Stability and Performance Analysis of Networked Control System Experienced Variable Uncertain Dynamics

Brijraj Singh Solanki*

Professor, Department of Computer Engineering, Poornima College of Engineering, Jaipur, India

***Abstract*: The rapid development has been seen in network control systems with the integration of sensors, actuators and controllers. Network Control Systems (NCS) are used in a several of fields due to their low maintenance, ease of installation, system cabling and monitoring. However, communication over the NCS network is vulnerable through targeted attacks. With large amount of information transmitted through communication channel/networks is more likely to be accessed by entrants to reduce the control over the network system. So, in this paper the problem due to uncertain disturbance in NCS is considered to improve the transient performance of networked system. To show the effectiveness of proposed methodology a numerical simulation is presented with different simulation diagrams with MATLAB Simulink environment.**

***Keywords*: Networked Control System, Denial of Service (DoS), Delay, Proportional Integral Derivative Control, Packet Loss.**

1. Introduction

With Network control system has been evolved as a technological field where components are distantly associated through a real-time communication network [1]. The NCS trust on the secure transmission of packets/message through communication channel to improve overall system performance. With rapid development in information technology NCS has many industrial applications such as in power distribution, oil and gas power plants, water management, transportation, robotics, process industry, space vehicles and medical treatment etc. [2]. Packets containing sensitive information transmitted through the network may be susceptible to attack. The intruder can access the information in various ways, such as eavesdropping, denial of service (DoS), and service degradation attack (SD).

The stability of DC/DC converters with CAN-bus system studied taking into account the performance degradation parameters such as time delay and packet dropout. Discrete time delay is modeled using Markov chains and stability is analyzed through set of linear matrix inequality equations. The voltage controller gain was determined to show stability of system [3].

The performance degrading parameter random delay and packet loss also discussed to analyze the stability of networked control system through application of position servo system. Employed system was used for calculating the optimal performance index and control gain [4].

In a network control system, latency and packet loss are key parameters to control stability, and packet loss is modeled using the Bernoulli function. Some stable methods are obtained to show the measurement quality of the defined method [5]-[8].

Lyapunov method presented to simulate the stochastic packet loss and sufficient condition with asymptotic stability for feedback networked control system discussed to capture the effect of time delay [9].

This paper deals with the problem due to uncertain disturbance in NCS is considered to improve the transient performance of networked system. To show the effectiveness of proposed methodology a numerical simulation is presented with different simulation diagrams with MATLAB Simulink environment.

The rest of the article presents the following different parts: In 2 section, the articles related to the attack types and the stability of the NCS are described. The formulation of the problem based on network uncertainty and malicious interference is presented in section 3. The effectiveness of the presented method will be presented in the 4 section. Finally, Section 5 provides conclusive observations and future work to be carried out.

2. Literature Review Work

The attack on non-linear network and sensor detected through introduction of neural-network based event triggered controller scheme employing dynamic programming approach. Attack is discovered with the help of residual exceeds a predefined threshold. The attack considered in this approach was time delay and packet loss in nature. The proposed methodology employed was faster in detection than conventional approach discussed in literature [10], [11].

The effect due to unwanted intrusive data studied in [12], [13] through introduction of Kalman-filter, linear quadratic Gaussian approach and proportional integral controller in networked control system. It has been presented that due to such methodology the effect on NCS was greatly reduced to an

*Corresponding author: brijraj.eic@gmail.com acceptable level. Various parameters determined to evaluate the performance metrics of proposed system.

Two queuing approaches discussed to model the performance degradation in networked control system which is prone to delay and packet loss attack. The Denial of Service (DoS) attack considered to be responsible for parameter degradation in control system. Such DoS attack worsen the quality-of-service parameter of network which drops the performance [14]-[17].

Predictive control approach applied to analyze the performance measures of closed loop networked control systems undergone communication network constraint [18], [19]. The Linear Quadratic Regulator (LQR) technique addressed to improve the performance of networked system with the help of an example of rotary inverted pendulum system. In this communication constraint such as packet loss and time delay considered as disturbing factor in closed loop networked system. By employing such techniques, the performance improved at desired level [20]-[22].

