International Journal of Systems Signal Control and Engineering Application

MEDWELL PUBLICATIONS SINCE 2000

Observer Based Resilient Control of Networked Control Systems Against Cyber Attacks to Sensor

Maryam Fattahi and Ahmad Afshar
Department of Electrical Engineering, Amirkabir University, Tehran, Iran

Key words: Observer-based resilient control, networked control systems, cyber attacks, lyapunov-krasovskii functional, exponential behavior

Corresponding Author:
Maryam Fattahi
Department of Electrical Engineering, Amirkabir University, Tehran, Iran

Page No.: 66-74
Volume: 13, Issue 3, 2020
ISSN: 1997-5422
International Journal of Systems Signal Control and Engineering Application

Abstract: The object of this article is to propose novel observer-based resilient control for Networked Control Systems (NCS) against cyber-attacks to sensor. It is assumed system is under cyber-attacks that occurred in sensor such that attacker can access to sensor and consequently injects false data to sensor. To achieve resilience in such conditions, at first a novel observer is proposed in order to estimate the actual states of system. Then a novel observer based controller is proposed in order to NCS in conditions of attack remains stable. Applying Lyapunov-Krasovskii functional method, delay dependent resilient criterion is established to show the exponential behavior of NCS in such conditions. Finally, for evaluating results, a practical example will be discussed.

INTRODUCTION

Recently the object of Networked Control Systems (NCS) has been an attractive topic for many mathematicians and engineers. This is due to successful applications of NCS in many areas such as telecommunications, automated highway systems, wired and wireless networks, water/power distribution networks, smart grids[1-7].

In NCS, physical process, sensors, actuators and network are linked together through communication protocols (Fig. 1). Hence, the present of the communication links leads to an inevitable delay in the information exchange between different parts of system. On the other hand, for implementation of controller, modern control systems use digital technology and hence, the sampled-data control theory is applied for NCS. One of the main approaches for sampled-data theory is based on modelling the sampled-data system as a continuous-time system with delayed control input. Delay in such systems can bring negative effects on the performance of the system and even it may lead to system unstable. Therefore, there is significant attention that has been devoted to obtain many important results on the stability and stabilization for NCS with unavoidable delays. For instance by Chen *et al*.[8] the problem of delay-dependent state feedback control for a class of NCS with nonlinear perturbations and two delay components has been studied. Zhang *et al*.[9] investigated the problems of stability and stabilization for NCS with additive time-varying delay in controller. Li *et al*.[10] considered the problem of extended dissipativity analysis and synthesis for NCS under an event-triggered scheme. By Zhang *et al*.[11] design and analysis problems of output feedback delay compensation controller for NCS with random network delay has been discussed. By Zhang *et al*.[12] the problem of networked output tracking control has been investigated by considering the delay compensations in both the feedback and forward channels in NCS.

Moreover, Because of the network structure in NCS that is responsible for control and monitoring many

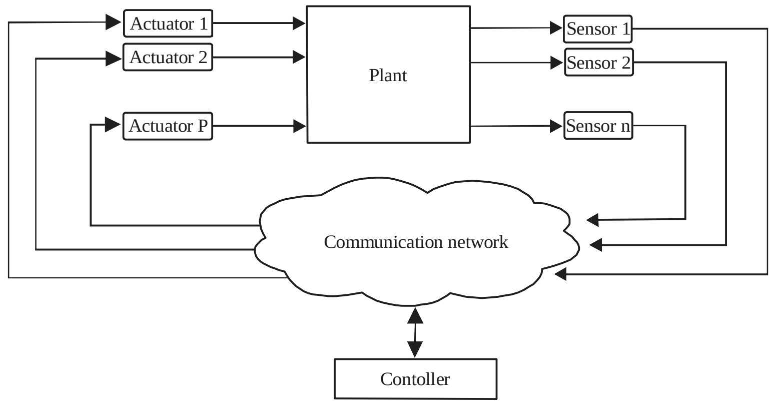

Fig. 1: Schematic of NCS

critical infrastructures and consequently the presence of large components in these systems, NCS are vulnerable to various malicious cyber-attacks. That is why security problems in NCS have attracted much attention in the control community due to the fact that large amount of data need to be transferred through networked communication channel which is exposed to cyber-attacks[13-16]. The cyber-attacks lead to incorrect control actions that may result poor performance of system. Recently, researchers have proposed some methods to protect the system against cyber-attacks. For instance,[17] proposed an active resilient control strategy for singular NCS with external disturbances and missing data scenario based on sampled-data scheme. By Tan *et al*.[18] stabilization of NCS with both network-induced delay and packet dropout has been studied. Tian *et al*.[19] studied the reliable controller design for NCS against both probabilistic sensor and actuator faults. By Feng and Tesi[20] NCS in the presence of Denial-of-Service (DoS) attacks that prevent transmissions over the communication network has been studied. By Sun and Peng[21] the phenomena of random delays and packet dropouts of both sides from a sensor to an estimator and from a controller to an actuator has been modeled via employing two groups of Bernoulli random variables. It should be noticed, one of the active problems in this field is modeling of injected false data from attacker to NCS such that the considered model covers a numerous unpredictable attacks in order to the presented model to be near to real world applications.

Additional to above problems, obtaining information from states of NCS is another challenge in this area. States of NCS may not be measured because of some reasons such as cyber-attacks to sensor that leads to loss of true measurement. Having states information for NCS is very important because control strategy in NCS is usually based on information from states of system. In such conditions, observer design is required to control system. However, until now in this area few papers are available. Among references in the area of observer design for NCS, the following papers can be mentioned: By Wang *et al*.[22] state observer for nonlinear NCS has been designed. Liu *et al*.[23], Wang *et al*.[24] investigated full order $H\infty$ observer design problem for NCS.

