) equation; $n_d = d_{upper}/d_{int}$, d_{upper} is the maximum delay in the sliding window; $P_i(k)$ is the probability of $d_{int}i < d(k) < d_{int}(i+1)$.

Remark 1: The Q_i and R_i in the cost function for each delay range should be different because each pair of Q_i and R_i should be the optimal values for the delays bounded in a specific range. They cannot guarantee a high level with the delays out of such boundaries.

The stability analysis is presented in Appendix A.0.1.

4.4.2. The Tolerant Control for Physical System Faults. Many existing works have addressed fault tolerant control design. Here, we adopt a traditional fault tolerant control (FTC) proposed in Yang *et al.* (2009).

5. SIMULATIONS

In this section, the proposed diagnosis scheme is evaluated by simulations in MATLAB. The resilience controller in Section. 4.4.1 is applied. A conventional stochastic optimal control Xu *et al.* (2012) is employed as a reference.

A continuous-time batch reactor system is taken as a case study. Its dynamics are given by Xu *et al.* (2012).

$$\dot{x} = \begin{bmatrix} 1.38 & -0.2077 & 6.715 & -5.676 \\ -0.5814 & -4.29 & 0 & 0.675 \\ 1.067 & 4.273 & -6.654 & 5.893 \\ 0.048 & 4.273 & 1.343 & -2.104 \end{bmatrix} x + \begin{bmatrix} 0 & 0 \\ 5.679 & 0 \\ 1.136 & -3.146 \\ 1.136 & 0 \end{bmatrix} u \tag{12}$$

The parameters of this CPS are selected as:

a) The sampling time is $100ms$;

b) The considered delays in the system model is less than 2 sampling interval, $d = 2$;

c) $d_{int} = 0.1s$;

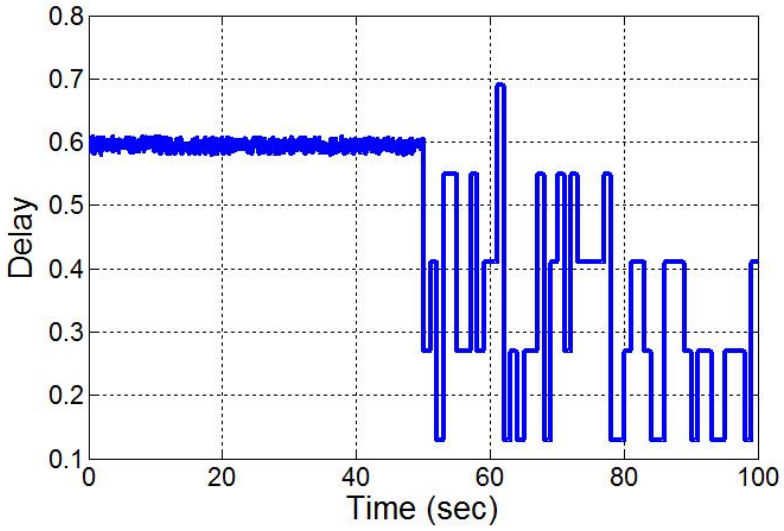


Figure 5. The simulated delays

The delays before $47s$ follows a normal distribution $(0.5, 0.05^2)$. The data number M in the sliding window is 30. By using kernel density estimation (KDE) to analyze these delays, a PDF profile for the "healthy" operating condition is obtained. Meanwhile, the threshold for fault detection is $0.1s$. Therefore, the expectation which exceeds the threshold is considered as a cyber fault.

The fault launched at $t = 47s$ leads to a series of abnormal delays shown in Fig. 5. The expectation gets across the threshold at $47.9s$. The cyber network fault is detected. Simultaneously, there is no unusual behavior detected by the observer (Fig. 7). Therefore, the fault only happens on the cyberspace side, not physical components side. At $47.9s$, the resilience control is triggered to mitigate the fault.

If the cyber network fault is not detected in time and no action is taken for fault mitigation, all of the system outputs overflow out of the physical limitation, even worse, the physical component might get unrepairable damages. In Fig. 8, visibly, the cyber fault can be captured in time and the degradations are reduced to at least 55%. The improvements can be found in Table. 2.

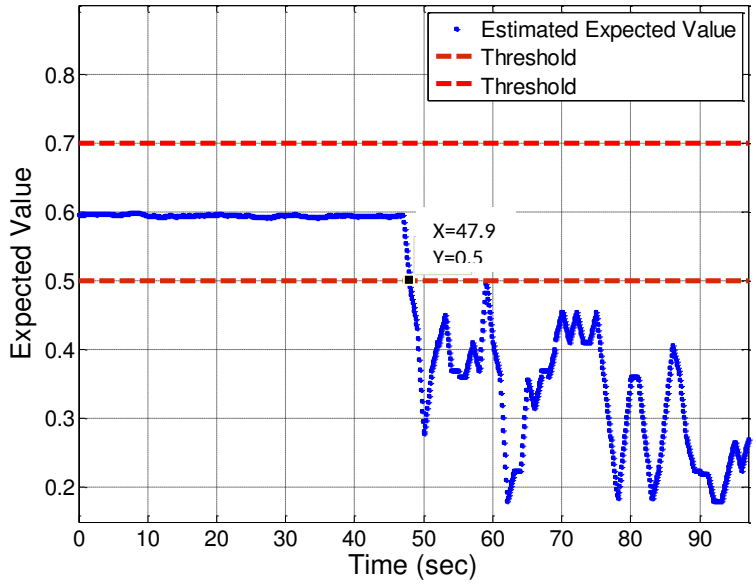


Figure 6. Expectation variation

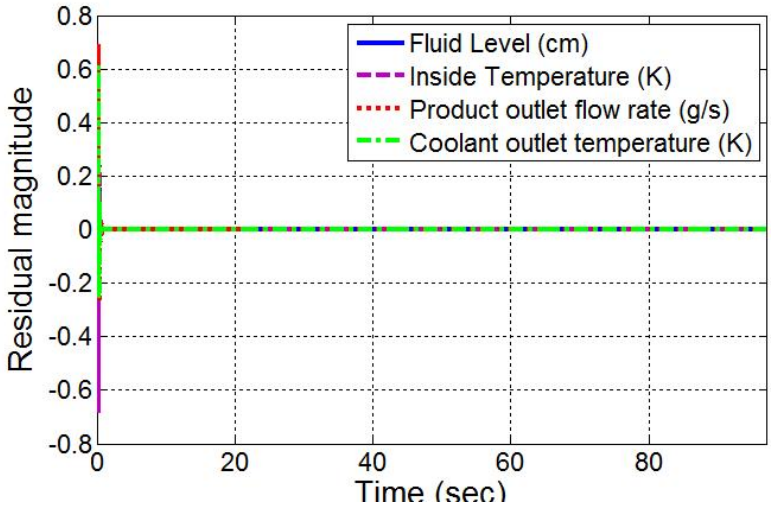


Figure 7. Modeled system output residual

Table 2. The comparison of overshoot and TTR

Variables	Overshoot			TTR		
	SOC	PTSOC	Improvement	SOC	PTSOC	Improvement
Fluid level	423.2cm	64.88cm	84.7%	9.4s	7.3s	22.3%
Inside temperature	58.54K	29.55K	49.5%	7.7s	5.6s	27.3%
Product outlet flow rate	457g/s	72.67g/s	84.1%	7.6s	4.5s	40.8%
Coolant outlet temperature	82.9K	45.56K	45%	8.7s	6.3s	27.6%

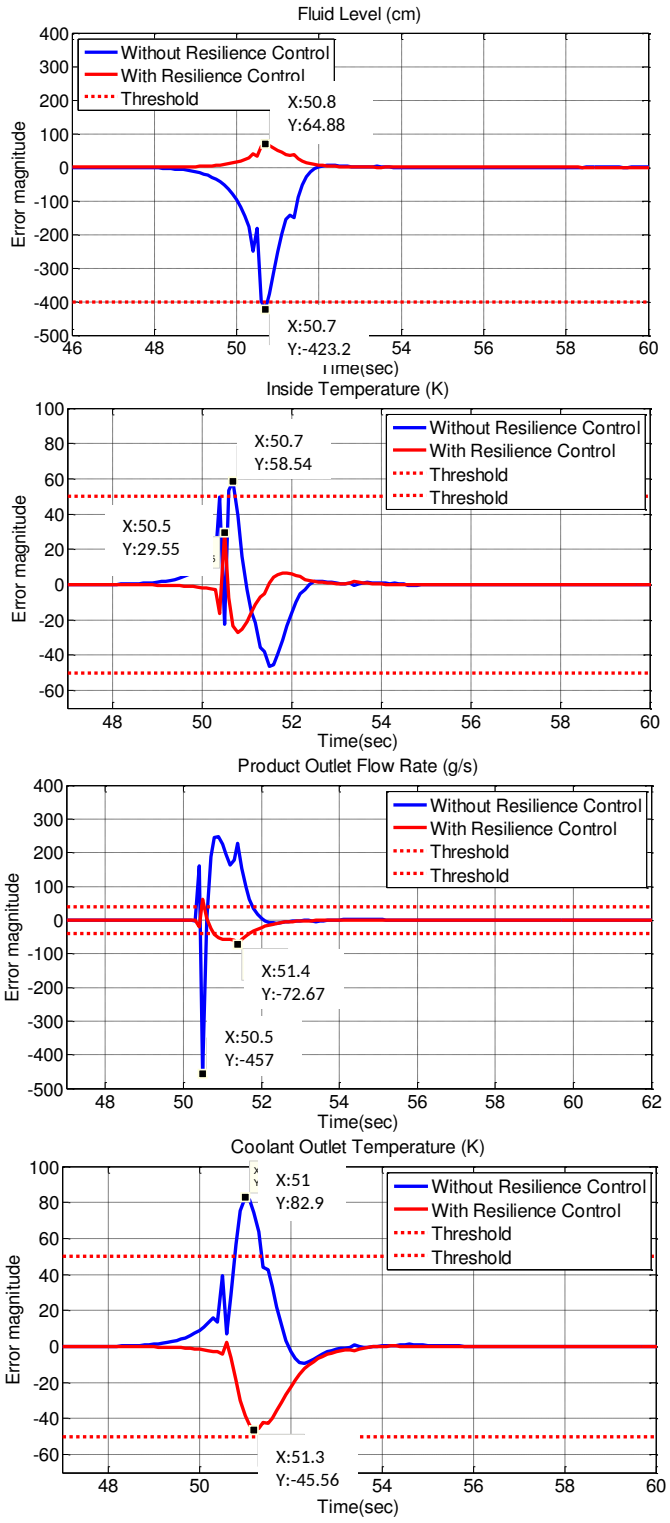


Figure 8. Fault mitigation performance

6. CONCLUSIONS

A novel diagnosis scheme is shown to quickly detect and isolate cyber network faults using PDF monitoring and estimation. With the proposed resilience controller, the adverse effects caused by cyber network faults are effectively mitigated. The stability for the proposed controller is proved using Lyapunov-based analysis.

The simulation results show that the proposed scheme accurately detect the cyber network faults. Moreover, the PTSOC is timely triggered to mitigate the negative effects on the CPSs performance. The overshoot is significantly reduced by at least 45% and TTR is shorten by 22% than that of the SOC because the continuously updating probability weights optimize the parameters of control law.

REFERENCES

Amin, S., Cárdenas, A. A., and Sastry, S., 'Safe and secure networked control systems under denial-of-service attacks.' in 'HSCC,' volume 5469, Springer, 2009 pp. 31–45.

Blundell, R. and Duncan, A., 'Kernel regression in empirical microeconomics,' Journal of Human Resources, 1998, pp. 62–87.

Fisher, A., Jacobson, C. A., Lee, E. A., Murray, R. M., Sangiovanni-Vincentelli, A., and Scholte, E., 'Industrial cyber-physical systems–icyphy,' in 'Complex Systems Design & Management,' pp. 21–37, Springer, 2014.

Gamage, T. T., McMillin, B. M., and Roth, T. P., 'Enforcing information flow security properties in cyber-physical systems: A generalized framework based on compensation,' in 'Computer Software and Applications Conference Workshops (COMPSACW), 2010 IEEE 34th Annual,' IEEE, 2010 pp. 158–163.

Jiang, W., Guo, W., and Sang, N., 'Periodic real-time message scheduling for confidentiality-aware cyber-physical system in wireless networks,' in 'Frontier of Computer Science and Technology (FCST), 2010 Fifth International Conference on,' IEEE, 2010 pp. 355–360.

Liang, J. and Du, R., 'Model-based fault detection and diagnosis of hvac systems using support vector machine method,' International Journal of refrigeration, 2007, **30**(6), pp. 1104–1114.

Liu, F.-C. and Yao, Y., 'Modeling and analysis of networked control systems using hidden markov models,' in 'Machine Learning and Cybernetics, 2005. Proceedings of 2005 International Conference on,' volume 2, IEEE, 2005 pp. 928–931.

Liu, G.-P., Xia, Y., Chen, J., Rees, D., and Hu, W., 'Networked predictive control of systems with random network delays in both forward and feedback channels,' IEEE Transactions on Industrial Electronics, 2007, **54**(3), pp. 1282–1297.

Liu, Y., Ning, P., and Reiter, M. K., 'False data injection attacks against state estimation in electric power grids,' ACM Transactions on Information and System Security (TISSEC), 2011, **14**(1), p. 13.

Mo, Y. and Sinopoli, B., 'Secure control against replay attacks,' in 'Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on,' IEEE, 2009 pp. 911–918.

Pasqualetti, F., Dörfler, F., and Bullo, F., 'Attack detection and identification in cyber-physical systems,' IEEE Transactions on Automatic Control, 2013, **58**(11), pp. 2715–2729.

Smith, R. S., 'A decoupled feedback structure for covertly appropriating networked control systems,' IFAC Proceedings Volumes, 2011, **44**(1), pp. 90–95.

Teixeira, A., Amin, S., Sandberg, H., Johansson, K. H., and Sastry, S. S., 'Cyber security analysis of state estimators in electric power systems,' in 'Decision and Control (CDC), 2010 49th IEEE Conference on,' IEEE, 2010 pp. 5991–5998.

Wang, Y., Ding, S. X., Ye, H., and Wang, G., 'A new fault detection scheme for networked control systems subject to uncertain time-varying delay,' IEEE Transactions on signal processing, 2008, **56**(10), pp. 5258–5268.

Xu, H., Jagannathan, S., and Lewis, F. L., 'Stochastic optimal control of unknown linear networked control system in the presence of random delays and packet losses,' Automatica, 2012, **48**(6), pp. 1017–1030.

Yang, C.-X., Guan, Z.-H., and Huang, J., 'Stochastic fault tolerant control of networked control systems,' Journal of the Franklin Institute, 2009, **346**(10), pp. 1006–1020.

Zhang, H., Yang, J., and Su, C.-Y., 'Ts fuzzy-model-based robust $h\infty$ design for networked control systems with uncertainties,' IEEE Transactions on Industrial Informatics, 2007, **3**(4), pp. 289–301.

Zhang-qing, Z. and Xian-zhong, Z., 'Fault detection based on the states observer for networked control systems with uncertain long time-delay,' in 'Automation and Logistics, 2007 IEEE International Conference on,' IEEE, 2007 pp. 2320–2324.

IV. A NOVEL CYBER FAULT PROGNOSIS AND RESILIENCE CONTROL FOR CYBER-PHYSICAL SYSTEMS

Shanshan Bi, Maciej Zawodniok

Department of Electrical & Computer Engineering

Missouri University of Science and Technology

Rolla, Missouri 65409–0050

Tel: 573–341–6622, Fax: 573–341–4115

Email: sbn65@mst.edu

ABSTRACT

Cyber-physical systems (CPSs) consists of a network, computation, and physical process. Embedded networks, which deliver control and sensing signal, can potentially affect CPSs performance. However, the degradation of physical system performance caused by the embedded networks is frequently oversimplified with strong assumptions. The proposed scheme effectively relaxes those assumptions in the existing works, that network delays are bounded in a specific range or its distribution is time invariant. Most of the existing works on fault diagnosis and prognosis addressed the physical system fault detection and isolation, and ignore cyber network faults. A novel cyber network fault prognosis scheme is proposed to detect and isolate cyber and physical device faults, then forecast the effects of cyber network faults on the performance of CPSs, and finally trigger resilience controller at an appropriate time to minimize the computational overhead. Thus, it can guarantee the stability of the entire CPS and substantially reduce computational overhead of the resilience control by triggering it if necessary.

Keywords: cyber physical system, fault prognosis, network fault, resilience

1. INTRODUCTION

Cyber-Physical systems (CPSs) refer to systems with integrated computational network and physical components. With the increasing connectivity among the cyberspace and physical systems, capturing the interactions between the cyber and the physical systems becomes increasingly important Fisher *et al.* (2014). In particularly, network imperfections and dynamics - such as limited channel capacity, traffic congestions, and malicious attacks - can degrade the performance or even destabilize the control system. This makes controller design more challenging and complex. In the existing literature, this issue is often oversimplified when designing CPS controllers, and could result in severe system failure. For example, hackers can remotely take control of a vehicle and cut its transmission on the highway Yağdereli *et al.* (2015). The threat of automotive cyber attacks also threatens people's life. Therefore, detection, estimation, isolation, and mitigation scheme of cyber attacks/faults has to be investigated to improve the resilience of the entire CPSs.

In the past few years, many control and system researchers have pioneered the development of approaches and tools to model and control CPSs. Some of them Liu and Yao (2005) - Zhang-qing and Xian-zhong (2007) addressed the fault detection, isolation, and mitigation in the physical subsystem alone (e.g. actuators, sensors, and controlled components). At the same time, communication and signal process researchers have made major breakthroughs in monitoring, identification, and defense of cyber attacks and other security issues on the cyber side Rawat *et al.* (2015) - Pasqualetti *et al.* (2013). Such existing approaches focus on either cyber or physical control aspects while ignoring or oversimplifying the other aspect. However, such decoupled designs will often fail in practical CPS. Therefore, system control and fault prognosis must be redesigned to take full account of the interaction between cyberspace and physical systems.

Inspired by this motivation, we proposed a novel prognosis scheme in this work. The main contributions are:

a) Proposed a novel prognosis scheme for cyber network fault detection and prediction.

b) Derived the estimation of network delay distribution based on time series analysis. The convergence of the estimation error is presented in **Lemma 1**.
c) Proposed an isolation scheme to distinguish soft and hard faults based on the prediction of potential failures on system states. **Theorem 1** shows the convergence of such prediction.
d) Developed a decision making scheme for resilience control triggering. The simulation results in Section. 5 illustrate that this scheme proactively trigger the resilience control and effectively avoid physical system failure.

The rest paper is organized as following. In Section. 1.1, a motivation example is given to illustrate the relationship of cyber condition and system behavior. Next, the related works on fault diagnosis and prognosis are presented in Section. 2. In Section. 3, the proposed prognosis scheme is demonstrated. The simulation results are shown in Section. 5 and the conclusions are given in Section. 6.

1.1. Motivation Example

In this section, the design challenge caused by interacting cyber network and physical system is discussed in a simple scenario. It illustrates the need to consider the interaction between physical components and network in resilient CPSs.

This example emulates a route hijacking by an attacker to eavesdrop control information that could later be used to take over the controller. Such an attack increases delay and delay variation when the attacker secretly relays and possibly alters the communication between the controller and actuators. A network is simulated using Network Simulator 2 (NS2) with a random topology of 11 nodes. Ad hoc On-Demand Distance Vector (AODV) routing scheme is adopted. The route through the topology is altered because the attacker node relays the transmission such that the packet delays vary for the controller loop, as shown in Fig. 1. (a). Note, that similar network performance could be a result of topology or traffic pattern changes. A feedback loop with the simulated delays employs an optimal controller to regulate a two input four output (2I4O) system Xu *et al.* (2012).

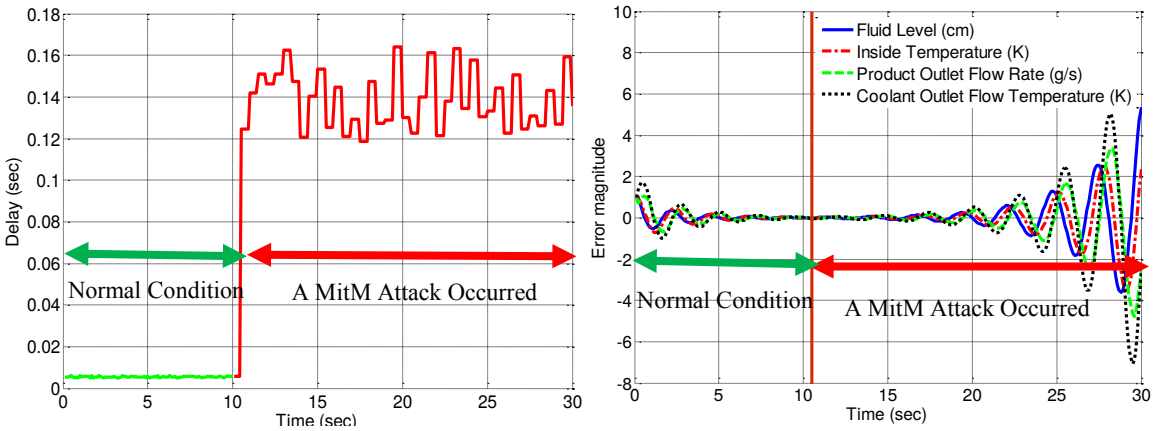


Figure 1. a) Delays
b) Tracking errors of optimal controller

The results show the disturbance in CPS induced by the network dynamics. Fig. 1. (b) shows the optimal controller make the system states converge before $10.5s$. Then, a route hijacking attack is launched. The sudden changes of delay at $t = 10.5s$ make the system states oscillating. Consequently, the CPS becomes unstable due to such network dynamics.

It is concluded that stochastic cyber attacks indeed affect the system performance. Cyberspace is particularly difficult to secure due to its vulnerabilities of linkages between cyber and physical systems. Of growing concern is the cyber threat to critical hardware devices. Cyber network faults could cause harm or disrupt services upon which our economy and the daily lives depend on. In light of the risk and potential consequences of cyber events, strengthening the risk awareness and resilience of CPSs has become an important mission.

To address the cyber network fault issues on the physical system side, a full knowledge of the relation between cyber condition and system performance is essential. Hence, we propose a scheme for detecting and isolating cyber and physical system faults. Also, a resilience control triggering strategy is added to proactively trigger the controller and accommodate the potential failures ahead of time.

2. RELATED WORKS

In this section, we first briefly discuss the existing works on cyber security. Next, the works on fault awareness of the physical system are discussed.

The overall goals of cyber security include integrity (the trustworthiness of data or resources), availability (accessibility upon demand), and confidentiality (keeping information secret from unauthorized users). Many researchers addressed these issues with different technologies, such as authentication schemes, access control, and other defense scheme Pasqualetti *et al.* (2013) - Cardenas *et al.* (2008). An assumption that the adversary/attack model is fully known is often required; however, it is challenging to obtain. In Amin *et al.* (2009) deception and denial of service attacks against a networked control system are addressed. They proposed a countermeasure based on semi-definite programming. This work and the following literature are only valid for a specific attack model which cannot be known in priori. A defense scheme without requiring the knowledge about the attack model is needed.

