IOP Conf. Series: Journal of Physics: Conf. Series **783** (2017) 012022 doi:10.1088/1742-6596/783/1/012022

Attack-tolerant networked control system: an approach for detection the controller stealthy hijacking attack

Amer Atta Yaseen, Mireille Bayart

Univ. Lille, CNRS UMR 9189 CRIStAL – Centre de Recherche en Informatique Signal et Automatique de Lille, Bât Polytech-Lille, 59655 Villeneuve d'Ascq Cedex, France

Email : amer.yaseen@polytech-lille.fr, mireille.bayart@univ-lille1.fr

Abstract. In this work, a new approach will be introduced as a development for the attack-tolerant scheme in the Networked Control System (NCS). The objective is to be able to detect an attack such as the Stuxnet case where the controller is reprogrammed and hijacked. Besides the ability to detect the stealthy controller hijacking attack, the advantage of this approach is that there is no need for a priori mathematical model of the controller. In order to implement the proposed scheme, a specific detector for the controller hijacking attack is designed. The performance of this scheme is evaluated be connected the detector to NCS with basic security elements such as Data Encryption Standard (DES), Message Digest (MD5), and timestamp. The detector is tested along with networked PI controller under stealthy hijacking attack. The test results of the proposed method show that the hijacked controller can be significantly detected and recovered.

1. Introduction

Any network medium is susceptible to be easily intercepted. Research in NCS were initialized as regards the safety and convenience in hazardous environments such as power plants, nuclear reactor space projects, military applications, etc. In all these applications, security is of utmost concern [1]. The cyber-attacks can have heavy consequences on the plant, but can also have wide-ranging effects on environment and the individuals. The cyber-attacks include the data modification, deceptive sender identity, and data replay [2]. Security mechanisms of NCS related to the cyber-attacks have been addressed in several directions.

Some works on network security algorithms: In [3], DES (Data Encryption Standard), 3DES (Triple Data Encryption Standard), and AES (Advanced Encryption Standard) are integrated with the application to secure the sensor as well as control data flow on the network, then 1-D gain scheduler was designed and implemented to alleviate the adverse effect due to security. The encryption of the data transmitted on the network is also realized by DES in [4], and they add message digest 5 (MD5) to detect the data integrity. In [5], the DES was also adopted as security solutions for the DC motor networked control system in TrueTime platform algorithm. In [6], to prevent most of the attacks in which the IP systems are vulnerable, the authors proposed a Network management of Named Data.

Others interest on communication and control with real times constraints: The trade-off between NCS security and its real-time performance was demonstrated in [7]. In [8], a detection module based on implementation of DES algorithm is given, furthermore, to protect NCSs from getting out of control,

the authors design also a response module. In [9], the authors described a quick detection approach against data-injection attack in the smart grid.
However, all the methods [3]- [9] are handled only with the attack cases, which are stated in [2].
From The British Columbia Institute of Technology Industrial Security Incident Database [1] we can note other attacks on process control and industrial networked systems (e.g. Stuxnet case) which are not mentioned in [2].
This paper deals with the effects of special attack scenario such as Stuxnet case [10] where a controller was reprogrammed and hijacked.
The Stuxnet case needs to the implementation of special attack detectors along with backup controller. Until now, a typical approach to implement such attack detectors is based on system models e.g. [11], [12] and it is inspired by fault diagnosis detectors [13], [14]. The Stuxnet attack detector, which not based on controller model was proposed in [15]. However, the restriction of [15] was represented by assuming the value of set point (operator's desired value) is always equal to zero.
The attack-tolerant scheme for NCS was introduced in [16]; this scheme considered three types of attacks in NCS, these types are represented by injection, modification, and replication of the sent and received data in the networked control loop. A modification for the scheme in [16] was adopted in [17] to handle the Stuxnet case. However, the approach of [17] is still need to develop the sensitivity of detection. In this paper, we specially focus on the controller hijacking attack with the injection of a destructive control signal into the networked control loop. The stealthy hijacking attack will be considering rather than the rough attack. The architecture of the attack-tolerant system developed will be detailed in the next sections.

2. The proposed secure NCS

Fig.1 illustrates the general block diagrams of the proposed secure NCS. Due to the real time nature of the NCS, UDP is preferred for use in NCS over IP network. The Data Encryption Standard (DES), Message Digest (MD5), and timestamp will be used along with the controller and plant sides' security mechanisms; the details of these mechanisms were described in [16]

In this paper, the controller hijacking attack detector will be introduced as a new enhancement to the attack tolerant scheme of [16].

