Stability and Security Analysis with Identification of Attack on Industrial Networked Control System: An Overview

Brijraj S. Solanki, Renu K., and Seshadhri Srinivasan

***Abstract*— A networked control system (NCS) is sensitive to the different types of attacks and it is essential to secure and stabilize it. In this manuscript, to represent the impact on the stability of the control system, an industrial NCS is considered. The process noise and measurement noise alongside certain attacks are assumed to be affecting the performance of this system. It is also assumed that the agent may inject false data to disrupt the performance of the control system. An overview of recent work done for stabilization of NCS in such scenario is presented here. Kalman filter along with some control system stability conditions are used to mitigate the effect of noise and attacks on NCS. A numerical example is presented here to exemplify the performance of the Kalman filter and Linear Quadratic Gaussian (LQG) controller along with PID controller on system state estimation. It is shown that Kalman filter estimates the states optimally which indicted by the eigenvalues of -4.87, -1.77, -12. The simulation and sampling timea were 20s and 10ms, respectively.**

***Index Terms*— Covert Attacks, Denial of Service, Industrial networked control system, Kalman filter, Linear quadratic Gaussian.**

I. INTRODUCTION

THE networked control systems (NCS) are wire/wireless communication networks which are intended to improve the performance capabilities. These are used to control and drive the industrial processes and systems [1]. The actuator/sensor signals and control signals may be corrupted by the agent while traveling through a communication channel [2]. In past, many such attacks have been reported, for example, Davis-Besse nuclear power plant attack, Maroochy service attack, electric grid attack, Stuxnet worm, etc. [1]-[4]. The risk of attack is increased by the sensors and actuators deployed in the NCS and can cause damages as addressed in [4]. The attacks may be introduced by agent on the communication channel in the feedback and/or forward stream. The communication delays, data loss due to packet dropouts and bandwidth congestions are some of the main constraints which affect the stability of NCS. An overview of different types of attacks and stability conditions for an NCS (as proposed in recent literature) are presented in this manuscript.

The focus of this paper is to do stability analysis of an NCS in presence of certain types of attacks, uncertain delays, disturbances, etc. in the communication process. It is assumed that known system dynamics is used by the agent to attack upon the communication network for degrading the system performance. The attacks, delays, disturbances, etc. that are encountered in the communication network are used to define the sensitivity of the system against such uncertainties. With reference to the recent literature, certain stability conditions are investigated in this paper. Further, Kalman filter, LQG controller and PID controller are used to mitigate the effect of noise and attacks on NCS. They make the system more robust against such attacks. To exemplify this, a numerical example is also presented. The simulation results depict that the system states are estimated optimally using Kalman filter. This study promotes the research work to explore efficient mechanisms and algorithms to avoid such attacks.

The organization of this paper is as follows: state of the art work is briefly discussed in Section II. In Section III, the problem formulation is proposed to mitigate the attacks that may be expected to be encountered in the control loop of an NCS. To understand the proposed methodology, a numerical problem and simulation results are summarized in Section IV. The conclusion and future work is discussed in Section V.

II. BACKGROUND WORK

Based on the information collected by other attack, the authors in [1] have proposed a covert attack for degrading the NCS service. Similarly, Hou and Sun [2]-[3] discussed a methodology for introducing false data into a discrete linear time invariant (LTI) system. The authors have used Kalman filter along with a failure detector to show the performance of the system. This proposed design assumes no knowledge in the first case and perfect knowledge of the physical plant in the latter case.

Authors in [5] proposed a technique that ensures that all the malicious sensor nodes in the system which are introducing any significant distortion are either detected or restricted to add further distortion. Hau and Jagannath [6] proposed an adaptive dynamic programming scheme for obtaining optimal controller of NCS under Transmission

Manuscript received August 2, 2019.

B. S. Solanki is with the Department of Electronics and Communication Engineering, Poornima College of Engineering, Jaipur, Rajasthan-302022, India (e-mail address: brijraj@poornima.org).

R. Kumawat is with the Department of Electronics and Communication Engineering, School of Electrical, Electronics & Communication Engineering, Manipal University Jaipur, Jaipur, Rajasthan-303007 (e-mail address: renukumawat@gmail.com).

