Scientific Research Publishing

Intelligent Control and Automation, 2017, 8, 164-174
http://www.scirp.org/journal/ica
ISSN Online: 2153-0661
ISSN Print: 2153-0653

Generalized Attack Model for Networked Control Systems, Evaluation of Control Methods

Arman Sargolzaei[1*], Kang Yen[2], Mohamed Abdelghani[3], Alireza Abbaspour[2], Saman Sargolzaei[4]

[1]Department of Electrical Engineering, Florida Polytechnic University, Lakeland, FL, USA
[2]Department of Electrical and Computer Engineering, Florida International University, Miami, FL, USA
[3]Department of Mathematics and Statistical Sciences, University of Alberta, Edmonton, Canada
[4]Department of Neurosurgery, University of California Los Angeles, Los Angeles, CA, USA
Email: *a.sargolzaei@gmail.com

How to cite this paper: Sargolzaei, A., Yen, K., Abdelghani, M., Abbaspour, A. and Sargolzaei, S. (2017) Generalized Attack Model for Networked Control Systems, Evaluation of Control Methods. *Intelligent Control and Automation*, **8**, 164-174.
http://dx.doi.org/10.4236/ica.2017.83013

Received: June 15, 2017
Accepted: August 20, 2017
Published: August 23, 2017

Abstract

Networked Control Systems (NCSs) have been implemented in several different industries. The integration with advanced communication networks and computing techniques allows for the enhancement of efficiency of industrial control systems. Despite all the advantages that NCSs bring to industry, they remain at risk to a spectrum of physical and cyber-attacks. In this paper, we elaborate on security vulnerabilities of NCSs, and examine how these vulnerabilities may be exploited when attacks occur. A general model of NCS designed with three different controllers, *i.e.*, proportional-integral-derivative (PID) controllers, Model Predictive control (MPC) and Emotional Learning Controller (ELC) are studied. Then three different types of attacks are applied to evaluate the system performance. For the case study, a networked pacemaker system using the Zeeman nonlinear heart model (ZHM) as the plant combined with the above-mentioned controllers to test the system performance when under attacks. The results show that with Emotional Learning Controller (ELC), the pacemaker is able to track the ECG signal with high fidelity even under different attack scenarios.

Keywords

Security of Control Systems, Denial of Service (DoS) Attack, Time-Delay-Switch (TDS) Attack, False Data Injection (FDI) Attack

1. Introduction

Control systems have many applications in the industry. New revolution in system designs using the strategy of networked control systems (NCSs) has created security issues in industries, which has been an important challenge for many researchers. Security of NCSs plays an important role in the protection of industrial, and critical infrastructure. For example, energy and power sectors, transportation system sectors, water and wastewater system sectors, healthcare and public health sectors are some industries facing high probability of attacks. Although the security schemes for control systems have been developed in the past several years, there are still many acknowledged cyber-attacks. Some recent specific events further confirm that attacks would have happened in control systems in different industries [1]. Therefore, in recent years, security of NCS has been at the center stage for researchers, engineers, and governmental entities because exploited security risks could have cause potential catastrophic consequences [2].

Most of conventional methods in control systems design assume that the system operates in a normal condition without any attacks involved. In this case, any interference, delay, and attack to any part of a control system, such as sensors and communication links, can drive the system from the required performance or even worst to an unstable mode.

Many researchers have studied control systems under attacks. A class of False Data Injection (FDI) attacks bypassing the bad data detection in Supervisory Control and Data Acquisition (SCADA) systems was proposed by [3]. In [4], adversaries launched FDI attacks against state estimates of power systems, knowing only the perturbed model of the power system. Y. Mo *et al.*, studied FDI attacks on a control system equipped with Kalman filter [3]. Fault attacks have also been critical concerns in aviation industries, where a small attack or faults can damage system itself and human life [5]. Abbaspour *et al.* introduced a neural network (NN) fault detection design for detection of abrupt faults in actuators and sensor of the control systems. They used extended Kalman filter to improve the NN ability in detection of faults [6]. A neural observer approach for detection of FDI attack is introduced in [7]. In [8], the smallest set of adversary controlled meters was identified to perform an unobservable attack. Recently, Amin *et al.* considered Denial of Service (DoS) attacks on the communication channels in which the measurements telemetered in remote terminal units (RTUs) were sent to the control center of power systems [9]. They demonstrated that an adversary could make power systems unstable by properly designing DoS attack sequences. Liu *et al.* considered how a switched-DoS attack on a smart grid could affect the dynamic performance of its power systems [10]. The Viking projects [11] considered cyber-attacks to the Load Frequency Control (LFC), one of a few automatic control loops in power systems. They analyzed the impacts of cyber-attacks on the control centers of power systems, by using reachability methods. However, they only considered attacks on the control centers which are usually harder to attack than the communication channels in the sensing loop of a power system. And in the area of biomedical devices the issue of security of these devices has been increasingly critical because the development trend of these devices will connect them to other entities through both wired and wireless channels. It is therefore important to consider medical device security issues

[12].