Based on above discussion and practical applications of NCS, cyber security and resilient analysis is an important and challenging problem in this area. Moreover, attacker can access to sensors of network such that manipulates sensor data. This problem may result instability of system. Also, considering much more real world regions for assumed constraints on modeling of injected false data of attacker is another topic in this area that is still an active problem. These applicable and technical assumptions will be a challenging analysis for NCS. Based on our researches in the works done, until know there is no similar work on the resilient sampled-data observer based control design for NCS with considering multiple time-varying delays and cyber-attack in sensor while injected data of attacker don’t need to satisfy constraints such as norm-bounded, sector nonlinearity, Lipchitz constrain, one side Lipchitz constraint. Based on these discussions, the question that arises is whether it is possible to propose a novel resilient observer based control design to guarantee performance of system in such conditions. This problem motivates us to offer this work.

To summarize, the main contributions of this paper are as follows: considering delay in the transmission of data from states of plant located in field to controller and also transmission delay among states of plant simultaneously. Observer design for NCS while considering accessibility of attacker to sensor that results creating a forgery channel by attacker to injects false data and mixes them with actual sensor data. In this scenario there is no need to false data satisfies any constraint on its nonlinear dynamic except some LMIs. Hence, such observer mechanism covers many unpredictable, unknown and random false data of attacker. This approach results real world applications of the proposed design. Unlike to some articles such as[25] that reach to uniformly ultimately bounded stability for NCS, this work achieves exponential stability region for NCS. In comparison and with respect to results in references[17, 19-21], the presented work has more advantages that will be discussed in the sequel.

Motivated by these considerations, in this issue at first required symbols and Lemmas are defined. Then it is assumed system is under sensor attack and an observer based resilient controller is proposed for stability of NCS against such cyber-attack. To achieve resilience in such conditions, Lyapunov-Krasovskii functional method is applied and delay dependent resilient criterion is established to show the exponential behavior of system in such attack scenario. Finally, for evaluating results, a practical example will be solved.

Preliminaries: In this research, we use some mathematical symbols with the following descriptions: R^n denotes n_dimensional Euclidean space; p>0 eans that the matrix P is symmetric and positive definite; I and 0 are identity matrix and the null matrix with appropriate dimension; '-1' and 'T' mean nverse and transpose of a given matrix; ||x|| means 2-norm of a matrix, $\lambda_{min}(A)$ means minimum eigenvalues of A, λ_{max} (A) means maximum eigenvalues of A, * means symmetric blocks in the matrix inequality. And some useful Lemmas used in this research are as:

Lemma 1 [17]: Let x $(t)\in R^n$ be a vector-valued function with first-order continuous-derivative entries. Then following integral inequality holds for any matrices X , M_1, $M_2 \in R^{n\times n}$, $Z\in R^{2n\times 2n}$ and a scalar function h: = h(t)≥0:

$$-\int_{t-d(t)}^{t}\dot{x}^T(s)X\dot{x}(s)ds \le \xi^T(t)T\xi(t)+h(t)\xi^T(t)Z\xi(t)$$

Where:

$$T=\begin{bmatrix} M_1^T+M_1 & -M_1^T+M_2 \\ * & -M_2^T-M_2 \end{bmatrix},\ \xi(t)=\begin{bmatrix} x(t) \\ x(t-d(t)) \end{bmatrix},$$

$$\begin{bmatrix} X & Y \\ * & Z \end{bmatrix}\ge 0 \text{ with } Y:=[M_1\ \ M_2]$$

Lemma 2 [23]: For given matrices C, E and equation HCE = E, a solution for H exists, if rank (CE) = rank (E). A general solution for H is given by:

$$H=E(CE)^{+}+Z\left(I-(CE)(CE)^{+}\right)$$

MATERIALS AND METHODS

Problem statement
Consider the following NCS:

$$\begin{aligned} &\dot{x}(t)=Ax(t)+A_d x(t-d(t))+Bu(t),\ i=1,\ ...,\ N \\ &y(t)=Cx(t)+f_s \\ &x(\theta)=\phi(\theta),\ \theta[-d_2,\ 0] \end{aligned} \quad (1)$$

Where, $x\in R^n$ is the state, $u\in R^p$ is the control input, $y\in R^l$ is the output, f_s is the sensor fault, A, Ad, B, C are the constant known matrices. $\{\phi(\theta)\}_{-d_2}^{0}$ are the initial conditions and d(t) satisfies:

$$d_1\le d(t)d_2,\ \dot{d}(t)\le\tau<1 \quad (2)$$

where d_1, d_2 are known.

Remark 1: It should be mentioned that in NCS, the data packets are transmitted through network, so, the control signal depends on the sampling period. Hence, control input can be considered as $u(t) = Kx(t_k)$, $t_k\le t\le t_{k+1}$, k = 0, 1, ... Assuming state variables of system Eq. 1 are measured at time instants t_k, t_{k+1}, k = 0, 1, ... with $t_k\le t\le t_{k+1}-t_k = h(t)$, $h_{1l}\le h_l(t)\le h_{2l}$, $\dot{h}_l(t)\le\upsilon_1<1$, controller based sampled data can be shown as u(t) = Kx(t-h(t)), $tk\le t\le t_{k+1}$, k = 0, 1. This problem will be considered in resilient controller design in the sequel.

Remark 2: In NCS there are sensors that transmit data from plant to network. Based on the geographical area of plant, sensors are distributed in different zoon of plant. Because position of each sensor is different from other sensors and a sensor may use data from other sensors, delay in communication link between sensors may be occur. That is why in the assumed model for NCS (1) A_d x(t-d(t)) has been considered. Based on above explanations, assumed model for NCS in this research is more general than models offered by Sakthivel *et al*.[17], Tan *et al*.[18], Tian *et al*.[19], Feng and Tesi[20], Sun and Ma[21], Wang *et al*.[22], Liu *et al*.[23], Wang and Han[24] and Sun *et al*.[25].