In [23], data backup-based compensation technique employed to guarantee the stability of the proposed system. Lyapunov function used to derive the set of stability conditions for networked system experienced induced delay and packet loss problem. Certain condition established which direct the required control input to maintain the response up to desired level [24]-[26]. The problem due to communication constraint addressed through deriving the set of condition using Lyapunov function, linear matrix inequality and Wirtinger inequality. Proposed interval type-2 fuzzy model revealed the improved performance of control system under communication constraint [27], [28].

The predictive controller is designed to describe the response of the designed method to the control system. This may affect the transfer of data due to the introduction of a denial-of-service attack [29], [30]. The attacks introduced for wireless network management systems have been calculated using an intrusion detection system, and the authors have also validated the proposed method for stability [31], [32].

The message data sent from the sensor to the controller or from the controller to the router can be corrupted using various attack methods such as denial of service and replay attacks. Horizontal reverse power law, exponential stability is proposed to derive stable methods for performance analysis [33], [34], [35]. Improved performance of the control system for distribution grid management is discussed in [36]. Time and strategy are used to demonstrate the effectiveness of the system. Also discussed is the impact of delay, jitter and packet loss in transmission, which is a key factor in system instability.

An approach to optimize the performance of stochastic linear time-invariant system presented through minimizing the weighted cost of linear quadratic Gaussian function. The networked system used shared communication resources and admit scheduling policies to find optimized cost [37].

3. Problem Formulation with Proposed Methodology

A. Description of the System

The block diagram of proposed network control system is shown in Figure 1. Here the response of the system is sampled by a sensor and forwarded to the controller through wireless communication network. The controller calculates the control signal based on the reference and sensor sampled received through communication network using an algorithm designed for the control purpose. The calculated signal directed through the communication channel to the actuator to operate system according to the desired output. In various literatures, it has been found that an attacker can interfere in any way (that is, in the forward and/or feedback direction) of the control system to worsen the performance of NCS.

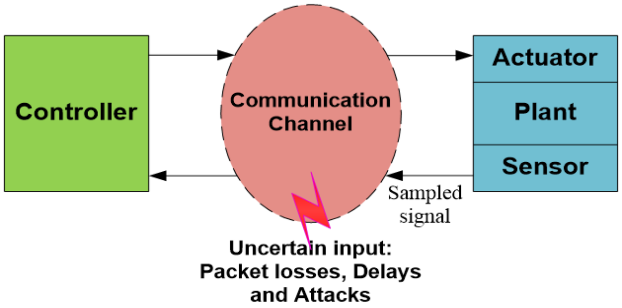

Fig. 1. NCS with uncertain parameters

The response modeled by the sensor is sent to the controller via communication, and the control signal generated by the controller is sent to the controller via the communication network. Therefore, there is a delay from the sensor to the controller and the controller to actuator (i.e. t_{sc} and t_{ca} , respectively).

B. Dynamics of Uncertain Delay

The sampled response taken by sensor is routed to controller through the communication channel and controller generated control signal is sent towards the actuator through the communication network. Hence, there are delays from sensor towards controller and controller towards actuator signal i.e. t_{sc} and t_{ca} , respectively. There are also processing delays that are as small as they should be in comparison to other delay (sensor to controller and controller to actuator delay). This random delay change depends on the length of the communication network, bandwidth, etc. The stochastic nature of the delayed disturbance causes the system to approach instability. Therefore, it is necessary to consider delay dynamics in system modeling and controller design [10].

For efficient packet delivery, sample time "τ_s" must meet the following criteria [12]:

$$\tau_s > t_{sc} + t_{ca} + (\text{processing delay}) \tag{1}$$

C. Packet Dropout Distribution

The controller receives the sampled sensor signal and sends signals to the actuator to control the process. There's a chance of packet loss when the signal travels through the communication network. The issue of packet loss can occur in both the forward and feedback directions. To model packet loss, consider the distribution function provided as [12]:

$$p(\gamma_k) = \begin{cases} p, & if\, \gamma_k = 1 \\ 1-p, & if\, \gamma_k = 0 \end{cases} \tag{2}$$

Here packet loss rate is represented by, $p \in [0,1]$. At an instant *k*, if packet is lost, then $\gamma_k = 0$, and for successful arrival of packet at an instant *k*, the $\gamma_k = 1$.