The rest of this paper is organized as follows: Section 2 illustrates three different types of attacks to NCSs. Section 3 provides the needed information for the proposed case study. Section 4 presents the results of the numerical simulation conducted in this study. Finally, in Section 5, the conclusion and remarks are presented.

2. Types of Attacks on NCSs

Here a generalized model for an NCS under attach is shown in Figure 1.

This system is described concisely as an output feedback system having the form:

$$\begin{aligned} \dot{x} &= f(t, x, u) \\ y &= g(x) \end{aligned} \tag{1}$$

and

$$u = h(y) \tag{2}$$

where x is the plant state vector; y is the information communicated with the controller about the plant state; u is the control vector; f is a function describing the plant behavior; g describes the plant output and the communication methodology used, and h is a description of the controller.

An attack on the NCS involves altering any component of the system. A general attack can be described by a function that alters any of components of the system

$$\left(\tilde{f}, \tilde{g}, \tilde{h}, \tilde{x}, \tilde{y}, \tilde{u}, \tilde{t}\right) = \Lambda\left(f, g, h, x, y, u, t\right) \tag{3}$$

where $\left(\tilde{f}, \tilde{g}, \tilde{h}, \tilde{x}, \tilde{y}, \tilde{u}, \tilde{t}\right)$ are the corrupted functions and information as the result of an attack Λ.

Three most possible attacks on NCSs, especially on Networked Power Control System (NPCS) are given below:

a) Denial of Service (DoS)

This attack seeks to sabotage an NCS by overwhelming its communication and computational resources in order to prevent it from working [13]. The DoS

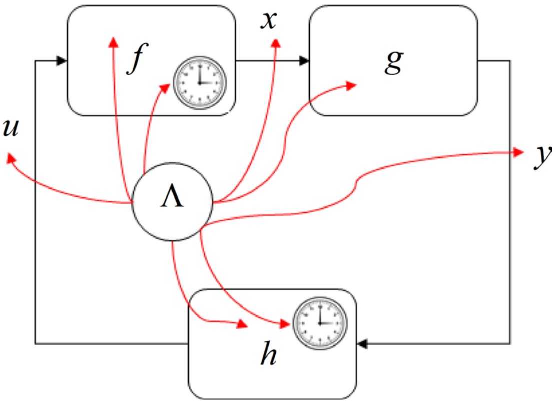

Figure 1. Generalized cyber attacks on a typical NCS.

attack can disconnect service or data from the plant to the controller, from the controller to the plant, or both at the same time. In our general model of attacks, this attack can be described as follows:

$$\tilde{y} = \begin{cases} y & \text{otherwise} \\ \alpha & \text{attack} \end{cases} \tag{4}$$

where α can be zero, or some random value.

b) Fault Analysis Attack

This class of attack injects faults into a device performing some computation. These faults can be caused by changing the environmental conditions, the injection of a laser beam at an appropriate frequency [14], or the injection of data packets that collide with legitimate packets [15]. The work of Yuan and Liu *et al.* has shown the load redistribution attack [16] [17] [18] which is a false data injection attack by modifying selected information in a Supervisory Control and Data Acquisition (SCADA) power system. This attack is especially dangerous due to its capabilities of being manipulating the estimation of system power flow. Depending on the attack is short term or long term, it can damage effects on the security-constrained economic dispatch (SCED) price estimation [17]. This attack can be modeled as follows:

$$\tilde{y} = \begin{cases} y & \text{otherwise} \\ z & \text{attack} \end{cases} \tag{5}$$

where z is an input signal designed by the attacker for the purpose of either misleading the control system, causing systems inefficiencies, or sabotaging it.

c) Time-Delay Switched Attack (TDS)