S. Srinivasan is with the Dept. of Biomedical Engineering, Kalasalingam Academy Research and Education (KARE), India (e-mail address: seshucontrol@gmail.com).

Control Protocol (TCP). The effect of SNR of the wireless channel on the stability of wireless NCS is analyzed by a linear matrix inequality in [7].

In [8]-[11], using Lyapunov Krasovskii function, an improved stability criterion for networked closed-loop system is measured. TrueTime Network Library is used in [12] to study the vulnerability in electrical cyber physical systems in presence of denial of service (DoS) attacks.

Pang *et al.* [13] proposed false data injection (FDI) attacks with the output tracking control of NCS using Kalman filter-based predictive control. An improved model-free and adaptive predictive control method is presented in [14] to improve NCS performance by compensating the packet losses. To boost the upper bound on the maximum allowable number of DoS attack, the Lyapunov functional stability criterion is used by Zhang *et al.* [15] and Sun *et al.* [16]. It is also used to derive stability conditions for NCSs with unknown communication delay. Hu *et al.* [17] identified the new necessary and sufficient conditions for insecurity by which NCS is insecure to FDI attacks.

For active system identification, De Sa *et al.* [18] have developed random switching controllers. These controllers design confer switching rules and control functions to optimize the performance of NCS. Jithish *et al.* [19] used the symmetric key encryption method to provide security for NCS against DoS and Deception attacks. Wo *et al.* [20] discussed the data injection attacks using switching law in cyber physical system in to derive the worst-case impact of location switching attacks.

Y. Li *et al.* [21], designed an intrusion detection system for recognizing the presence of attacks. In this paper, authors addressed about the DoS attack, replay attack and bias injection attack which can manipulate the data. H. Zhang *et al.* [22] designed an optimal attack schedules which optimizes the Linear Quadratic Gaussian (LQG) control cost function along with considering the energy constraint. In this context, authors also analyzed the system stability to improve the performance for wireless NCS with multiple systems.

In paper [23], the authors presented the mean square stabilization with denial of service for a network control system. Authors computed the rules for designing the state-feedback controllers by using linear matrix inequalities. S. Han *et al.* [24], presented the challenges and techniques to protect the cyber physical system against intrusion made by attackers. In this paper, authors also discussed the requirement, detection techniques and properties required for reliability and security in cyber physical system.

The system theoretic and graph theoretic approach is presented by F. Pasqualetti *et al.* [25], to analyze the undetectable and unidentifiable attacks on the system and designed the distributed and centralized monitors, which are robust to the system noise. Huang *et al.* [26], designed the compensator to stabilize performance due to effect of the attack. In the paper, upper bound for stealth attack is presented by integrating frequency characteristics of the attack and the information of the detector.

Nonlinear time delay is assumed for NCS and Cho *et al.* [27], designed the predictive control using neural networks, dynamic Bayesian networks, and reset control. This control improved the transient response and settling time for given input of square wave and it has shown excellent performance towards disturbances. In the paper [28], exponentially mean square stability condition is used for analyzing the stability of wireless NCS subjected to the network induced delay and packet dropout, while considering the multiple-packet transmission with ZigBee network. A time varying coding matrix is designed by Miao *et al.* [29], to code the sensor output, which increases the estimation residues under data injection attacks. By employing the coding matrix the attacker cannot inject the correct sequence of data to actuators and sensors.

Hu *et al.* [30], discussed the DoS and quantization attack to design the controller for the event-triggered NCS. Here, the Lyapunov function and LMIs are used for defining the stability of the NCS. The designed controller maintained the essential control performance of the system. Zhong-Hua Pang *et al.* [31], designed predictive control system that is comprised of secure networked predictive control architecture, Message Digest and Data Encryption Standard algorithm, and recursive networked predictive control to guarantee the confidentiality, integrity and authenticity of the transmitted data which may suffer from denial of service attacks.

It can be summarized that the performance of NCS is affected by noise, timing jitters, packet dropouts and by different types of attacks like DoS, Deception, quantization, etc. In this scenario, the necessary and sufficient conditions for stabilization of NCS have been reported. Moreover, various tools/techniques/methodologies that are reported in the literature to upgrade the system performance under presence of such uncertainties. Some of these techniques include Kalman filter, Lyapunov function, linear matrix inequality, Linear Quadratic Gaussian Controller, etc. These are listed below in Table I.