The concept of timestamp theory is applied to packet transmission, where packets are placed in a buffer with timestamps. The system with networked delay τ_s and packet loss is depicted as a linear time-invariant (LTI) system as [12],

$$x(k+1) = Ax(k) + \gamma_k Bu(k-\tau_s) \tag{3}$$

$$y(k) = Cx(k) \tag{4}$$

The state vectors are $x(k)$ and control vectors are $u(k)$ as represented in Eq. (3). Similarly, in Eq. (4), $y(k)$ is output signal and different matrices with appropriate dimensions is represented by "A, B, C".

4. Result Analysis with Proposed Designs

The effectiveness of proposed methodology is presented with different simulation diagrams with MATLAB Simulink environment.

The plant dynamics are presented by different matrices i.e. A= [-15,-1,0;75,0,-1;-125,0,0], B=[-15;75;-125], C= [1.05, -2.00, -2.00] and D=[0]. The parameters of proportional integral derivation control are given as P=0.3784, I=0.0541 and D=0.0757.

Figures 2 through 5 depicts the various simulations performed. Figure 2 depicts the simulation results that indicate the response signal generated in disturbance and employing PID control. The response signal tracks the step input after introducing disturbance. Figure 3 depicts the control input generation considering disturbance with no disturbance rejection control policy.

The figure 4 simulate the response signal generation considering disturbance along with disturbance rejection control policy. The response signal tracks well the step input after introducing disturbance and control policy for disturbance rejection.