In Liu *et al.* (2011), false data injection attacks against static state estimators are introduced. Undetectable false data injection attacks can be designed even when the attacker has limited resources. Also, stealthy deception attacks against the Supervisory Control and Data Acquisition system are studied in Teixeira *et al.* (2010). Mo and Sinopoli (2009) studied the effect of replay attacks on a control system. In Smith (2011), the effect of covert attacks against control systems is investigated. A parameterized decoupling structure alter the behavior of the physical plant while remaining undetected from the original controller. Gamage *et al.* (2010) proposed a general theory of event compensation as an information flow security enforcement mechanism for CPSs. Message scheduling methods were given to improve the security quality of wireless networks for mission-critical CPSs in Jiang *et al.* (2010).

With respect to the above works, Pasqualetti *et al.* (2013) proposed a mathematical framework for CPSs, attacks, and monitors, and given the fundamental limitations of monitors from system-theoretic and graph-theoretic perspectives. Finally, centralized and distributed attack detection and identification monitors were designed. Overall, many cyber attacks can be addressed on the cyber side. However, the effects of cyber attacks/faults on the physical system behavior are oversimplified in the above mentioned existing works. Moreover, the injection time and model of the attacks/faults are difficult to learn ahead of time in practical CPSs.

The control researchers focused on the conventional fault detection techniques that have successfully applied to industrial networked control systems (NCSs). They indeed considered the network delay and packet loss in various ways. In Zhu and Martinez (2011), a resilient control problem is studied, in which control packets transmitted over a network are corrupted by a human adversary. They proposed a receding-horizon Stackelberg control law to stabilize the control system despite the attack. However, the proposed approach required a priori knowledge on attack model and type. In Liu and Yao (2005), network delays were modeled as a constant delay (time buffer), an independent random delay, and a delay with known probability distribution governed by the Markov chain model. In Liu *et al.* (2007), a networked predictive controller in the presence of random delay in both forward and feedback channels was proposed to minimized the effects of network failures. A robust H_∞ control for a nonlinear T-S fuzzy model system was proposed to address the network delays and packet drop in Zhang *et al.* (2007). However, they assumed the upper bound of delays is known. This is challenging to be satisfied in reality. Wang *et al.* (2008) and Zhang-qing and Xian-zhong (2007) employed a state observer-based fault detection method on the uncertain long time delay. Although, the network delays and packet drop caused by network faults/failures were considered in above works, the assumptions, such as

known bounds and time-invariant distribution of delays and packet loss, are always made. In addition, most of the above works aimed to detect the faults of physical components (sensors, actuators, and system plant), not the faults in the cyberspace.

This work is motivated to address cyber network faults detection, isolation, and prediction. Meanwhile, the tolerant control scheme and it triggering strategy are proposed to stabilize the CPS despite cyber network faults and optimize the computational overhead.

3. THE PROPOSED PROGNOSIS SCHEME

In this section, the overview of the proposed prognosis scheme is given in Section. 3.1. An online kernel density estimation (KDE) based probability density function (PDF) identifier is introduced in Section. 3.2. Then, the details of the proposed prognosis scheme are presented in Section. 4. At last, the resilience controller is designed in Section. 4.3.

3.1. Overview

In this work, the uncertainties in the cyberspace, including traffic congestions, topology changes, and attacks, are causing abnormal delays and packet losses on the physical system side. Monitoring such delays and packet losses online is required for detection of cyber network faults. Moreover, an observer is needed to detect physical system faults and isolate them from cyber network faults Zhang-qing and Xian-zhong (2007).

The proposed prognosis scheme is shown in Fig. 2. It includes four main steps that are continuously repeated:

a) Data collection of network delays. n delays ($[d_{k-n+1}, \cdots, d_k]$) in the sliding window are used to do the PDF estimation at time k (PDF_k). When the new delay is measured, the data in the sliding window is updated.

b) Cyber Network Fault Detection. The PDF of these n delays is obtained by using the online KDE-based PDF identifier. The probability for each delay interval P_i^k is calculated. Compare P_i^k to P_i^{k-1} to compute the variation of probabilities ΔP_i^k. If ΔP_i^k

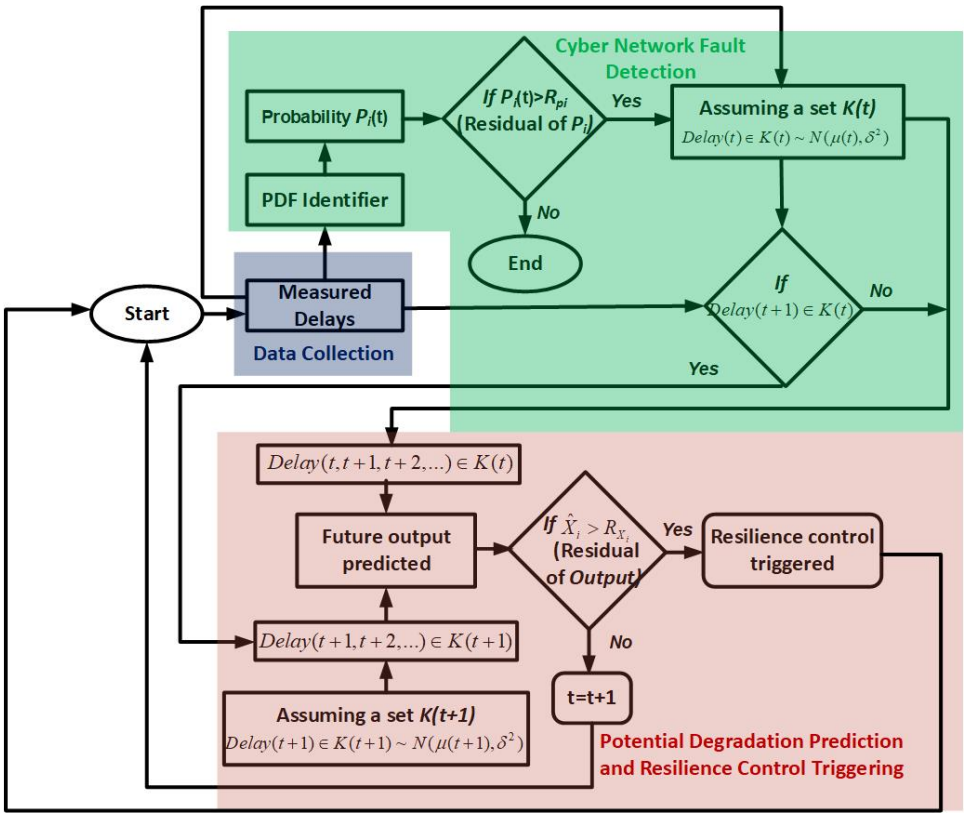


Figure 2. Flow chart of cyber network fault prognosis scheme

exceeds the set threshold R_{p_i}, the PDF variation is captured and a cyber network fault is detected. Meanwhile, if there is no abnormal behavior presented in the observer, it can be confirmed that only cyber network fault happens.

c) Potential degradation prediction. If a cyber network fault is detected, the PDF of new delay distribution is predicted by using time series analysis. Then, the delays following the new distribution are resampled. Finally, the prediction of the future physical system outputs is obtained. If the system states deviate out of the acceptable range, the hard fault is detected. Otherwise, it is a soft fault which is not severe enough to trigger the resilience controller. More details about fault isolation are presented in Section. 4.

d) Resilience controller triggering. If a hard fault is detected, the resilience controller is triggered and its parameters are tuned online by the probabilities of delays computed in b).

Such a scheme can detect stochastic cyber failures/attacks without requiring the knowledge of attack model and its injection time a priori. Only monitoring the PDF of delays in real-time is required to do PDF and system states prediction. Moreover, the resilience control law tuned by the probabilities of delays is derived accurately for the given cyber performance. Its details are introduced in Section. 4.

3.2. PDF Identifier

To obtain the probability information mentioned in Step (b), a PDF identifier is employed Bi and Zawodniok (2017). It uses kernel density estimation (KDE) to estimate the distribution of delays iteratively. The data used to make the identification is updated every sampling interval for a window of n last packet delays. The main steps of online PDF identification are shown in Appendix. (B.0.1). Here, a normal kernel smoother is selected for PDF estimation.

Such a sliding window based PDF identifier provides the PDF profile of delays in real-time such that the variation of PDF can be captured and observed easily.

4. CYBER NETWORK FAULT DETECTION AND ISOLATION

Cyber network fault is detected by monitoring probability residual (PR). The other residuals - modeled system output residual and system performance residual - are used to isolate cyber network and physical components fault. Then, the prediction of the future new delay distribution and system state prediction are used to isolate soft and hard cyber network fault. Finally, the decision of resilience control triggering is made.

4.1. Cyber Network Fault Detection

For cyber network fault detection, three residuals have to be monitored in an online manner:

a) Probability Residual (PR): It is the difference of the probability at k and the last interval $k-1$. Such information is provided by the proposed PDF identifier. The PR at time k for each delay interval is denoted as $\Delta P_i^k = P_i^k - P_i^{k-1}$. The corresponding threshold R_{p_i} is customizable by the users for satisfying the requirement of fault awareness capability. If $\Delta P_i^k > R_{p_i}$, the cyber network fault is detected.

b) Modeled system output residual ($MSOR$): It is provided by the observer, which is the difference of outputs of modeled and that of actual systems: $MSOR = x(k) - \widehat{x}(k)$. The corresponding threshold R_{MSOR} is selected to detect physical system faults. If $MSOR > R_{MSOR}$, the physical system fault is detected.

c) System performance residual (SPR): It is the difference between actual and desired system outputs: $SPR = x_d(k) - x(k)$. The threshold for each system output variable R_{SPR} is determined by the acceptable error magnitudes of system states. This residual is used to evaluate the system performance and determine when the system should shut down.

If PR exceeds its threshold, a cyber network fault is detected. Meanwhile, $MSOR$ and SPR should be supervised to do the root-cause analysis of the degradation of system performance. If a cyber network fault is detected, the type of this fault (soft or hard fault) should be learned before triggering the resilience controller. That is because not all types of cyber network fault need to be mitigated by the resilience controller. Unnecessary triggering will result in additional computational resource wasting. When soft faults happen, the adverse effects on system performance can be handled by the existing controller. Therefore, there is no need to take other control actions. Typically, an alarm or warning is sufficient. On the contrary, hard faults potentially threaten the system performance in terms of overshoot, time-to-recover (TTR), and cost of regulation, even stability. Moreover, wear and tear or severe damages of the system components might be induced by such faults. Hence, timely detecting hard faults and triggering the resilience controller are vital for guaranteeing system stability. Moreover, with isolating of soft and hard faults, inefficient triggering of the resilience controller is avoided and the overall computational cost is reduced.

4.2. Soft and Hard Cyber Network Fault Isolation

To recognize hard cyber network fault, we proposed an approach to trend the delay distribution into the future. Next, a system state prediction scheme evaluates system performance for the estimated future delay distribution. In most cases, there is no need to perform the computation expensive prediction. Hence, it is triggered based on a user-defined threshold. As shown in Fig. 2, R_{p_i} is a user-defined threshold for each probability variation $P_i(t)$. If $P_i(t) > R_{p_i}$ is true and the new delay $Delay(t)$ follows the distribution of time $t-1$, there is no cyber network fault. The distribution and system states predictors will not be activated. Otherwise, a delay distribution change will be observed in PDF identifier and the predictors are activated.

The predictions include four main steps that are repeated until the resilience controller is triggered:

Step 1: new distribution estimation;

Step 2: resampling;

Step 3: system output prediction;

Step 4: soft and hard fault isolation and resilience control triggering.

These steps are discussed in details next.

4.2.1. Step 1: New Distribution Estimation. The expectation and standard deviation of the new distribution are estimated based on the delays which induce a new distribution.

Time series analysis is utilized to estimate the autoregressive (AR) model for the expectation E and standard deviation D of the new distribution. The hypothesis of the model is given by:

$$\begin{bmatrix} E(k+1|k) \\ D(k+1|k) \end{bmatrix} = \begin{bmatrix} \beta_{E0} \\ \beta_{D0} \end{bmatrix} + \begin{bmatrix} \beta_{E1} & 0 \\ 0 & \beta_{D1} \end{bmatrix} \begin{bmatrix} E(k) \\ D(k) \end{bmatrix} \tag{1}$$

$\widehat{E}(k+1|k)$ is the forecast of $E(k+1|k)$ and $D(k+1|k)$ based on $E(k)$ and $D(k)$, using the estimated coefficients $\widehat{\beta}_{E0}$, $\widehat{\beta}_{D0}$, $\widehat{\beta}_{E1}$, and $\widehat{\beta}_{D1}$.

$$\begin{aligned}\begin{bmatrix}\widehat{E}(k+1|k)\\ \widehat{D}(k+1|k)\end{bmatrix} &= \begin{bmatrix}\widehat{\beta}_{E0}\\ \widehat{\beta}_{D0}\end{bmatrix} + \begin{bmatrix}\widehat{\beta}_{E1}(k) & 0\\ 0 & \widehat{\beta}_{D1}(k)\end{bmatrix}\begin{bmatrix}E(k)\\ D(k)\end{bmatrix}\\ &= \widehat{\theta}(k)\varphi(k) + C_0(k)\end{aligned} \tag{2}$$

where $\varphi(k) = \begin{bmatrix}E(k) & D(k)\end{bmatrix}^T$, and $\widehat{\theta}(k) = \begin{bmatrix}\widehat{\beta}_{E1}(k) & 0\\ 0 & \widehat{\beta}_{D1}(k)\end{bmatrix}$.

The one-period ahead forecast error is:

$$\begin{bmatrix}e_E(k+1)\\ e_D(k+1)\end{bmatrix} = \begin{bmatrix}E(k+1|k)\\ D(k+1|k)\end{bmatrix} - \begin{bmatrix}\widehat{E}(k+1|k)\\ \widehat{D}(k+1|k)\end{bmatrix} \tag{3}$$

The forecast errors converge by minimizing the following objective index:

$$J = \begin{bmatrix}\alpha e_E(k+1)\\ \beta e_D(k+1)\end{bmatrix}^T \begin{bmatrix}\alpha e_E(k+1)\\ \beta e_D(k+1)\end{bmatrix} \tag{4}$$

where α and β, which can be customized by users, are the weights for the estimate errors of E and D respectively. Such parameters balance the trade-off between the degree of optimization of two errors. For our case, we take $\alpha = \beta = 1$ meaning these two errors are minimized to the same degree.

Such that the update law of $\widehat{\theta}(k)$, $L(k)$, and $O(k)$ can be obtained.

$$\begin{aligned}\widehat{\theta}(k) &= \widehat{\theta}(k-1) + L(k)e(k)\\ L(k) &= \frac{O(k-1)\varphi(k)}{\varphi(k)^T O(k-1)\varphi(k)}\\ O(k) &= (I - L(k)\varphi(k)^T)O(k-1)\end{aligned} \tag{5}$$

where $L(k)$ and $O(k)$ denote estimator gain and estimation of error variance, respectively. Their initial values are randomly set.

Remark 1: The parameters $\widehat{\theta}(k)$, $L(k)$, and $O(k)$ are continuously updated by the training data in the sliding window at time K. We assume that the distribution of time $k+1$ does not change so that the one step prediction for time $k+1$ is valid to predict the system behavior.

Lemma 1: With the update law (5) and more new delays loaded in the sliding window, the objective index (4) is continuously minimized. Then the following statements are true:

a) the estimation errors of the expected value and standard deviation of new delays converge.

b) $\left(\parallel \sum_{j=1}^{n} \widetilde{P}_{(k+1)j} \parallel - \parallel \sum_{j=1}^{n} \widetilde{P}_{kj} \parallel \right) < 0$ holds.

The proof can be found in Qin (1998) and Simon (2006).

Remark 2: Even if the network condition is perfect, unexpected delays, which are out of the healthy range, occasionally occurs in a long period. That can lead to the inefficient triggering of resilience control. Using the above time series analysis, not only the distribution change can be tracked in real-time, but also the trend of distribution change is identified and predicted. Such that the occasional event can be filtered without resilience control triggering.

4.2.2. Step 2: Resampling. Based on the future delay distribution provided by step 1, a series of random delays is generated, which follows the new distribution.

4.2.3. Step 3: System Output Prediction. The resampled delays are fed to the system model which takes into account dynamic delays and packet losses. Such a time-varying system is given by:

$$z(k+1) = A_z(k)z(k) + B_z(k)u(k) \tag{6}$$

where $z = \begin{bmatrix} x(k)^T & u(k-1)^T & \dots & u(k-d)^T \end{bmatrix}^T$ is the state variables vector; u_k is the control input; $A_z(k)$ and $B_z(k)$ are the system dynamic matrices and given by

$$A_z(k) = \begin{bmatrix} A & \gamma(k-1)B_1(k) & \dots & \gamma(k-i)B_i(k) & \dots & \gamma(k-d)B_d(k) \\ 0 & 0 & \dots & \dots & \dots & 0 \\ 0 & I_m & \dots & \dots & 0 & 0 \\ \vdots & 0 & I_m & \dots & \dots & 0 \\ \vdots & \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & \dots & I_m & 0 \end{bmatrix},$$

$$B_z(k) = \begin{bmatrix} \gamma(k)B_0(k) & I_m & 0 & 0 & \vdots & 0 \end{bmatrix}^T,$$

$$\gamma(k) = \begin{cases} I^{n\times n} & \text{if the control input is received at time k} \\ 0^{n\times n} & \text{if the control input is lost at time k} \end{cases}$$

Finally, the possible system behavior induced by the new distribution of delays are estimated and denoted as $\widehat{z}_k$.

Prediction Convergence Analysis: The prediction error $\widetilde{z_k}$ convergence is demonstrated in **Theorem 1**. The dynamic matrices A_{zj} and B_{zj} for each delay interval are deterministic and their calculation can be found in Xu *et al.* (2012).

Theorem 1 (Error of system states prediction convergence): As the delay data keeps updating PDF identifier and $\left(\parallel \sum_{j=1}^{n} \widetilde{P}_{(k+1)j} \parallel - \parallel \sum_{j=1}^{n} \widetilde{P}_{kj} \parallel \right) < 0$ is satisfied, then the prediction error for system output $\parallel \widetilde{z}(k) \parallel$ asymptotically converges to zero.

Proof: The prediction error is given by

$$\begin{aligned}\widetilde{z}_k &= z_k - \widehat{z}_k \\ &= (A_z(k) - B_z(k)K(k))z(k) - (\widehat{A}_z(k) - \widehat{B}_z(k)K(k))z(k) \\ &= (A_z(k) - \widehat{A}_z(k))z(k) - (B_z(k) - \widehat{B}_z(k))K(k)z(k) \\ &= (\widetilde{A}_z(k) - \widetilde{B}_z(k)K(k))z(k)\end{aligned}$$

Therefore, the convergence of $\widetilde{z}_i$ can be proven by proving the convergence of $\widetilde{A}_z(k)$ and $\widetilde{B}_z(k)$

We define the prediction error of $A_z(k)$ as $\widetilde{A}_z(k) = A_z(k) - \widehat{A}_z(k)$. $A_z(k)$ can be expressed as $\sum_{j=1}^{n} P_j(k)A_{zj}$ $P_j(k)$ is the actual probability at k. Similarly, we denote $\widehat{A_z(k)} = \sum_{j=1}^{n} \widehat{P}_j(k)A_{zj}$. $\widehat{P}_j(k)$ is the estimate probability provided by the PDF profile. The estimation error of the probability is $\widetilde{P}_j(k) = P_j(k) - \widehat{P}_j(k)$. Then, Lyapunov function candidate is $V_{A_z(k)} = \widetilde{A}_z(k)^T \widetilde{A}_z(k)$.

$$
\begin{aligned}
\Delta V_{A_z(k)} &= \widetilde{A}_z(k+1)^T \widetilde{A}_z(k+1) - \widetilde{A}_z(k)^T \widetilde{A}_z(k) \\
&= \Big(\sum_{j=1}^{n} P_j(k+1) A_{zj} - \sum_{j=1}^{n} \widehat{P}_j(k+1) A_{zj} \Big)^T \Big(\sum_{j=1}^{n} P_j(k+1) A_{zj} - \sum_{j=1}^{n} \widehat{P}_j(k+1) A_{zj} \Big) \\
&- \Big(\sum_{j=1}^{n} P_j(k) A_{zj} - \sum_{j=1}^{n} \widehat{P}_j(k) A_{zj} \Big)^T \Big(\sum_{j=1}^{n} P_j(k) A_{zj} - \sum_{j=1}^{n} \widehat{P}_j(k) A_{zj} \Big) \\
&= \Big(\| \sum_{j=1}^{n} \widetilde{P}_j(k+1) \|^2 - \| \sum_{j=1}^{n} \widetilde{P}_j(k) \|^2 \Big) \| A_{zj} \|^2 \\
&= \underbrace{\Big(\| \sum_{j=1}^{n} \widetilde{P}_j(k+1) \| + \| \sum_{j=1}^{n} \widetilde{P}_j(k) \| \Big)}_{\Delta_1} \\
&\Big(\| \sum_{j=1}^{n} \widetilde{P}_j(k+1) \| - \| \sum_{j=1}^{n} \widetilde{P}_j(k) \| \Big) \| A_{zj} \|^2 \\
&= \Delta_1 \Big(\| \sum_{j=1}^{n} \widetilde{P}_j(k+1) \| - \| \sum_{j=1}^{n} \widetilde{P}_j(k) \| \Big) \| A_{zj} \|^2
\end{aligned}
$$

$\Delta_1 > 0$

Since $V_{A_z(k)}$ is positive definite and $\Delta V_{A_z(k)}$ is negative definite provided $\Big(\| \sum_{j=1}^{n} \widetilde{P}_j(k+1) \| - \| \sum_{j=1}^{n} \widetilde{P}_j(k) \| \Big) < 0$ (**Lemma 1**). Therefore, the prediction error of $A_z(k)$ asymptotically converge to zero. Similarly, the prediction error of $B_z(k)$ can be proven with the same procedure. Such that $\widetilde{z}(k)$ asymptotically converge to zero. ■

Remark 3: The maximum error occurs when the first sample of the new distribution comes in the sliding window. Then, the accuracy of PDF estimation improves as the sliding window includes more and more new samples from the new distribution after the PDF change occurs. Therefore, $\Big(\| \sum_{j=1}^{n} \widetilde{P}_{(k+1)j} \| - \| \sum_{j=1}^{n} \widetilde{P}_{kj} \| \Big) < 0$ holds.

4.2.4. Step 4: Soft and Hard Fault Isolation and Resilience Control Triggering Strategy. The acceptable error magnitude of state i is defined as $R_{\widehat{z}_i}$. If $\widehat{z}_i > R_{\widehat{z}_i}$, this fault is marked as a hard cyber network fault. A warning is triggered as well as the resilience controller. Otherwise, this is a soft fault that can be handled with the original controller operating normally.