Time Delay Switched Attack (TDS) has been proposed to NCSs by Sargolzaei *et al.* who has shown that this type of attacks can destabilize NCSs [2]. In [19] authors has applied this attack on a networked nonlinear heartbeat system and proposed a controller that is more robust to TDS attacks. In [20] a time-delay-switch (TDS) attack has been used to introduce time delays in the dynamics of power systems. TDS attacks can cause devastating consequences on smart grids if no prevention measures are considered in the design of these power systems. TDS attacks can be modeled as delay of the output signals telemetered to the controller

$$\tilde{y} = \begin{cases} y & \text{otherwise} \\ y(t-\tau) & \text{attack} \end{cases} \tag{6}$$

or as an attack on the clocking and synchronization mechanisms in NCSs

$$\tilde{t} = \begin{cases} t & \text{otherwise} \\ t-\tau & \text{attack} \end{cases} \tag{7}$$

where τ is a random variable time-delay that is always less than time t.

3. Case Study

To evaluate the effectiveness of the performance of different controllers on the pacemakers influenced under DoS, FDI and TDS attacks, we need to have a ma-

Table 1. Parameters value.

Parameter	x_d	T	ε	x_s
value	1.024	1	0.2	−1.38

thematical model for the heartbeat. There are many researches in the area of heart signal and pacemakers [21] [22] which shows that its importance.

The 2nd-order heartbeat model is selected for the case study in this paper [19]. The model is described as follows:

$$\begin{bmatrix} \dot{x}_1(t) \\ \dot{x}_2(t) \end{bmatrix} = \begin{bmatrix} -\frac{1}{\varepsilon}\left\{x_1^3(t) - Tx_1(t) + x_2(t)\right\} \\ \left(x_1(t) - x_d\right) + \left(x_d - x_s\right)u(t) \end{bmatrix} \tag{8}$$

where x_1 and x_2 indicates the length of a muscle fiber and the state related to electrochemical activities respectively; x_d indicates a typical muscle fiber length when the heart is in the systolic state; x_s is an additional parameter representing a typical fiber length; ε is a small positive constant; T represents tension in the muscle fiber; and $u(t)$ is the cardiac pacemaker control that leads the heart into the diastolic and the systolic states. The parameters adopted are described in the table below [19] (Table 1).

Three different controllers are adopted to compare their performance. The optimal state feedback controller, the PID controller, and the ELCPID are given below:

$$u(t) = -K\tilde{x}_2(t) \tag{9}$$

$$u(t) = K_p e(t) + K_D \dot{e}(t) + K_I \int_0^t e(t) \tag{10}$$

$$u(t) = \left(G_A - G_{OC}\right) I_S \tag{11}$$

Here $\tilde{x}_2(t)$ represents anyone of the possible attack signals described in the Equations (5) to (7). The error signal is defined as $e(t) = r(t) - \tilde{x}_2(t)$. In the representation of ELCPID, I_S can be a PID controller and the controller parameters G_A and G_{OC} can be calculated as described in [19] [23].

4. Stability Analysis of the Nonlinear Heartbeat Model

Now we will discuss the stability of the 2nd-order nonlinear as given in (8). First, we consider the cardiac pacemaker control signal to be in the form of 0 and 1, which indicates the on-off control. If the control signal of the pacemaker, $u(t)$, in zero when $T = 1$, $\varepsilon = 0.2$, and $x_d = 0$, then the equilibrium point at point (0, 0) is not stable. This can be calculated by solving the following equation

$$\dot{\boldsymbol{x}} = \begin{bmatrix} -\frac{1}{\varepsilon}\left(x_1^3 - Tx_1 + x_2\right) \\ x_1 - x_d \end{bmatrix} = \begin{bmatrix} -5\left(x_1^3 - x_1 + x_2\right) \\ x_1 \end{bmatrix} = 0 \tag{12}$$

It can be shown that the equilibrium point for the system described in (12) is not stable. This conclusion can be confirmed by analyzing the stability of the equilibrium point using the Lyapunov indirect stability theorem. To do this, we calculate the Jocobian matrix $\boldsymbol{A}$, of (12) at the origin

$$\boldsymbol{A}=\begin{bmatrix}\frac{\partial \dot{x}_1}{\partial x_1} & \frac{\partial \dot{x}_1}{\partial x_2}\\ \frac{\partial \dot{x}_2}{\partial x_1} & \frac{\partial \dot{x}_2}{\partial x_2}\end{bmatrix}=\begin{bmatrix}-\frac{1}{\varepsilon}\left(3x_1^2-T\right) & -\frac{1}{\varepsilon}\\ 1 & 0\end{bmatrix} \tag{13}$$