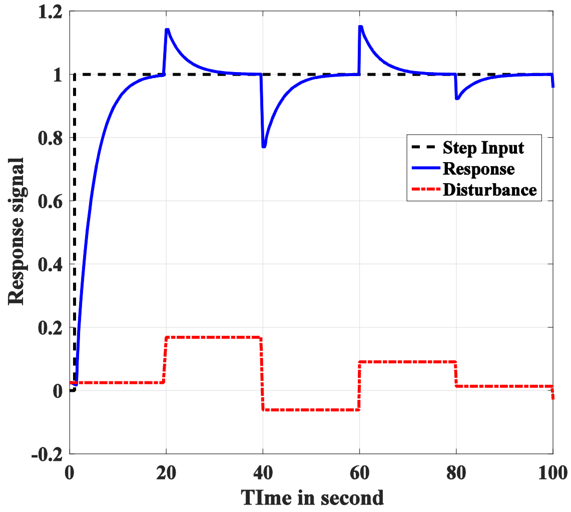

Fig. 2. Response signal generated in disturbance and employing PID control

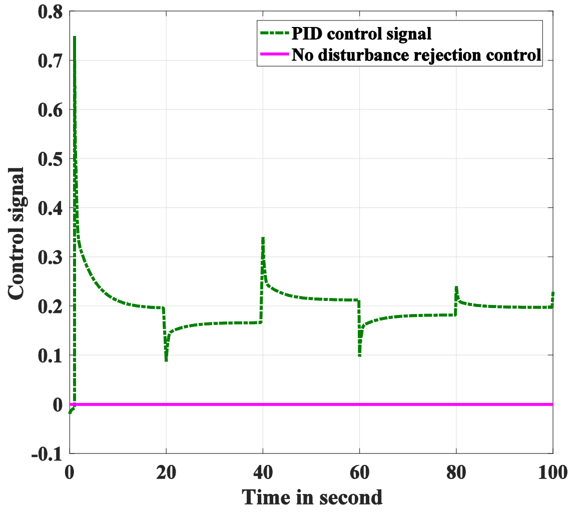

Fig. 3. Control input with no disturbance rejection

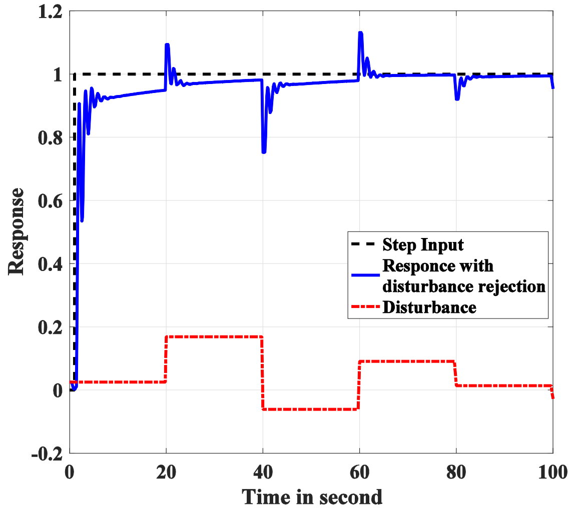

Fig. 4. Response signal generated with disturbance and PID control with disturbance rejection control policy

Similarly, figure 5 presents the control input generation considering disturbance with disturbance rejection control policy. The disturbance rejection control policy generates improved PID control signal which is directed to control NCS system. These simulations represent the effectiveness of the employed methodology.

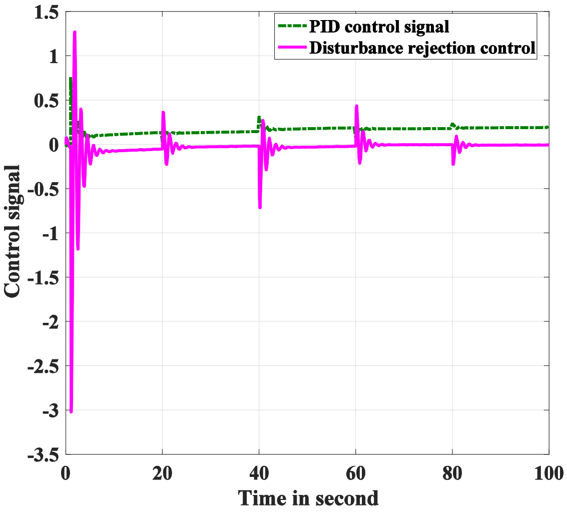

Fig. 5. PID control signal generation with disturbance rejection control policy

5. Conclusion and Future Scope of Work

The conclusive remarks over the performance metrics of networked control system under different uncertain conditions are presented in this section. To simulate the proposed model MATLAB Simulink environment is used. From Fig. 2 to Fig. 5, the simulation result shows that system performance improved with proposed methodology.

Figure 2 depicts the simulation results that indicate the response signal generated in disturbance and employing PID control. The response signal tracks the step input after introducing disturbance. Figure 3 depicts the control input generation considering disturbance with no disturbance rejection control policy.

The figure 4 simulate the response signal generation considering disturbance along with disturbance rejection control policy. The response signal tracks well the step input after introducing disturbance and control policy for disturbance rejection. Similarly figure 5 presents the control input generation considering disturbance with disturbance rejection control policy. The disturbance rejection control policy generates improved PID control signal which is directed to control NCS system.

The future work will consider the optimal control design for non-linear NCS to overcome the impact of uncertain disturbances.

References

[1] 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.

[2] P. R. Dunaka and B. McMillin, “Cyber-physical security of a chemical plant,” Proc. IEEE Int. Symp. High Assur. Syst. Eng., no. 60, pp. 33–40, 2017.

[3] H. Mejdi, S. Elmadssia, and T. Ezzedine, “A Study of a Networked Control System under Time Delay,” 2023 Int. Symp. Networks, Comput. Commun. ISNCC 2023, pp. 1–5, 2023.

[4] P. Wang and G. Feng, “A study of optimal control strategy of networked control systems with stochastic delay and packet losses,” CARE 2013 - 2013 IEEE Int. Conf. Control. Autom. Robot. Embed. Syst. Proc., pp. 1–5, 2013.