TABLE I
TECHNIQUES / TOOLS USED FOR INVESTIGATING NCS STABILITY CRITERIA

Sr. No.	Techniques/Tools	Reference No.
1	Kalman Filter and Chi-square merit function	[2], [3]. [13],[17]
2	Lyapunov Function	[14], [15], [23], [28]
3	Linear Matrix Inequality	[14], [23], [27]
4	Linear Quadratic Gaussian Controller	[2], [22]
5	Network Predictive Control	[12], [14], [16], [31]
6	True Time: MATLAB based simulation Tool	[6], [11], [12], [14]

III. PROBLEM FORMULATION

In this section, a mathematical formulation is presented for NCS, its controller and attacks on the NCS. The general block diagram along with attacks in an NCS is shown in Fig. 1. The sensor signals (y) and control signals (u) travel over a wireless/wired communication network. The sensor directs the sampled response of the plant to the controller through communication channel periodically. Plant receives control signal (u') and controller receives sensor signal (y') through the communication channel.

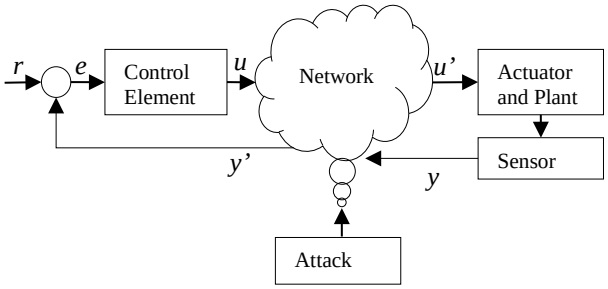

Fig. 1. Block diagram representation for a Networked Control System along with Attack Scienario.

The controller processed the command signals according to the control law and directs the processed signal to the actuator through communication channel. In this paper, discrete linear time-invariant (LTI) system is considered to model the system dynamics. The attackers by using known system dynamics can degrade the control performance and even can create damaging environment. Hence, it is needed to secure the control system to avert the fatal consequences. In the literature few important attacks such as DoS, deception, etc. are discussed briefly.

TABLE II
DESCRIPTION OF THE SYMBOLS USED

Symbol	Description
$x(k)$	State Vector
$u(k)$	Control Vector
$u(t)$	Control Signal
$y(k)$	Output of Measurement Signal
$\omega(k)$	Process Gaussian White Noise with zero mean
$\upsilon(k)$	Measurement Gaussian White Noise with zero mean
$\beta(k)$	Gaussian White noise with zero mean
A, B, C	Constant Matrices
Q	Covariances of Process Noise
R	Covariances of Measurement Noise
$P_{k\|k-1}$	Prior Estimate of error covariance matrix
K_K	Kalman Filter Gain
P_k	Error Covariance matrix
e'(k)	Prior estimation error
z(k)	Estimation residue
L	Control gain matrix
J	Cost function
M	Symmetric, Square Weighting Matrix
N	Symmetric Control Cost Matrix
$\alpha_f(k)$	False Data Signal or Attack
χ^2	Anomaly Detector
C	Output matrix
D	Transmission matrix
$g(k)$	Criterion for Detection of Anomaly
α	Threshold value
$e(t)$	Error Signal
K_p	Proportional Gain
T_i	Integral Time
T_d	Derivative Time
p	Proportional Gain
i	Integral Gain
d	Derivative Gain
N	Filter Coefficient

In the attack scenario, an adversary sends improper information such that $y' \neq y$ or $u' \neq u$ from sensors to controllers and controller to actuator, respectively. The agent can congest the communication channel by flooding it with more traffic and inhibit them from sending data. The mathematical formulation is discussed in the subsequent subsections and the list of symbols used here are summarized in Table II.

A. Plant Description

In this paper, as shown in (1) and (2), the system dynamics of a discrete linear time-invariant system with noise is considered:

$$x(k+1) = Ax(k) + Bu(k) + \omega(k) \quad (1)$$

$$y(k) = Cx(k) + \nu(k) \quad (2)$$

Here, the state vector is $x(k)$, the control vector is $u(k)$, output of measurement signal is $y(k)$, and A, B, C are the known constant matrices having appropriate dimensions. In (1) and (2), $\omega(k)$ and $\nu(k)$ are the process and measurement Gaussian white noises with zero mean and covariance's Q and R, respectively. It is assumed that the controllability and observability is satisfied by (A, B) and (A, C), respectively.