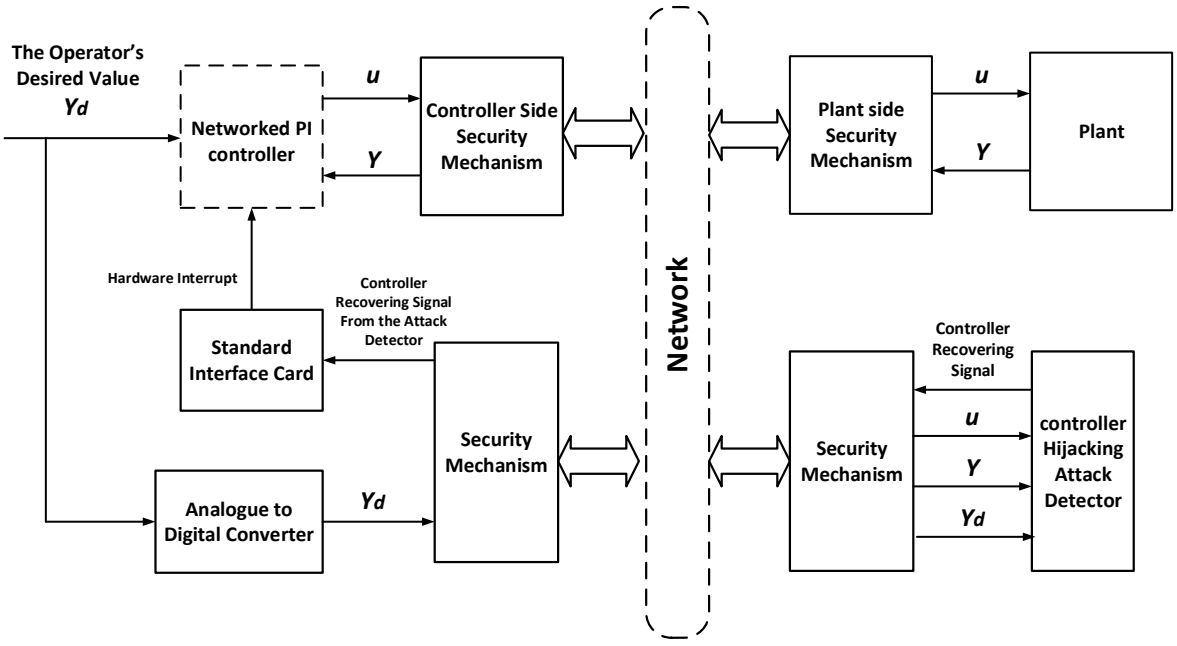

Figure 1. The block diagram of the proposed NCS

3. Detection of the controller hijacking attack

The block diagram of the NCS is illustrated in Fig. 1. For detecting the attacks on the controller, a new approach is proposed. The advantage of this proposed approach is that there is no need for a priori mathematical model of the controller. The detector is connected separately from the controller and plant sides to the NCS with basic security elements such as Data Encryption Standard (DES), Message Digest (MD5), and timestamp, which are used for the secure communication over NCS. Assume we have a controller (see Fig. 2) and that one wants to monitor the controller behaviour by mean of the controller input and output. The controller with a single input variable *e* and a single output variable *u* is selected.

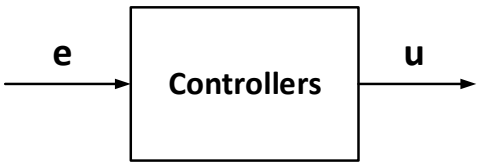

Figure 2. SISO Controller

The attack on the plant was expressed in [18] as follows

$$ur_k = u_k(1-\psi) \tag{1}$$

where, ψ, $0 \le \psi \le 1$, is the loss of the response efficiency of the plant due to control signal which is sent from the attacker. ur_k , is the true control variable.
Rewrite (1) for the attack on the controller (e.g. controller hijacking attack) or,

$$er_k = e_k(1-\phi) \tag{2}$$

where, er_k is the true error variable which is measured at the controller input during all cases including the presence of an attack on controller side, e_k is the nominal error value and ϕ, $0 \le \phi \le 1$, is the controller performance index.
Rewrite (1),

$$\phi = 1 - \frac{er_k}{e_k} \tag{3}$$

In this paper, the controller performance index will be used to detect the controller hijacking attack. Now, the objective is to estimate the nominal error as well as the true error. Recall the ultra-local model which is given in [19] and introduced for the controller in [17]

$$u^{(v)} = F + \alpha e \tag{4}$$

where,

- $\alpha \in R$ is a non-physical constant parameter. It is chosen by the designer such that αe and $u^{(v)}$ are of the same magnitude. It should be therefore clear that its numerical value, which is obtained by trials and errors during attack free condition, is not a priori precisely defined.
- ***F*** represents all the unusual input-output behavior of the controller;

- The order ***v*** is also a design parameter of the numerical model of (4) that can be arbitrarily chosen by the designer. In this paper, first order derivative $\dot{u}$ will be chosen.
- $e = y_d - y$, *yd*. is the operator's desired set point and y is the plant response.