RESULTS AND DISCUSSION

Observer design: In this study, we want to obtain sufficient condition to estimate the states of NCS by designing a novel observer as follows:

$$\begin{aligned} \dot{\hat{x}}(t) &= F\hat{x}(t)+G\hat{x}(t-d(t))+L_1\dot{y}(t)+ \\ & L_3y(t-d(t))-L_1\hat{f}_s-L_2\dot{\hat{f}}-L_3\hat{f}(t-d(t)) \end{aligned} \quad (3)$$

Where:

$\hat{x}$	=	The states of observer
$\hat{f}$	=	The sensor attack estimator
F, G, L_1, L_2, L_3	=	Are parameters of the proposed observer. We can write Eq. 3 as:

$$\begin{aligned} \dot{\hat{x}}(t) &= (F+L_1C+L_2CA)\hat{x}(t)+(G+L_2CA_d+L_3C)\hat{x}(t-d(t))+ \\ & L_2(f_s-\hat{f}_s)+L_2\left(\dot{f}_s-\dot{\hat{f}}_s\right)+L_3\left(f_s(t-d(t))-\dot{\hat{f}}_s(t-d(t))\right) \end{aligned} \quad (4)$$

Defining $e_s(t)=x(t)-\hat{x}(t)$ as the observer error and $\tilde{f}_s(t)=f_s(t)$ as the attack estimation error we have:

$$\dot{e}_s(t) = Fe_s(t)+Ge_s(t-d(t))+ \\ (A-F-L_1C-L_2CA)x(t)(A_d-G-L_2CA_d-L_3C)x(t-d(t))+ \\ ((I-L_2C)B)u(t-h(t))+L_1\tilde{f}_s+L_2\dot{\tilde{f}}_s+L_3\tilde{f}_s(t-d(t)) \quad (5)$$

assuming:

$$A-F = L_1C+L_2CA, \\ A_d-G = L_2CA_d+L_3C, \\ (I-L_2C)B \quad (6)$$

and substituting Eq. 5 and 6 we will have:

$$\dot{e}_s(t) = Fe_s(t)+Ge_s(t-d(t)))+L_1\tilde{f}_s+L_2\dot{\tilde{f}}_s+L_3\tilde{f}_s(t-d(t)) \quad (7)$$

For convergence of states of observer to states of NCS we should have $e_s(t)\to 0$ and $\tilde{f}(t)\to 0$.
From Eq. 7 it easy to find that if the following systems are stable, system Eq. 7 is also stable and observer error will be zero:

$$\dot{e}_s(t) = Fe_s(t)+Ge_s(t-d(t))) \quad (8)$$

$$\dot{\tilde{f}}_s = -L_2^+L_1\tilde{f}_s-L_2^+L_3\tilde{f}_s(t-d(t)) \quad (9)$$

Hene in the sequel we analysis stability of systems Eq. 8 and 9 separatly. At first stability analysis of system Eq. 8 is introduced. For this aim we select the following Lyapunov-Krasovskii functional:

$$V_1 = V_{11}+V_{12}+V_{13}+V_{14}+V_{15}+V_{16}+V_{17} \quad (10)$$

With:

$$V_{11} = 1/2e_s(t)^T P_1e_s(t) \\ V_{12} = \int_{t-d(t)}^{t} e^{\alpha_1(s-t)}e_s^T(s)Q_1e_s(s)ds \\ V_{13} = \int_{t-d(t)}^{t} e^{\alpha_1(s-t)}e_s^T(s)W_1e_s(s)ds \\ V_{14} = \int_{t-d(t)}^{t} e^{\alpha_1(s-t)}e_s^T(s)R_1e_s(s)ds \\ V_{15} = \int_{-d_2}^{0}\int_{t-\theta}^{t} e^{\alpha_1(s-t)^T}\dot{e}_s(s)Z_1\dot{e}_s(s)dsd\theta \\ V_{16} = \int_{t-d(t)}^{0}\int_{t+\theta}^{t} e^{\alpha_1(s-t)}\dot{e}_s^T(s)S_1\dot{e}_s(s)dsd\theta \\ V_{17} = \int_{t-d_1}^{0}\int_{t+\theta}^{t} e^{\alpha_1(s-t)}\dot{e}_s^T(s)T_1\dot{e}_s(s)dsd\theta$$

Now, the time-derivative of V_1 is computes:

$$\dot{V}_{11} = 1/2e_s^T(t)P_1Fe_s(t)+1/2e_s^T(t)P_1Ge_s(t-d(t))+ \\ 1/2e_s^T(t)F^TP_1e_s(t)+1/2e_s^T(t-d(t))G^TP_1e_s(t) \quad (11)$$

$$\dot{V}_{12} = e_s^T(t)Q_1e_s(t)-e^{-\alpha_1d(t)}(t-\tau)e_s^T(t-d(t))Q_1e_s(t-d(t))- \\ \alpha_1V_{12} \geq e_s^T(t)Q_1e_s(t)-e^{-\alpha_1d_1}(1-\tau)e_s^T(t-d(t))Q_1e_s(t-d(t))-\alpha_1V_{12} \quad (12)$$

$$\dot{V}_{13} = e_s^T(t)W_1e_s(t)-e^{-\alpha_1d_1}(1-\tau)e_s^T(t-d_1)W_1e_s(t-d_1)-\alpha_1V_{13} \quad (13)$$

$$\dot{V}_{14} = e_s^T(t)R_1e_s(t)-e^{-\alpha_1d_2}(1-\tau)e_s^T(t-d_2)R_1e_s(t-d_2)-\alpha_1V_{14} \quad (14)$$

$$\dot{V}_{15} \leq d_2\dot{e}_s^T(t)Z_1\dot{e}_s(t)-\int_{t-d_2}^{t} e^{\alpha_1d_2}\dot{e}_s^T(s)Z_1\dot{e}_s(s)ds-\alpha_1V_{15} \quad (15)$$

$$\dot{V}_{16} \leq d_2\dot{e}_s^T(t)S_1\dot{e}_s(t)-\int_{t-d(t)}^{t} e^{\alpha_1d_2}\dot{e}_s^T(s)S_1\dot{e}_s(s)ds-\alpha_1V_{16} \quad (16)$$

$$\dot{V}_{17} \leq d_2\dot{e}_s^T(t)T_1\dot{e}_s(t)-\int_{t-d_1}^{t} e^{\alpha_1d_1}\dot{e}_s^T(s)T_1\dot{e}_s(s)ds-\alpha_1V_{17} \quad (17)$$