B. Control and State Prediction with estimator

The Kalman filter is used for estimation of the system states [13].

$$P_{k|k-1} = AP_{k-1}A^T + Q \quad (3)$$

$$K_k = P_{k|k-1}C^T(CP_{k|k-1}C^T + R)^{-1} \quad (4)$$

$$P_k = (I - K_kC)P_{k|k-1} \quad (5)$$

$$\hat{x}(k \mid k-1) = A\hat{x}(k-1) + Bu(k-1) \quad (6)$$

$$\hat{x}(k) = \hat{x}(k \mid k-1) + K_k(y(k) - C\hat{x}(k \mid k-1)) \quad (7)$$

In (3), $P_{k|k-1}$ is prior estimate of error covariance matrix and it is also represented as:

$$P_{k|k-1} = E[e'(k)e^{T'}(k)] \quad (8)$$

The co-variances of process noise and measurement noise with zero mean, is defined as follows by Q and R, respectively:

$$Q = E[\omega(k)\omega(k)^T] \quad (9)$$

$$R = E[\nu(k)\nu(k)^T] \quad (10)$$

Here, the state estimator and controller are used to define the following state equation using the Kalman filter gain

$$\hat{x}(k) = A\hat{x}(k \mid k-1) + Bu(k-1) + K_kz(k) \quad (11)$$

$$z(k) = y(k) - C\hat{x}(k \mid k-1) + Bu(k-1) \quad (12)$$

The state feedback control law is defined by (13):

$$u(k) = -L\hat{x}(k) \quad (13)$$

In (11)-(13), the state estimation is $\hat{x}(k)$ while estimation residue is $z(k)$ and control gain matrix is denoted by L. The estimation error $e'(k+1)$ is defined as follows:

$$e'(k+1) = x(k+1) - \hat{x}'(k+1) = Ae(k) + \omega(k) \quad (14)$$

C. Linear Quadratic Gaussian (LQG) controller

The LQG controller is based on a linear state space approach with a quadratic objective function. A state-space representation of the LQG compensator is expressed as:

$$x(k+1) = (A - BK - LC + LDK)x(k) + Ly(k)$$

$$u(k) = -Kx(k) \quad (15)$$

where K and L are Kalman filter and optimal regulator

gain matrices, respectively.

This controller minimizes the cost function

$$J = \int_0^{\infty} \left[x^T Mx + u^T Nu \right] dt \quad (16)$$

where *M* is symmetric, square weighting matrix and *N* is symmetric, square control cost matrix.

D. Attack formulation

The attackers, by using known system dynamics, can degrade the control performance and even can create damaging environment. Such attacks may be introduced in the forward and/or feedback stream. The attacks may be deception or DoS (as reported in the literature).

The attacker may design the feedback attack, as shown below in (17)

$$\alpha_f(k) = -y_f(k) + CA\hat{x}_f(k-1) + CBu_f(k-1) + \beta(k) \quad (17)$$

where $\beta(k)$ is Gaussian white noise with zero mean, $\alpha_f(k)$ is false data signal designed by the attacker, $\hat{x}_f(k-1)$ is the estimated states attained by attacker.

Definition: By using following expressions, it is defined that a control system is insecure for the given attack sequence if:

a) State difference

$$\lim_{k\to\infty} \left\| \Delta x(k) \right\| \to \infty \quad (18)$$

b) Estimation residual difference

$$\left\| \Delta z(k) \right\| \le l \quad (19)$$

c) Error estimation difference

$$\lim_{k\to\infty} \left\| \Delta e(k) \right\| \to \infty \quad (20)$$

where l is positive constant.