For the attack free controller, the values of $\dot{u}$ and αe are equal in magnitude [17] or,

$$\left| \left\langle \left\langle e \right\rangle \right\rangle_T^C (t) \right| = \left| \frac{\left\langle \left\langle \dot{u} \right\rangle \right\rangle_T^C (t)}{\alpha} \right| \tag{5}$$

where, $\left\langle \left\langle \dot{u} \right\rangle \right\rangle_T^C (t)$ is continuous-time estimation of the first derivative of the controller output.

Due to the network effects e.g. noise [20], packet drop, and the out of sequence [16], the estimated values for the first derivative of the controller output and the true error will be used in this paper.

By applying the derivative estimation method which introduced in [21], the first derivative of the controller output can be estimated as follows:

Let *um* be a measured value of the controller output *u*, and *um* is the image of *u* and we consider that *u* is distorted by some of added noise Ω, therefore we have*: um* = *u* + Ω.

The objective is to estimate the derivatives of the controller output *u*, up to a finite order of derivation, from its measurement *um* observed on a given time interval.

The Taylor expansion of the controller output around *0* is given by

$$u(\tau) = \sum_{n=0}^{\infty} u^{(n)}(0) \frac{\tau^n}{n!} \tag{6}$$

By the polynomial we can approximate *u(t)* for the interval *[0,T], T>0*.

$$u_N(\tau) = \sum_{n=0}^{N} u^{(n)}(0) \frac{\tau^n}{n!} \tag{7}$$

For *N* degree, *ΦN* is the operational analogue of *uN* and can be written as

$$\Phi_N(s) = \frac{u(0)}{s} + \frac{\dot{u}(0)}{s^2} + \ldots + \frac{u^{(N)}(0)}{s^{N+1}} \tag{8}$$

By applying a convenient operator to *ΦN(s)*, we can separate each coefficient $u^{(n)}(0)$ appearing in previous expression. Thus,

$$\begin{gathered} \forall i = 0,\ldots,N \\ \frac{u^{(i)}(0)}{s^{2N+1}} = \frac{(-1)^i}{N!(N-i)!} \cdot \frac{1}{s^{N+1}} \cdot \frac{d^i}{ds^i} \cdot \frac{1}{s} \\ \cdot \frac{d^{N-i}}{ds^{N-i}} \left(s^{N+i} \Phi_N(s) \right) \end{gathered} \tag{9}$$

The expression of $u^{(i)}(0)$ in the time domain can be written as

$$u^{(i)}(0) = \int_0^T P(\delta;T)\, u_N(\delta)\, d\delta \tag{10}$$

where $P(\delta;T)$ is polynomial in δ and T. Notice that (11) gives the calculation of $u^{(i)}(0)$ from an integral on the time interval [0; T] for a given small $T > 0$.

As $\left.\frac{d^i u(t-\delta)}{d\delta^i}\right|_{\delta=0} = (-1)^i u^{(i)}(t)$ it is possible to express $u^{(i)}(t)$ as an integral, which includes values of u_N on the time interval $[t - T, t]$:

$$u^{(i)}(t) = (-1)^{(i)} \int_0^T P(\delta;T)\, u_N(t-\delta)\, d\delta \tag{11}$$

By using the noisy signal *um*, a simple estimator of the derivative $u^{(i)}(t)$ can be expressed as follows:

$$\left\langle\left\langle u^{(i)}\right\rangle\right\rangle_T^C(t) = (-1)^{(i)} \int_0^T P(\delta;T)\, u_m(t-\delta)\, d\delta \tag{12}$$

(13) is realized from (12) by changing *uN* by *um*. Noting that the integral operation acting the rule of low-pass filter and reduced the noise that distorts *um*. The choice of *T* results in a trade-off: small value of *T* leads to the effect of the noise; the large value of *T* is leads to better integrals low pass filtering but there is error due to truncation.

In practice, the integral expressed in (13) is obtained by a numerical integration method; therefore, the estimator $\left\langle\left\langle u^{(i)}\right\rangle\right\rangle_T^C(t)$ will be performed at each sample of *k*.

Let *Ts* is the sampling period, then the discretization of any continuous time function f will be denoted by *f[k]* i.e.

$$f[k] = f(k,Ts), \quad k \in Z$$

With these notations, the discrete-time approximation of the first derivative estimation of the controller output is simply a discrete sum that can be written as:

$$\left\langle\left\langle \dot{u}\right\rangle\right\rangle_{Ts,ns}^d[k] = \sum_{j=0}^{n_s} w(j)\, P(jT_s; n_s T_s)\, u_m[k-j] \tag{13}$$

Where *ns* is the number of samples used in the time window $T = nsTs$ and the *w(j)* is the weight related to the used numerical integration method.

To eliminate the effects of network which are mentioned above, the true error function values will be integrated as a tabular data. These values are taken at certain discrete points during the same time window of the derivative output estimation.