So:

$$e_s^T(t)(1/2G^TP_1+1/2P_1G)e_s(t-d(t))- \\ e_s^T(t-d(t))e^{-\alpha_1d_2}(1-\tau)Q_1e_s(t-d_1(t))-e^{-\alpha_1d_2}e_s^T(t-d_2)R_1e_s(t-d_2)- \\ e^{-\alpha_1d_1}e_s^T(t-d_1)W_1e_s(t-d_1)+\dot{e}_s^T(s)(d_1T_1+d_2(S_1+Z_1))\dot{e}_s(s)- \\ \int_{t-d_2}^{t} e^{\alpha_1d_2}\dot{e}_s^T(s)Z_1\dot{e}_s(s)ds-\int_{t-d(t)}^{t} e^{\alpha_1d_2}\dot{e}_s^T(s)S_1\dot{e}_s(s)ds- \\ \int_{t-d_1}^{t} e^{\alpha_1d_1}\dot{e}_s^T(s)T_1\dot{e}_s(s)ds \quad (18)$$

Now, we assume $\aleph$ = [e_s (t)e_s (t-d(t)) e_s (t-d_1) e_s (t-d_2)^T], using lemma 1, defining: $H_1 = [M_1\ 0\ \ 0\ M_4]^T$, $L_1[M_1\ M_2\ 0\ 0]^T$, $N_1 = [M_1\ 0\ M_3\ 0]^T$. And applying shur complement if:

$$\begin{bmatrix} \Xi_1 & d_2H_1 & d_2L_1 & d_1N_1 & A_c^T(d_1T_1+d_2(S_1+Z_1)) \\ * & -e^{-\alpha_1d_2}Z_1 & 0 & 0 & 0 \\ * & * & -e^{-\alpha_1d_2}S_1 & 0 & 0 \\ * & * & * & -e^{-\alpha_1d_1}T_1 & 0 \\ * & * & * & * & -(d_1T_1+d_2(S_1+Z_1)) \end{bmatrix} < 0 \quad (19)$$

with:

$$\Xi_1 = \begin{bmatrix} \Xi_{11} & 1/2P_1G-M_1^T+M_2 & -M_1^T+M_3 & -M_1^T+M_4 \\ * & -(1-\tau)e^{-\alpha_1d_2}Q_1-M_2^T-M_2 & 0 & 0 \\ * & * & -e^{-\alpha_1d_1}W_1-M_3^T-M_3 & 0 \\ * & * & * & -e^{-\alpha_1d_2}R_1-M_4^T-M_4 \end{bmatrix}$$

with:

$$f(x, t) = \lfloor 1/x_1 \quad \tanh(0.5x_1)+0.04e^{-0.1}t \rfloor$$

we will have:

$$\dot{V}_1+\alpha_1V_1<0 \quad (20)$$

Now for stability analysis os system Eq. 8 the filliwing Lyaonov-Krasofski functional is selected:

$$V_2 = V_1\left(\alpha_2, \tilde{f}\right) \tag{21}$$

$$\begin{bmatrix} \Xi_1 & d_2H_1+ & d_2L_1 & d_1N_1 & A_c^T\left(d_1T_1+d_2\left(S_1+Z_1\right)\right) \\ * & -e^{-\alpha_1 d_2}Z_1 & 0 & 0 & 0 \\ * & * & -e^{-\alpha_1 d_2}S_1 & 0 & 0 \\ * & * & * & -e^{-\alpha_1 d_2}T_1 & 0 \\ * & * & * & * & -\left(d_1T_1+d_2\left(S_1+Z_1\right)\right) \end{bmatrix} < 0 \tag{22}$$

where:

$$\Xi_1 = \begin{bmatrix} \Xi_{11} & 1/2P_1G-M_1^T+M_2 & -M_1^T+M_3 & -M_1^T+M_4 \\ * & \begin{matrix}-(1-\tau)e^{-\alpha_1 d_2}Q_1 \\ -M_2^T-M_2\end{matrix} & 0 & 0 \\ * & * & -e^{-\alpha_1 d_1}W_1-M_3^T-M_3 & 0 \\ * & * & * & \begin{matrix}-e^{-\alpha_1 d_2}R_1- \\ M_4^T-M_4\end{matrix} \end{bmatrix}$$

with:

$$\Xi_{11} = 1/2P_1-L_2^+L_1+1/2\left(L_2^+L_1\right)^T P_1+\alpha_1P_1+Q_1+R_1+ W_1+3M_1^T+3M_1,\ A_c = \left[L_2^+L_1E-L_2^+L_3 \quad 0 \quad 0\right]$$

$$\dot{V}_2 + \alpha_2 V_2 < 0 \tag{23}$$

Theorem 1: Exponential convergence of states of observer to states of NCS Eq. 1 with the proposed observer Eq. 3 is achieved if conditions in Eq. 6 are satisfied and also there exist positive definite matrices P_1, Q_1, R_1, W_1, Z_1, S_1, T_1 and matrices H_1, L_1, N_1 such that LMIs Eq. 23 and 26 to be feasible.

Remark 3: It should be noticed, from Eq. 7 it is easy to find that in order to state estimation error $\tilde{x}(t)$ reach to zero, at first sensor attack estimation error $\tilde{f}(t)$ should be zero. This means exponential rates α_1,α_2 shall be selected such that $\alpha_1<\alpha_2$.

Observer-based resilient control design: In this step we want to reach resilience for NCS Eq. 1 against cyber-attack to sensor (Fig. 2) by our proposed observer in Eq. 3. For this aim and based on Remark 1 we propose the following sampled data controller:

$$u(t) = K\hat{x}\left(t-h(t)\right) \tag{24}$$

where $K \in R^{p\times n}$ is the gain of controller.