In summary, the proposed prognosis scheme can timely detect cyber network faults and isolate soft and hard faults because the dynamics of the network is continuously monitored. Accurately isolating soft and hard fault optimize the decision of resilience controller triggering as well as the computational resources allocation. When hard faults occur, the resilience controller can be timely triggered before adverse effects on system performance happening.

4.3. Resilience Control Strategy

In this section, the employed resilience controller is presented for completeness. PDF-based tuning of stochastic optimal controller (PTSOC) Bi and Zawodniok (2017) mitigates the adverse effects induced by the uncertainties of cyberspace and adapt to the random occurrence of cyber network faults.

Remark 4: PTSOC has a good adaptability to a time-varying distribution of delays, but lead to more computation overhead than the traditional resilience controller. Therefore, the above strategy Section. 4.2.4 aims to determine an appropriate time to trigger the resilience controller without consuming the computational overhead. Meanwhile, the proposed strategy based on fault isolation proactively trigger the controller, rather than triggering it when a failure or damage has occurred. Such that, the system performance and stability are guaranteed.

The PTSOC control law considers the PDF of delays by optimizing a weighted summation of cost functions of different delay ranges (7). Each weight is the probability of its corresponding delay intervals from the PDF identifier.

$$J^k = E\left[\sum_{i=1}^{n} P_i J_i^k\right] = E\left[\sum_{i=1}^{n} P_i (x_i^{kT} Q_{zi} x_i^k + u_i^{kT} R_{zi} u_i^k)\right] \tag{7}$$

where i presents the delay interval ($d_{int}i < d^k < d_{int}(i+1)$); n is the total number of delay cases; k represents sampling interval; P_i is probability of delay within $d_{int}i$ to $d_{int}(i+1)$ provided by the PDF identifier; x_i is the states vector; u_i is the control inputs vector; $Q_{zi} = diag[Q_i, \frac{R_i}{d}, ...]$ and $R_{zi} = \frac{R_i}{d}$ are symmetric positive semi-definite and symmetric positive definite respectively. $E[\bullet]$ is the expectation operator.

By optimizing (7), the control input is given by:

$$u(k) = -K(k)Z(k) \tag{8}$$

$$\begin{aligned} K(k) = \sum_{i=1}^{n_d} & P_i(k)(B_{zi}(k)^T Z_i(k) B_{zi}(k) + R_z(k))^{-1} \\ & (B_{zi}(k)^T Z_i(k) A_{zi}(k) + S_{zi}(k)) \end{aligned} \tag{9}$$

where $K(k)$ is the optimal gain and $u(k)$ is the control input; $S_{zi}(k) \geq 0$ is the solution of the algebraic riccati equation (ARE) equation; $n_d = d_{upper}/d_{int}$, d_{upper} is the maximum delay in the sliding window; $P_i(k)$ is the probability of $d_{int}i < d(k) < d_{int}(i+1)$.

Remark 5: The Q_i and R_i in the cost function for each delay range should be different because each pair of Q_i and R_i should be the optimal values for the delays bounded in a specific range. They cannot guarantee a high level with the delays out of such boundaries.

Stability Analysis Bi and Zawodniok (2017):

Two theorems and their corresponding proofs are presented to demonstrate the stability of the proposed PTSOC. Lyapunov-based stability analysis is used. **Theorem 2** (Appendix (B.0.2)) shows the control gain estimation asymptotically converges even

if PDF estimation has an error provided it asymptotically converges to zero. **Theorem 3** (Appendix (B.0.3)) considers the irremovable bias of PDF estimation as a bounded disturbance. However, a UUB stability is guaranteed. The proofs for these theorems can be found in Bi and Zawodniok (2017).

5. SIMULATION AND DISCUSSION

In this section, the proposed prognosis scheme is evaluated by simulations in MATLAB. Section. 5.1 demonstrates the convergence of the system state prediction. In this case, the resilience controller triggering is disabled to observe the prediction performance alone. Then, both soft and hard cyber network fault scenarios are presented separately to demonstrate the cyber network fault detection and isolation performance in Sections. 5.2 and 5.3. The resilience controller in Section. 4.3 is applied. A conventional stochastic optimal control Xu *et al.* (2012) is employed as a reference.

A continuous-time batch reactor system is taken as a case study. Its dynamics are given by

$$\dot{x} = \begin{bmatrix} 1.38 & -0.2077 & 6.715 & -5.676 \\ -0.5814 & -4.29 & 0 & 0.675 \\ 1.067 & 4.273 & -6.654 & 5.893 \\ 0.048 & 4.273 & 1.343 & -2.104 \end{bmatrix} x + \begin{bmatrix} 0 & 0 \\ 5.679 & 0 \\ 1.136 & -3.146 \\ 1.136 & 0 \end{bmatrix} u \tag{10}$$

The parameters of this CPS are selected as:

a) The sampling time is $100ms$;

b) The considered delays in the system model is less than 2 sampling interval, $d = 2$;

c) $d_{int} = 0.1s$;

d) The threshold of the probability variation R_{pi} is $0.03s$, unless otherwise states;

e) The sliding window size M is 30.

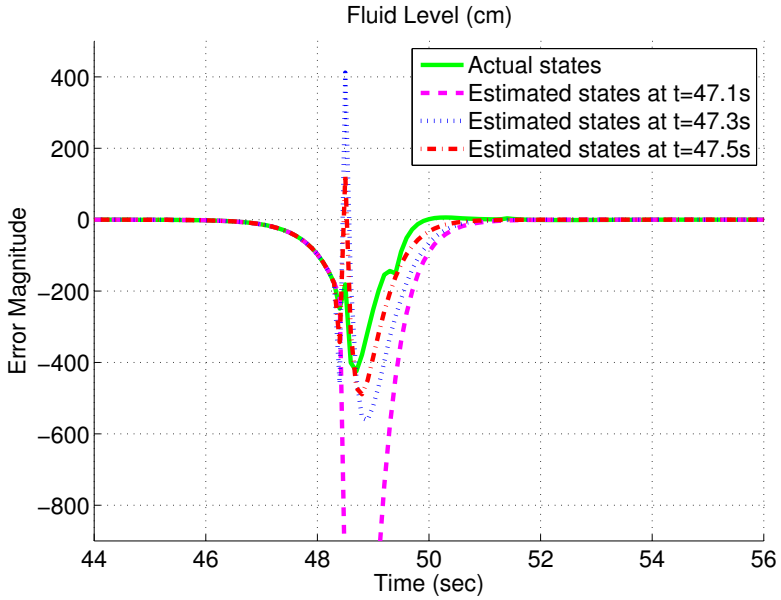


Figure 3. Case A: Actual and predicted system behavior

5.1. System State Prediction Evaluation

This scenario demonstrates that the accuracy of the system state prediction improves as more new delay measurements update the distribution estimation.

Here, the PTSOC triggering is disabled to allow continuous, uninterrupted predictions of system states. The fault is injected at $47s$. Fig. 3 shows that the prediction at $47.1s$ significantly diverges from the actual system behavior. As more new delays are loaded in the sliding window, the PDF estimation of the new distribution improves. Such that the predicted system states become more accurate. The predictions at $47.5s$ is more accurate than that at $47.1s$. Other results are shown in Appendix (B.0.4).

5.2. Soft Cyber Network Fault

In this scenario, a network congestion fault is simulated, which occurs when a network node is relaying more data than it can handle. It usually causes a gradual increase of delays. R_{pi} and M are user-defined parameters. These simulations are repeated 50

times for the statistical validation. With 50 repeated simulations for different soft faults, the proposed scheme only needs $0.42s$ in average to detect the fault. With $R_{pi} = 0.03s$, the faults are 100% detected. The results in Figs. 4 are only for one case to illustrate the performance of the proposed prognosis scheme.

Before the first $50s$, the delays follow a normal distribution $N(0.3, 0.05^2)$. Then, a network congestion attack (e.g. denial-of-service) is launched at $50s$ and the delays after $50s$ follow a new normal distribution $N(0.5, 0.1^2)$. Fig. 4 presents the result for fluid level. As shown in Fig. 4 (a), the probability variation exceeds the threshold at $50.2s$. A cyber network fault is detected. Simultaneously, the awareness of the cyber network fault triggers the system state prediction shown in Fig. 4 (b) and Appendix (B.0.4). The oscillation are observed, but are small enough for the basic controller to handle. Therefore, this fault is a soft fault. The resilience controller does not have to be triggered.

The traditional diagnosis scheme Xu *et al.* (2012) usually preset an threshold, which is a constant, for the network delay to capture the delay variation. When the delay exceeds the bound, the resilience controller will be activated. Such that some unnecessary triggering might occur resulting in increased computational overhead and false reactions of resilience controller. According to Fig. 4 (a), the resilience controller should be activated 12 times if the traditional fault diagnosis is applied. However, applying the resilience control is not necessary and induce more resource waste and wear and tear of system hardware. On the contrary, such negative consequence can be avoided with applying our proposed scheme.

Remark 6: There are several cyber network fault detection before $50s$ because R_{pi} for this scenario is selected at low level. Hence, false detection occur. However, they would only cause more computational overhead and have no input on system stability. Overall, this trade-off should be considered when selecting R_{pi}.

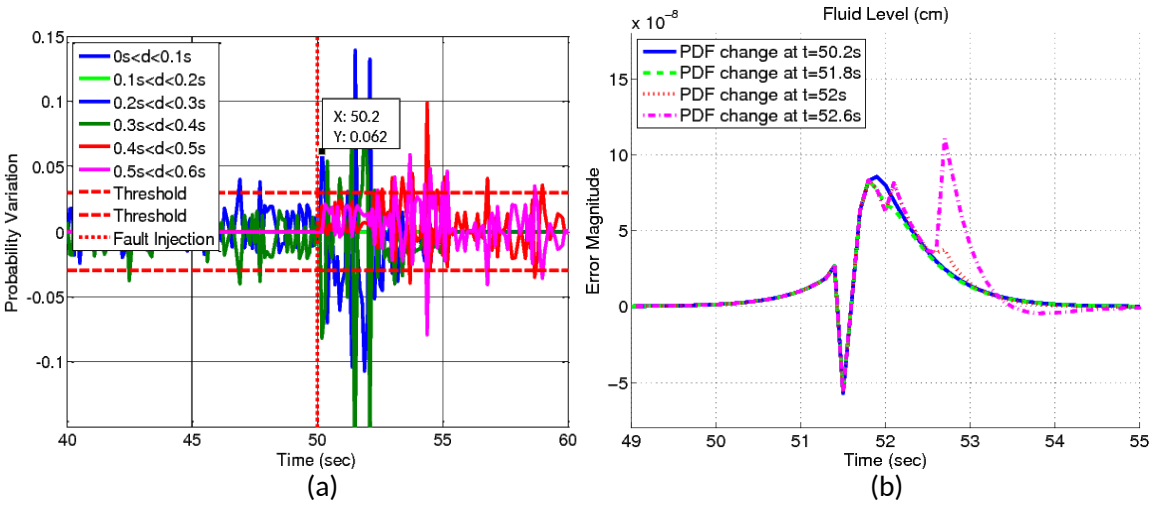


Figure 4. Case B: a) Selected probability variation
b) Predicted and actual system output

Table 1. The crossing points

Variables	Estimated point	Actual point	Estimation Error
Fluid level	48.4s	48.7s	0.6%
Inside temperature	48.4s	48.6s	0.4%
Product outlet flow rate	48.2s	48.2s	0%
Coolant outlet temperature	48.2s	48.3s	0.2%

Remark 7: After the first soft fault detection, the proposed scheme should continuously supervise the cyber condition. That is because a soft fault possibly becomes a hard fault in the near future. Also, a warning should be issued to human supervisor to take additional precautions (e.g. investigate attack or update firewall)

5.3. Hard Cyber Network Fault

In this scenario, a man-in-the-middle attack (MitM) is simulated. The attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other. The transmitted information, such as control commands and feedback measurements, can be eavesdropped and delayed. Here, the delays before $47s$ follows a normal distribution $(0.3, 0.05^2)$. Then, the attacker injects

Table 2. The comparison of overshoot and TTR

Variables	Overshoot/TTR					TTR				
	SOC	PTSOC	Improve	PID	Improve	SOC	PTSOC	Improve	PID	Improve
Fluid Level	425.5cm	44.11cm	89.6%	6792cm	99.4%	6.4s	4.4s	31.2%	6.9s	36.2%
Inside Temperature	57.5K	4.71K	91.8%	1573K	99.7%	4.8s	3.1s	35.4%	5.3s	41.5%
Product Outlet Flow Rate	460.7g/s	47.51g/s	89.7%	6599g/s	99.3%	4.4s	2.4s	45.5%	4.5s	46.7%
Coolant Outlet Temperature	80.75K	8.61K	89.3%	4604K	99.8%	7.7s	4.3s	44.2%	8.1s	46.9%

MitM attacks intermittently. As the results, the distribution of delays is varied over time (Fig. 5.(a)). The acceptable error magnitudes are set for four system states: $400cm$ for the fluid level; $50k$ for the inside temperature; $40g/s$ for the product outlet flow rate; and $50k$ for the coolant outlet temperature.

As Fig. 5. (b) showing, the sudden change of delay at $47s$ is detected at $47.1s$ because the probability of delays within $[0.2, 0.3]$ suddenly decreases. In Fig. 6. (a) and Appendix (B.0.4), all the predicted system outputs exceed their acceptable range. The estimated and actual points that the system states pass through the acceptable error are shown in Table. 1. This prediction can achieve at least 99.6% accuracy. It is concluded that this fault is a hard cyber network fault and its adverse effects on the system performance is predicted. The resilience control is triggered at $47.1s$ to mitigate such effects. Comparing with the original SOC, the overshoots are reduced by at least 89.6%, the TTRs are shortened by 31.2%. The summary of improvements can be found in Table. 2.

When applying the proposed scheme, the fault is quickly detected and the resilience controller is timely triggered ahead of the serious degradation of system performance. Also, the overshoot of each system output is significantly reduced in term of its corresponding TTR. In contrast, without applying the proposed scheme, the fault still can be detected when the system states exceed the acceptable error magnitude at $48.5s$. The fault tolerant controller, which is a tuned PID controller, is triggered. However, it is too late to recover the system performance with such a late activation of the resilience controller. In such case, the basic controller will try to apply excessive actuation (Table. 2) to stabilize. This might lead to significantly damage of the components or cause an unscheduled downtime. Even worse, the system could be compelled to stop. The above simulation is repeated for 50 times. All the faults are accurately detected.

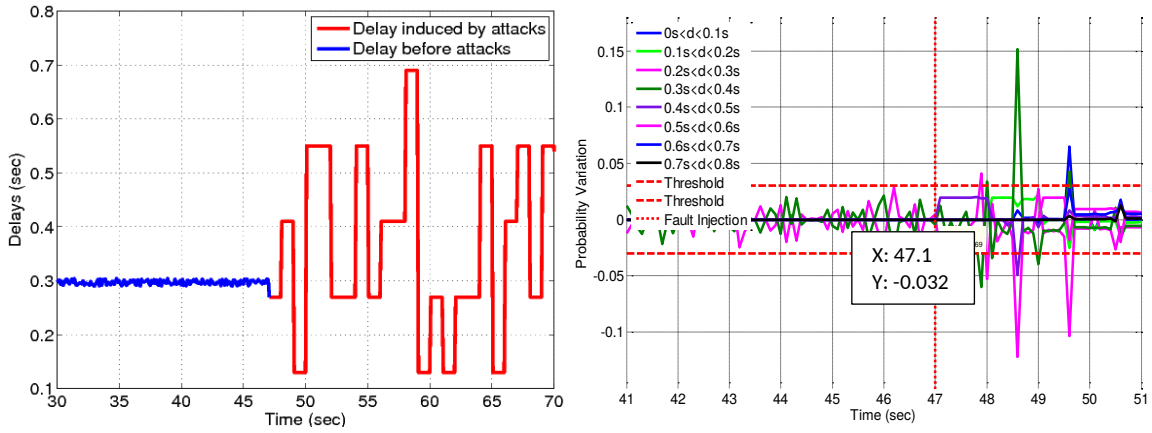


Figure 5. Case C: a) The simulated delays
b) Selected probability variation

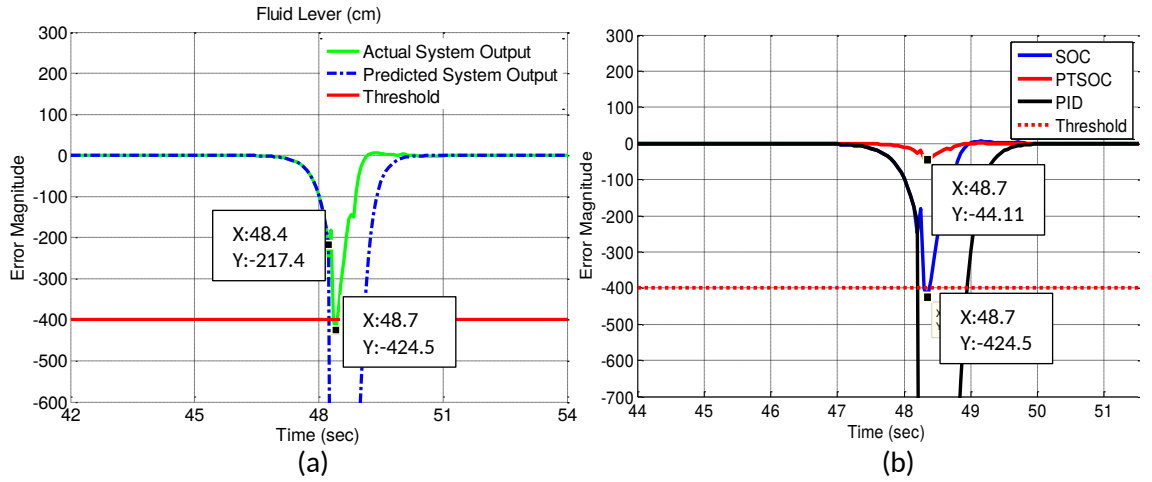


Figure 6. Case C: a) Predicted and actual system output
b) Fault mitigation performance

5.4. Discussion

We conducted 100 simulations with 50 soft and 50 hard fault cases and, to evaluate the isolation accuracy of the proposed scheme. All of the faults are detected. However, 58 hard faults are identified, that is 8 soft faults are incorrectly recognized as hard faults. The threshold for fault isolation is set ensure 100% correct isolation of hard faults. Those false hard fault identification have no negative impact on system stability and performance, only increase the computational overhead.

It is important to note that the traditional physical system fault detection, which is a model-based observer, cannot detect any abnormalities in cyberspace. The network dynamics concurrently change the mathematical model of the physical system and the model used for observer design. Such that the outputs from the observer and physical system are same. Therefore, the model-based observer can only be used for physical component fault detection, not cyber network fault. In addition, designing an traditional observer for cyber network fault detection is impossible because, in realistic CPS, cyber network fault model cannot be obtained ahead of time.

6. CONCLUSIONS

The proposed novel prognosis scheme is shown to quickly detect and predict cyber network faults using PDF monitoring and estimation. Moreover, soft and hard faults are isolated to optimize the computational cost of resilience control. The convergence of the future delay distribution estimation and the system state prediction are theoretically proven. With the proposed resilience controller, the adverse effects caused by cyber network faults are efficiently mitigated.

The simulation results show that the proposed scheme accurately detect the cyber network faults before the performance degrades beyond the acceptable range. Moreover, the PTSOC is timely triggered to mitigate the negative effects on the CPSs performance.

The overshoot is significantly reduced by 90% and TTR is shorten by 30%. Although the accuracy of the soft and hard fault isolation can only achieve 84%, the hard faults are 100% detected. Those soft faults which are misclassified to hard faults only consume the resources for triggering resilience controller. However, the stability of the entire CPS is always guaranteed.

REFERENCES

Amin, S., Cárdenas, A. A., and Sastry, S., 'Safe and secure networked control systems under denial-of-service attacks.' in 'HSCC,' volume 5469, Springer, 2009 pp. 31–45.

Bi, S. and Zawodniok, M., 'Pdf based tuning of stochastic optimal controller design for cyber-physical systems with uncertain delay dynamics,' IET Cyber-Physical Systems: Theory & Applications, 2017, **2**(1), pp. 1–9.

Cardenas, A. A., Amin, S., and Sastry, S., 'Secure control: Towards survivable cyber-physical systems,' in 'Distributed Computing Systems Workshops, 2008. ICDCS'08. 28th International Conference on,' IEEE, 2008 pp. 495–500.

Fisher, A., Jacobson, C. A., Lee, E. A., Murray, R. M., Sangiovanni-Vincentelli, A., and Scholte, E., 'Industrial cyber-physical systems–icyphy,' in 'Complex Systems Design & Management,' pp. 21–37, Springer, 2014.

Gamage, T. T., McMillin, B. M., and Roth, T. P., 'Enforcing information flow security properties in cyber-physical systems: A generalized framework based on compensation,' in 'Computer Software and Applications Conference Workshops (COMPSACW), 2010 IEEE 34th Annual,' IEEE, 2010 pp. 158–163.

Jiang, W., Guo, W., and Sang, N., 'Periodic real-time message scheduling for confidentiality-aware cyber-physical system in wireless networks,' in 'Frontier of Computer Science and Technology (FCST), 2010 Fifth International Conference on,' IEEE, 2010 pp. 355–360.

Liu, F.-C. and Yao, Y., 'Modeling and analysis of networked control systems using hidden markov models,' in 'Machine Learning and Cybernetics, 2005. Proceedings of 2005 International Conference on,' volume 2, IEEE, 2005 pp. 928–931.

Liu, G.-P., Xia, Y., Chen, J., Rees, D., and Hu, W., 'Networked predictive control of systems with random network delays in both forward and feedback channels,' IEEE Transactions on Industrial Electronics, 2007, **54**(3), pp. 1282–1297.

Liu, Y., Ning, P., and Reiter, M. K., 'False data injection attacks against state estimation in electric power grids,' ACM Transactions on Information and System Security (TISSEC), 2011, **14**(1), p. 13.

Mo, Y. and Sinopoli, B., 'Secure control against replay attacks,' in 'Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on,' IEEE, 2009 pp. 911–918.

Pasqualetti, F., Dörfler, F., and Bullo, F., 'Attack detection and identification in cyber-physical systems,' IEEE Transactions on Automatic Control, 2013, **58**(11), pp. 2715–2729.

Qin, S. J., 'Recursive pls algorithms for adaptive data modeling,' Computers & Chemical Engineering, 1998, **22**(4-5), pp. 503–514.

Rawat, D. B., Rodrigues, J. J., and Stojmenovic, I., *Cyber-physical systems: from theory to practice*, CRC Press, 2015.

Simon, D., *Optimal state estimation: Kalman, H infinity, and nonlinear approaches*, John Wiley & Sons, 2006.

Smith, R. S., 'A decoupled feedback structure for covertly appropriating networked control systems,' IFAC Proceedings Volumes, 2011, **44**(1), pp. 90–95.