First is to fit a curve through the true error data, and then integrate the resulting curve. It is possible to use any integration methods, but the most common approach is to use a piecewise polynomial such as a spline as follows:

- Suppose we are given as set of true error samples point *(t, er(t))*

- Fit a spline *E(t)*, through this samples, keep in mind that *E(t)* is a piecewise polynomial on several intervals in particular.

$$Er(t)=\begin{cases} erp_1(t) & t_0 \le t \le t_1 \\ erp_2(t) & t_1 \le t \le t_2 \\ \vdots & \\ erp_{ns}(t) & t_{ns-1} \le t \le t_{ns} \end{cases} \tag{14}$$

Then

$$\left\langle\left\langle er\right\rangle\right\rangle_T^c(t)=\int_{t-nsT}^{t} e(t)\,dt \approx \int_{t-nsT}^{t} E(t)\,dt=\sum_{j=0}^{ns}\int_{t_{j-1}}^{t_j} erp_j(t)\,dt \tag{15}$$

It is possible to use a cubic spline interpolant. In this case, each $erp_j(t)$ is a cubic polynomial, which can be written as

$$erp_j(t)=a_{j,1}(t-t_{j-1})^3+a_{j,2}(t-t_{j-1})^2+a_{j,3}(t-t_{j-1})+a_{j,4} \tag{16}$$

Solving for $a_{j,1}, a_{j,2}, a_{j,3}$, and $a_{j,4}$ using Gauss elimination [22], then we can easily integrate $erp_j(t)$

$$\int_{t_{j-1}}^{t_j} erp_j(t)\,dt=\frac{a_{j,1}}{4}(t_j-t_{j-1})^4+\frac{a_{j,2}}{3}(t_j-t_{j-1})^3+\frac{a_{j,3}}{2}(t_j-t_{j-1})^2+a_{j,4}(t_j-t_{j-1}) \tag{17}$$

Let, $T=t_j-t_{j-1}$ then,

$$\int_{t_{j-1}}^{t_j} erp_j(t)\,dt=\frac{a_{j,1}}{4}T^4+\frac{a_{j,2}}{3}T^3+\frac{a_{j,3}}{2}T^2+a_{j,4}T \tag{18}$$

Thus, the estimated true error is given by

$$\left\langle\left\langle er\right\rangle\right\rangle_{Ts,ns}^d[k]=\sum_{j=0}^{ns}\left(\frac{a_{j,1}}{4}Ts^4+\frac{a_{j,2}}{3}Ts^3+\frac{a_{j,3}}{2}Ts^2+a_{j,4}Ts\right) \tag{19}$$

Note that a direct implantation of this summation would require 7*ns* multiplications, 3*ns* additions, and 3*ns* exponentiations. An algebraic rearrangement results in a nested approach of this computation [22],

$$\left\langle\left\langle e_r \right\rangle\right\rangle^{d}_{Ts,ns}[k] = \sum_{j=0}^{ns} Ts\left(Ts\left(Ts\left(\frac{a_{j,1}}{4}Ts + \frac{a_{j,2}}{3}\right) + \frac{a_{j,3}}{2}\right) + a_{j,4}\right) \tag{20}$$

(20) requires only 7*ns* multiplications, 3*ns* additions, and no exponentiations.
Assuming nominal and true error are in the same sign (i.e. stealthy controller hijacking attack) then, rewrite (3) in term of estimated values

$$\phi\, k = 1 - \left| \frac{\alpha \left\langle\left\langle e_r \right\rangle\right\rangle^{d}_{Ts,ns}[k]}{\left\langle\left\langle \dot{u} \right\rangle\right\rangle^{d}_{Ts,ns}[k]} \right| \tag{21}$$

Or,

$$\phi\, k = 1 - \frac{\alpha \sum_{j=0}^{ns} Ts\left(Ts\left(Ts\left(\frac{a_{j,1}}{4}Ts + \frac{a_{j,2}}{3}\right) + \frac{a_{j,3}}{2}\right) + a_{j,4}\right)}{\sum_{j=0}^{ns} w(j)\, P(jTs; nsTs)\, um[k-j]} \tag{22}$$

If $\phi=0$ means that there is no controller hijacking attack.
$0<\phi<1$ means that there is stealthy controller hijacking attack.
If $\phi=1$ implies that the controller is completely hijacked.
.

4. Controller recovering

On referring to Fig.1, at each sample time *k*, the controller hijacking attack detector receives *yd*, *y*, and *u* over NCS and calculates ϕ according to the (22). If ϕ increased, a recovering signal will be sent over NCS to the interface circuit. The interface circuit converts the recovering signal to hardware interrupt, which restores the controller software to its design parameters.

5. Simulation results

The proposed method is developed as per the scheme mentioned with a simulation of the local downstream controller at the Partiteur cross-regulator in the Gignac canal which located 40 km north-west of Montpellier, in the south of France.
The Integrator Delay (ID) model is an approximate representation of the dynamics of canal pool for low frequencies, this model and its parameters were given in [23] as follows,

$$y = \frac{1}{A_d\, s}\left(e^{-\tau_d s} u - p\right) \tag{23}$$

where,

- *y* is the downstream water elevation.
- τ_d is the delay of the canal pool.
- *p* the downstream perturbation.