The eigenvalues of $\boldsymbol{A}$ are

$$\begin{bmatrix}\lambda_1\\ \lambda_2\end{bmatrix}=\begin{bmatrix}\frac{1}{2\varepsilon}\left\{-\left(3x_1^2-T\right)+\sqrt{\left(3x_1^2-T\right)^2-4\varepsilon}\right\}\\ \frac{1}{2\varepsilon}\left\{-\left(3x_1^2-T\right)-\sqrt{\left(3x_1^2-T\right)^2-4\varepsilon}\right\}\end{bmatrix} \tag{14}$$

At the equilibrium point (0, 0), we obtain

$$\begin{bmatrix}\lambda_1\\ \lambda_2\end{bmatrix}=\begin{bmatrix}\frac{1}{2\varepsilon}\left\{T+\sqrt{T^2-4\varepsilon}\right\}\\ \frac{1}{2\varepsilon}\left\{T-\sqrt{T^2-4\varepsilon}\right\}\end{bmatrix}=\begin{bmatrix}\frac{1}{0.4}\left\{1+\sqrt{0.2}\right\}\\ \frac{1}{0.4}\left\{1-\sqrt{0.2}\right\}\end{bmatrix}$$

i.e., both eigenvalues are positive when $T = 1$ and $\varepsilon = 0.2$, which indicates that the system is not stable at the origin.

However, the system described in (12) is stable if the condition $3x_1^2-T>0$ is satisfied. So, this condition reaches if value of x_d is substituted by 1.024 based on literature [24]. For $x_d=1.024$ and $T = 1$, the equilibrium point is stable at (1.024, −0.0497) as shown in **Figure 2** which is the phase portrait with the new value of x_d. All the trajectories, regardless of their initial values, go to the diastolic equilibrium point shown by the cubic. Since the equilibrium point is stable, system stays at this point unless there is an external excitation that forces the system to a new equilibrium point.

Now, we consider the system described in (8) with $u(t) = 1$, $x_d = 1.024$, $x_s = -1.3804$, $T = 1$, and $\varepsilon = 0.2$. By setting with these parameter values we move the heart to the systolic state (**Figure 3**). Based on this study, the control signal will direct the heart from diastolic to systolic state and adversaries can disrupt this

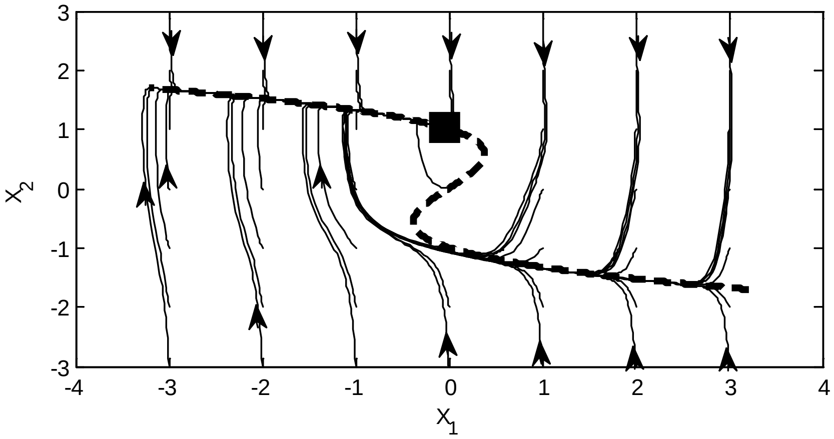

Figure 2. Phase portrait of Heartbeat model in diastolic state, the black cube shows the equilibrium point.

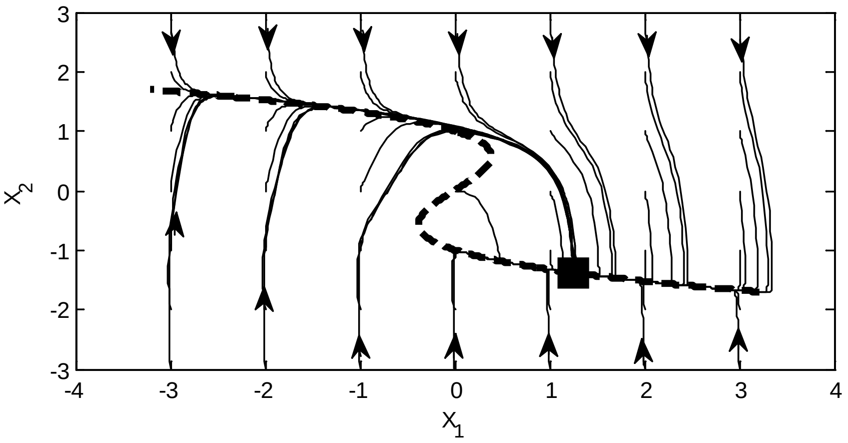

Figure 3. Phase portrait of heart model in systolic state, the cube denotes the equilibrium point.