Teixeira, A., Amin, S., Sandberg, H., Johansson, K. H., and Sastry, S. S., 'Cyber security analysis of state estimators in electric power systems,' in 'Decision and Control (CDC), 2010 49th IEEE Conference on,' IEEE, 2010 pp. 5991–5998.

Wang, Y., Ding, S. X., Ye, H., and Wang, G., 'A new fault detection scheme for networked control systems subject to uncertain time-varying delay,' IEEE Transactions on signal processing, 2008, **56**(10), pp. 5258–5268.

Xu, H., Jagannathan, S., and Lewis, F. L., 'Stochastic optimal control of unknown linear networked control system in the presence of random delays and packet losses,' Automatica, 2012, **48**(6), pp. 1017–1030.

Yağdereli, E., Gemci, C., and Aktaş, A. Z., 'A study on cyber-security of autonomous and unmanned vehicles,' The Journal of Defense Modeling and Simulation, 2015, **12**(4), pp. 369–381.

Zhang, H., Yang, J., and Su, C.-Y., 'Ts fuzzy-model-based robust $h\infty$ design for networked control systems with uncertainties,' IEEE Transactions on Industrial Informatics, 2007, **3**(4), pp. 289–301.

Zhang-qing, Z. and Xian-zhong, Z., 'Fault detection based on the states observer for networked control systems with uncertain long time-delay,' in 'Automation and Logistics, 2007 IEEE International Conference on,' IEEE, 2007 pp. 2320–2324.

Zhu, M. and Martinez, S., 'Stackelberg-game analysis of correlated attacks in cyber-physical systems,' in 'American Control Conference (ACC), 2011,' IEEE, 2011 pp. 4063–4068.

V. ONE-CLASS SVM-BASED CYBER NETWORK FAULT PROGNOSTICS IN CYBER-PHYSICAL SYSTEMS

Shanshan Bi, Maciej Zawodniok

Department of Electrical & Computer Engineering

Missouri University of Science and Technology

Rolla, Missouri 65409–0050

Tel: 573–341–6622, Fax: 573–341–4115

Email: sbn65@mst.edu

ABSTRACT

Cyber-physical systems (CPSs) according to NSF require seamless integration of computational algorithms and physical component. The performance of the embedded network which delivers signals between computational world and physical components likely influence on the physical system performance in terms of functionality and stability. Our objective is to enable efficient development of high-resilience CPSs that is a system capable of changing its behavior and structure to adapt to dynamic uncertainties in cyber space, such as cyber attacks, delay variation, and packet losses. Motivated by this, we propose an one-class support vector machine (OCSVM) based prognostic scheme to detect cyber network faults and predicted its effects on physical world, leading to predictable and reliable behavior of the entire CPS. Then, a fault tolerant control is triggered at an appropriate time to prevent unscheduled down-time and minimize the computational overhead. Finally, we analyze and validate the proposed scheme in simulations.

Keywords: Cyber-physical system, fault prognostic, one-class SVM, networked control system, resilience

1. INTRODUCTION

Cyber-physical systems (CPS) plays an increasingly important role in industry and everyday life. Self-driving cars, smart building controls, and smart grids are examples of CPSs. All these applications include smart networked subsystems with embedded sensors, processors, and actuators that sense and interact with the physical world. Whether enhancing the forward collision prevention capability of a car, or improving the energy efficiency of a building, CPSs are a source of competitive advantage in today's innovation economy. At the same time, networking the system components or subsystems increases the complexity and vulnerability of the entire system, such as cyber security risks and attacks. The consequences of cyber network faults could have severe impact on human lives and the environment. Proactive efforts are needed to strengthen resilience and reliability for CPSs.

The overarching goal of this work is to ensure CPS network vulnerabilities are online identified and addressed during physical system designs. For soft faults that affects network performance but has no influence on physical system performance and stability, a warning should be provided to human operators. Otherwise, hard faults resulting in hardware or components get unrepairable damages and instability should be detected and addressed ahead of time.

Inspired by this motivation, we proposed a novel prognosis scheme. The main contributions are:

a) A novel one-class SVM based prognosis scheme for cyber network fault detection and prediction.

b) Derived the estimation of network delay distribution based on time series analysis. The convergence of the estimation error is presented in **Lemma 1**.

c) Proposed an isolation scheme to distinguish soft and hard faults based on the prediction of potential failures on system states. **Theorem 1** shows the convergence of such prediction.

d) Developed a decision making scheme for proactively triggering resilience control that effectively avoids physical system failures.

The rest paper is organized as following. In Section. 2, a motivation example is given to illustrate the relationship of cyber condition and system behavior. Next, the related works on SVM based fault diagnosis and prognosis are presented in Section. 3. In Section. 4, the proposed OCSVM based prognosis scheme is demonstrated. The simulation results are shown in Section. 5 and the conclusions are given in Section. 6.

2. MOTIVATION

In this section, an example is given to illustrate the relation between cyber uncertainties/faults and system behavior. A feedback loop with the simulated delays employs an optimal controller to regulate a two input four output (2I4O) system Xu *et al.* (2012).

As a fault scenario, we assume that a route hijacking occurs to eavesdrop control information is emulated. Such an attack increases delay and delay variation when the attacker secretly relays and possibly alters the communication between the controller and actuators. The simulated network has a random topology of 11 nodes. The route through the topology is altered because the attacker node relays the transmission such that the packet delays vary for the controller loop, as shown in Fig. 1.

Fig. 2 shows the optimal controller making the system states converge before $10.5s$. Then, a route hijacking attack occurs. The sudden changes of delay at $t = 10.5s$ makes the system states vibrate. Consequently, the CPS becomes unstable due to such delay dynamics.

According to the above results, we can conclude that stochastic network dynamics indeed affect the system performance. It is important to note that delay dynamics may occur due to other network failures, such as traffic congestion, hardware damages in network, and other types of cyber attacks. Cyberspace is particularly difficult to secure due to its vulnerabilities of linkages between cyber and physical systems. Of growing concern is the cyber threat to critical hardware devices. Cyber attacks could cause harm or disrupt

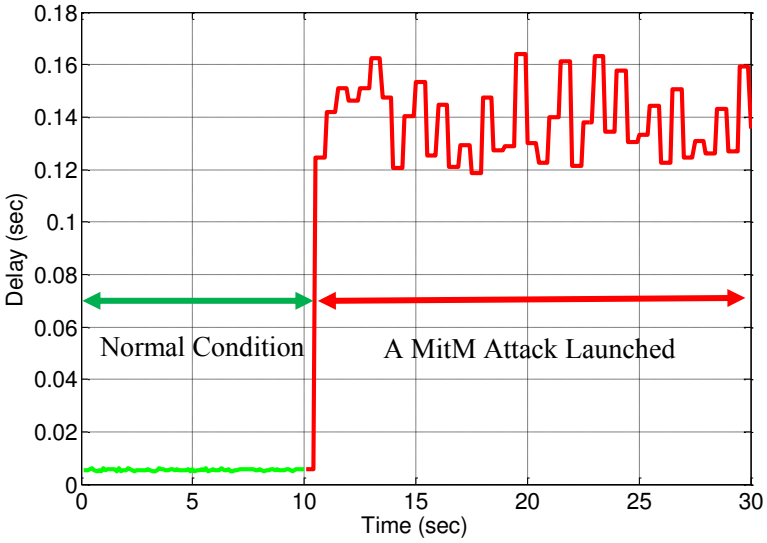


Figure 1. Delays

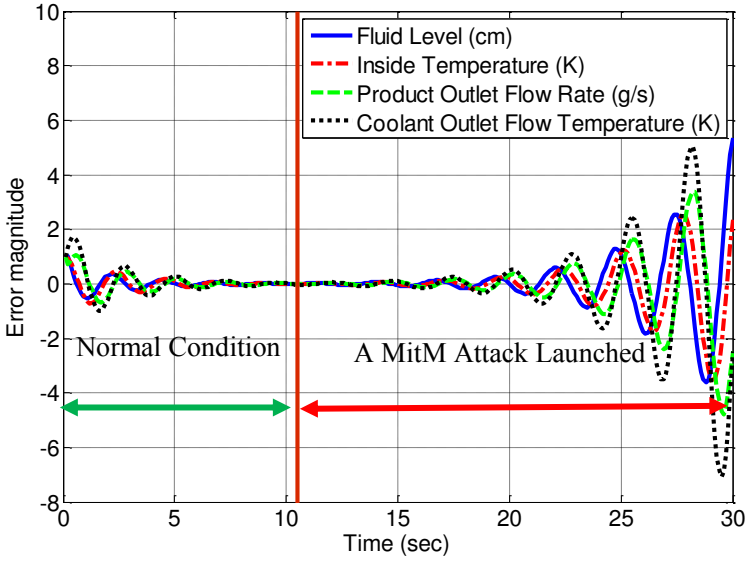


Figure 2. Tracking errors of optimal controller

services upon which our economy and the daily lives depend on. In light of the risk and potential consequences of cyber events, strengthening the risk awareness and resilience of CPSs has become an important mission.

3. RELATED WORKS

In this section, the related works about SVM and and fault diagnosis and prognosis are presented separately. Section. 3.1 introduces the successful application of SVMs in fault diagnosis and prognosis. Then, the literature review about addressing network uncertainties and dynamics in CPSs is presented in Section. 3.2.

3.1. SVM-based Approaches for Fault Diagnosis and Prognosis

Support vector machine (SVM) is a computational learning method based on the statistical learning theory. Such technology becomes popular fault diagnostic and prognostic field due to the excellence of data classification than the traditional method such as neural network. In SVM community, one-class SVM (OCSVM) that can separate the data with different distributions is suitable for the issues to be addressed in our work. According to the motivation example, the system instability is not induced by the occasionally long time delay, but by the stochastic dynamics of delay and its distribution defined as cyber network faults. Therefore, we propose an OCSVM based fault prognostic scheme to capture cyber network faults and optimize the resilience control triggering.

Next, a survey of fault diagnosis and prognosis using SVM is presented.

The earliest application of SVM for fault diagnosis is Yan and Shao (2002). They didn't proposed any novel method for fault diagnosis. However, they first time employed an non-linear SVM to classify healthy and faulty data samples.

Then, many researchers applied SVMs for fault diagnosis to bearing, induction motor, machine tools, and other industrial system components, such as pump, compressors, valve and turbine. In addition, the revised or improved SVMs are widely used in fault

diagnosis of HVAC system, engine, rotating machine Yuan and Chu (2006), Yuan and Chu (2007), and other machines. Samanta (2004) and Samanta (2004) employed genetic algorithm (GA) to optimize the parameters of SVMs and extract features from original and preprocessed signals. The trained SVM classifier was validated using the experimental vibration data of a rotating machine and presented a better performance than artificial neural network (ANN) based fault detection.

Zhang *et al.* (2006) proposed a learning method of probabilistic active SVM (ProASVM) to detect fault of bearing with less number of samples on the condition of keeping the classification accuracy. Sugumaran *et al.* (2007) employed decision tree (DT) and proximal SVM (PSVM) to do fault diagnosis of roller bearing. Hu *et al.* (2007) proposed a scheme combining wavelet package transform and SVM ensemble for fault diagnosis of rolling element bearing.

In addition, Widodo *et al.* (2007) - Widodo and Yang (2008) applied SVM combined by feature extraction via component analysis (PCA, ICA, KPCA, and KICA) to fault diagnosis. Later, an advanced wavelet SVM (W-SVM) is proposed to improve the transient current signal classification. Yuan and Chu (2006), Yuan and Chu (2007) applied PCA to extract the optimal features and reduce the dimension of features. Then, artificial immunization algorithm was used to optimize the parameters of SVM. The above SVM-based fault diagnosis performed well with a plenty of data and a relatively enough training time. However, these methods might not be suitable for complicated system fault diagnosis, such as CPSs, because the collected data are massive, thus the training time could be too long to feedback the fault information timely. Therefore, an improved SVM which potentially provides a good performance on fault diagnosis in terms of accuracy, training time, and dateset requirement is expected and needed.

Inspired by this motivation, Yin *et al.* (2014) proposed a hybrid voting mechanism based SVM (HVM-SVM) for satellite fault diagnosis with considering the characteristics of small training data, multiple faults, and enormous parameters. The accuracy of fault classification was validated.

Salahshoor *et al.* (2010) proposed a novel fault detection and diagnosis scheme for condition machinery of an industrial steam turbine using the fusion of a SVM and adaptive neuro-fuzzy inference system (ANFIS). Such methodology can deal with a diverse set of faults. Wang *et al.* (2014) proposed a ν-SVM which used the nearest neighbor (NN) to realize the fast selection of ν based on training samples and applied locality preserving projection (LPP) method to reduce the dimension of feature vectors by extracting the lower dimensional manifold characteristics. Such that the training time was reduced as well as computational overhead. Each residual work is designed to be sensitive to a subset of faults, while remain insensitive to other faults. Unfortunately, few of the above works can be applied to network fault prognosis in CPSs because network fault is diverse, stochastic, and unpredictable about its type and time of occurrence.

Hence, a general and efficient fault prognosis scheme that can detect different types of fault and predict their effects on the entire CPS is needed. The work presented in this paper mainly focuses on cyber network fault prognosis of CPSs by a novel fusion of one-class SVM, PDF identification, and system state prediction.

3.2. Fault Diagnosis and Prognosis of CPSs

The overall goals of cyber security include integrity (the trustworthiness of data or resources), availability (accessibility upon demand), and confidentiality (keeping information secret from unauthorized users). Many researchers addressed these issues with different technologies, such as authentication schemes, access control, and other defense schemes Amin *et al.* (2009) - Pasqualetti *et al.* (2013). An assumption that the adversary/attack model is fully known is often required; however, it is challenging to obtain. In Amin

et al. (2009) deception and denial of service attacks against a networked control system are addressed. They proposed a countermeasure based on semi-definite programming. This work and the following literature are only valid for a specific attack model which cannot be known in priori. A defense scheme without requiring the knowledge about the attack model is needed.

In Liu *et al.* (2011), false data injection attacks against static state estimators are introduced. Undetectable false data injection attacks can be designed even when the attacker has limited resources. Also, stealthy deception attacks against the Supervisory Control and Data Acquisition system are studied in Teixeira *et al.* (2010). Mo and Sinopoli (2009) studied the effect of replay attacks on a control system. In Amin *et al.* (2009), the effect of covert attacks against control systems is investigated. A parameterized decoupling structure alter the behavior of the physical plant while remaining undetected from the original controller. Gamage *et al.* (2010) proposed a general theory of event compensation as an information flow security enforcement mechanism for CPSs. Message scheduling methods were given to improve the security quality of wireless networks for mission-critical CPSs in Jiang *et al.* (2010). With respect to the above works, Pasqualetti *et al.* (2013) proposed a mathematical framework for CPSs, attacks, and monitors, and given the fundamental limitations of monitors from system-theoretic and graph-theoretic perspectives. Finally, centralized and distributed attack detection and identification monitors were designed. Overall, many cyber attacks can be addressed on the cyber side. However, the effects of cyber attacks/faults on the physical system behavior are oversimplified in the above mentioned existing works. Moreover, the injection time and model of the attacks/faults are difficult to learn ahead of time in practical CPSs.

The control researchers focused on the conventional fault detection techniques that have successfully applied to industrial networked control systems (NCSs). They indeed considered the network delay and packet loss in various ways. In Zhu and Martinez (2011), a resilient control problem is studied, in which control packets transmitted over a network

are corrupted by a human adversary. They proposed a receding-horizon Stackelberg control law to stabilize the control system despite the attack. However, the proposed approach required a priori knowledge on attack model and type. In Liu and Yao (2005), network delays were modeled as a constant delay (time buffer), an independent random delay, and a delay with known probability distribution governed by the Markov chain model. In Liu *et al.* (2007), a networked predictive controller in the presence of random delay in both forward and feedback channels was proposed to minimized the effects of network failures. A robust H_∞ control for a nonlinear T-S fuzzy model system was proposed to address the network delays and packet drop in Zhang *et al.* (2007). However, they assumed the upper bound of delays is known. This is challenging to be satisfied in reality. Wang *et al.* (2008) and Zhang-qing and Xian-zhong (2007) employed a state observer-based fault detection method on the uncertain long time delay. Although, the network delays and packet drop caused by network faults/failures were considered in above works, the assumptions, such as known bounds and time-invariant distribution of delays and packet loss, are always made. In addition, most of the above works aimed to detect the faults of physical components (sensors, actuators, and system plant), not the faults in the cyberspace.

This work is motivated to address cyber network faults detection, isolation, and prediction. Meanwhile, the the tolerant control scheme and it triggering strategy are proposed to stabilize the CPS despite cyber network faults and optimize the computational overhead.

4. OCSVM-BASED CYBER NETWORK FAULT PROGNOSIS SCHEME

In this section, the overview of the OCSVM-based cyber fault prognosis scheme is given in Section. 4.1. The main idea of the fault detection is introduced in Section.4.2. Then, the isolation of cyber hard and soft fault is demonstrated in Section. 4.3. At last the resilience control scheme is introduced in Section. 4.4.

4.1. Overview

In this work, the uncertainties in the cyberspace, including traffic congestions, topology changes, and attacks, are considered erroneous delays and packet losses on the physical system side. Monitoring such delays and packet losses online is required for detection of cyber faults. Moreover, an observer is needed to detect physical system faults and isolate them from cyber network faults.

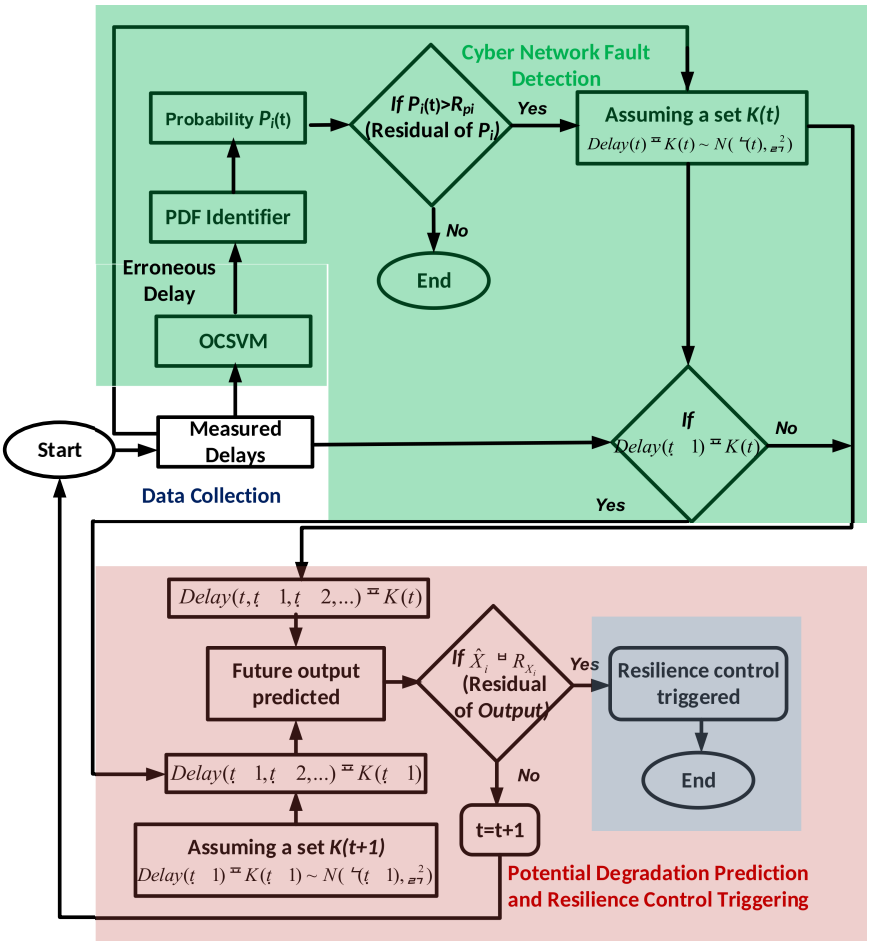


Figure 3. Flowchart of OCSVM-based prognosis scheme

The proposed prognosis scheme is shown in Fig. 3. It includes four main steps that are continuous repeated:

a) Data collection of network delays. n delays ($[d_{k-n+1}, \cdots, d_k]$) in the sliding window will be the inputs of OCSVM to labeled as normal or erroneous data. The data in the sliding window is updated over time.

b) Cyber fault detection. The input delays are classified into normal and abnormal group. When the new abnormal delay is labeled, we consider an abnormality occurs in the cyberspace. However, only one abnormal delay detection can not be consider a cyber network fault because unexpected delay might presents even the cyber condition is perfect. Therefore, the probability for erroneous delays P_f^k is calculate and a threshold R_{p_f} is defined. If P_f^k exceeds R_{p_f}, the cyber network fault is detected and the following computation for fault isolation is active as the same time.

c) Potential degradation prediction. If a cyber network fault is detected, the PDF of erroneous delay distribution is predicted by using time series analysis. Then, the delays following the new distribution are resampled. Finally, the prediction of the physical system states is obtained. If the system states deviate out of the acceptable range, the hard fault is detected. Such type of faults might lead to wear and tear of devices, instability of the entire CPSs, even hardware damages. Otherwise, the soft fault is not severe enough to trigger the resilience controller. It is hard to detect by traditional fault diagnosis schemes because such faults will not immediately affect the CPS stability. Hence, an early warning could be missed. However, such type of faults should not be ignored because they might become severe problems in the near future. Therefore, detecting them and giving a warning to the human operators are necessary and essential. More details about fault isolation are presented in Section. 4.3.

d) Resilience controller triggering. If a hard fault is detected, the resilience controller is triggered and its parameters are tuned online by the probabilities of delays computed in c).

Such a scheme can detect stochastic cyber failures/attacks without requiring the knowledge of attack model and its injection time a priori. Only real-time OCSVM classification of delays is required to do distribution and system states prediction. Moreover, the resilience control law tuned by the probabilities of predicted delays is derived accurately for the given cyber performance. Its details are introduced in Section. 4.4.

4.2. OCSVM-based Cyber Network Fault Detection

One-class SVM model estimates the support of a distribution by identifying regions in input space where most of the cases lie. It projects the data into a feature space, in where separating the data from the origin by as large a margin as possible.

In this paper, we are interested in the ability of the one-class SVM algorithm to model the distribution of network delays, i.e., the normal delays without cyber fault. All abnormal delays will be recognized as outliers. These outliers are the inputs of system state predictor to predict the potential threats for the system stability.

To facilitate the identification of outliers as abnormal delays, we assume the distribution of normal delays are known. The one-class SVM can model a decision boundary of there normal delays. When the outliers are detected, we consider an abnormality happens. Then, the abnormal delays can be classified to one of "healthy" and "faulty" group.

To give a precise problem statement for the one-class SVM algorithm, some notations are needed:

a) Let $\Phi : \Re^n \rightarrow F$ be the nonlinear mapping from data space $\Re^n$ to feature space F that is implicit and usually unknown in all kernel method;

b) ξ_i is slack variable for each point in the dataset;

c) ρ is the distance to the origin in feature space;

d) ω is the parametrization of the hyper-plane separating the origin from the data in F;

e) ν is the expected fraction of data points outside the estimated support.