When the control input *u* is a discharge, *Ad* represents the backwater area, and when *u* is the upstream gate opening, *Ad* is the inverse integrator gain.

For the Partiteur Left Bank cross regulator, the *Ad* = 25.2113 and τ_d =30 seconds. The PI controller will be used in this paper as the downstream controller with *Kp=0.60* and *Ti=96* seconds [23].
Initially, the system was tested without any attack; the test result is illustrated in Fig.3. After that, the simulation is carried out by randomly reprogramming the PI controller, in this case the original settings of the controller will be lost and its behaviour will be unknown (i.e. hijacked by the attacker). The detection of the controller hijacking attack and the controller recovering method which described in sections 2, 3 and 4 are applied to the NCS.
In order to evaluate the proposed detector, the controller reprogramed for three times (attack A, attack B, and attack C), this is made by change the parameters (*kp* and *Ki*) of *PI* controller in stealthy way. The test results are shown in Fig 4., Fig.5., Fig.6 and Fig.7. The attack is successfully detected and the controller recovered to its normal operation.

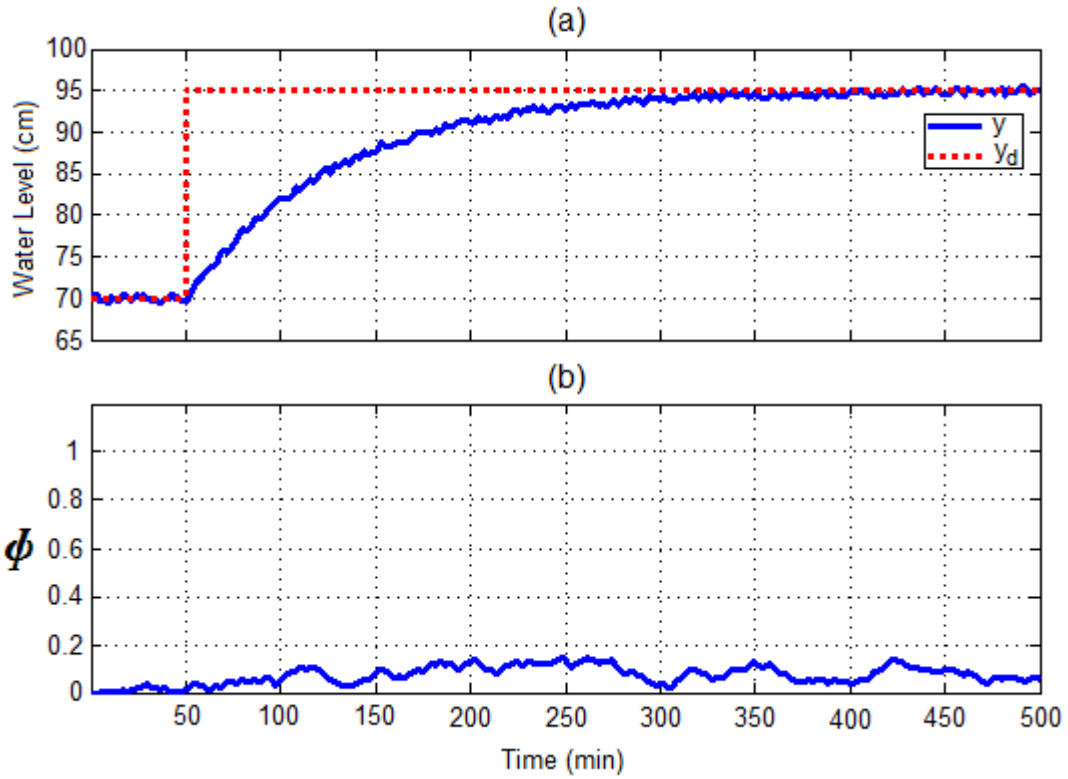

Figure 3. The NCS response without any attack

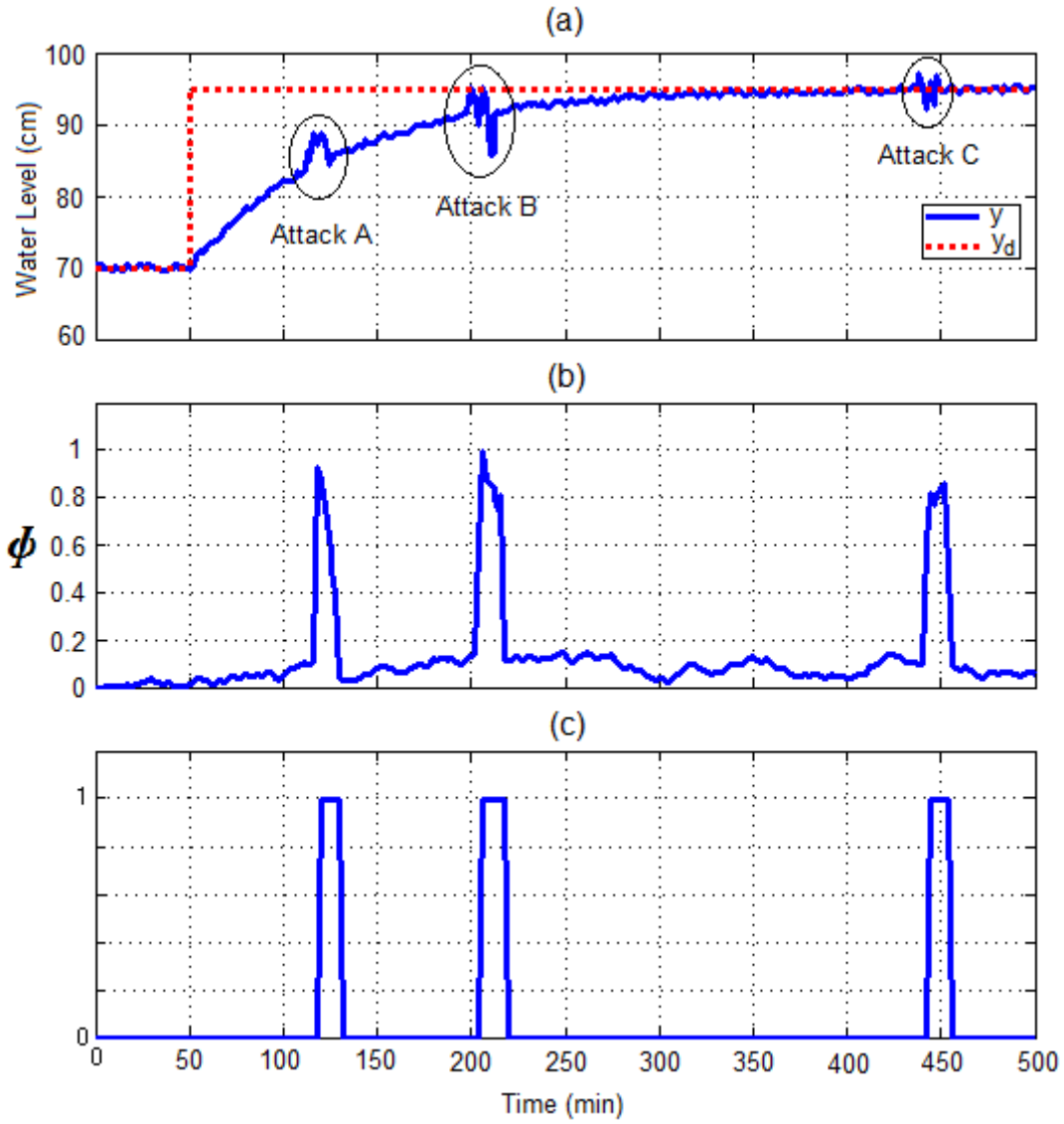

Figure 4. (a) The response of the plant when the attack is (or has been) detected and the controller is recovered. (b) The effect of the controller hijacking attack on the value of ϕ (c) controller recovering signal

From Fig.5.b, Fig.6.b, and Fig.7.b, one can note the effect of controller hijacking attack on the value of ϕ The abnormal change of ϕ will be used to generate controller recovering signal as illustrate in Fig.4.c.

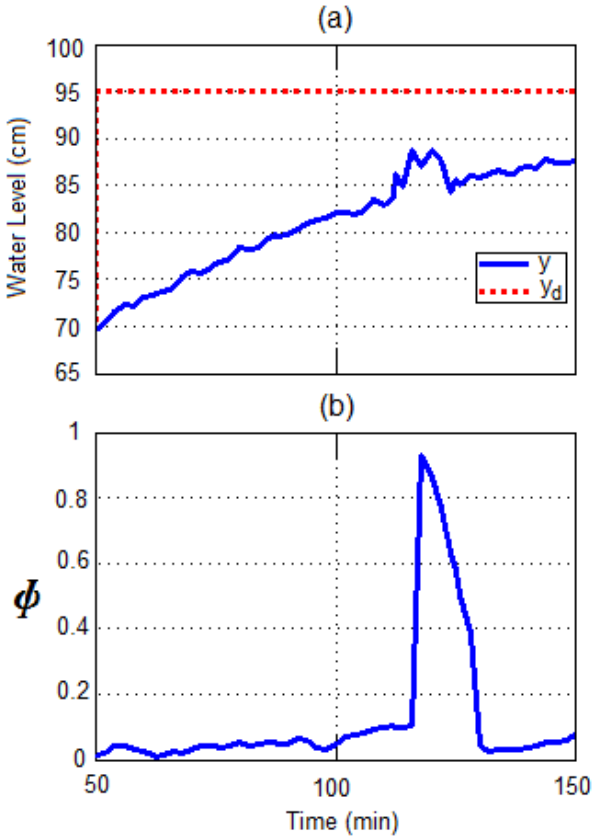

Figure 5. (a) The response of the plant when the ***attack A*** is detected and the controller is recovered, (b) The effect of the controller hijacking attack on the value of ϕ (with zoom)