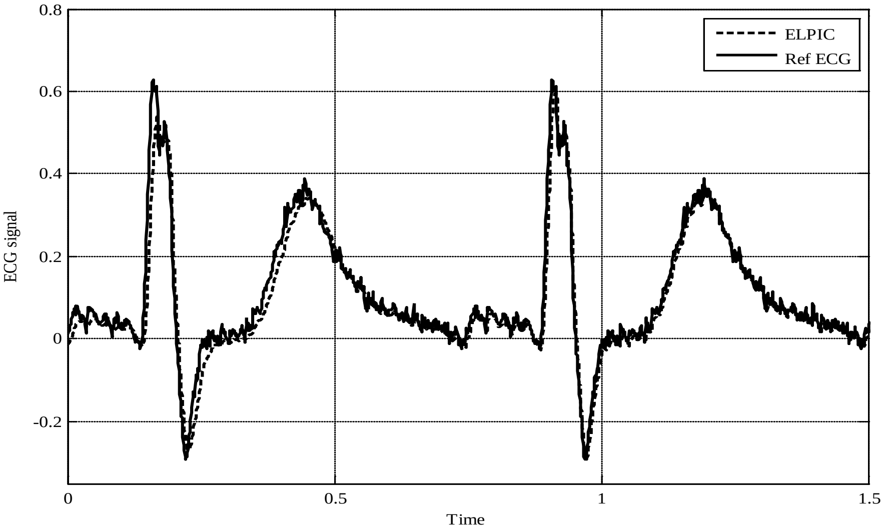

Figure 4. Simulation result of ECG tracking for 2nd order heartbeat model based on ELPIC pacemaker signal.

process by injecting attacks to the sensory and/or control signal.

Also the controllability and the observability are assumed for the heartbeat model based on literature [24].

5. Simulations and Results

The above mentioned 2nd-order heartbeat model using the Emotional Learning PI Control (ELPIC) technique has been simulated first to test whether this model can adequately represent the mechanism of heartbeat in the ECG signal generation. Figure 4 shows that the output from the model with ELPIC controller does accurately match that from the measurement. In the figure, the dashed line shows the output of the model controlled by the ELPIC technique and the solid line indicates the patient’s ECG signal which serves as the referenced signal [25]. More details about ELPIC technique can be found in [19].

Three different attacks, TDS attack, DoS attack and FDI attack, are applied to the Heartbeat model with different controllers. The controllers evaluated are the ELPIC, the classical PI, and the MPC adopted in MATLAB. To compare the performance of these three controllers to the above mentioned attacks, we apply the attacks to the model with different controllers in the time interval between t_s = 1.4 sec and t_f = 1.45 sec to check the corresponding responses. In the simulation, a time delay of τ = 0.01 sec is adopted in the TDS attack small random variables were injected to the model to simulate the FDI attack.

The results are shown in Figures 5-7. In all of the figures, the ECG signal and the signals from different controllers, ELPIC, MPC and PID, are represented by solid line, dashed line, dotted line and dash-dot line, respectively. The figures