The one-class SVM algorithm computes the support vectors in D by considering the constrained quadratic optimization problem (primal form):

$$\min_{\omega \in F, \xi_i \in \Re^n, \rho \in \Re} \qquad \frac{1}{2} \parallel \omega \parallel^2 + \frac{1}{m\nu} \Sigma_{i=1}^{m} \xi_i - \rho \tag{1}$$

subject to

$$\omega \Phi(x_i) \geq \rho - \xi_i,$$

$$\xi_i \geq 0 \qquad \forall i = 1, \ldots, m$$

which is transformed into its dual form:

$$\min_{\alpha \in \Re^n} \qquad \sum_{i,j=1}^{m} \alpha_i \alpha_j k(x_i, x_j) \tag{2}$$

subject to

$$0 \leq \alpha_i \leq \frac{1}{m\nu} \qquad \forall_i = 1, \ldots, m$$

$$\sum_{i=1}^{m} \alpha_i = 1$$

to introduce the kernel function $k(x_i, x_j) = \Phi(x_i).\Phi(x_i)$ into the calculation.

α_i can be obtained by solving the dual problem and the decision function (3) can be obtained.

$$f(x) = \sum_{i=1}^{m} \alpha_i k(x_i, x) - \rho \tag{3}$$

If x is an outlier, $f(x)$ will be a negative value. The data points x_i for which $0 < \alpha_i < \frac{1}{m\nu}$ holds are the support vectors; They directly lie on the separating hyperplane in F.

Here, we used the Gaussian (4) with width parameter σ as kernel function.

$$k(x_i, x) = exp(-\frac{\parallel x_i - x \parallel^2}{2\sigma^2}) \tag{4}$$

By using this method, erroneous delays and it distribution can be easily obtained for the next fault isolation.

4.3. Soft and Hard Cyber Network Fault Isolation

In this subsection, an algorithm for distinguishing soft and hard cyber network faults is proposed. First, the delay distribution in the future is predicted. Next, its potential effects on system performance is evaluated.

The isolation scheme includes three main steps that are repeated until the resilience controller is triggered:

Step 1: future delay distribution estimation and resampling;

Step 2: system performance prediction;

Step 3: soft and hard fault isolation and resilience control triggering

These steps are discussed in details next.

4.3.1. Step 1: Future Delay Distribution Estimation and Resampling. One-class SVM provides the faulty delays. Then, the KDE-based PDF identifier Bi and Zawodniok (2017) can estimate the distribution of those delays assuming they follow a normal distribution. The expectation and standard deviation can be obtained.

Time series analysis is used to estimate the autoregressive (AR) model for the expectation E and standard deviation D of the future distribution. The main point of this algorithm is that use the difference between the estimate of the future expectation and actual one to update the coefficients of AR model. When the coefficients converge, the AR model can provide an accurate approximation of the future distribution features. The following part presents the details about our application.

The hypothesis of the model is given by:

$$\begin{bmatrix} E(k+1|k) \\ D(k+1|k) \end{bmatrix} = \begin{bmatrix} \beta_{E0} \\ \beta_{D0} \end{bmatrix} + \begin{bmatrix} \beta_{E1} & 0 \\ 0 & \beta_{D1} \end{bmatrix} \begin{bmatrix} E(k) \\ D(k) \end{bmatrix} \tag{5}$$

where $\widehat{E}(k+1|k)$ is the forecast of $E(k+1|k)$ and $D(k+1|k)$ based on $E(k)$ and $D(k)$, using the estimated coefficients $\widehat{\beta}_{E0}$, $\widehat{\beta}_{D0}$, $\widehat{\beta}_{E1}$, and $\widehat{\beta}_{D1}$ that are to be tuned by the update law (9).

$$\begin{aligned}\begin{bmatrix}\widehat{E}(k+1|k)\\ \widehat{D}(k+1|k)\end{bmatrix} &= \begin{bmatrix}\widehat{\beta}_{E0}\\ \widehat{\beta}_{D0}\end{bmatrix} + \begin{bmatrix}\widehat{\beta}_{E1}(k) & 0\\ 0 & \widehat{\beta}_{D1}(k)\end{bmatrix}\begin{bmatrix}E(k)\\ D(k)\end{bmatrix}\\ &= \widehat{\theta}(k)\varphi(k) + C_0(k)\end{aligned} \tag{6}$$

where $\varphi(k) = \begin{bmatrix}E(k) & D(k)\end{bmatrix}^T$, and $\widehat{\theta}(k) = \begin{bmatrix}\widehat{\beta}_{E1}(k) & 0\\ 0 & \widehat{\beta}_{D1}(k)\end{bmatrix}$.

The one-period ahead forecast error is:

$$\begin{bmatrix}e_E(k+1)\\ e_D(k+1)\end{bmatrix} = \begin{bmatrix}E(k+1|k)\\ D(k+1|k)\end{bmatrix} - \begin{bmatrix}\widehat{E}(k+1|k)\\ \widehat{D}(k+1|k)\end{bmatrix} \tag{7}$$

The forecast errors converge by minimizing the following objective index:

$$J = \begin{bmatrix}e_E(k+1)\\ e_D(k+1)\end{bmatrix}^T \begin{bmatrix}e_E(k+1)\\ e_D(k+1)\end{bmatrix} \tag{8}$$

Such that the update law of $\widehat{\theta}(k)$, $L(k)$, and $O(k)$ can be obtained.

$$\begin{aligned}\widehat{\theta}(k) &= \widehat{\theta}(k-1) + L(k)e(k)\\ L(k) &= \frac{O(k-1)\varphi(k)}{\varphi(k)^T O(k-1)\varphi(k)}\\ O(k) &= (I - L(k)\varphi(k)^T)O(k-1)\end{aligned} \tag{9}$$

where $L(k)$ and $O(k)$ denote estimator gain and estimation of error variance, respectively. Their initial values are randomly set.

Lemma 1: With the update law (9) and more new delays loaded in the sliding window, the objective index (8) is continuously minimized. Then the following statements are true:

a) the estimation errors of the expected value and standard deviation of faulty delays converge.

b) $\left(\| \sum_{j=1}^{n} \widetilde{P}_{(k+1)j} \| - \| \sum_{j=1}^{n} \widetilde{P}_{kj} \| \right) < 0$ holds.

The proof can be found in Qin (1998) and Simon (2006).

Remark 1: Even if the network condition is perfect, unexpected delays, which are out of the healthy range, occasionally occurs in a long period. That can lead to the inefficient triggering of resilience control. Using the above time series analysis, not only the distribution change can be tracked in real-time, but also the trend of distribution change is identified and predicted. Such that the occasional event can be filtered without resilience control triggering.

Then, based on the future delay distribution provided by (1), a series of random delays is generated, which follows the new distribution.

4.3.2. Step 2: System Output Prediction. The resampled delays are fed to the system model which takes into account dynamic delays and packet losses. Such a time-varying system is given by:

$$z(k+1) = A_z(k)z(k) + B_z(k)u(k) \tag{10}$$

where $z = \begin{bmatrix} x(k)^T & u(k-1)^T & \dots & u(k-d)^T \end{bmatrix}^T$ is the state variables vector; u_k is the control input; $A_z(k)$ and $B_z(k)$ are the system dynamic matrices and given by

$$A_z(k) = \begin{bmatrix} A & \gamma(k-1)B_1(k) & \dots & \gamma(k-i)B_i(k) & \dots & \gamma(k-d)B_d(k) \\ 0 & 0 & \dots & \dots & \dots & 0 \\ 0 & I_m & \dots & \dots & 0 & 0 \\ \vdots & 0 & I_m & \dots & \dots & 0 \\ \vdots & \vdots & & \ddots & & \vdots \\ 0 & 0 & \dots & \dots & I_m & 0 \end{bmatrix},$$

$$B_z(k) = \begin{bmatrix} \gamma(k)B_0(k) & I_m & 0 & 0 & \vdots & 0 \end{bmatrix}^T,$$

$$\gamma(k) = \begin{cases} I^{n\times n} & \text{if the control input is received at time k} \\ 0^{n\times n} & \text{if the control input is lost at time k} \end{cases}$$

Finally, the possible system behavior induced by the new distribution of delays are estimated and denoted as $\widehat{z}_k$.

Prediction Convergence Analysis: The prediction error $\widetilde{z}_k$ convergence is demonstrated in **Theorem 1**. The dynamic matrices A_{zj} and B_{zj} for each delay interval are deterministic and their calculation can be found in Xu *et al.* (2012).

Theorem 1 (Error of system states prediction convergence): As the delay data keeps updating PDF identifier and $\left(\parallel \sum_{j=1}^{n} \widetilde{P}_{(k+1)j} \parallel - \parallel \sum_{j=1}^{n} \widetilde{P}_{kj} \parallel \right) < 0$ is satisfied, then the prediction error for system output $\parallel \widetilde{z}(k) \parallel$ asymptotically converges to zero.

Proof: The prediction error is given by

$$\begin{aligned} \widetilde{z}_k &= z_k - \widehat{z}_k \\ &= (A_z(k) - B_z(k)K(k))z(k) - (\widehat{A}_z(k) - \widehat{B}_z(k)K(k))z(k) \\ &= (A_z(k) - \widehat{A}_z(k))z(k) - (B_z(k) - \widehat{B}_z(k))K(k)z(k) \\ &= (\widetilde{A}_z(k) - \widetilde{B}_z(k)K(k))z(k) \end{aligned}$$

Therefore, the convergence of $\widetilde{z_i}$ can be proven by proving the convergence of $\widetilde{A}_z(k)$ and $\widetilde{B}_z(k)$

We define the prediction error of $A_z(k)$ as $\widetilde{A}_z(k) = A_z(k) - \widehat{A}_z(k)$. $A_z(k)$ can be expressed as $\sum_{j=1}^{n} P_j(k)A_{zj}$ $P_j(k)$ is the actual probability at k. Similarly, we denote $\widehat{A_z(k)} = \sum_{j=1}^{n} \widehat{P}_j(k)A_{zj}$. $\widehat{P}_j(k)$ is the estimate probability provided by the PDF profile. The estimation error of the probability is $\widetilde{P}_j(k) = P_j(k) - \widehat{P}_j(k)$. Then, Lyapunov function candidate is $V_{A_z(k)} = \widetilde{A}_z(k)^T \widetilde{A}_z(k)$.

$$
\begin{aligned}
\Delta V_{A_z(k)} &= \widetilde{A}_z(k+1)^T \widetilde{A}_z(k+1) - \widetilde{A}_z(k)^T \widetilde{A}_z(k) \\
&= \Big(\sum_{j=1}^{n} P_j(k+1)A_{zj} - \sum_{j=1}^{n} \widehat{P}_j(k+1)A_{zj} \Big)^T \Big(\sum_{j=1}^{n} P_j(k+1)A_{zj} - \sum_{j=1}^{n} \widehat{P}_j(k+1)A_{zj} \Big) \\
&- \Big(\sum_{j=1}^{n} P_j(k)A_{zj} - \sum_{j=1}^{n} \widehat{P}_j(k)A_{zj} \Big)^T \Big(\sum_{j=1}^{n} P_j(k)A_{zj} - \sum_{j=1}^{n} \widehat{P}_j(k)A_{zj} \Big) \\
&= \Big(\| \sum_{j=1}^{n} \widetilde{P}_j(k+1) \|^2 - \| \sum_{j=1}^{n} \widetilde{P}_j(k) \|^2 \Big) \| A_{zj} \|^2 \\
&= \underbrace{\Big(\| \sum_{j=1}^{n} \widetilde{P}_j(k+1) \| + \| \sum_{j=1}^{n} \widetilde{P}_j(k) \| \Big)}_{\Delta_1} \\
&\Big(\| \sum_{j=1}^{n} \widetilde{P}_j(k+1) \| - \| \sum_{j=1}^{n} \widetilde{P}_j(k) \| \Big) \| A_{zj} \|^2 \\
&= \Delta_1 \Big(\| \sum_{j=1}^{n} \widetilde{P}_j(k+1) \| - \| \sum_{j=1}^{n} \widetilde{P}_j(k) \| \Big) \| A_{zj} \|^2
\end{aligned}
$$

$\Delta_1 > 0$

Since $V_{A_z(k)}$ is positive definite and $\Delta V_{A_z(k)}$ is negative definite provided $\big(\parallel \sum_{j=1}^{n} \widetilde{P}_j(k+1) \parallel - \parallel \sum_{j=1}^{n} \widetilde{P}_j(k) \parallel \big) < 0$ (**Lemma 1**). Therefore, the prediction error of $A_z(k)$ asymptotically converge to zero. Similarly, the prediction error of $B_z(k)$ can be proven with the same procedure. Such that $\widetilde{z}(k)$ asymptotically converge to zero. ■

Remark 2: The maximum error occurs when the first sample of the new distribution comes in the sliding window. Then, the accuracy of PDF estimation improves as the sliding window includes more and more new samples from the new distribution after the PDF change occurs. Therefore, $\big(\parallel \sum_{j=1}^{n} \widetilde{P}_{(k+1)j} \parallel - \parallel \sum_{j=1}^{n} \widetilde{P}_{kj} \parallel \big) < 0$ holds.

4.3.3. Step 3: Soft and Hard Fault Isolation and Resilience Control Triggering Strategy. The acceptable error magnitude of state i is defined as $R_{\widehat{z}_i}$. If the deviation of the state $\widehat{z}_i$ exceeds its residual $R_{\widehat{z}_i}$, this fault is marked as a hard cyber network fault. A warning is triggered as well as the resilience controller. Otherwise, this is a soft fault that can be handled with the original controller operating normally.

In summary, the proposed prognosis scheme can timely detect cyber network faults and isolate soft and hard faults because the dynamics of the network is continuously monitored. Accurately isolating soft and hard fault optimize the decision of resilience controller triggering as well as the computational resources allocation. When hard faults occur, the resilience controller can be timely triggered before adverse effects on system performance happening.

4.4. Resilience Control Strategy

The employed resilience controller is presented for completeness. PDF-based tuning of stochastic optimal controller (PTSOC) Bi and Zawodniok (2017) mitigates the adverse effects induced by the uncertainties of cyberspace and adapt to the random occurrence of cyber network faults. The stability analysis can be found in Bi and Zawodniok (2017).

The PTSOC control law considers the PDF of future delays by optimizing a weighted summation of cost functions of different delay ranges (11). Each weight is the probability of its corresponding delay intervals from the PDF identifier.

$$J^k = E\left[\sum_{i=1}^{n} P_i J_i^k\right] = E\left[\sum_{i=1}^{n} P_i (x_i^{kT} Q_{zi} x_i^k + u_i^{kT} R_{zi} u_i^k)\right] \tag{11}$$

where i presents the delay interval ($d_{int}i < d^k < d_{int}(i+1)$); n is the total number of delay cases; k represents sampling interval; P_i is probability of delay within $d_{int}i$ to $d_{int}(i+1)$ provided by the PDF identifier; x_i is the states vector; u_i is the control inputs vector; $Q_{zi} = diag[Q_i, \frac{R_i}{d}, ...]$ and $R_{zi} = \frac{R_i}{d}$ are symmetric positive semi-definite and symmetric positive definite respectively. $E[\bullet]$ is the expectation operator.

By optimizing (11), the control input is given by:

$$u(k) = -K(k)Z(k) \tag{12}$$

$$\begin{aligned} K(k) = \sum_{i=1}^{n_d} & P_i(k)(B_{zi}(k)^T Z_i(k) B_{zi}(k) + R_z(k))^{-1} \\ & (B_{zi}(k)^T Z_i(k) A_{zi}(k) + S_{zi}(k)) \end{aligned} \tag{13}$$

where $K(k)$ is the optimal gain and $u(k)$ is the control input; $S_{zi}(k) \geq 0$ is the solution of the algebraic riccati equation (ARE) equation; $n_d = d_{upper}/d_{int}$, d_{upper} is the maximum delay in the sliding window; $P_i(k)$ is the probability of $d_{int}i < d(k) < d_{int}(i+1)$.

5. SIMULATION AND DISCUSSION

In this section, the proposed prognosis scheme is evaluated by simulations in MATLAB. Both soft and hard cyber network fault scenarios are presented separately in Sections. 5.1 and 5.2. The resilience controller in Section. 4.4 is applied. A conventional fault detection scheme is employed as a reference.

A continuous-time batch reactor system is taken as a case study. Its dynamics are given by Xu *et al.* (2012).

$$\dot{x} = \begin{bmatrix} 1.38 & -0.2077 & 6.715 & -5.676 \\ -0.5814 & -4.29 & 0 & 0.675 \\ 1.067 & 4.273 & -6.654 & 5.893 \\ 0.048 & 4.273 & 1.343 & -2.104 \end{bmatrix} x + \begin{bmatrix} 0 & 0 \\ 5.679 & 0 \\ 1.136 & -3.146 \\ 1.136 & 0 \end{bmatrix} u = Ax + Bu \quad (14)$$

where A and B are system dynamic matrices that correspond to the A and B in (10).

The parameters of this CPS are selected as:

a) The sampling time is $100ms$;

b) The considered delays in the system model is less than 2 sampling interval, $d = 2$;

c) The delay interval d_{int} (11) is $0.1s$;

d) The threshold of the probability variation R_{pi} is $0.03s$, unless otherwise states;

e) The sliding window size M is 30.

5.1. Soft Fault Scenario

A network congestion is taken as an soft fault example. Such congestion leads to a gradually fluctuation of network delays. A big challenge of such fault detection is the distribution of the faulty data usually overlaps with the one of healthy data. Thus, the accuracy of data classification cannot be always guaranteed.

The following example will demonstrate the soft fault detection performance of the proposed scheme and also provide its limitations. The results are only for a specific scenario. Before the first $50s$, the delays follow a normal distribution $N(0.52, 0.02^2)$. Then, a network congestion attack (e.g. denial-of-service) occurs at $50s$ and the delays after $50s$ follow a new normal distribution $N(0.55, 0.1^2)$. The window size is 100.

Table 1. Fault capturing accuracy over time

Time	Precision	Recall	Accuracy
t=50.3s	0	0	0
t=50.5s	36.4%	80%	80%
t=50.7s	71.4%	71.4%	71.4%
t=50.9s	75%	72.7%	72.7%
t=51.1s	66.7%	76.9%	76.9%
t=51.3s	66.7%	76.9%	76.9%

Fig. 4 and Table. 1 shows that the proposed scheme can detect the faulty data from 50.3s. However, the accuracy is low because of the severe overlap of the healthy and fault data. As the number of faulty data increasing, the precision, recall, and accuracy are significantly improved.

When the fault is detected, the state prediction is activated to estimate the possibly negative effects on the system performance in the future. Fig. 5 shows the three time predictions at $50.3s$, $50.5s$, and $51.3s$. The oscillation are observed, but small enough for the basic controller to handle. Therefore, this fault is a soft fault. The resilience controller does not have to be triggered.

Moreover, it is clear that the state prediction becomes closer and closer to the actual system behavior over time. That is because more faulty data coming in the sliding window provides more information about the fault data distribution, thus its estimate become more and more accurate.

5.2. Hard Fault Scenario

As a hard fault scenario, a man-in-the-middle attack -attacker secretly relays and possibly alters the communication between two parties who believe they are directly communicating with each other- is simulated. The transmitted information, such as control commands and feedback measurements, can be eavesdropped and delayed.

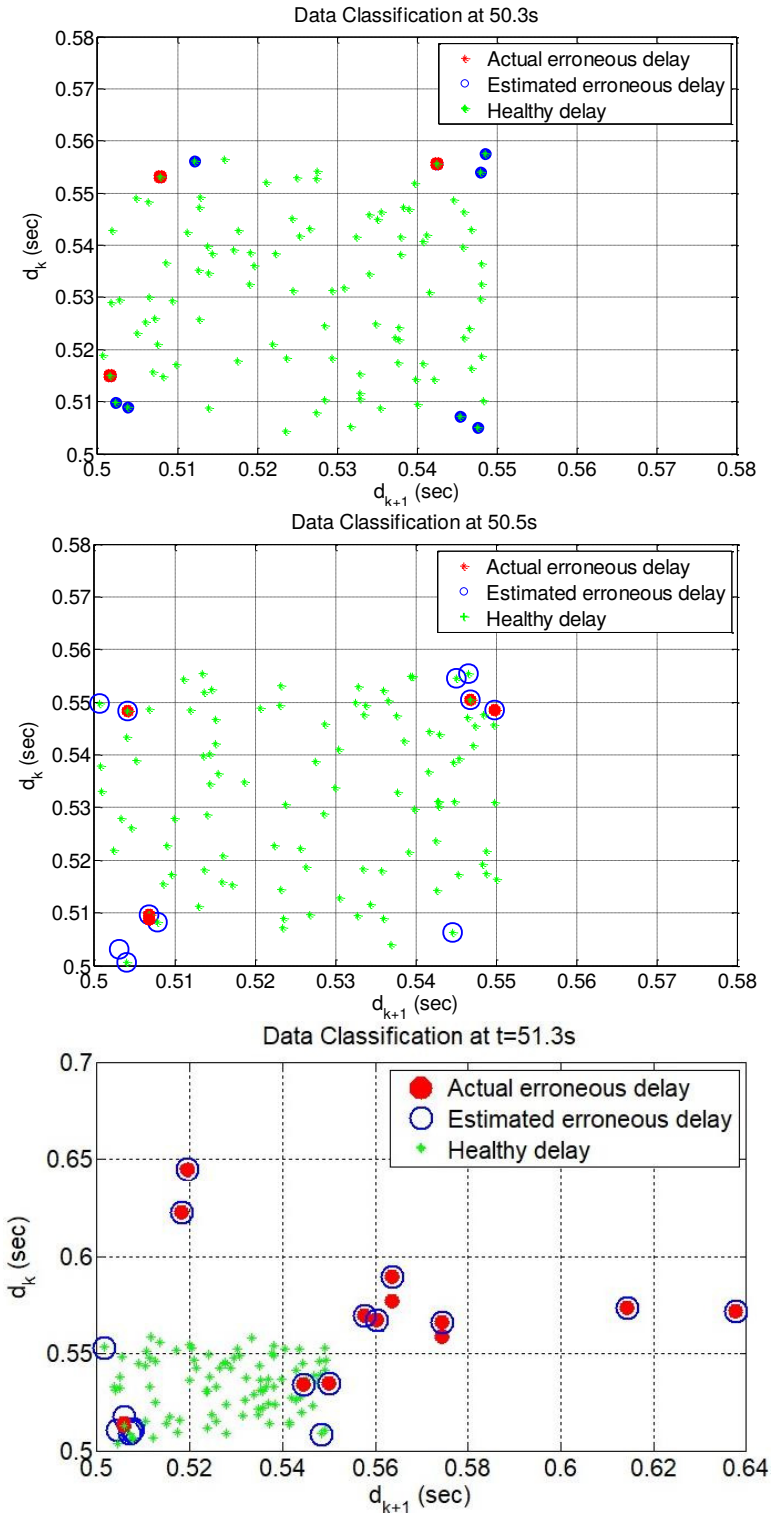


Figure 4. Data classification performance

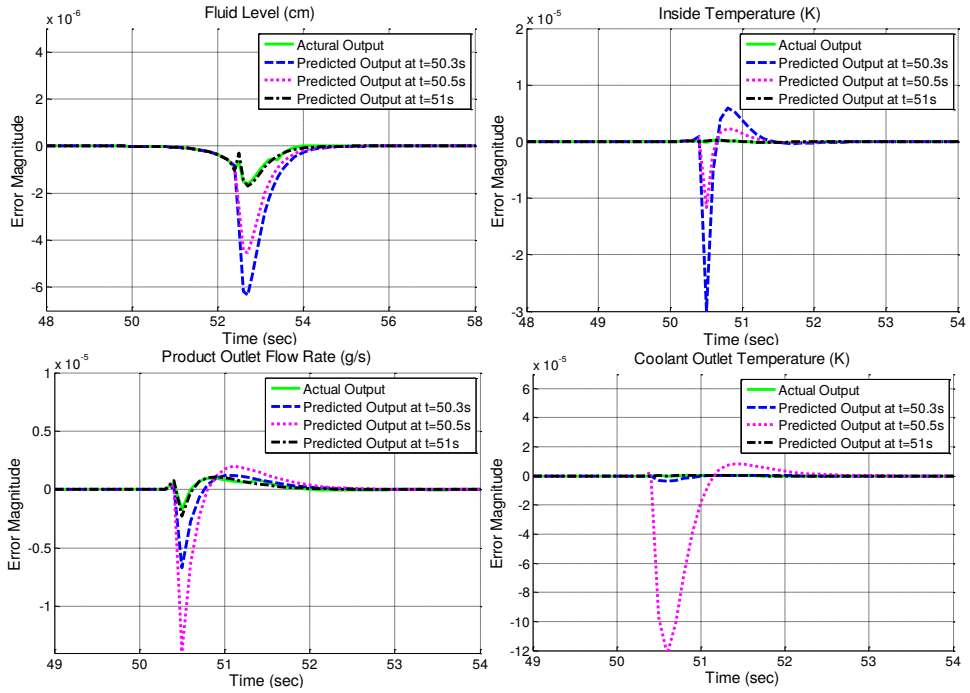


Figure 5. System states prediction performance

Table 2. The crossing points

Variables	Estimated point	Actual point	Estimation Error
Fluid level	48s	48s	0
Inside temperature	48.4s	48.6s	0.4%
Product outlet flow rate	48.2s	48.2s	0%
Coolant outlet temperature	48.2s	48.3s	0.2%

Here, the delays before $47s$ follows a normal distribution $(0.25, 0.1^2)$. Then, the attacker injects MitM attacks intermittently. As the results, the distribution of delays is varied over time. The acceptable error magnitudes are set for four system states: $100cm$ for the fluid level; $50k$ for the inside temperature; $50g/s$ for the product outlet flow rate; and $50k$ for the coolant outlet temperature.