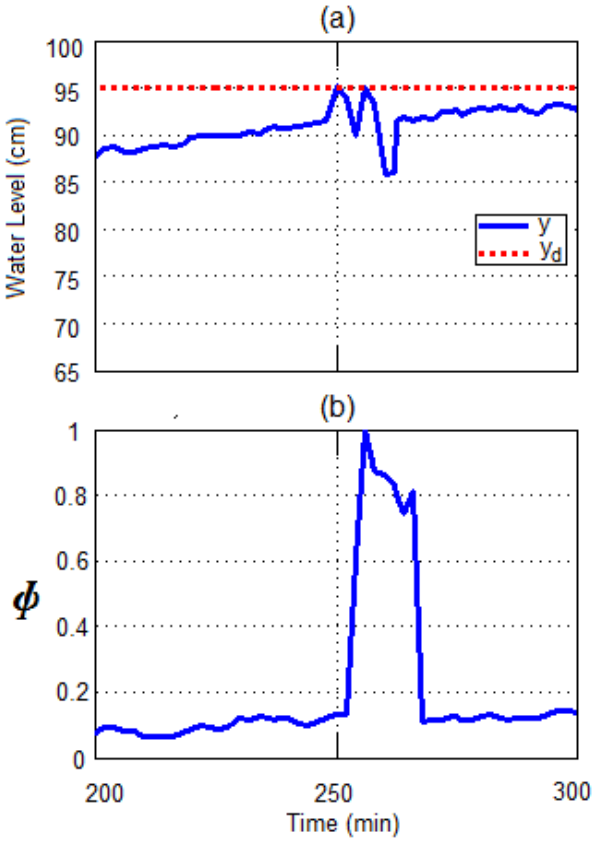

Figure 6. (a) The response of the plant when the ***attack B*** is detected and the controller is recovered, (b) The effect of the controller hijacking attack on the value of ϕ (with zoom)

6. Conclusion and perspectives

In this paper, an attack-tolerant networked control system in presence of the controller hijacking attack is introduced.

The facility of this method is that no a priori controller mathematical model is required to detect this type of attacks.

The proposed detector is connected to the NCS separately from the controller and plant sides. The secure mechanism is used for the secure communication of the proposed detector over NCS.

Even though only one type of controllers is used in this paper, the proposed attack detector is suitable enough to be considered as basis for the future development with other types of the controllers.

The investigation reveals that the proposed attack tolerant scheme can be used successfully for NCS in presence of the controller hijacking attack such as Stuxnet case.

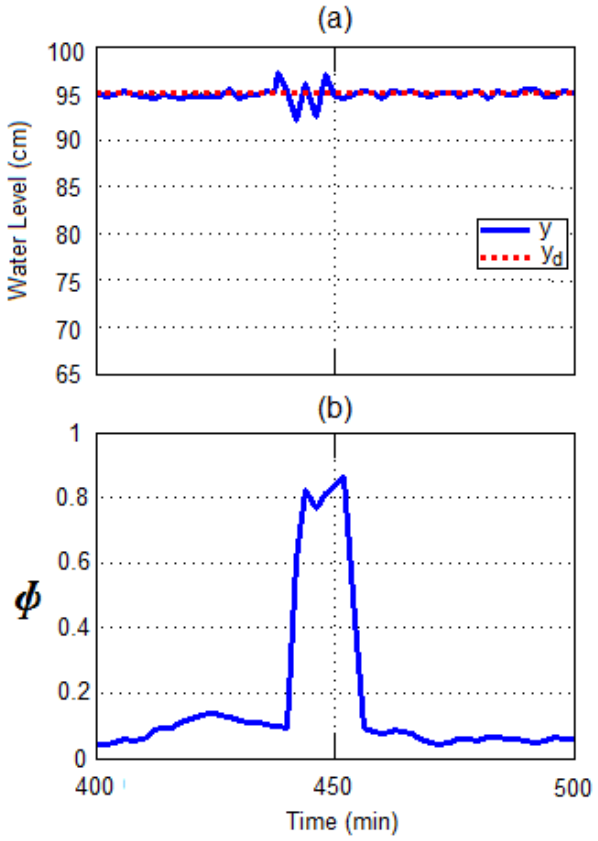

Figure 7. (a) The response of the system when the ***attack C*** is detected and the controller is recovered, (b) The effect of the controller hijacking attack on the value of ϕ (with zoom)

7. References

[1] Gupta, R.A.; Mo-Yuen Chow, *Networked Control System: Overview and Research Trends, IEEE Transactions on Industrial Electronics,* , vol.57, no.7, pp.2527-2535, July 2010.

[2] W. Stallings, *Cryptography and Network Security: Principles and Practice*, 4th ed. Englewood Cliffs, NJ: Pearson/Prentice-Hall, 2006.