Remark 4: It should be noticed, because delay in transmission of data from sensor to controller and among

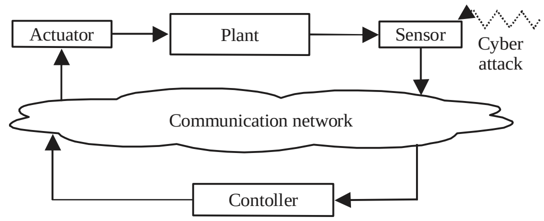

Fig. 2: Schematic of cyber-attack to sensor in NCS

sensors can be different in this work such problem has been considered. Hence, in this work we deal with a multiple-time-varying delay problem. It should be noticed based on Eq. 4 if LMI in Eq. 26 is satisfied we will have:

$$\begin{aligned}\dot{\hat{x}}(t) &= \left(F+L_1C+L_2CA\right)\hat{x}(t)+ \\ &\left(G+L_2CA_d+L_3C\right)\hat{x}\left(t-d(t)\right)+L_2CBu(t)\end{aligned} \tag{25}$$

applying controller in Eq. 28-29 the following closed loop system for states of observer is obtained:

$$\begin{aligned}\dot{\hat{x}}(t) &= \left(F+L_1C+L_2CA\right)\hat{x}(t)+ \\ &\left(G+L_2CA_d+L_3C\right)\hat{x}\left(t-d(t)\right)+L_2CBK\hat{x}\left(t-h(t)\right)\end{aligned} \tag{26}$$

For the resilient analysis of system Eq. 30 the following Lyapunov-Krasovskii functional is selected:

$$V_3 = V_{31}+V_{32}+V_{33}+V_{34}+V_{35}+V_{36}+V_{37} \tag{27}$$

with:

$$V_{31} = 1/2\hat{x}(t)^T P_3\hat{x}(t)$$

$$V_{32} = \int_{t-d(t)}^{t} e^{\alpha_3(s-t)}\hat{x}^T(s)Q_{3d}\hat{x}(s)ds+\int_{t-h(t)}^{t} e^{\alpha_3(s-t)}\hat{x}^T(s)Q_{2h}\hat{x}(s)ds$$

$$V_{33} = \int_{t-d_2}^{t} e^{\alpha_3(s-t)}\hat{x}^T(s)R_{3d}\hat{x}(s)ds+\int_{t-h_2}^{t} e^{\alpha_3(s-t)}\hat{x}^T(s)R_{3h}\hat{x}(s)ds$$

$$V_{34} = \int_{t-d_1}^{t} e^{\alpha_3(s-t)}\hat{x}^T(s)W_{3d}\hat{x}(s)ds+\int_{t-h_1}^{t} e^{\alpha_3(s-t)}\hat{x}^T(s)W_{2h}\hat{x}(s)ds$$

$$V_{35} = \int_{-d_2}^{t}\int_{t+\theta}^{t} e^{\alpha_3(s-t)}\dot{\hat{x}}^T(s)Z_{3h}\dot{\hat{x}}(s)dsd\theta+$$

$$\int_{-h_2}^{t}\int_{t+\theta}^{t} e^{\alpha_3(s-t)}\dot{\hat{x}}^T(s)Z_{3h}\dot{\hat{x}}(s)dsd\theta$$

$$V_{36} = \int_{t-d(t)}^{t}\int_{t+\theta}^{t} e^{\alpha_3(s-t)}\dot{\hat{x}}^T(s)S_{3h}\dot{\hat{x}}(s)dsd\theta+$$

$$\int_{t-h(t)}^{t}\int_{t+\theta}^{t} e^{\alpha_3(s-t)}\dot{\hat{x}}^T(s)S_{3h}\dot{\hat{x}}(s)dsd\theta$$

$$V_{37} = \int_{t-d_1}^{t}\int_{t+\theta}^{t} e^{\alpha_3(s-t)}\dot{\hat{x}}^T(s)T_{3h}\dot{\hat{x}}(s)dsd\theta+$$

$$\int_{t-h_1}^{t}\int_{t+\theta}^{t} e^{\alpha_3(s-t)}\dot{\hat{x}}^T(s)T_{3h}\dot{\hat{x}}(s)dsd\theta$$

now the time-derivative of V_3 is computed:

$$\begin{aligned}&\dot{V}_{31} = 1/2\hat{x}^T(t)P_3(F+L_1C+L_2CA)\hat{x}(t)+\\&1/2\hat{x}^T(t)P_3(G+L_2CA_d+L_3C)\hat{x}(t-d(t))+\\&1/2\hat{x}^T(t)(F+L_1C+L_2CA)^T P_3)\hat{x}(t)+\\&1/2\hat{x}^T(t-d(t))\left(L\otimes(G+L_2CA_d+L_3C)^T P_3\right)\hat{x}(t)+\\&\hat{x}^T(t)P_2L_2CBK\hat{x}(t-h(t))-\hat{x}^T(t-d(t))e^{-\alpha_3 d_2}(1-\tau)Q_{3d}\hat{x}(t-d(t))-\\&\hat{x}^T(t)P_2L_2CBK\hat{x}(t-h(t))\end{aligned} \qquad (28)$$

similar to Eq. 11-17 and 32:

$$\begin{aligned}&\dot{V}_3+\alpha_3V_3 \le 1/2\hat{x}^T(t)P_3(F+L_1C+L_2CA)\hat{x}(t)+\\&1/2\hat{x}^T(t)P_3(G+L_2CA_d+L_3C)\hat{x}(t-d(t))+\\&1/2\hat{x}^T(t)(F+L_1C+L_2CA)^T P_3)\hat{x}(t)+\\&1/2\hat{x}^T(t-d(t))\left(L\otimes(G+L_2CA_d+L_3C)^T P_3\right)\hat{x}(t)+\\&\hat{x}^T(t)P_2L_2CBK\hat{x}(t-h(t))-\\&\hat{x}^T(t-d(t))e^{-\alpha_3 d_2}(1-\tau)Q_{3d}\hat{x}(t-d(t))-\\&\hat{x}^T(t)P_2L_2CBK\hat{x}(t-h(t))-\\&\hat{x}^T(t-d(t))e^{-\alpha_3 h_2}(1-\tau)Q_{3h}\hat{x}(t-d(t))-\\&\hat{x}^T(t-d(t))e^{-\alpha_3 h_2}(1-\upsilon)Q_{3h}\hat{x}(t-d(t))\\&-e^{-\alpha_3 d_2}\hat{x}^T(t-d_2)R_{3d}\hat{x}(t-d_2)-e^{-\alpha_3 h_2}\hat{x}^T(t-h_2)R_{3h}\hat{x}(t-h_2)-\\&e^{-\alpha_3 d_1}\hat{x}^T(t-d_1)W_{3d}\hat{x}(t-d_1)-e^{-\alpha_3 h_1}\hat{x}^T(t-h_1)W_{3h}\overline{\xi}(t-h_1)-\\&\dot{\hat{x}}^T(s)\left(d_1T_{3d}+d_2(S_{3d}+Z_{3d})\right)\dot{\hat{x}}(s)+\\&\dot{\hat{x}}^T(s)\left(h_1T_{3h}+h_2(S_{3h}+Z_{3h})\right)\dot{\hat{x}}(s)-\\&\int_{t-d_2}^{t}e^{-\alpha_3 d_2}\dot{\hat{x}}^T(s)Z_{3d}\dot{\hat{x}}(s)ds-\int_{t-h_2}^{t}e^{-\alpha_3 d_2}\dot{\hat{x}}^T(s)Z_{3h}\dot{\hat{x}}(s)ds-\\&\int_{t-d(t)}^{t}e^{-\alpha_3 d_2}\dot{\hat{x}}^T(s)S_{3d}\dot{\hat{x}}(s)ds-\int_{t-h(t)}^{t}e^{-\alpha_3 d_2}\dot{\hat{x}}^T(s)S_{3h}\dot{\hat{x}}(s)ds-\\&\int_{t-d_1}^{t}e^{-\alpha_3 d_1}\dot{\hat{x}}^T(s)T_{3d}\dot{\hat{x}}(s)ds-\int_{t-h_1}^{t}e^{-\alpha_3 d_1}\dot{\hat{x}}^T(s)T_{3h}\dot{\hat{x}}(s)ds\end{aligned} \qquad (29)$$

assuming

$$\eta = \left[\hat{x}(t)\hat{x}(t-d(t))\hat{x}(t-d_1)\hat{x}(t-d_2)\hat{x}(t-h(t))\hat{x}(t-h_1)\hat{x}(t-h_2)\right]^T$$

using Lemma 1 and defining:

$$\begin{aligned}&H_{3d} = [M_{31}\ 0\ 0\ M_{34}\ \ 0\ 0\ 0]^T,\ L_{3d} =\\&[M_{31}\ \ M_{32}\ 0\ 0\ 0\ 0\ 0]^T,\ N_{3d} = [M_{31}\ 0\ M_{33}\ 0\ 0\ 00]^T\\&H_{3h} = [M_{31}\ 0\ 0\ 0\ 0\ 0\ \ M_{37}]^T,\ L_{3h} =\\&[M_{31}\ 0\ 0\ 0\ \ M_{35}\ 0\ \ 0]^T,\ N_{3h} = [M_{31}\ 0\ 0\ 0\ 0\ \ M_{36}\ \ 0]^T\end{aligned}$$

applying schur complement the inequality in Eq. 29 is equal to:

$$\begin{bmatrix}\Xi_3 & d_2H_{3d} & d_2L_{3d} & d_1N_{3d} & \hat{A}_{cd}^T\left(d_1T_{3d}+d_2(S_{3d}+Z_{3d})\right) & h_2H_{3h} & h_2L_{3h} & h_1N_{3h} & \hat{A}_{ch}^T\left(h_1T_{3h}+h_2(S_{3h}+Z_{3h})\right)\\ * & -e^{-\alpha_3 d_2}Z_{3d} & 0 & 0 & 0 & 0 & 0 & 0 & 0\\ * & * & -e^{-\alpha_3 d_2}S_{3d} & 0 & 0 & 0 & 0 & 0 & 0\\ * & * & * & -e^{-\alpha_3 d_1}T_{3d} & 0 & 0 & 0 & 0 & 0\\ * & * & * & * & -\left(d_1T_{3d}+d_2(S_{3d}+Z_{3d})\right) & 0 & 0 & 0 & 0\\ * & * & * & * & * & -e^{-\alpha_3 h_2}Z_{3h} & 0 & 0 & 0\\ * & * & * & * & * & * & -e^{-\alpha_3 h_2}S_{3h} & 0 & 0\\ * & * & * & * & * & * & * & -e^{-\alpha_3 h_1}T_{3h} & 0\\ * & * & * & * & * & * & * & * & -\left(h_1T_{3d}+h_2(S_{3h}+Z_{3h})\right)\end{bmatrix}<0 \qquad (30)$$

where:

$$\Xi_3 = \begin{bmatrix}\Xi_{31} & \Xi_{32} & -M_{31}^T+M_{33} & -M_{31}^T+M_{34} & -M_{31}^T+M_{35} & -M_{31}^T+M_{36} & -M_{31}^T+M_{37}\\ * & \Xi_{33} & 0 & 0 & 0 & 0 & 0\\ * & * & \Xi_{34} & 0 & 0 & 0 & 0\\ * & * & * & \Xi_{35} & 0 & 0 & 0\\ * & * & * & * & \Xi_{36} & 0 & 0\\ * & * & * & * & * & \Xi_{37} & 0\\ * & * & * & * & * & * & \Xi_{38}\end{bmatrix}$$