[5] Y. F. Guo and S. Y. Li, “Transmission probability condition for stabilisability of networked control systems,” IET Control Theory Appl., vol. 4, no. 4, pp. 672–682, 2010.

[6] B. Singh Solanki, R. Kumawat, and S. Srinivasan, “Optimal switching control design for industrial networked control system with uncertain exogenous dynamics,” Mater. Today Proc., vol. 79, no. xxxx, pp. 286–291, 2023.

[7] S. Solanki, B.S., Kumawat, R., Srinivasan, “Optimized Control Function with Estimation of System Parameters Against Attack for Networked Control System,” in Intelligent Computing Techniques for Smart Energy Systems. Lecture Notes in Electrical Engineering, 2022, vol. 862, pp. 515–528.

[8] B. S. Solanki, “Mitigating Effect of Uncertain Exogenous Dynamics by Parametric Performance Improvement with Optimal Control Design,” Int. J. Eng. Trends Technol., vol. 70, no. 5, pp. 209–220, Jun. 2022.

[9] X. Wang, Z. Yang, Qiangao, and X. Wei, “Analysis and control of networked control systems with time-delay and stochastic packet-dropout process,” 2010 Chinese Control Decis. Conf. CCDC 2010, pp. 1936–1941, 2010.

[10] H. Niu, C. Bhowmick, and S. Jagannathan, “Attack Detection and Approximation in Nonlinear Networked Control Systems Using Neural Networks,” IEEE Trans. Neural Networks Learn. Syst., vol. 31, no. 1, pp. 235–245, 2020.

[11] B. S. Solanki, R. Kumawat, and S. Srinivasan, “Averting and Mitigating the Effects of Uncertainties with Optimal Control in Industrial Networked Control System,” Proc. - 2021 IEEE Int. Symp. Smart Electron. Syst. iSES 2021, pp. 316–318, 2021.

[12] B. S. Solanki, R. Kumawat, and S. Srinivasan, “An Impact of Different Uncertainties and Attacks on the Performance Metrics and Stability of Industrial Control System,” in Lecture Notes in Networks and Systems, 2021, vol. 204, pp. 557–574.

[13] B. S. Solanki, “Controlled Output Feedback to Stabilize Networked Control System,” Int. J. Mod. Dev. Eng. Sci., vol. 3, no. 9, pp. 1–5, 2024.

[14] M. Long, C. H. Wu, and J. Y. Hung, “Denial of service attacks on network-based control systems: Impact and mitigation,” IEEE Trans. Ind. Informatics, vol. 1, no. 2, pp. 85–96, 2005.

[15] G. Bhatnagar, N. Gobi, H. Aqeel, and B. S. Solanki, “Sparrow-based Differential Evolutionary Search Algorithm for Mobility Aware Energy Efficient Clustering in MANET Network,” Int. J. Intell. Syst. Appl. Eng., vol. 11, no. 8s, pp. 135–142, 2023.

[16] J. N. Singh and B. S. Solanki, “Utilization of Computational Intelligence in the Development of a Health Monitoring System for Induction Machines,” 2022 Int. Conf. Futur. Technol. INCOFT 2022, pp. 1–6, 2022.

[17] S. P. Singh and B. S. Solanki, “A Trading Model on Block chain Smart Contracts for the Shared Energy in Brazil,” 4th Int. Conf. Emerg. Res. Electron. Comput. Sci. Technol. ICERECT 2022, pp. 1–5, 2022.

[18] F. Chen and X. Zhou, “Design of predictive controller for Networked Control Systems,” ITNEC 2023 - IEEE 6th Inf. Technol. Networking, Electron. Autom. Control Conf., vol. 6, pp. 1544–1547, 2023.

[19] B. S. Solanki, K. Renu, and S. Srinivasan, “Stability and Security Analysis with Identification of Attack on Industrial Networked Control System: An Overview,” Internetworking Indones. J., vol. 11, no. 2, pp. 3–8, 2019.