As discussed in [3], anomaly detectors χ^2 are used here to detect system abnormal operation. This computes the following criterion:

$$g(k) = z^T(k) P^{-1} z(k) \quad (21)$$

where the estimation error covariance matrix is represented by $P = CPC^T + R$. This detector compare $g(k)$ with the threshold value μ. If μ is less than $g(k)$, this detector will trigger an alarm. The probability of detection $\beta(k)$ is calculated as in (22):

$$\beta(k) \overset{\Delta}{=} P(g(k) \ge \mu) \quad (22)$$

E. Control Element

The PID controller is used for providing the control action to the actuator, which governs the plant to obtain the desired response. The PID algorithm is defined as

$$u(t) = K_p \left(e(t) + \frac{1}{T_i} \int_0^t e(t)dt + T_d \frac{de(t)}{dt} \right) \quad (23)$$

where the control signal is represented by $u(t)$, proportional gain by K_p, error signal by $e(t)$, integral time by T_i and derivative time by T_d. The (23) can also be expressed as given below in (24):

$$G(s) = p + i\frac{1}{s} + d\frac{N}{1+Ns} \quad (24)$$

where integral gain represented by i, proportional gain by p and derivative gain by d. Here, filter coefficient is denoted by the variable N. Gain values of the PID controller are determined by tuning the parameters.

IV. Explanation of Numerical Example

A numerical example with the simulation results is discussed in this section to demonstrate the optimum performance of the Kalman filter and LQG controller along with PID controller. In this numerical example, the physical plant with following system matrices are defined as,

$$A = \begin{bmatrix} -1.7 & 50 & 260 \\ 0.22 & -1.4 & -32 \\ 0 & 0 & -12 \end{bmatrix}, B = \begin{bmatrix} -272 \\ 0 \\ 14 \end{bmatrix}$$

$$C = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{bmatrix}, D = \begin{bmatrix} 0 \end{bmatrix}$$

$$F = \begin{bmatrix} 0.02 & 0.1 \\ -0.0035 & 0.004 \\ 0 & 0 \end{bmatrix}$$

Here λ = -4.87, -1.77, -12 are the eigenvalues of the system matrix and it is observed that the Kalman filter is stable. The filter and control gain considering co-variances of measurement noise ($R = 0.1I_2$) and process noise ($Q = 0.01I_3$) with zero mean is computed as:

$$K = \begin{bmatrix} 0.9982 & -0.0172 \\ -0.0172 & 0.8330 \\ 0.0045 & 0.3966 \end{bmatrix}$$

$$L = \begin{bmatrix} 0.0020 & -0.0326 & -1.0393 \end{bmatrix}$$

The simulation is performed in the MATLAB/Simulink using PID controller along with Kalman Filter and LQG controller for estimation of the state of the given system. The PID controller parameter are chosen by tuning the parameters as p = -0.0746, i = -0.0371 and d = -0.0181, N = 36.75. The simulation time is 20s and sampling time is 10ms. The estimation of system state $x(k)$ is shown in Fig. 2 while the estimation of the measurement states $y(k)$ using are shown in Fig. 3. It has been shown in Fig. 2 and Fig. 3 that PID controller along with Kalman filter and LQG controller estimates the system states optimally.

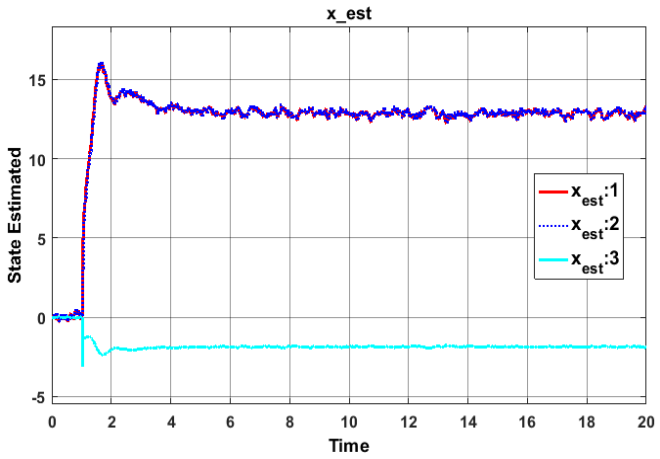

Fig. 2. Simulation result for the estimation of State.