[3] Gupta, R.A.; Mo-Yuen Chow, *Performance assessment and compensation for secure networked control systems, 34th Annual Conference of IEEE Industrial Electronics (IECON 2008)*, Orlando, Florid, pp.2929-2934, 10-13 Nov. 2008

[4] Pang Zhong hua; Liu Guoping, *Secure networked control systems under data integrity attacks, 29th Chinese Control Conference (CCC)*, Beijing, China, pp.5765-5771, 29-31 July 2010

[5] Liying Zhang, Lun Xie, Weize Li, Zhiliang Wang, *Security Solutions for Networked Control Systems Based on DES Algorithm and Improved Grey Prediction Model* , IJCNIS, vol.6, no.1, pp.78-85, 2014.

[6] Perez, V.; Garip, M.T.; Lam, S.; Lixia Zhang, *Security evaluation of a control system using Named Data Networking, 21st IEEE International Conference on Network Protocols (ICNP)*, Goettingen, Germany, pp.1-6, 7-10 Oct. 2013

[7] Wente Zeng; Mo-Yuen Chow, *A trade-off model for performance and security in secured Networked Control Systems, 2011 IEEE International Symposium on Industrial Electronics (ISIE)*, Gdansk, Poland, pp. 1997- 2002, 27-30 June 2011.

[8] Zhang Liying; Xie Lun; Li Weize; Wang Zhiliang, *A secure mechanism for networked control systems based on TrueTime, International Conference on Cyberspace Technology (CCT 2013)*, Beijing, China, pp.44-49, 23-23 Nov. 2013.

[9] Shuguang Cui; Zhu Han; Kar, S.; Kim, T.T.; Poor, H.V.; Tajer, A., *Coordinated data-injection attack and detection in the smart grid: A detailed look at enriching detection solutions,IEEE Signal Processing Magazine*, vol.29, no.5, pp. 106-115, Sept. 2012

[10] Nourian, A.; Madnick, S., *A Systems Theoretic Approach to the Security Threats in Cyber Physical Systems Applied to Stuxnet, IEEE Transactions on Dependable and Secure Computing*, vol.PP, no.99, pp.1-1. 2015.

[11] Y. Mo and B. Sinopoli, *False data injection attacks in control systems, in First Workshop on Secure Control Systems*, Cyber Physical Systems Week 2010, April 2010.

[12] I. Shames, A. M. Teixeira, H. Sandberg, and K. H. Johansson, *Distributed fault detection for interconnected second-order systems, Automatica*, vol. 47, no. 12, pp. 2757 – 2764, 2011.

[13] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, *Diagnosis and Fault-Tolerant Control, 2nd ed. Springer*, 2006

[14] J. Gertler, *Fault Detection and Diagnosis in Engineering Systems*. New York: Marcel Dekker, Inc., 1998.

[15] Rosich, A.; Voos, H.; Yumei Li; Darouach, M., *A model predictive approach for cyber-attack detection and mitigation in control systems, 52nd IEEE Conference on Decision and Control (CDC)*, Florence, Italy, pp.6621-6626, 10-13 Dec. 2013.

[16] A. Yaseen, Mireille Bayart, *Attack-Tolerant Networked Control System Based on the Deception for the Cyber-Attacks, World Congress on Industrial Control Systems Security (WCICSS-2015)*, London, UK , pp.37-44, 14-16 Dec. 2015

[17] A. Yaseen, Mireille Bayart, *Attack-tolerant networked control system in presence of the controller hijacking attack, 2016 International Conference on Military Communications and Information Systems (ICMCIS)*, Brussels, Belgium, pp. 1-8, 2016

[18] A. Yaseen, Mireille Bayart, *Intelligent Generalized Predictive Control Strategy for Networked Control System with an Internal Cyber Attack Detector, 21st IEEE International Conference on Emerging Technologies and Factory Automation (IEEE ETFA'2016)*, Berlin, Germany , 6 - 9 Sep. 2016.

[19] M. Fliess, C. Join, *Model-Free Control*, *International Journal of Control*, Vol. 86, Issue 12, pp. 2228–2252, 2013.

[20] Xi-Sheng Zhanb, a, Jie Wua,Tao Jiangb, Xiao-Wei Jiangb, *Optimal performance of networked control systems under the packet dropouts and channel noise, ISA Transactions*,Volume 58, September 2015, Pages 214–221.

[21] E. Delaleau, *A proof of stability of model-free control, 2014 IEEE Conference on Norbert Wiener in the 21st Century (21CW)*, Boston, MA, pp. 1-7, 2014.

[22] Joe D. Hoffman, *Numerical Methods for Engineers and Scientists*, Marcel Dekker, Inc, second edition,2001

[23] Litrico, X., Malaterre, P., Baume, J., Vion, P., and Ribot-Bruno, J., *Automatic Tuning of PI Controllers for an Irrigation Canal Pool*, *Journal of Irrigation and Drainage Engineering*, 2007 133:1, 27-37.