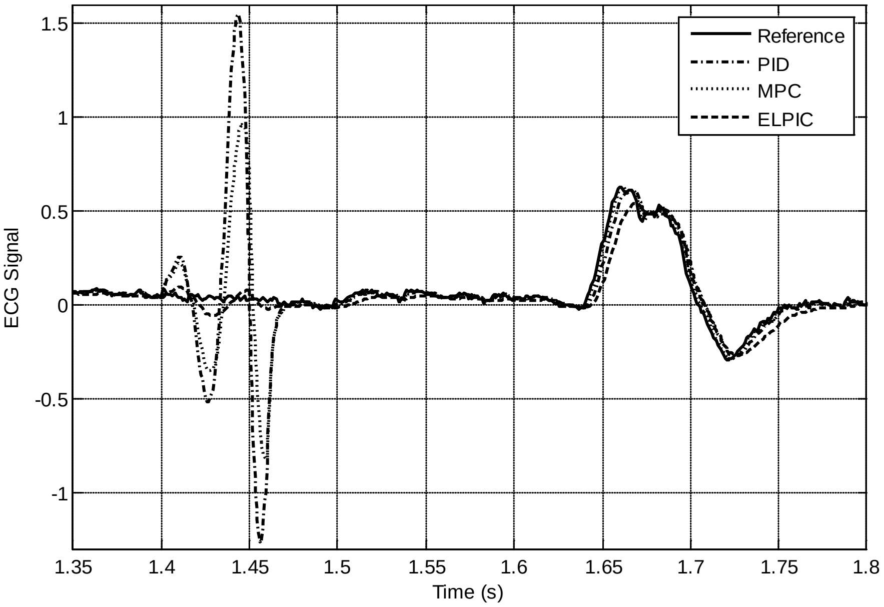

Figure 5. Effect of TDS attack.

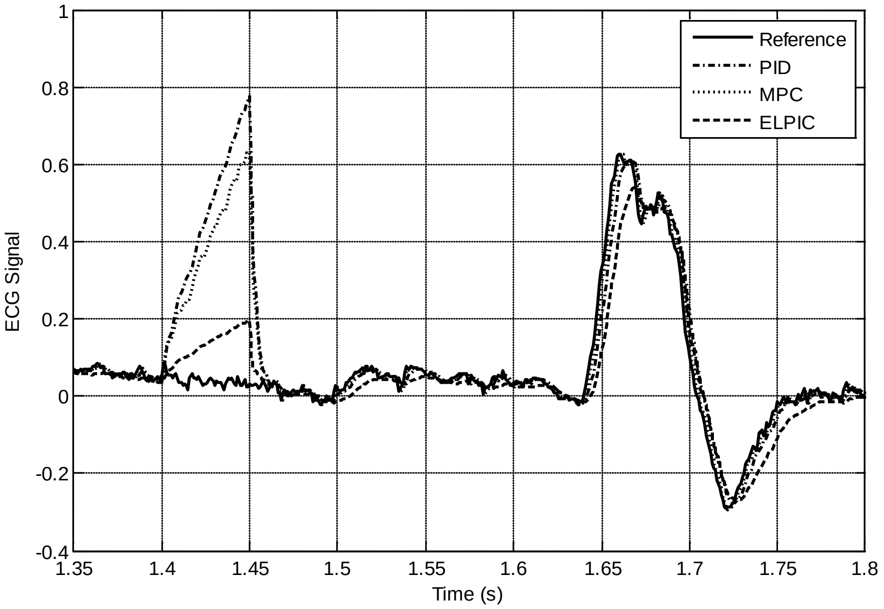

Figure 6. Effect of DoS attack.

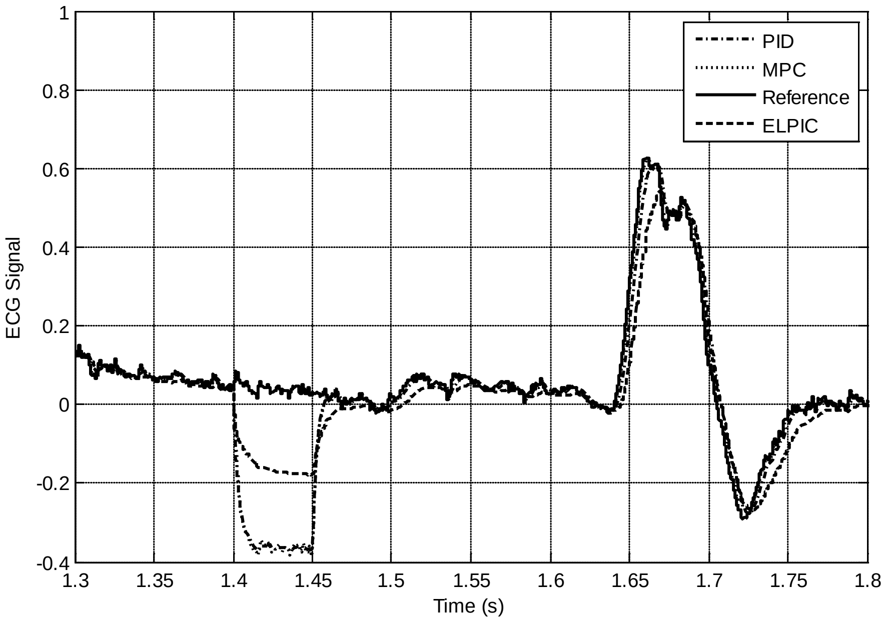

Figure 7. Effect of FDI attack.