$$\begin{aligned}&\Xi_{31} = 1/2P_3(F+L_1C+L_2CA)+1/2(F+L_1C+L_2CA)^T P_3+\\&\alpha_3P_3+Q_{3d}+R_{3d}+W_{3h}+6M_{31},\ \hat{A}_{cd} = \begin{bmatrix}F+L_1C+L_2CA\ G+L_2CA_d+\\ L_3C\ \ 0\ \ 0\ \ 0\ \ 0\ \ 0\end{bmatrix},\\&\hat{A}_{ch} = [F+L_1C+L_2CA\ \ 0\ \ 0\ \ 0\ \ L_2CBK\ \ 0\ \ 0]\\&\Xi_{32} = 1/2P_3(G+L_2CA_d+L_3C)-M_{31}^T+M_{32},\ \Xi_{33} = -\\&(1-\tau)-e^{-\alpha_3 d_2}Q_{3d}-M_{32}^T-M_{32},\ \Xi_{34} = -e^{-\alpha_3 d_1}W_{3d}-M_{33}^T-M_{33}\\&\Xi_{35} = -e^{-\alpha_3 d_2}R_{3d}-M_{34}^T-M_{34},\ \Xi_{36} = -(1-\upsilon)e^{-\alpha_3 h2}Q_{3h}-\\&M_{35}^T-M_{35},\ \Xi_{37} = -e^{-\alpha_3 d_1}W_{3h}-M_{36}^T-M_{36},\ \Xi_{38} = -e^{-\alpha_3 h_2}R_{3h}-M_{37}^T-M_{37}\end{aligned}$$

hence, if Eq. 35 is satisfied, we will have:

$$\dot{V}_3+\alpha_3V_3<0 \qquad (31)$$

Theorem 2: Exponential resilience in NCS Eq. 1 with observer Eq. 3 and control input Eq. 24 is achieved if conditions of theorem 1 are satisfied and there is P_3, Q_{3d},

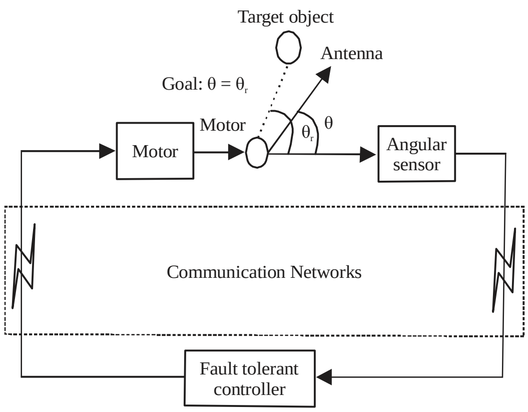

Fig. 3: The angular positioning system

R_{3d}, W_{3d}, Z_{3d}, S_{3d}, T_{3d}, Q_{3h}, R_{3h}, W_{3h}, Z_{3h}, S_{3h}, T_{3h},>0 and matrices H_{3d}, L_{3d}, N_{3d}, H_{3h}, L_{3h}, N_{3h} such that LMI in Eq. 30 to be feasible.

Remark 5: It should be noticed, from Eq. 7 it is easy to find that in order to dynamic of observer satisfies Eq. 29 at first sensor attack estimation error $\tilde{f}(t)$ should be zero. This means exponential rates α_2 shall be selected such that $\alpha_3<\alpha_2$.

Remark 6: By comparison and with respect to results by Sakthivel *et al*.[17], Tian *et al*.[19], Feng and Tesi[20] and Sun and Ma[21], the presented work has extra issues as follows:

By Sakthivel *et al*.[17] assumed dynamic for sensor attacker are belong 2-norm space. By Tian *et al*.[19], it was assumed communication link between controller and sensors is unreliable and limited such attack only as communication delay. By Feng and Tesi[20] sensor attack was bounded by a positive integer. By Sun and Ma[21] attack model to sensor was white noise. This means in these works in order to solve their problems, they impose constraints on the dynamic of attack. On the other hand, as per previously mentioned, because cyber-attacks are unpredictable, one of the active problems in this field is modeling of false data injected by attacker such that the considered model covers a numerous unpredictable attack in real world applications. Hence, in this work there is no any constraint on the dynamic of false data of attacker and for solving problem only some matrix inequalities need to be feasible. Considering delayed states in the model of NCS that results multiple-time-varying problem in NCS. Such assumption is more general than results in the mentioned articles.

Numerical simulation

Example: In this study to illustrate the effectiveness of the obtained approach, a classical angular positioning system offered is considered as (Fig. 3). This system consists of a rotating antenna at the origin of the plane and antenna is driven by an electric motor. Assuming:

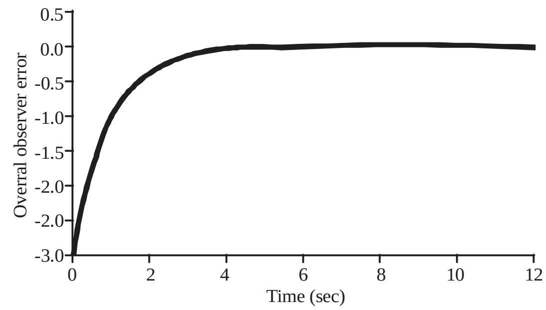

Fig. 4: Estimation error in NCS (32) with observer (3)

- θ Angular position of antenna
- θ Velocity of antenna model of system can be presented as the following NCS:

$$\dot{x}(t) = Ax(t)+A_d x(t\text{-}d(t))+Bu(t),\ y = Cx(t)\ x = \begin{bmatrix}\theta\\ \theta\end{bmatrix},\ A = \begin{bmatrix}1 & 0.1\\ 0 & 0.99\end{bmatrix},\ A_d = \begin{bmatrix}0 & 0.001\\ 0.001 & 0\end{bmatrix},\ B = \begin{bmatrix}-0.0787 & 0\\ 0 & 0.0787\end{bmatrix},\ C = [1\ 0] \tag{32}$$

we assume delay of NCS as:

$$d(t) = h(t) = 0.03|\sin(t)$$

also, it is assumed there is cyber-attack to sensor such that attacker send the following false data to sensor:

$$f(x,\ t) = \lfloor 1/x_1\ \tanh(0.5x_1)+0.04e^{-0.1}t \rfloor$$

In order to control system in such condition we want to use our obtained results in theorems 1 and 2. At first to estimate the states of NCS Eq. 32 we can use our obtained result in Theorem 1. Results of simulation of observer error:

$$\sum_{i=1}^{2}\left(x_i(t)\text{-}\hat{x}_i(t)\right)$$

(Fig. 4) show that observer states reach to states of NCS. Also to achieve resilient control in such conditions, we can use our obtained result in theorem 2. Applying Matlab LMI Toolbox for solving the matrix inequality in Eq. 30, the gain of controller Eq. 24 for satisfying theorem 2 is:

$$K = \begin{bmatrix}3.1 & -0.01\\ -0.01 & -3.1\end{bmatrix}$$

Results of simulation of states of NCS Fig. 5 shows that we could reach to resilience for NCS (32).