As Fig. 6 showing, the sudden change of delay at $47s$ is detected at $t = 47.3s$, a fault is detected because the probability of faulty data exceeds the threshold (3%) as shown in Fig. 7. The actual faulty delays are 100% recognized.

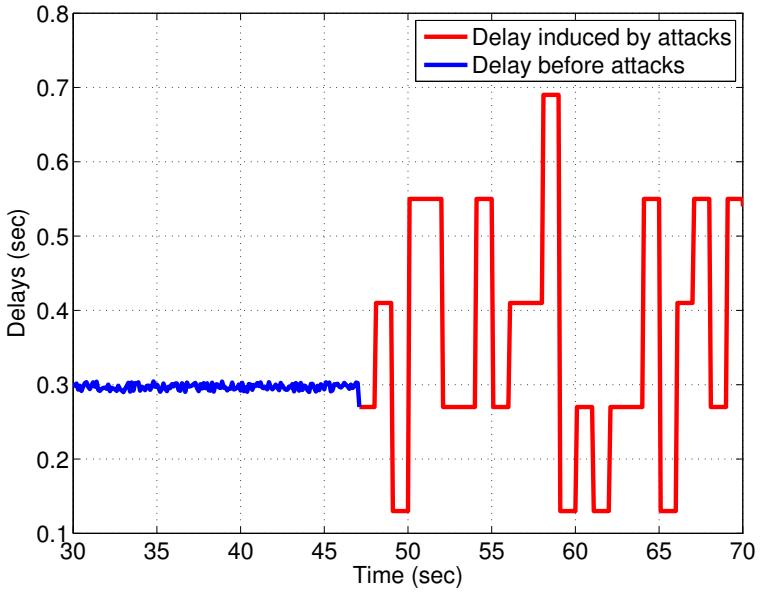


Figure 6. Delays

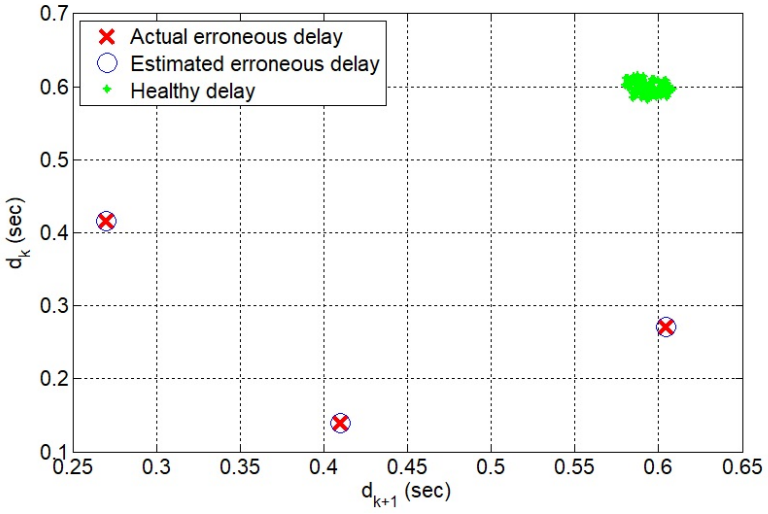


Figure 7. Data classification performance at t=47.3s

In Fig. 8 all the predicted system outputs exceed their acceptable range. The estimated and actual points that the system states pass through the acceptable error are shown in Table. 2. This prediction can achieve at least 99% accuracy. Therefore, we can conclude that this fault is a hard cyber network fault and the resilience control (PTSOC)

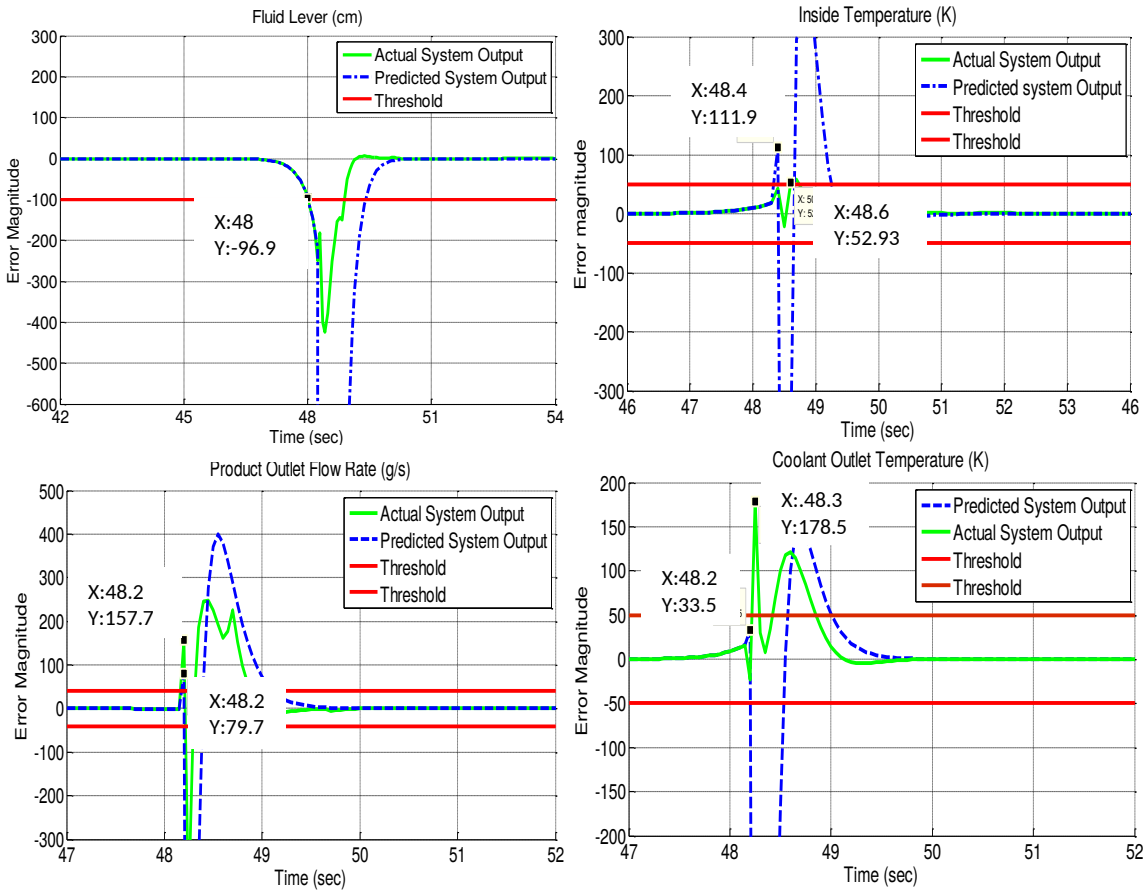


Figure 8. State prediction performance at t=47.3s

is triggered at 47.3s to mitigate such effects. The overshoots are reduced by at least 70% comparing with the original controller SOC, the TTRs are shortened by 10%. The summary of improvements can be found in Table. 3.

The proposed scheme quickly detects the fault because OCSVM can accurately separate the faulty and healthy data and isolate the hard fault quickly based on the state prediction. Then, the resilience controller is timely triggered ahead of the serious degradation of system performance.

The above simulation is repeated for 50 times. All the faults are accurately detected. Meanwhile, the overshoot of each system output is significantly reduced in term of its corresponding TTR. In contrast, without applying the proposed scheme, the fault still can

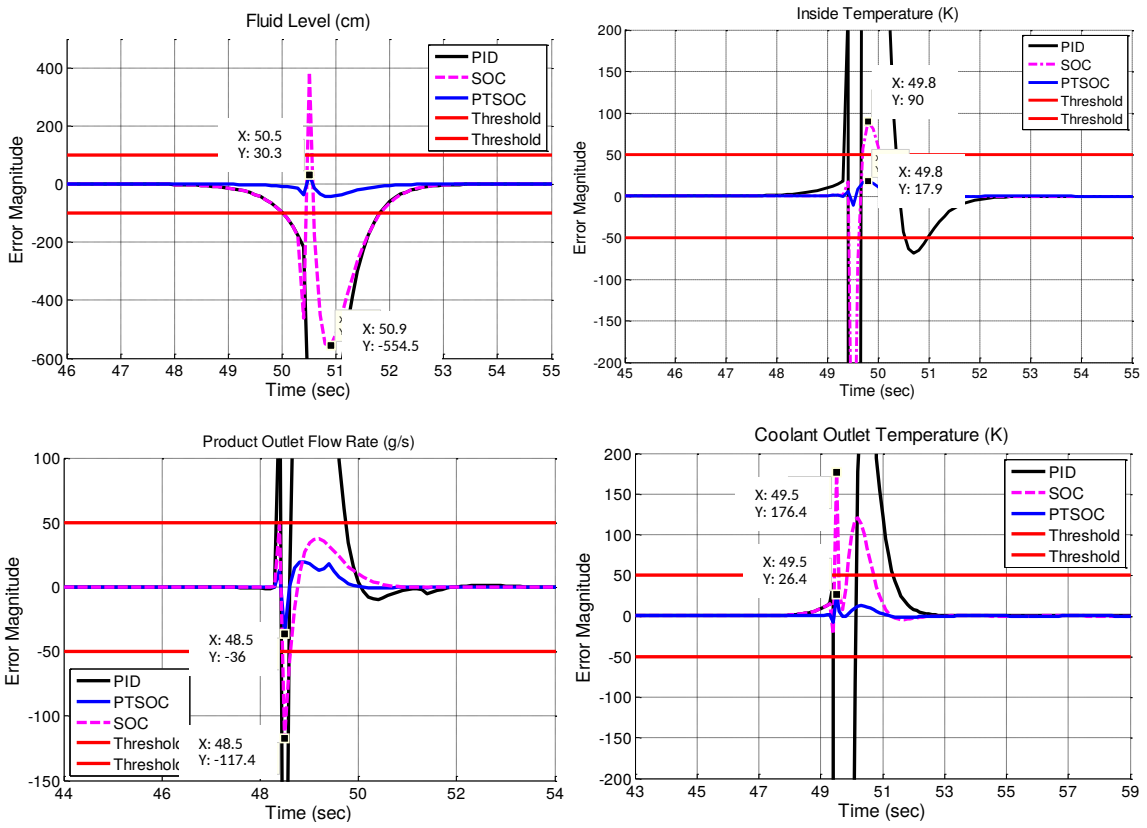


Figure 9. Fault tolerant performance

be detected when the system states exceed the acceptable error magnitude at 48s. However, it is too late to recover the system performance with such a late activation of the resilience controller. In such case, the basic controller PID will try to apply excessive actuation to stabilize. This might lead to significantly damage of the components or cause an unscheduled downtime. Even worse, the system could be compelled to stop.

6. CONCLUSION AND FUTURE WORK

The proposed novel prognosis scheme is shown to quickly detect and predict cyber network faults using one-class SVM and PDF estimation. Combining with the state prediction and future delay distribution estimation, soft and hard faults can accurately isolated to

Table 3. The comparison of overshoot and TTR

Variables	Overshoot					TTR				
	SOC	PTSOC	Improvement	PID	Improvement	SOC	PTSOC	Improvement	PID	Improvement
Fluid Level	551.4cm	30.3cm	94.5%	1419cm	97.9%	5.5s	4.4s	20%	6s	26.7%
Inside Temperature	454.9K	17.9K	96.1%	1774K	99%	4.6s	4.1s	10.9%	6.8s	39.7%
Product Outlet Flow Rate	117.4g/s	36g/s	69.3%	460.7g/s	92.2%	3.1s	2.9s	6.5%	7.2s	59.7%
Coolant Outlet Temperature	176.4K	26.4K	85.03%	1283K	97.9%	6.3s	6.1s	3.2%	7s	10%

optimize the computational cost of resilience control. Their convergence are theoretically proven. With the proposed resilience controller, the adverse effects caused by cyber network faults are efficiently mitigated.

The simulation results show that the proposed scheme accurately detect the cyber network faults before the performance degrades beyond the acceptable range. Moreover, the PTSOC is timely triggered to mitigate the negative effects on the CPSs performance. Comparing with the traditional SOC, the overshoot is significantly reduced by 70% and TTR is shorten by 10%. Comparing with PID controller, the improvements of the overshoot and TTR achieve 92% and 10%.

In this work, we applied the proposed scheme to a model-based CPS. For the future work, more applications to other CPSs without the knowledge of system model will be investigated and studied.

REFERENCES

Amin, S., Cárdenas, A. A., and Sastry, S., 'Safe and secure networked control systems under denial-of-service attacks.' in 'HSCC,' volume 5469, Springer, 2009 pp. 31–45.

Bi, S. and Zawodniok, M., 'Pdf based tuning of stochastic optimal controller design for cyber-physical systems with uncertain delay dynamics,' IET Cyber-Physical Systems: Theory & Applications, 2017, **2**(1), pp. 1–9.

Gamage, T. T., McMillin, B. M., and Roth, T. P., 'Enforcing information flow security properties in cyber-physical systems: A generalized framework based on compensation,' in 'Computer Software and Applications Conference Workshops (COMPSACW), 2010 IEEE 34th Annual,' IEEE, 2010 pp. 158–163.

Hu, Q., He, Z., Zhang, Z., and Zi, Y., 'Fault diagnosis of rotating machinery based on improved wavelet package transform and svms ensemble,' Mechanical Systems and Signal Processing, 2007, **21**(2), pp. 688–705.

Jiang, W., Guo, W., and Sang, N., 'Periodic real-time message scheduling for confidentiality-aware cyber-physical system in wireless networks,' in 'Frontier of Computer Science and Technology (FCST), 2010 Fifth International Conference on,' IEEE, 2010 pp. 355–360.

Liu, F.-C. and Yao, Y., 'Modeling and analysis of networked control systems using hidden markov models,' in 'Machine Learning and Cybernetics, 2005. Proceedings of 2005 International Conference on,' volume 2, IEEE, 2005 pp. 928–931.

Liu, G.-P., Xia, Y., Chen, J., Rees, D., and Hu, W., 'Networked predictive control of systems with random network delays in both forward and feedback channels,' IEEE Transactions on Industrial Electronics, 2007, **54**(3), pp. 1282–1297.

Liu, Y., Ning, P., and Reiter, M. K., 'False data injection attacks against state estimation in electric power grids,' ACM Transactions on Information and System Security (TISSEC), 2011, **14**(1), p. 13.

Mo, Y. and Sinopoli, B., 'Secure control against replay attacks,' in 'Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on,' IEEE, 2009 pp. 911–918.

Pasqualetti, F., Dörfler, F., and Bullo, F., 'Attack detection and identification in cyber-physical systems,' IEEE Transactions on Automatic Control, 2013, **58**(11), pp. 2715–2729.

Qin, S. J., 'Recursive pls algorithms for adaptive data modeling,' Computers & Chemical Engineering, 1998, **22**(4-5), pp. 503–514.

Salahshoor, K., Kordestani, M., and Khoshro, M. S., 'Fault detection and diagnosis of an industrial steam turbine using fusion of svm (support vector machine) and anfis (adaptive neuro-fuzzy inference system) classifiers,' Energy, 2010, **35**(12), pp. 5472–5482.

Samanta, B., 'Gear fault detection using artificial neural networks and support vector machines with genetic algorithms,' Mechanical Systems and Signal Processing, 2004, **18**(3), pp. 625–644.

Simon, D., *Optimal state estimation: Kalman, H infinity, and nonlinear approaches*, John Wiley & Sons, 2006.

Sugumaran, V., Muralidharan, V., and Ramachandran, K., 'Feature selection using decision tree and classification through proximal support vector machine for fault diagnostics of roller bearing,' Mechanical systems and signal processing, 2007, **21**(2), pp. 930–942.

Teixeira, A., Amin, S., Sandberg, H., Johansson, K. H., and Sastry, S. S., 'Cyber security analysis of state estimators in electric power systems,' in 'Decision and Control (CDC), 2010 49th IEEE Conference on,' IEEE, 2010 pp. 5991–5998.

Wang, G., Yang, Y., Zhang, Y., and Xie, Q., 'Vibration sensor based tool condition monitoring using ν support vector machine and locality preserving projection,' Sensors and Actuators A: Physical, 2014, **209**, pp. 24–32.

Wang, Y., Ding, S. X., Ye, H., and Wang, G., 'A new fault detection scheme for networked control systems subject to uncertain time-varying delay,' IEEE Transactions on signal processing, 2008, **56**(10), pp. 5258–5268.

Widodo, A. and Yang, B.-S., 'Wavelet support vector machine for induction machine fault diagnosis based on transient current signal,' Expert Systems with Applications, 2008, **35**(1), pp. 307–316.

Widodo, A., Yang, B.-S., and Han, T., 'Combination of independent component analysis and support vector machines for intelligent faults diagnosis of induction motors,' Expert systems with applications, 2007, **32**(2), pp. 299–312.

Xu, H., Jagannathan, S., and Lewis, F. L., 'Stochastic optimal control of unknown linear networked control system in the presence of random delays and packet losses,' Automatica, 2012, **48**(6), pp. 1017–1030.

Yan, W. and Shao, H., 'Application of support vector machine nonlinear classifier to fault diagnoses,' in 'Intelligent Control and Automation, 2002. Proceedings of the 4th World Congress on,' volume 4, IEEE, 2002 pp. 2697–2700.

Yin, H., Yang, S., Zhu, X., Jin, S., and Wang, X., 'Satellite fault diagnosis using support vector machines based on a hybrid voting mechanism,' The Scientific World Journal, 2014, **2014**.

Yuan, S. and Chu, F., 'Fault diagnosis based on support vector machines with parameter optimisation by artificial immunisation algorithm,' Mechanical Systems and Signal Processing, 2007, **21**(3), pp. 1318–1330.

Yuan, S.-F. and Chu, F.-L., 'Support vector machines-based fault diagnosis for turbo-pump rotor,' Mechanical Systems and Signal Processing, 2006, **20**(4), pp. 939–952.

Zhang, H., Yang, J., and Su, C.-Y., 'Ts fuzzy-model-based robust $h\infty$ design for networked control systems with uncertainties,' IEEE Transactions on Industrial Informatics, 2007, **3**(4), pp. 289–301.

Zhang, Z., Lv, W., and Shen, M., 'Active learning of support vector machine for fault diagnosis of bearings,' Advances in Neural Networks-ISNN 2006, 2006, pp. 390–395.

Zhang-qing, Z. and Xian-zhong, Z., 'Fault detection based on the states observer for networked control systems with uncertain long time-delay,' in 'Automation and Logistics, 2007 IEEE International Conference on,' IEEE, 2007 pp. 2320–2324.

Zhu, M. and Martinez, S., 'Stackelberg-game analysis of correlated attacks in cyber-physical systems,' in 'American Control Conference (ACC), 2011,' IEEE, 2011 pp. 4063–4068.

SECTION

2. SUMMARY AND CONCLUSIONS

In the first paper, a novel routing scheme is proposed to improve the QoS and performance of network in CPSs. This work is done by using RBF neural network to model the relation between power and maximum communication capacity which is the critical reference for routing optimization. Such scheme is applied to P2P and E2E path optimization to guarantee the vital transmission safety. Also, this scheme can ensure a high quality of service (QoS) under imperfect network condition, even cyber attacks.

Next, in the second paper, the imperfection, uncertainties, and dynamics in the cyberspace are considered both in system model and controller design. A online PDF identifier is proposed to capture the time-varying delays and its distribution. With the modification of traditional stochastic optimal control using PDF of delays, the assumption of full knowledge of network imperfection in priori is relaxed. Comparing with traditional stochastic control, the proposed controller achieves a better performance in terms of overshoot, time-to-recover, and operation cost. Also, this controller is considered a novel resilience control strategy for latter papers about cyber fault diagnosis and prognosis.

After that, in the third paper, we turn to the development of a general framework for cyber fault diagnosis scheme for CPSs wherein the cyberspace performance affect the physical system and vice versa. The proposed diagnosis scheme is capable of detecting cyber fault by monitoring the probability of delays. Also, the isolation of cyber and physical system fault is achieved with cooperating with the traditional observer based physical system fault detection. The adverse effects caused by cyber network faults are effectively mitigated with appropriately triggering the PTSOC resilience controller.