Table 2. Mean squared error for controllers under attacks.

	TDS attack	DOS attack	FDI attack
MPC	0.0068	0.0742	0.0756
PID	0.0074	0.1118	0.0750
ELPIC	0.00029	0.0057	0.0207

clearly show that the responses of the model with ELPIC are closely matched the referenced ECG signal when the model is under attack of any of these attacks. The responses of the model with the classical PI controller, and the MPC are significantly off. Although ELPIC is less powerful in tracking the highly nonlinear referenced ECG signal, it is more robust under the TDS, DoS and FDI attacks.

Table 2 shows the mean squared error (MSE) value between the system's output and the referenced ECG signal for the time slot of 1.4 seconds to 1.5 seconds which the system is under attack. The results verify our visual findings.

6. Conclusion

In this paper, we have described a general model of NCSs under attack and reviewed the mathematical model of some possible attacks. Through simulations we have shown the impacts of those attacks on the performance of a networked pacemaker. The simulation results also show that the ELPIC method provides much better performance than that of the PID and the MPC when the system is under DoS, TDS and FDI attacks.

References

[1] Lopez, C., Sargolzaei, A., Santana, H. and Huerta, C. (2015) Smart Grid Cyber Secu-

rity: An Overview of Threats and Countermeasures. *Journal of Energy and Power Engineering*, **9**, 632-647.

[2] Sargolzaei, A., Kang, K.Y. and Abdelghani, M.N. (2016) Preventing Time-Delay Switch Attack on Load Frequency Control in Distributed Power Systems. *IEEE Transactions on Smart Grid*, **7**, 1176-1185.

[3] Liu, Y., Ning, P. and Reiter, M.K. (2009) False Data Injection Attacks against State Estimation in Electric Power Grids. *The* 16*th ACM Conference on Computer and Communications Security*, New York, 9-13 November 2009, 21-32. https://doi.org/10.1145/1653662.1653666

[4] Teixeira, A., Amin, S., Sandberg, H., Johansson, K.H. and Sastry, S.S. (2010) Cyber Security Analysis of State Estimators in Electric Power Systems. *The Decision and Control* (*CDC*), Atlanta, 15-17 December 2010, 5991-5998. https://doi.org/10.1109/CDC.2010.5717318

[5] Abaspour, A., Sadeghi, M. and Sadati, H. (2013) Using Fuzzy Logic in Dynamic Inversion Flight Controller with Considering Uncertainties. 13*th Iranian Conference on Fuzzy Systems* (*IFSC*), Qazvin, 27-29 August 2013, 1-6.

[6] Abbaspour, A., Aboutalebi, P., Yen, K.K. and Sargolzaei, A. (2017) Neural Adaptive Observer-Based Sensor and Actuator Fault Detection in Nonlinear Systems: Application in UAV. *ISA Transactions*, **67**, 317-329. https://doi.org/10.1016/j.isatra.2016.11.005

[7] Abbaspour, A., Yen, K.K., Noei, S. and Sargolzaei, A. (2016) Detection of Fault Data Injection Attack on UAV Using Adaptive Neural Network. *Procedia Computer Science*, **95**, 193-200. https://doi.org/10.1016/j.procs.2016.09.312

[8] Kosut, O., Liyan, J., Thomas, R.J. and Lang, T. (2011) Malicious Data Attacks on the Smart Grid. *IEEE Transactions on Smart Grid*, **2**, 645-658. https://doi.org/10.1109/TSG.2011.2163807

[9] Amin, S., Cardenas, A.A. and Sastry, S.S. (2009) Safe and Secure Networked Control Systems under Denial-of-Service Attacks. *The* 12*th International Conference on Hybrid Systems*: *Computation and Control*, San Francisco, 13-15 April 2009, 31-45. https://doi.org/10.1007/978-3-642-00602-9_3

[10] Liu, S., Liu, X.P. and Saddik, A.E. (2013) Denial-of-Service (dos) Attacks on Load Frequency Control in Smart Grids. *Innovative Smart Grid Technologies* (*ISGT*), *IEEE PES*, Washington DC, 24-27 February 2013, 1-6.