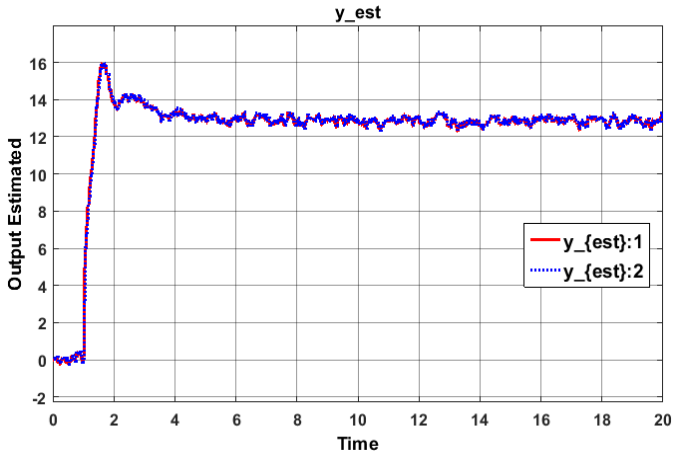

Fig. 3. Simulation result for the estimation of output.

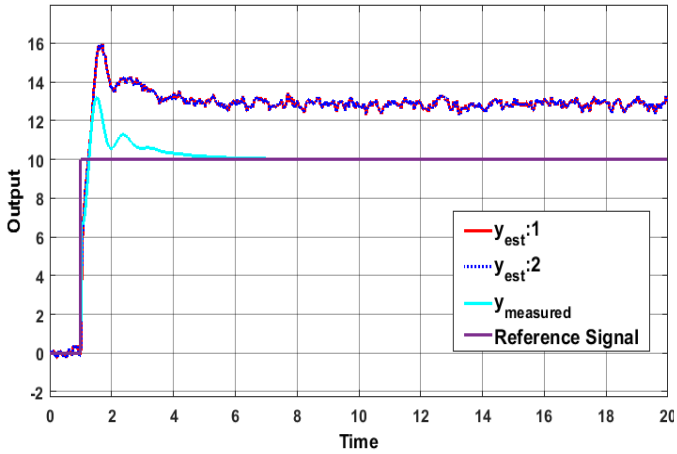

Fig. 4. Simulation result for the Measured and Estimated Output w.r.t. reference signal.

To present a comparison with respect to reference signal, the measured output and estimated output are plotted in Fig. 4. It is observed that even in presence of noise, the estimated output is optimally converging towards the reference signal. The estimation of the residual z1 and z2 is depicted by Fig. 5.

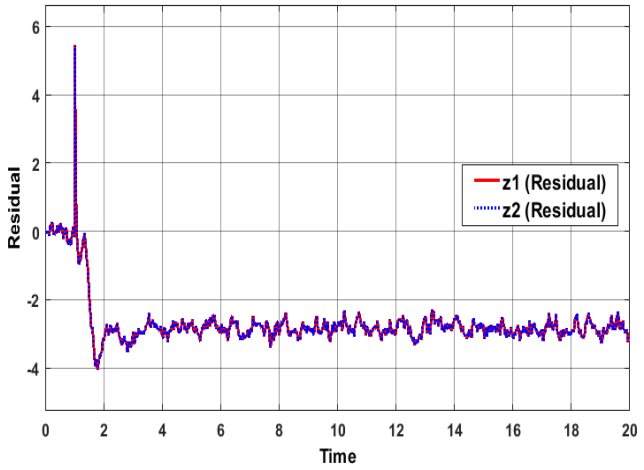

Fig. 5. Simulation result of the Residual.

V. Conclusion and Future Work

The effect of disturbances on NCS is investigated using a numerical example with simulation. Such attacks may be introduced in the forward and/or feedback stream through communication link. The effect of these attacks along with presence of process noise and measurement noise on the performance of the control system is investigated using Kalman filter. Certain sufficient conditions are described here to the estimate system states. The estimation of system state $x(k)$ and the measurement states $y(k)$ in presence of process and measurement noise and by using the discussed methodology are plotted in Fig. 2 and Fig. 3, respectively. It is depicted from these figures that Kalman filter along with PID and LQG controllers estimate the states optimally.

In the future, more sufficient conditions for stability of the control system will be discussed using practical experimentation. Also, for mitigating the network imperfections and attacks, the countermeasures will be investigated by designing an optimal controller.

References

[1] A. O. De Sá, L. F. R. D. C. Carmo, and R. C. S. Machado, "Covert Attacks in Cyber-Physical Control Systems," *IEEE Trans. Ind. Informatics*, vol. 13, no. 4, pp. 1641–1651, 2017.