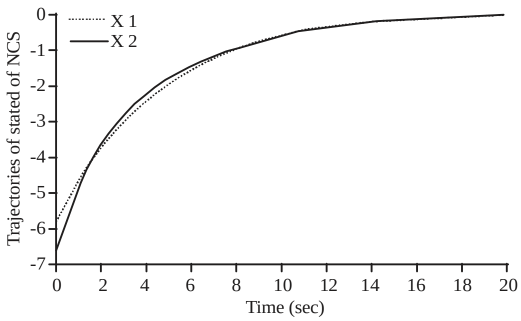

Fig. 5: Trajectories of states in the controlled system (32)

CONCLUSION

This research proposed novel observer-based resilient control for networked control systems (NCS) against cyber-attacks to sensor. To achieve resilience in such conditions, at first a novel observer was proposed in order to estimate the states of system.

Then a novel observer based controller was proposed in order to NCS in conditions of attack remains stable. Applying Lyapunov-Krasovskii functional method, delay dependent resilient criterion was established to show the exponential behavior of system in such conditions. Finally, for evaluating results, a practical example has been solved.

REFERENCES

01. Heemels, W.P.M.H. and N. Van De Wouw, 2010. Stability and Stabilization of Networked Control Systems. In: Networked Control Systems, Bemporad A., M. Heemels and M. Johansson (Eds.). Springer, London, UK., pp: 203-253.
02. Zhang, D., P. Shi, Q.G. Wang and L. Yu, 2017. Analysis and synthesis of networked control systems: A survey of recent advances and challenges. ISA Trans., 66: 376-392.
03. Murray, R.M., 2003. Future directions in control, dynamics and systems: Overview, grand challenges and new courses. Eur. J. Control, 9: 144-158.
04. Zhang, L., H. Gao and O. Kaynak, 2012. Network-induced constraints in networked control systems-a survey. IEEE. Trans. Ind. Inf., 9: 403-416.
05. Antsaklis, P. and J. Baillieul, 2004. Guest editorial special issue on networked control systems. IEEE Trans. Autom. Control, 49: 1421-1423.
06. Gupta, R.A. and M.Y. Chow, 2010. Networked control system: Overview and research trends. IEEE Trans. Ind. Electron., 57: 2527-2535.
07. Hu, L.S., T. Bai, P. Shi and Z. Wu, 2007. Sampled-data control of networked linear control systems. Automatica, 43: 903-911.
08. Chen, G., J. Xia, G. Zhuang and J. Zhao, 2017. Improved delay-dependent stabilization for a class of networked control systems with nonlinear perturbations and two delay components. Applied Math. Comput., 316: 1-17.
09. Zhang, R., D. Zeng, X. Liu, S. Zhong and Q. Zhong, 2018. Improved results on state feedback stabilization for a networked control system with additive time-varying delay components controller. ISA Trans., 75: 1-14.
10. Li, M., J. Zhao, J. Xia, G. Zhuang and W. Zhang, 2018. Extended dissipative analysis and synthesis for network control systems with an event-triggered scheme. Neurocomputing, 312: 34-40.
11. Zhang, J., J. Lam and Y. Xia, 2014. Output feedback delay compensation control for networked control systems with random delays. Inf. Sci., 265: 154-166.
12. Zhang, J ., Y. Lin and P. Shi, 2015. Output tracking control of networked control systems via delay compensation controllers. Automatica, 57: 85-92.
13. Sandberg, H., S. Amin and K.H. Johansson, 2015. Cyberphysical security in networked control systems: An introduction to the issue. IEEE. Control Syst. Mag., 35: 20-23.
14. Amin, S., A.A. Cardenas and S.S. Sastry, 2009. Safe and secure networked control systems under denial-of-service attacks. Proceedings of the International Workshop on Hybrid Systems: Computation and Control, April 13-15, 2009, Springer, Berlin, Germany, pp: 31-45.
15. Liu, S., P.X. Liu and A. El Saddik, 2014. A stochastic game approach to the security issue of networked control systems under jamming attacks. J. Franklin Inst., 351: 4570-4583.
16. Sun, H., C. Peng, T. Yang, H. Zhang and W. He, 2017. Resilient control of networked control systems with stochastic denial of service attacks. Neurocomputing, 270: 170-177.
17. Sakthivel, R., S. Santra and B. Kaviarasan, 2018. Resilient sampled-data control design for singular networked systems with random missing data. J. Franklin Inst., 355: 1040-1072.
18. Tan, C., L. Li and H. Zhang, 2015. Stabilization of networked control systems with both network-induced delay and packet dropout. Automatica, 59: 194-199.
19. Tian, E., D. Yue and C. Peng, 2010. Reliable control for networked control systems with probabilistic sensors and actuators faults. IET Control Theor. Appl., 4: 1478-1488.
20. Feng, S. and P. Tesi, 2017. Networked control systems under denial-of-service: Co-located vs. Remote architectures. Syst. Control Lett., 108: 40-47.

21. Sun, S. and J. Ma, 2014. Linear estimation for networked control systems with random transmission delays and packet dropouts. Inf. Sci., 269: 349-365.
22. Wang, W., D. Nešic and R. Postoyan, 2017. Observer design for networked control systems with FlexRay. Automatica, 82: 42-48.
23. Liu, L., X. Liu, C. Man and C. Xu, 2015. Delayed observer-based H8 control for networked control systems. Neurocomputing, 179: 101-109.
24. Wang, Y.L. and Q.L. Han, 2014. Modelling and observer-based H8 controller design for networked control systems. IET. Control Theor. Appl., 8: 1478-1486.
25. Sun, H., C. Peng, W. Zhang, T. Yang and Z. Wang, 2018. Security-based resilient event-triggered control of networked control systems under denial of service attacks. J. Franklin Inst., 356: 10277-10295.