[20] B. Thongsakul, A. Numsomran, V. Tipsuwanporn, and J. Chaoraingern, “Event-Based LQR Control for Rotary Inverted Pendulum Using Wireless Networked Control System,” Int. Conf. Control. Autom. Syst., no. Iccas, pp. 573–578, 2023.

[21] R. Gupta, B. S. Solanki, M. Kumar, and R. Murugan, “Detecting Malware on the Android Phones Based on Golden Jackal Optimized Support Vector Machine,” Int. J. Intell. Syst. Appl. Eng., vol. 11, no. 8s, pp. 01–07, 2023.

[22] B. S. Solanki, R. Kumawat, and S. Srinivasan, “Synthesize the Effect of Intrusion and Imperfection on Networked-Connected Control System with Optimal Control Strategy,” 2021 10th Int. Conf. Inf. Autom. Sustain. ICIAfS 2021, pp. 105–110, 2021.

[23] T. B. Wang and M. Sun, “Event-triggered H∞Control for Networked Control Systems with Packet Dropout Compensation,” Chinese Control Conf. CCC, vol. 2021-July, pp. 2020–2026, 2021.

[24] T. Kumar, M. Sharma, and B. S. Solanki, "New Designs and Analysis of Multi-Core Photonic Crystal Fiber Using Ellipse with Different Radiuses and Angles," in International Conference on Artificial Intelligence: Advances and Applications 2019, 2020, pp. 151–159.

[25] B. S. Solanki, "Control System for Wind Power Plant," Int. J. Sci. Dev. Res., vol. 4, no. 3, pp. 473–476, 2019.

[26] B. Singh and O. P. Sharma, "Analysis of Coded and Uncoded Digital Modulation Techniques," Int. J. Electron. Commun. Technol., vol. 4, no. 4, pp. 46–48, 2013.

[27] Z. Lu, J. Lu, G. Ran, and F. Xu, "H∞ Filtering for Nonlinear Networked Control Systems with Mixed Random Delays and Packet Dropouts," Proc. 31st Chinese Control Decis. Conf. CCDC 2019, no. 1, pp. 2572–2577, 2019.

[28] B. Singh, "Solar Power Generation by PV Technology," IRE Journals, vol. 1, no. 9, pp. 260–265, 2018.

[29] Z. H. Pang and G. P. 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, 2012.

[30] 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.

[31] A. W. Al-Dabbagh, Y. Li, and T. Chen, "An intrusion detection system for cyber attacks in wireless networked control systems," IEEE Trans. Circuits Syst. II Express Briefs, vol. 65, no. 8, pp. 1049–1053, 2018.

[32] B. Singh and O. P. Sharma, "Analysis of BER in BPSK and GMSK Employing Different Coding," IFRSA's Int. J. Comput., vol. 2, no. 4, pp. 736–741, 2012.

[33] M. Zhu and S. Martinez, "On the performance analysis of resilient networked control systems under replay attacks," IEEE Trans. Automat. Contr., vol. 59, no. 3, pp. 804–808, 2014.

[34] K. L. Miao, J. W. Zhu, and W. A. Zhang, "Distributed guaranteed cost control of networked interconnected systems under denial-of-service attacks: A switched system approach," Proc. - 2018 33rd Youth Acad. Annu. Conf. Chinese Assoc. Autom. YAC 2018, pp. 911–915, 2018.

[35] B. S. Solanki, "Design of an Optimal Reliable Controller for Industrial Networked Control System to Mitigate Network Imperfections," 2022.

[36] Z. Liang, Y. Guo, Y. Yang, and G. Chen, "Distribution network control system scheduling strategy," Proc. 2019 IEEE 3rd Inf. Technol. Networking, Electron. Autom. Control Conf. ITNEC 2019, no. Itnec, pp. 1424–1428, 2019.

[37] M. Klugel et al., "Joint Cross-Layer Optimization in Real-Time Networked Control Systems," IEEE Trans. Control Netw. Syst., vol. 7, no. 4, pp. 1903–1915, 2020.