[11] Esfahani, P.M., Vrakopoulou, M., Margellos, K., Lygeros, J. and Andersson, G. (2010) A Robust Policy for Automatic Generation Control Cyber Attack in Two Area Power Network. *The Decision and Control* (*CDC*), Atlanta, 15-17 December 2010, 5973-5978.

[12] Arney, D., Venkatasubramanian, K.K., Sokolsky, O. and Lee, I. (2011) Biomedical Devices and Systems Security. *Engineering in Medicine and Biology Society*, *EMBC*, 2011 *Annual International Conference of the IEEE*, Boston, 30 August-3 September 2011, 2376-2379. https://doi.org/10.1109/IEMBS.2011.6090663

[13] Li, X., Liang, X., Lu, R., Shen, X., Lin, X. and Zhu, H. (2012) Securing Smart Grid: Cyber Attacks, Countermeasures, and Challenges. *Communications Magazine*, *IEEE*, **50**, 38-45. https://doi.org/10.1109/MCOM.2012.6257525

[14] Di-Battista, J., Courrege, J.-C., Rouzeyre, B., Torres, L. and Perdu, P. (2010) When Failure Analysis Meets Side-Channel Attacks. *Cryptographic Hardware and Embedded Systems*, *CHES*, Springer, New York, 188-202. https://doi.org/10.1007/978-3-642-15031-9_13

[15] Moradi, A., Mischke, O., Paar, C., Li, Y., Ohta, K. and Sakiyama, K. (2011) On the

Power of Fault Sensitivity Analysis and Collision Side-Channel Attacks in a Combined Setting. *Cryptographic Hardware and Embedded Systems-CHES* 2011, Springer, New York, 292-311. https://doi.org/10.1007/978-3-642-23951-9_20

[16] Yuan, Y., Li, Z. and Ren, K. (2011) Modeling Load Redistribution Attacks in Power Systems. *IEEE Transactions on Smart Grid*, **2**, 382-390. https://doi.org/10.1109/TSG.2011.2123925

[17] Yuan, Y., Li, Z. and Ren, K. (2012) Quantitative Analysis of Load Redistribution Attacks in Power Systems. *IEEE Transactions on Parallel and Distributed Systems*, **23**, 1731-1738. https://doi.org/10.1109/TPDS.2012.58

[18] Mo, Y., Garone, E., Casavola, A. and Sinopoli, B. (2010) False Data Injection Attacks against State Estimation in Wireless Sensor Networks. 49*th IEEE Conference on Decision and Control* (*CDC*), Atlanta, 15-17 December 2010, 5967-5972. https://doi.org/10.1109/CDC.2010.5718158

[19] Sargolzaei, A., Yen, K.K. and Abdelghani, M. (2014) Control of Nonlinear Heartbeat Models under Time-Delay-Switched Feedback Using Emotional Learning Control. *International Journal on Recent Trends in Engineering and Technology*, **10**, 85-91.

[20] Sargolzaei, A., Yen, K.K. and Abdelghani, M. (2013) Time-Delay Switch Attack on Load Frequency Control in Smart Grid. *Advances in Communication Technology*, **5**, 55-64.

[21] Sargolzaei, S., Faez, K. and Sargolzaei, A. (2008) Signal Processing Based for Fetal Electrocardiogram Extraction. *International Conference on Biomedical Engineering and Informatics*, Sanya, 27-30 May 2008, 492-496. https://doi.org/10.1109/BMEI.2008.304

[22] Sargolzaei, A., Faez, K. and Sargolzaei, S. (2009) A New Robust Wavelet Based Algorithm for Baseline Wandering Cancellation in ECG Signals. 2009 *IEEE International Conference on Signal and Image Processing Applications* (*ICSIPA*), Kuala Lumpur, 18-19 November 2009, 33-38. https://doi.org/10.1109/ICSIPA.2009.5478671

[23] Moren, J. and Balkenius, C. (2000) A Computational Model of Emotional Learning in the Amygdala. *From Animals to Animats*, **6**, 115-124.

[24] Thanom, W. and Loh, R.N. (2011) Nonlinear Control of Heartbeat Models. *Journal on Systemics*, *Cybernetics and Informatics*, **9**, 21-27.

[25] Lambert, M., Engroff, A., Dyer, M. and Byer, B. https://www.clear.rice.edu/elec301/Projects02/empiricalMode/extras.html