Based on the study presented in the third paper, we turns out a novel cyber fault prognosis scheme in the fourth paper, which can detect and estimate cyber fault and its negative effects on system performance ahead of time. Not only cyber and physical system faults are distinguished, but also soft and hard cyber faults are isolated depending on whether potential threats on system stability is predicted. Moreover, the convergence of the future delay distribution estimation and the system state prediction are theoretically proven. With the proposed resilience controller, the adverse effects caused by cyber network faults are efficiently mitigated.

Finally, the fifth paper presents an improve prognosis scheme with applying one-class SVM (OCSVM) to enhance the accuracy of fault detection and isolation.The results demonstrate that the detection of the attacks is faster than the traditional approach where one has to wait for the physical states to be deteriorated. However, the proposed scheme is applicable only to those network attacks causing delays and packets losses while revealing limitation to sophisticated attacks.

APPENDIX A

APPENDIX OF PAPER III

1. Stability Analysis for the PTSOC

Two theorems and their corresponding proofs are presented to demonstrate the stability of the proposed PTSOC. Lyapunov-based stability analysis is used. **Theorem 1** shows the control gain estimation asymptotically converges even if PDF estimation has an error provided it asymptotically converges to zero. **Theorem 2** considers the irremovable bias of PDF estimation as a bounded disturbance. However, a UUB stability is guaranteed.

Theorem 1 (Control gain estimation error convergence): As the delay data keeps updating PDF identifier and $\left(\parallel \sum_{j=1}^{n} \widetilde{P}_{(k+1)j} \parallel - \parallel \sum_{j=1}^{n} \widetilde{P}_{kj} \parallel \right) < 0$ is satisfied, then the estimation error for control gain $\parallel \widetilde{K}_k \parallel$ asymptotically converges to zero.

Proof:

First, we define the estimation error of control gain K as $\widetilde{K}_k = K_k - \widehat{K}_k = \sum_{j=1}^{n} P_{kj}K_j - \sum_{j=1}^{n} \widehat{P}_{kj}K_j$. P_{ij} is the actual probability at k. Then, Lyapunov function candidate is $V_{K_k} = \widetilde{K}_k^T \widetilde{K}_k$.

$$
\begin{aligned}
\Delta V_{K_k} &= V_{K_{k+1}} - V_{K_k} \\
&= \widetilde{K}_{k+1}^T \widetilde{K}_{k+1} - \widetilde{K}_k^T \widetilde{K}_k \\
&= (K_{k+1} - \widehat{K}_{k+1})^T (K_{k+1} - \widehat{K}_{k+1}) - (K_k - \widehat{K}_k)^T (K_k - \widehat{K}_k) \\
&= (\sum_{j=1}^{n_d} P_{(k+1)j} K_j - \sum_{j=1}^{n_d} \widehat{P}_{(k+1)j} K_j)^T (\sum_{j=1}^{n_d} P_{(k+1)j} K_j - \sum_{j=1}^{n_d} \widehat{P}_{(k+1)j} K_j) \\
&\quad - (\sum_{j=1}^{n_d} P_{kj} K_j - \sum_{j=1}^{n_d} \widehat{P}_{kj} K_j)^T (\sum_{j=1}^{n_d} P_{kj} K_j - \sum_{j=1}^{n_d} \widehat{P}_{kj} K_j) \\
&= \| \sum_{j=1}^{n_d} (P_{(k+1)j} - \widehat{P}_{(k+1)j}) K_j \|^2 - \| \sum_{j=1}^{n_d} (P_{kj} - \widehat{P}_{kj}) K_j \|^2 \\
&= \| \sum_{j=1}^{n_d} \widetilde{P}_{(k+1)j} K_j \|^2 - \| \sum_{j=1}^{n_d} \widetilde{P}_{kj} K_j \|^2 \\
&= \underbrace{\big(\| \sum_{j=1}^{n_d} \widetilde{P}_{(k+1)j} K_j \| + \| \sum_{j=1}^{n_d} \widetilde{P}_{kj} K_j \| \big)}_{\Delta_2} \\
&\quad \big(\| \sum_{j=1}^{n_d} \widetilde{P}_{(k+1)j} K_j \| - \| \sum_{j=1}^{n_d} \widetilde{P}_{kj} K_j \| \big) \\
&= \Delta_2 \big(\| \sum_{j=1}^{n_d} \widetilde{P}_{(k+1)j} K_j \| - \| \sum_{j=1}^{n_d} \widetilde{P}_{kj} K_j \| \big) \\
&= \Delta_2 [(\| \widetilde{P}_{(k+1)1} \| - \| \widetilde{P}_{k_1} \|) \| K_1 \| + \| \widetilde{P}_{(k+1)2} \| - \| \widetilde{P}_{k_2} \|) \| K_2 \| + \cdots \\
&\quad + \| \widetilde{P}_{(k+1)n_d} \| - \| \widetilde{P}_{k_{n_d}} \|) \| K_{n_d} \|] \\
&\leq \Delta_2 \big(\| \sum_{j=1}^{n} \widetilde{P}_{(k+1)j} \| - \| \sum_{j=1}^{n} \widetilde{P}_{kj} \| \big) \| K_{max} \|
\end{aligned}
$$

$$
\Delta_2 > 0, K_{max} = max\{K_1, K_2, \cdots, K_{n_d}\}
$$

Since V_{K_k} is positive definite and ΔV_{K_k} is negative definite provided $\widetilde{K}_k = K_k - \widehat{K}_k = \sum_{j=1}^{n} P_{kj}K_j - \sum_{j=1}^{n} \widehat{P}_{kj}K_j$. Therefore, the estimation error of control gain asymptotically converge to zero. ■

Theorem 2: (UUB Stability of the Regulation Error). Given the initial conditions as the system state z_0 and system matrices A_{z0}, and B_{z0}, let $u_0(z_k)$ be an initially admissible control policy for the CPS (2). Let the control update law be given by (10) and (11) and if the disturbance induced by the irremovable bias of PDF estimation has a bound $\| d_{KDE} \|$ and $K_{min} < 1/b_{min}$ such that the regulation error of system states has a uniformly ultimate bounded convergence in the mean.

Proof:

Consider the following positive definite Lyapunov function candidate: $V_{z_k} = z_K^T z_k$. z_k is the state vector of k. The corresponding estimated Lyapunov is $\widehat{V}_{z_k}$, therefore, $\Delta\widehat{V}_{z_k} = \widehat{V}_{z_{k+1}} - \widehat{V}_{z_k}$. We consider $\Delta\widehat{V}_{z_{km}} = \widehat{V}_{z_{(k+1)m}} - \widehat{V}_{z_k}$ for each possible system matrices (A_{zkm} and B_{zkm}). m represents one of the possible cases. If the maximum value of $\Delta\widehat{V}_{z_k m}$ is negative definite, the system convergence is proved. The irremovable bias of PDF estimation is considered the system state disturbance d_k bounded by d_M.

$$
\begin{aligned}
\Delta\widehat{V}_{z_k m} &= \widehat{V}_{z_{k+1} m} - \widehat{V}_{z_k m} \\
&= \| A_{zkm} - B_{zkm}K_k z_k + d_k \|^2 - \| z_k \|^2 \\
&= \underbrace{\left(\| A_{zkm} - B_{zkm}K_k z_k + d_k \| + \| z_k \| \right)}_{\Delta_3} \\
&\quad \left(\| A_{zkm} - B_{zkm}K_k z_k + d_k \| - \| z_k \| \right) \\
&= \Delta_3 \left(\| A_{zkm} - B_{zkm}K_k z_k + d_k \| - \| z_k \| \right) \\
&\leq \Delta_3 \left(\| a_{max} - b_{min}K_{min} z_k + d_M \| - \| z_k \| \right) \\
&\leq \Delta_3 \left(a_{max} + b_{min}K_{min} \| z_k \| + \| d_M \| - \| z_k \| \right) \\
&\forall k = 1, 2, \cdots, \forall m = 1, 2, \cdots, n_d
\end{aligned}
$$

where Δ_3 is positive definite, $b_{min} = min\{ \| B_{zk1} \|, \| B_{zk2} \|, \cdots, \| B_{zkm} \| \}$, $K_{min} = min\{ \| K_1 \|, \| K_2 \|, \cdots, \| K_{n_d} \| \}$.

Since $\widehat{V}_{z_k}$ is positive definite and $\Delta\widehat{V}_{K_k}$ is negative definite provided the system state $\| z_k \| \geq \frac{\|d_M\|+A_{max}}{1-b_{min}K_{min}}$ and $K_{min} < 1/b_{min}$. Therefore, UUB stability of the regulation error is proved. ■

For each delay interval, the cost function is (A.1) and the optimal control law is derived using A.1. The cost function of PTSOC defined by (A.2) is a probability weighted sum of the cost functions for all delay intervals. Similarly, the PTSOC law derived in Section. 4.4.1 is the summation of the weighted SOC laws of delay intervals. These weights are probabilities from the delay PDF.

$$J = E[\sum_{m=k}^{\infty}(z_m^T Q_z z_m + u_m^T R_z u_m)] \quad k = 0, 1, 2, \cdots \tag{A.1}$$

where $Q_z = diag\{Q, R/d, \cdots\}$, and $R_z = R/d$ are symmetric positive semi-definite and symmetric positive definite respectively. z_m is the state variables vector, and u_m is the control inputs vector. $E(\bullet)$ is the expected operator of $\sum_{m=k}^{\infty}(z_m^T Q_z z_m + u_m^T R_z u_m)$.

$$J^k = \sum_{i=1}^{n} P_i J_i^k = \sum_{i=1}^{n} P_i (x^{kT} Q_i x^k + u_i^{kT} R_i u_i^k) \tag{A.2}$$

where d_{int} represents the delay interval that we take 0.1s in the simulation section. If $d_{int} < d^k < d_{int}(i+1)$, d^k is classified in i^{th} delay case; n is the total number of delay cases; k represents sampling interval; P_i is probability of delay within $d_{int}i$ to $d_{int}(i+1)$ provided by the KDE-based PDF identifier; x is states vector; u_i is control inputs vector; Q_i and R_i are weighted constants of states and control inputs, respectively.

As the probabilities of each possible delay changes, PTSOC continuously tracks the network dynamics with a PDF identifier and updates its parameters based on PDF information of delay to adapt to the given system situation.

APPENDIX B

APPENDIX OF PAPER IV

1. PDF Identification Algorithm

The algorithm is shown in the following table:

Online PDF Identification Algorithm

1. Determining the data in the sliding window for time k:
   a) Choosing a kernel function K centered on x with a bandwidth h;
   b) Each observation x_i receives a specific weight proportional to the scaled distance from the observation x_i to x, which is $u = (x - x_i)/h$;
   c) At a given x, the estimate is found by vertically summing up over the k shapes.
   This can be synthesized as:
   $$\widehat{f}(x) = \frac{1}{nh} x_i \in [x - \frac{h}{2}, x + \frac{h}{2}]$$
   The general formula for KDE will be given by
   $$\widehat{f_k}(x) = \frac{1}{nh} \sum_{i=1}^{n} K(\frac{x - x_i}{h})$$
   where the dependence of the estimate on the kernel function $K(.)$ is denoted as $\widehat{f_k}$.
2. Updating the new data for time $k + 1$ in the sliding window and go back to Step 1;

2. Theorem 2 and Proof (To be included in paper as the approach)

Theorem 2 (Control gain estimation error convergence): As the delay data keeps updating PDF identifier and $\left(\| \sum_{j=1}^{n} \widetilde{P}_{(k+1)j} \| - \| \sum_{j=1}^{n} \widetilde{P}_{kj} \| \right) < 0$ is satisfied, then the estimation error for control gain $\| \widetilde{K}_k \|$ asymptotically converges to zero.

Proof:

First, we define the estimation error of control gain K as $\widetilde{K}_k = K_k - \widehat{K}_k = \sum_{j=1}^{n} P_{kj}K_j - \sum_{j=1}^{n} \widehat{P}_{kj}K_j$. P_{ij} is the actual probability at k. Then, Lyapunov function candidate is $V_{K_k} = \widetilde{K}_k^T \widetilde{K}_k$.

$$
\begin{aligned}
\Delta V_{K_k} &= V_{K_{k+1}} - V_{K_k} \\
&= \widetilde{K}_{k+1}^T \widetilde{K}_{k+1} - \widetilde{K}_k^T \widetilde{K}_k \\
&= (K_{k+1} - \widehat{K}_{k+1})^T (K_{k+1} - \widehat{K}_{k+1}) - (K_k - \widehat{K}_k)^T (K_k - \widehat{K}_k) \\
&= (\sum_{j=1}^{n_d} P_{(k+1)j}K_j - \sum_{j=1}^{n_d} \widehat{P}_{(k+1)j}K_j)^T (\sum_{j=1}^{n_d} P_{(k+1)j}K_j \\
&\quad - \sum_{j=1}^{n_d} \widehat{P}_{(k+1)j}K_j) - (\sum_{j=1}^{n_d} P_{kj}K_j - \sum_{j=1}^{n_d} \widehat{P}_{kj}K_j)^T (\sum_{j=1}^{n_d} P_{kj}K_j - \sum_{j=1}^{n_d} \widehat{P}_{kj}K_j) \\
&= \| \sum_{j=1}^{n_d} (P_{(k+1)j} - \widehat{P}_{(k+1)j})K_j \|^2 - \| \sum_{j=1}^{n_d} (P_{kj} - \widehat{P}_{kj})K_j \|^2 \\
&= \| \sum_{j=1}^{n_d} \widetilde{P}_{(k+1)j}K_j \|^2 - \| \sum_{j=1}^{n_d} \widetilde{P}_{kj}K_j \|^2 \\
&= \underbrace{\big(\| \sum_{j=1}^{n_d} \widetilde{P}_{(k+1)j}K_j \| + \| \sum_{j=1}^{n_d} \widetilde{P}_{kj}K_j \| \big)}_{\Delta_2} \\
&\quad \big(\| \sum_{j=1}^{n_d} \widetilde{P}_{(k+1)j}K_j \| - \| \sum_{j=1}^{n_d} \widetilde{P}_{kj}K_j \| \big) \\
&= \Delta_2 \big(\| \sum_{j=1}^{n_d} \widetilde{P}_{(k+1)j}K_j \| - \| \sum_{j=1}^{n_d} \widetilde{P}_{kj}K_j \| \big) \\
&= \Delta_2 [(\| \widetilde{P}_{(k+1)1} \| - \| \widetilde{P}_{k_1} \|) \| K_1 \| + \| \widetilde{P}_{(k+1)2} \| - \| \widetilde{P}_{k_2} \|) \| K_2 \| + \cdots \\
&\quad + \| \widetilde{P}_{(k+1)n_d} \| - \| \widetilde{P}_{k_{n_d}} \|) \| K_{n_d} \|] \\
&\leq \Delta_2 \big(\| \sum_{j=1}^{n} \widetilde{P}_{(k+1)j} \| - \| \sum_{j=1}^{n} \widetilde{P}_{kj} \| \big) \| K_{max} \|
\end{aligned}
$$

$\Delta_2 > 0, K_{max} = max\{K_1, K_2, \cdots, K_{n_d}\}$

Since V_{K_k} is positive definite and ΔV_{K_k} is negative definite provided $\widetilde{K}_k = K_k - \widehat{K}_k = \sum_{j=1}^{n} P_{kj} K_j - \sum_{j=1}^{n} \widehat{P}_{kj} K_j$. Therefore, the estimation error of control gain asymptotically converge to zero. ■

3. Theorem 3 and Proof (To be included in paper as the approach)

Theorem 3: (UUB Stability of the Regulation Error). Given the initial conditions as the system state z_0 and system matrices A_{z0}, and B_{z0}, let $u_0(z_k)$ be an initially admissible control policy for the CPS (6). Let the control update law be given by (8) and (9) and if the disturbance induced by the irremovable bias of PDF estimation has a bound $\| d_{KDE} \|$ and $K_{min} < 1/b_{min}$ such that the regulation error of system states has a uniformly ultimate bounded convergence in the mean.

Proof:

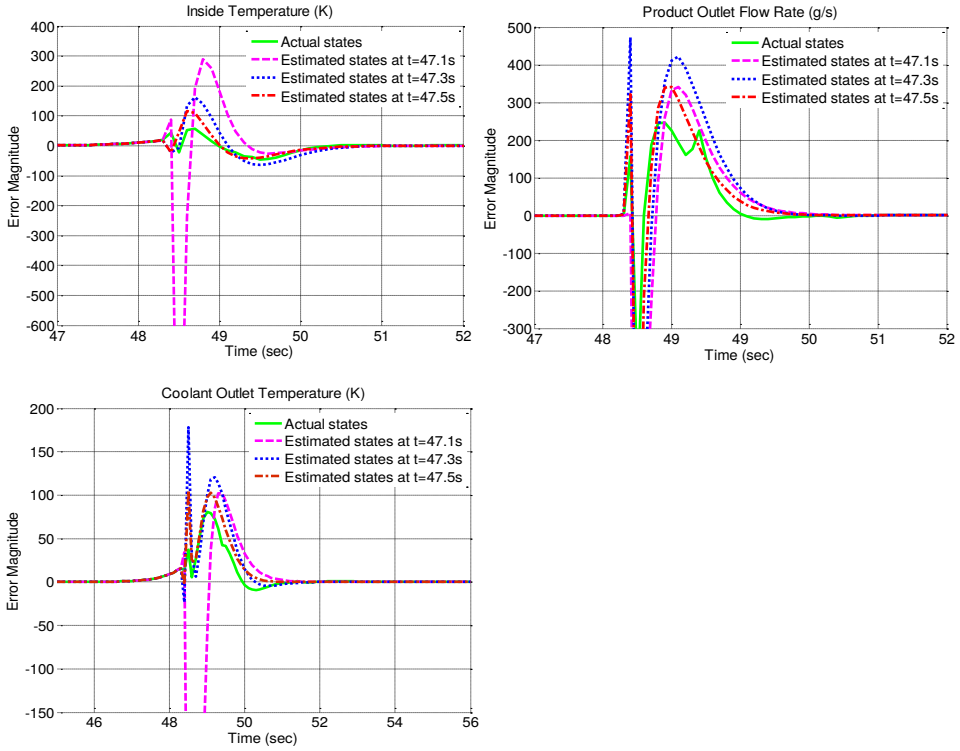
Consider the following positive definite Lyapunov function candidate: $V_{z_k} = z_K^T z_k$. z_k is the state vector of k. The corresponding estimated Lyapunov is $\widehat{V}_{z_k}$, therefore, $\Delta \widehat{V}_{z_k} = \widehat{V}_{z_{k+1}} - \widehat{V}_{z_k}$. We consider $\Delta \widehat{V}_{z_{km}} = \widehat{V}_{z_{(k+1)m}} - \widehat{V}_{z_k}$ for each possible system matrices (A_{zkm} and B_{zkm}). m represents one of the possible cases. If the maximum value of $\Delta \widehat{V}_{z_k m}$ is negative definite, the system convergence is proven. The irremovable bias of PDF estimation is considered the system state disturbance d_k bounded by d_M.

$$
\begin{aligned}
\Delta\widehat{V}_{z_k m} &= \widehat{V}_{z_{k+1} m} - \widehat{V}_{z_k m} \\
&= \| A_{zkm} - B_{zkm} K_k z_k + d_k \|^2 - \| z_k \|^2 \\
&= \underbrace{\left(\| A_{zkm} - B_{zkm} K_k z_k + d_k \| + \| z_k \| \right)}_{\Delta_3} \\
&\quad \left(\| A_{zkm} - B_{zkm} K_k z_k + d_k \| - \| z_k \| \right) \\
&= \Delta_3 \left(\| A_{zkm} - B_{zkm} K_k z_k + d_k \| - \| z_k \| \right) \\
&\leq \Delta_3 \left(\| a_{max} - b_{min} K_{min} z_k + d_M \| - \| z_k \| \right) \\
&\leq \Delta_3 \left(a_{max} + b_{min} K_{min} \| z_k \| + \| d_M \| - \| z_k \| \right) \\
&\forall k = 1, 2, \cdots \\
&\forall m = 1, 2, \cdots, n_d
\end{aligned}
$$

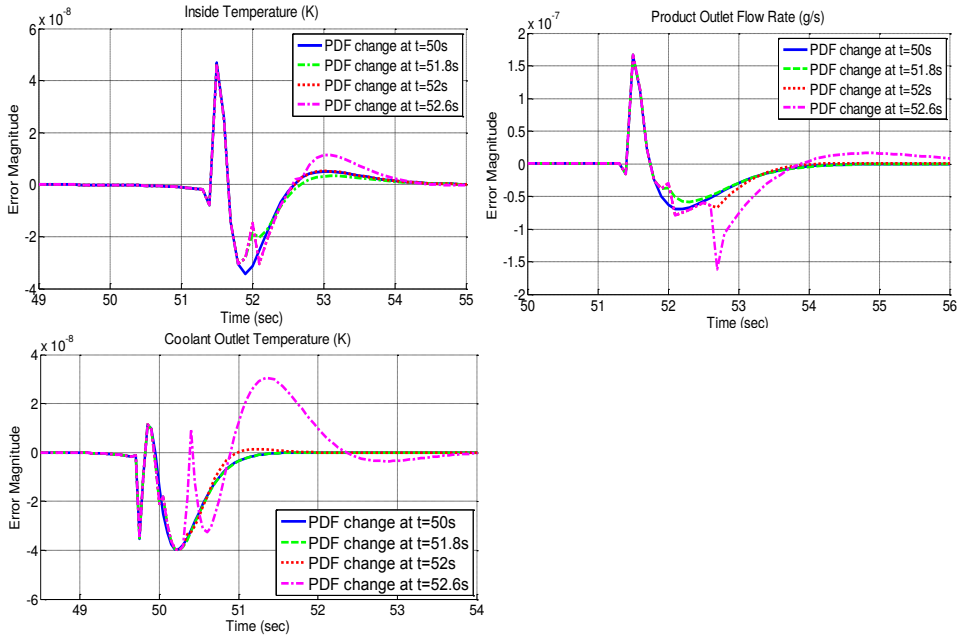
where Δ_3 is positive definite, $b_{min} = min\{ \| B_{zk1} \|, \| B_{zk2} \|, \cdots, \| B_{zkm} \| \}$, $K_{min} = min\{ \| K_1 \|, \| K_2 \|, \cdots, \| K_{n_d} \| \}$.