[2] F. Hou and J. Sun, "Covert attacks against output tracking control of cyber-physical systems," *Proc. IECON 2017 - 43rd Annu. Conf. IEEE Ind. Electron. Soc.*, vol. 2017–Janua, pp. 5743–5748, 2017.

[3] F. Hou and J. Sun, "Fasle data injection attacks in cyber-physical systems based on inaccurate model," *Proc. IECON 2017 - 43rd Annu. Conf. IEEE Ind. Electron. Soc.*, vol. 2017–Janua, pp. 5791–5796, 2017.

[4] M. S. Ayas and S. M. Djouadi, "Undetectable sensor and actuator attacks for observer based controlled Cyber-Physical Systems," *2016 IEEE Symp. Ser. Comput. Intell. SSCI 2016*, 2017.

[5] B. Satchidanandan and P. R. Kumar, "Secure control of networked cyber-physical systems," *2016 IEEE 55th Conf. Decis. Control. CDC 2016*, no. Cdc, pp. 283–289, 2016.

[6] Hao Xu and S. Jagannathan, *Stochastic optimal controller design for unknown networked control system under TCP*, no. 1, pp. 6503–6508, 2014.

[7] T. Li, Z.-H. Guan, F.-S. Yuan, and F.-L. Qu, "Stabilisation of wireless networked control systems with packet loss," *IET Control Theory Appl.*, vol. 6, no. 15, pp. 2362–2366, 2012.

[8] X. Zhu and G. Yang, "Jensen integral inequality approach to stability analysis of continuous-time systems with time-varying delay," *IET Control Theory Appl.*, vol. 2, no. 6, pp. 524–534, 2008.

[9] G. Irwin, J. Colandairaj, and W. Scanlon, "Understanding wireless networked control systems through simulation," *Comput. Control Eng.*, vol. 16, no. 2, pp. 26–31, 2005.