Since $\widehat{V}_{z_k}$ is positive definite and $\Delta\widehat{V}_{K_k}$ is negative definite provided the system state $\| z_k \| \geq \frac{\|d_M\| + A_{max}}{1 - b_{min} K_{min}}$ and $K_{min} < 1/b_{min}$. Therefore, UUB stability of the regulation error is proven. ■

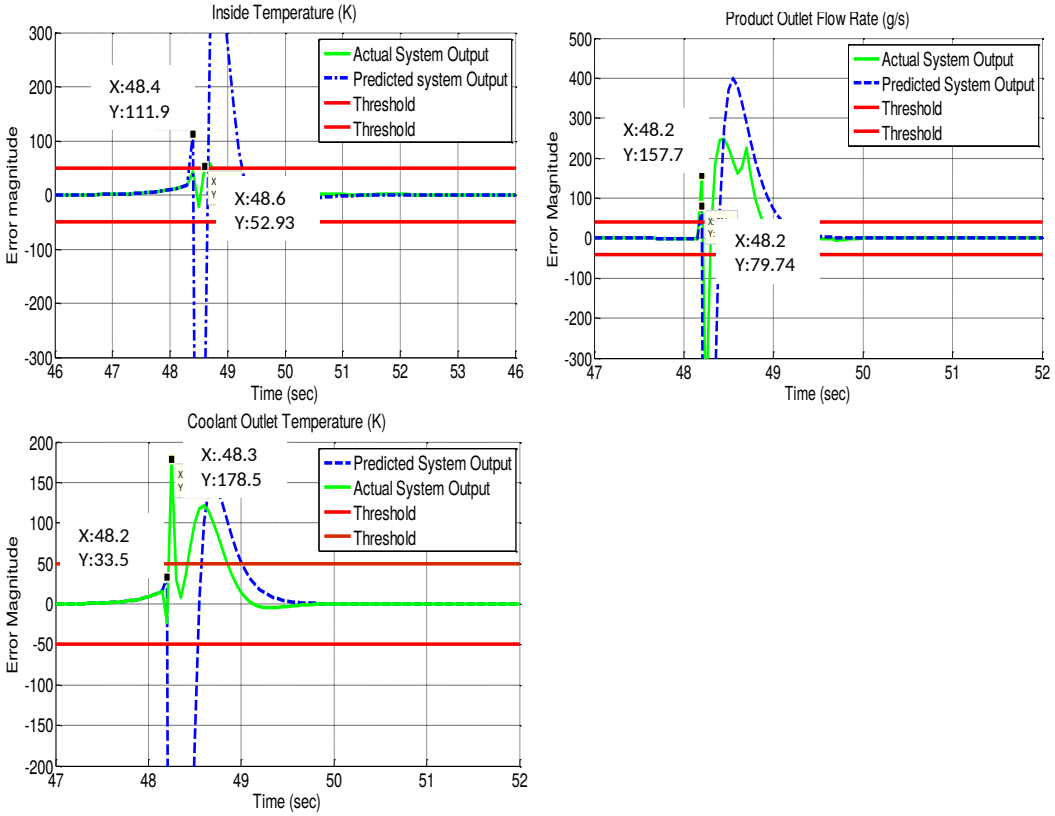
4. Other results for Case A, B, and C



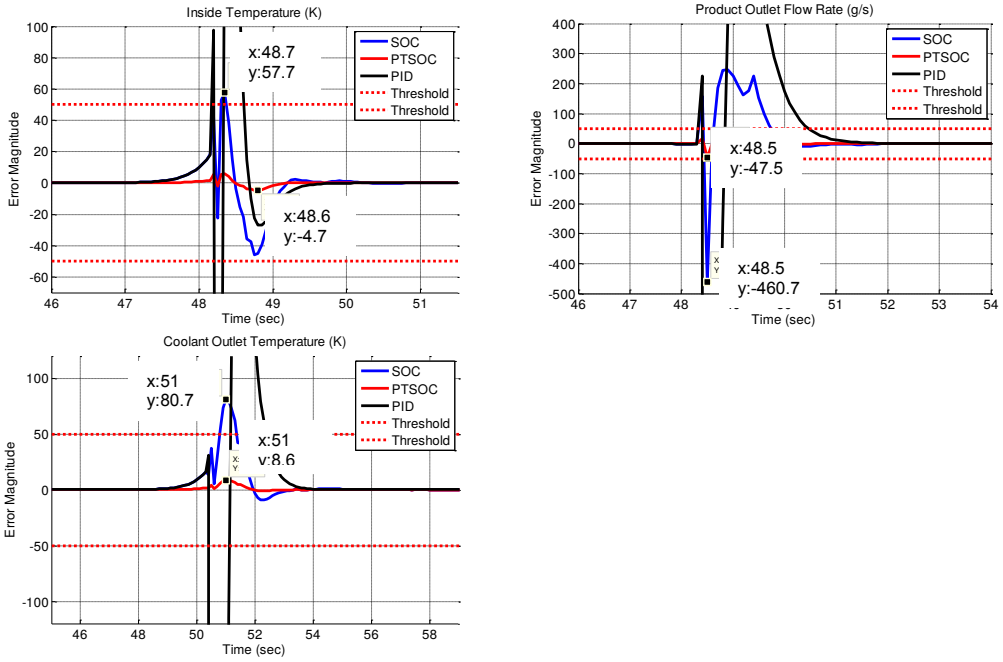
Case A: Actual and predicted system behavior



Case B: Predicted and Actual System Behavior



Case C: Predicted and Actual System Behavior



Case C: Fault mitigation performance

REFERENCES

Al-Karaki, J. N. and Kamal, A. E., 'Routing techniques in wireless sensor networks: a survey,' IEEE wireless communications, 2004, **11**(6), pp. 6–28.

Amin, S., Cárdenas, A. A., and Sastry, S., 'Safe and secure networked control systems under denial-of-service attacks.' in 'HSCC,' volume 5469, Springer, 2009 pp. 31–45.

Arcara, P. and Melchiorri, C., 'Control schemes for teleoperation with time delay: A comparative study,' Robotics and Autonomous systems, 2002, **38**(1), pp. 49–64.

Asgeirsson, E. I. and Mitra, P., 'On a game theoretic approach to capacity maximization in wireless networks,' in 'INFOCOM, 2011 Proceedings IEEE,' IEEE, 2011 pp. 3029–3037.

Bi, S. and Zawodniok, M., 'Pdf based tuning of stochastic optimal controller design for cyber-physical systems with uncertain delay dynamics,' IET Cyber-Physical Systems: Theory & Applications, 2017, **2**(1), pp. 1–9.

Blundell, R. and Duncan, A., 'Kernel regression in empirical microeconomics,' Journal of Human Resources, 1998, pp. 62–87.

Bors, A. G. and Nasios, N., 'Kernel bandwidth estimation for nonparametric modeling,' IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics), 2009, **39**(6), pp. 1543–1555.

Calabrese, R. and Zenga, M., 'Bank loan recovery rates: Measuring and nonparametric density estimation,' Journal of Banking & Finance, 2010, **34**(5), pp. 903–911.

Cardenas, A. A., Amin, S., and Sastry, S., 'Secure control: Towards survivable cyber-physical systems,' in 'Distributed Computing Systems Workshops, 2008. ICDCS'08. 28th International Conference on,' IEEE, 2008 pp. 495–500.

Carnevale, D., Teel, A. R., and Nesic, D., 'A lyapunov proof of an improved maximum allowable transfer interval for networked control systems,' IEEE Transactions on Automatic Control, 2007, **52**(5), pp. 892–897.

Chang, F.-J., Liang, J.-M., and Chen, Y.-C., 'Flood forecasting using radial basis function neural networks,' IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 2001, **31**(4), pp. 530–535.

Chang, P.-R. and Yang, W.-H., 'Environment-adaptation mobile radio propagation prediction using radial basis function neural networks,' IEEE transactions on vehicular technology, 1997, **46**(1), pp. 155–160.

Chen, M., Chiang, M., Chou, P., Li, J., Liu, S., and Sengupta, S., 'P2p streaming capacity: Survey and recent results,' in 'Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on,' IEEE, 2009 pp. 378–387.

Chen, T.-W. and Gerla, M., 'Global state routing: A new routing scheme for ad-hoc wireless networks,' in 'Communications, 1998. ICC 98. Conference Record. 1998 IEEE International Conference on,' volume 1, IEEE, 1998 pp. 171–175.

Chen, X., Tharmarasa, R., Kirubarajan, T., and McDonald, M., 'Online clutter estimation using a gaussian kernel density estimator for multitarget tracking,' IET Radar, Sonar & Navigation, 2014, **9**(1), pp. 1–9.

Elgammal, A., Duraiswami, R., and Davis, L. S., 'Efficient kernel density estimation using the fast gauss transform with applications to color modeling and tracking,' IEEE transactions on pattern analysis and machine intelligence, 2003, **25**(11), pp. 1499–1504.

Fisher, A., Jacobson, C. A., Lee, E. A., Murray, R. M., Sangiovanni-Vincentelli, A., and Scholte, E., 'Industrial cyber-physical systems–icyphy,' in 'Complex Systems Design & Management,' pp. 21–37, Springer, 2014.

Gamage, T. T., McMillin, B. M., and Roth, T. P., 'Enforcing information flow security properties in cyber-physical systems: A generalized framework based on compensation,' in 'Computer Software and Applications Conference Workshops (COMPSACW), 2010 IEEE 34th Annual,' IEEE, 2010 pp. 158–163.

Gao, H. and Chen, T., 'Network-based $h\infty$ output tracking control,' IEEE Transactions on Automatic control, 2008, **53**(3), pp. 655–667.

Gao, H., Meng, X., and Chen, T., 'Stabilization of networked control systems with a new delay characterization,' IEEE Transactions on Automatic Control, 2008, **53**(9), pp. 2142–2148.

Gao, Y., Chiu, D.-M., and Lui, J., 'Determining the end-to-end throughput capacity in multi-hop networks: methodology and applications,' in 'ACM SIGMETRICS Performance Evaluation Review,' volume 34, ACM, 2006 pp. 39–50.

Gastpar, M. and Vetterli, M., 'On the capacity of wireless networks: The relay case,' in 'INFOCOM 2002. Twenty-First Annual Joint Conference of the IEEE Computer and Communications Societies. Proceedings. IEEE,' volume 3, IEEE, 2002 pp. 1577–1586.

Gisbert, F. J. G., 'Weighted samples, kernel density estimators and convergence,' Empirical Economics, 2003, **28**(2), pp. 335–351.

Gorinevsky, D., 'On the persistency of excitation in radial basis function network identification of nonlinear systems,' IEEE Transactions on Neural Networks, 1995, **6**(5), pp. 1237–1244.

Gupta, P. and Kumar, P. R., 'The capacity of wireless networks,' IEEE Transactions on information theory, 2000, **46**(2), pp. 388–404.

Hao, F. and Zhao, X., 'Linear matrix inequality approach to static output-feedback stabilisation of discrete-time networked control systems,' IET control theory & applications, 2010, **4**(7), pp. 1211–1221.

Haque, S. A., Aziz, S. M., and Rahman, M., 'Review of cyber-physical system in healthcare,' International Journal of Distributed Sensor Networks, 2014, **10**(4), p. 217415.

He, Y., Mao, Y., Chen, W., and Chen, Y., 'Nonlinear metric learning with kernel density estimation,' IEEE Transactions on Knowledge and Data Engineering, 2015, **27**(6), pp. 1602–1614.

Hu, Q., He, Z., Zhang, Z., and Zi, Y., 'Fault diagnosis of rotating machinery based on improved wavelet package transform and svms ensemble,' Mechanical Systems and Signal Processing, 2007, **21**(2), pp. 688–705.

Hurter, C., Ersoy, O., and Telea, A., 'Graph bundling by kernel density estimation,' in 'Computer Graphics Forum,' volume 31, Wiley Online Library, 2012 pp. 865–874.

Jagannathan, S., Zawodniok, M., and Shang, Q., 'Distributed power control for cellular networks in the presence of channel uncertainties,' IEEE Transactions on Wireless Communications, 2006, **5**(3), pp. 540–549.

Jiang, W., Guo, W., and Sang, N., 'Periodic real-time message scheduling for confidentiality-aware cyber-physical system in wireless networks,' in 'Frontier of Computer Science and Technology (FCST), 2010 Fifth International Conference on,' IEEE, 2010 pp. 355–360.

Johansson, K. H., Törngren, M., and Nielsen, L., 'Vehicle applications of controller area network,' Handbook of networked and embedded control systems, 2005, pp. 741–765.

Kawamoto, Y., Nishiyama, H., and Kato, N., 'Ma-ltrt: A novel method to improve network connectivity and power consumption in mobile ad-hoc based cyber-physical systems,' IEEE Transactions on Emerging Topics in Computing, 2013, **1**(2), pp. 366–374.

Lee, J., Bagheri, B., and Kao, H.-A., 'A cyber-physical systems architecture for industry 4.0-based manufacturing systems,' Manufacturing Letters, 2015, **3**, pp. 18–23.

Lee, K. C., Lee, S., and Lee, M. H., 'Qos-based remote control of networked control systems via profibus token passing protocol,' IEEE Transactions on Industrial Informatics, 2005, **1**(3), pp. 183–191.

Leung, H., Dubash, N., and Xie, N., 'Detection of small objects in clutter using a ga-rbf neural network,' IEEE Transactions on Aerospace and Electronic systems, 2002, **38**(1), pp. 98–118.

Li, P., Zhang, C., and Fang, Y., 'The capacity of wireless ad hoc networks using directional antennas,' IEEE Transactions on Mobile Computing, 2011, **10**(10), pp. 1374–1387.

Li, X.-Y., 'Multicast capacity of wireless ad hoc networks,' IEEE/ACM Transactions on Networking (TON), 2009, **17**(3), pp. 950–961.

Liang, J. and Du, R., 'Model-based fault detection and diagnosis of hvac systems using support vector machine method,' International Journal of refrigeration, 2007, **30**(6), pp. 1104–1114.

Liang, W. and Guo, X., 'Online multicasting for network capacity maximization in energy-constrained ad hoc networks,' IEEE Transactions on Mobile Computing, 2006, **5**(9), pp. 1215–1227.

Lien, S.-Y., Cheng, S.-M., Shih, S.-Y., and Chen, K.-C., 'Radio resource management for qos guarantees in cyber-physical systems,' IEEE Transactions on Parallel and Distributed Systems, 2012, **23**(9), pp. 1752–1761.

Liu, F.-C. and Yao, Y., 'Modeling and analysis of networked control systems using hidden markov models,' in 'Machine Learning and Cybernetics, 2005. Proceedings of 2005 International Conference on,' volume 2, IEEE, 2005 pp. 928–931.

Liu, G.-P., Xia, Y., Chen, J., Rees, D., and Hu, W., 'Networked predictive control of systems with random network delays in both forward and feedback channels,' IEEE Transactions on Industrial Electronics, 2007a, **54**(3), pp. 1282–1297.

Liu, G.-P., Xia, Y., Rees, D., and Hu, W., 'Design and stability criteria of networked predictive control systems with random network delay in the feedback channel,' IEEE Transactions on Systems, Man, and Cybernetics, Part C (Applications and Reviews), 2007b, **37**(2), pp. 173–184.

Liu, Y., Ning, P., and Reiter, M. K., 'False data injection attacks against state estimation in electric power grids,' ACM Transactions on Information and System Security (TISSEC), 2011, **14**(1), p. 13.

Mitchell, R. and Chen, R., 'Modeling and analysis of attacks and counter defense mechanisms for cyber physical systems,' IEEE Transactions on Reliability, 2016, **65**(1), pp. 350–358.

Mo, Y. and Sinopoli, B., 'Secure control against replay attacks,' in 'Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on,' IEEE, 2009 pp. 911–918.

Pasqualetti, F., Dörfler, F., and Bullo, F., 'Attack detection and identification in cyber-physical systems,' IEEE Transactions on Automatic Control, 2013, **58**(11), pp. 2715–2729.

Pindoriya, N., Singh, S., and Singh, S., 'An adaptive wavelet neural network-based energy price forecasting in electricity markets,' IEEE Transactions on Power Systems, 2008, **23**(3), pp. 1423–1432.

Qin, S. J., 'Recursive pls algorithms for adaptive data modeling,' Computers & Chemical Engineering, 1998, **22**(4-5), pp. 503–514.

Qu, F., Wang, F.-Y., and Yang, L., 'Intelligent transportation spaces: vehicles, traffic, communications, and beyond,' IEEE Communications Magazine, 2010, **48**(11).

Rawat, D. B., Rodrigues, J. J., and Stojmenovic, I., *Cyber-physical systems: from theory to practice*, CRC Press, 2015.

Royer, E. M. and Toh, C.-K., 'A review of current routing protocols for ad hoc mobile wireless networks,' IEEE personal communications, 1999, **6**(2), pp. 46–55.

Salahshoor, K., Kordestani, M., and Khoshro, M. S., 'Fault detection and diagnosis of an industrial steam turbine using fusion of svm (support vector machine) and anfis (adaptive neuro-fuzzy inference system) classifiers,' Energy, 2010, **35**(12), pp. 5472–5482.

Samanta, B., 'Gear fault detection using artificial neural networks and support vector machines with genetic algorithms,' Mechanical Systems and Signal Processing, 2004, **18**(3), pp. 625–644.

Shah, R. C. and Rabaey, J. M., 'Energy aware routing for low energy ad hoc sensor networks,' in 'Wireless Communications and Networking Conference, 2002. WCNC2002. 2002 IEEE,' volume 1, IEEE, 2002 pp. 350–355.

Silverman, B. W., *Density estimation for statistics and data analysis*, volume 26, CRC press, 1986.

Simon, D., *Optimal state estimation: Kalman, H infinity, and nonlinear approaches*, John Wiley & Sons, 2006.

Smith, R. S., 'A decoupled feedback structure for covertly appropriating networked control systems,' IFAC Proceedings Volumes, 2011, **44**(1), pp. 90–95.

Sridhar, S., Hahn, A., and Govindarasu, M., 'Cyber–physical system security for the electric power grid,' Proceedings of the IEEE, 2012, **100**(1), pp. 210–224.

Sugumaran, V., Muralidharan, V., and Ramachandran, K., 'Feature selection using decision tree and classification through proximal support vector machine for fault diagnostics of roller bearing,' Mechanical systems and signal processing, 2007, **21**(2), pp. 930–942.

Teixeira, A., Amin, S., Sandberg, H., Johansson, K. H., and Sastry, S. S., 'Cyber security analysis of state estimators in electric power systems,' in 'Decision and Control (CDC), 2010 49th IEEE Conference on,' IEEE, 2010 pp. 5991–5998.

Tian, E., Yue, D., and Peng, C., 'Reliable control for networked control systems with probabilistic sensors and actuators faults,' IET Control Theory & Applications, 2010, **4**(8), pp. 1478–1488.

Tiberi, U., Fischione, C., Johansson, K. H., and Di Benedetto, M. D., 'Energy-efficient sampling of networked control systems over ieee 802.15. 4 wireless networks,' Automatica, 2013, **49**(3), pp. 712–724.

Wang, G., Yang, Y., Zhang, Y., and Xie, Q., 'Vibration sensor based tool condition monitoring using ν support vector machine and locality preserving projection,' Sensors and Actuators A: Physical, 2014, **209**, pp. 24–32.

Wang, S., Meng, X., and Chen, T., 'Wide-area control of power systems through delayed network communication,' IEEE Transactions on Control Systems Technology, 2012, **20**(2), pp. 495–503.

Wang, W. and Wu, R., 'Capacity maximization for ofdm two-hop relay system with separate power constraints,' IEEE Transactions on Vehicular Technology, 2009, **58**(9), pp. 4943–4954.

Wang, Y., Ding, S. X., Ye, H., and Wang, G., 'A new fault detection scheme for networked control systems subject to uncertain time-varying delay,' IEEE Transactions on signal processing, 2008, **56**(10), pp. 5258–5268.

Widodo, A. and Yang, B.-S., 'Wavelet support vector machine for induction machine fault diagnosis based on transient current signal,' Expert Systems with Applications, 2008, **35**(1), pp. 307–316.

Widodo, A., Yang, B.-S., and Han, T., 'Combination of independent component analysis and support vector machines for intelligent faults diagnosis of induction motors,' Expert systems with applications, 2007, **32**(2), pp. 299–312.

Xie, S., Low, K. S., and Gunawan, E., 'An adaptive tuning algorithm for ieee 802.15. 4-based network control system,' in 'Intelligent Sensors, Sensor Networks and Information Processing (ISSNIP), 2014 IEEE Ninth International Conference on,' IEEE, 2014 pp. 1–6.

Xu, H., Jagannathan, S., and Lewis, F. L., 'Stochastic optimal control of unknown linear networked control system in the presence of random delays and packet losses,' Automatica, 2012, **48**(6), pp. 1017–1030.

Xue, F., Xie, L.-L., and Kumar, P. R., 'The transport capacity of wireless networks over fading channels,' IEEE Transactions on Information Theory, 2005, **51**(3), pp. 834–847.

Yağdereli, E., Gemci, C., and Aktaş, A. Z., 'A study on cyber-security of autonomous and unmanned vehicles,' The Journal of Defense Modeling and Simulation, 2015, **12**(4), pp. 369–381.

Yan, W. and Shao, H., 'Application of support vector machine nonlinear classifier to fault diagnoses,' in 'Intelligent Control and Automation, 2002. Proceedings of the 4th World Congress on,' volume 4, IEEE, 2002 pp. 2697–2700.

Yang, C.-X., Guan, Z.-H., and Huang, J., 'Stochastic fault tolerant control of networked control systems,' Journal of the Franklin Institute, 2009, **346**(10), pp. 1006–1020.

Yin, H., Yang, S., Zhu, X., Jin, S., and Wang, X., 'Satellite fault diagnosis using support vector machines based on a hybrid voting mechanism,' The Scientific World Journal, 2014, **2014**.

Yuan, S. and Chu, F., 'Fault diagnosis based on support vector machines with parameter optimisation by artificial immunisation algorithm,' Mechanical Systems and Signal Processing, 2007, **21**(3), pp. 1318–1330.

Yuan, S.-F. and Chu, F.-L., 'Support vector machines-based fault diagnosis for turbo-pump rotor,' Mechanical Systems and Signal Processing, 2006, **20**(4), pp. 939–952.

Yun, Z., Quan, Z., Caixin, S., Shaolan, L., Yuming, L., and Yang, S., 'Rbf neural network and anfis-based short-term load forecasting approach in real-time price environment,' IEEE Transactions on power systems, 2008, **23**(3), pp. 853–858.

Zhang, H., Yang, J., and Su, C.-Y., 'Ts fuzzy-model-based robust $h\infty$ design for networked control systems with uncertainties,' IEEE Transactions on Industrial Informatics, 2007, **3**(4), pp. 289–301.

Zhang, Z., Lv, W., and Shen, M., 'Active learning of support vector machine for fault diagnosis of bearings,' Advances in Neural Networks-ISNN 2006, 2006, pp. 390–395.

Zhang-qing, Z. and Xian-zhong, Z., 'Fault detection based on the states observer for networked control systems with uncertain long time-delay,' in 'Automation and Logistics, 2007 IEEE International Conference on,' IEEE, 2007 pp. 2320–2324.

Zhu, M. and Martinez, S., 'Stackelberg-game analysis of correlated attacks in cyber-physical systems,' in 'American Control Conference (ACC), 2011,' IEEE, 2011 pp. 4063–4068.

VITA

Shanshan Bi was born in China in 1988. She earned a bachelor's degree of science and a master's degree of science in Electrical Engineering, both at North China Electric Power University, 2010 and 2013 respectively. She received her Ph.D degree in Electrical Engineering from Missouri University of Science and Technology in May 2018.