[10] Y. Xia, J. Chen, and L. Zhou, "Networked control systems with different control inputs," *Proc. 26th Chinese Control Conf. CCC 2007*, no. 6, pp. 539–543, 2007.
[11] Z. Song and X. Zhou, "Research and *simulation of wireless sensor and actuator networked control system," 2013 25th Chinese Control Decis. Conf. CCDC 2013*, pp. 3995–3998, 2013.
[12] P. Ding, Y. Wang, G. Yan, and W. Li, "DoS attacks in electrical cyber-physical systems: A case study using TrueTime simulation tool," *Proc. - 2017 Chinese Autom. Congr. CAC 2017*, vol. 2017–Janua, no. 2015, pp. 6392–6396, 2017.
[13] Z. H. Pang, G. P. Liu, D. Zhou, F. Hou, and D. Sun, "Two-Channel False Data Injection Attacks Against Output Tracking Control of Networked Systems," *IEEE Trans. Ind. Electron.*, vol. 63, no. 5, pp. 3242–3251, 2016.
[14] S. Zhen, Z. Hou, and C. Yin, "A novel data-driven predictive control for networked control systems with random packet dropouts," *Proc. 2017 IEEE 6th Data Driven Control Learn. Syst. Conf. DDCLS 2017*, pp. 335–340, 2017.
[15] J. Zhang, C. Peng, S. Masroor, H. Sun, and L. Chai, "Stability analysis of networked control systems with denial-of-service attacks," *2016 UKACC Int. Conf. Control. UKACC Control 2016*, pp. 1–6, 2016.
[16] J. Sun, J. Chen, and L. Dou, "Networked predictive control for linear systems with unknown communication delay," *2014 UKACC Int. Conf. Control. Control 2014* - Proc., no. July, pp. 668–672, 2014.
[17] L. Hu, Z. Wang, and W. Naeem, "Security analysis of stochastic networked control systems under false data injection attacks," *2016 UKACC Int. Conf. Control. UKACC Control 2016*, pp. 1–6, 2016.
[18] A. O. De Sa, L. F. R. D. C. Carmo, and R. C. S. Machado, "Use of Switching Controllers for Mitigation of Active Identification Attacks in Networked Control Systems," *Proc. - 2017 IEEE 15th Int. Conf. Dependable, Auton. Secur. Comput. 2017 IEEE 15th Int. Conf. Pervasive Intell. Comput. 2017 IEEE 3rd Int. Conf. Big Data Intell. Compu*, vol. 2018–Janua, pp. 257–262, 2018.
[19] J. Jithish and S. Sankaran, "Securing networked control systems: Modeling attacks and defenses," *2017 IEEE Int. Conf. Consum. Electron. ICCE-Asia 2017*, vol. 2018–Janua, pp. 7–11, 2018.
[20] G. Wu, J. Sun, and J. Chen, "Optimal data injection attacks in cyber-physical systems," *IEEE Trans. Cybern.*, vol. 48, no. 12, pp. 3302–3312, 2018.
[21] A. W. Al-Dabbagh, Y. Li, and T. Chen, "An intrusion detection system for cyber attacks in wireless networked control systems," *IEEE Tras. Circuits Syst. II Express Briefs*, vol. 65, no. 8, pp. 1049–1053, 2018.
[22] H. Zhang, P. Cheng, L. Shi, and J. Chen, "Optimal DoS Attack Scheduling in Wireless Networked Control System," *IEEE Trans. Control Syst. Technol.*, vol. 24, no. 3, pp. 843–852, 2016.
[23] J. Hu, C. Liu, and Y. Song, "Switching control for networked control system with denial-of-service attacks," *Chinese Control Conf. CCC*, pp. 7667–7672, 2017.
[24] S. Han, M. Xie, H. H. Chen, and Y. Ling, "Intrusion Detection in Cyber-Physical Systems: Techniques and Challenges," *IEEE Syst. J.*, vol. 8, no. 4, pp. 1052–1062, 2014.
[25] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Trans. Automat. Contr.*, vol. 58, no. 11, pp. 2715–2729, 2013.
[26] X. Huang and J. Dong, "Reliable control policy of cyber-physical systems against a class of frequency-constrained sensor and actuator attacks," *IEEE Trans. Cybern.*, vol. 48, no. 12, pp. 3432–3439, 2018.
[27] H. C. Cho and M. S. Fadali, "Nonlinear network-induced time delay systems with stochastic learning," *IEEE Trans. Control Syst. Technol.*, vol. 19, no. 4, pp. 843–851, 2011.
[28] L. Jianning, "Stabilization of wireless networked control system with multi-packet transmission policy," *Control Conf.* (…, pp. 5770–5774, 2012.
[29] F. Miao, Q. Zhu, M. Pajic, and G. J. Pappas, "Coding Schemes for Securing Cyber-Physical Systems Against Stealthy Data Injection Attacks," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 106–117, 2017.
[30] S. Hu, Y. Zhou, X. Chen, and Y. Ma, "H∞ controller design of event-triggered networked control systems under quantization and denial-of-service attacks," *Chinese Control Conf. CCC*, vol. 2018-July, pp. 6338–6343, 2018.
[31] Zhong-Hua Pang and Guo-Ping Liu, "Design and Implementation of Secure Networked Predictive Control Systems Under Deception Attacks," *IEEE Trans. Control Syst. Technol.*, vol. 20, no. 5, pp. 1334–1342, 2011.

Brijraj Singh Solanki received his B.E. in Electronic Instrumentation and Control Engineering and M. Tech. in Electronics and Communication Engineering, in 2006 and 2013, respectively. Currently he is pursuing the Ph.D. degree in Electronics and Communication Engineering from Manipal University Jaipur. His research interest includes control system.

Renu Kumawat received her B.E. in Computer Science & Engineering in 2004, M. Tech. in VLSI Design in 2006. She received her PhD in 2015 from National Institute of Technology, Jaipur, India. Her research interest includes VLSI & Embedded System Design, Machine Learning and AI. She is a Senior Member of IEEE and member of ACM. She is currently working as an Associate Professor in Dept. of Electronics and Communication Engineering at Manipal University Jaipur.

Seshadhri Srinivasan obtained his Ph.D. from National Institute of Technology, Tiruchirappalli, India in 2010, specializing in networked control systems. He was an Assoc. Scientist in ABB Corporate Research, Scientist in CENS, Estonia, Technical University of Munich, Germany, Unisannio, Italy, Kalasalingam University, India and BEARS, Singapore. His research interests are in Building automation, smart grids, optimization and control. Currently he is Professor, Dept. of Biomedical Engineering, Kalasalingam Academy Research and Education (KARE), India.