



HAL
open science

Temporal framing of a finite memory observer for network control systems applied to measurement losses and integrity recovery

Julien Thuillier, David Delouche, Jacques Fantini, Frédéric Kratz

► To cite this version:

Julien Thuillier, David Delouche, Jacques Fantini, Frédéric Kratz. Temporal framing of a finite memory observer for network control systems applied to measurement losses and integrity recovery. 2020. hal-02908533

HAL Id: hal-02908533

<https://hal.science/hal-02908533v1>

Preprint submitted on 29 Jul 2020

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.

Temporal framing of a finite memory observer for network control systems applied to measurement losses and integrity recovery

Julien Thuillier, David Delouche, Jacques Fantini and Frédéric Kratz

Abstract—This paper focuses on a tool to estimate lost data on network control systems. The tool is also able to detect loss of data integrity and estimate the correct value. A new formulation of the Finite Memory Observer using a finite collection of measurements and input is proposed to achieve these goals.

First, the realisation of this tool is based on a Markov chain used to implement an event triggering mechanism applied to models of lost network measurement packets. The Finite Memory Observer (FMO) is based on a continuous time system model which corresponds better to time management in further works. The new formulation, dealing with loss of measurement packets, uses timestamping of data received to adjust the data estimation-predictions generated. The propagation of data loss in the observer’s window and its effect on the estimate is presented. Finally, on a simple packet loss scenario, the accuracy of this prediction-estimation observer is presented.

Secondly, the FMO is used to detect modification of data. Given the packet strategy, when a data modification is detected, the associated measurement will be not used for its estimation/prediction.

I. INTRODUCTION

Emerging industries reveal new challenges especially to digital communication. The correct functioning of production lines relies on reliable communication networks. However, today, most industrial systems face communication problems, such as packet losses and delay. The system safety and reliability becomes doubtful.

This paper focuses on two of the most frequent communication disturbances of real time systems: measurement loss and integrity loss. Packet losses of measurements drastically impact the control and diagnosis of these systems.

The packet loss behaviour model in communication network has been well explained in [1], [2], [3] and [4]. The impact of perturbation on performance of system tools is analysed in [5], [6], [7], [8] and [9].

Therefore, it is proven that the loss of data in the communication network disturbs the performance and diagnosis of the system.

Given the complexity of network control systems, the perturbation model has to be defined for each communication system structure ([10] and [11]).

First, the characteristics of time-triggered transmission network are modified (Fig. 1).

J. Thuillier is with INSA Centre Val de Loire, Laboratory PRISME EA 4229, France julien.thuillier@insa-cvl.fr

D. Delouche is with HEI campus Centre, Laboratory PRISME EA 4229, France david.delouche@yncrea.fr

J. Fantini is with University Orleans, Laboratory PRISME EA 4229, France jacques.fantini@univ-orleans.fr

F. Kratz is with INSA Centre Val de Loire, Laboratory PRISME EA 4229, France frederic.kratz@insa-cvl.fr

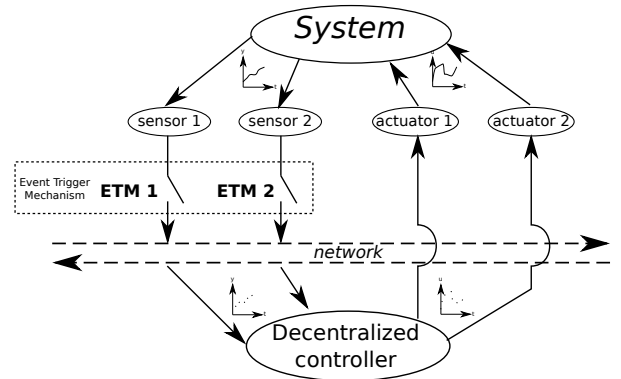


Fig. 1: Even trigger transmission scheme

Sensors are triggered with constant sampling period $T_S \in S = \{T_S, 2 * T_S, \dots, k * T_S\}$ in \mathbb{N} . Communication over the network follows the same period, therefore some data in S will be lost on the network at the sample time.

In this paper, a tool based on a FMO is proposed to estimate the lost data and recover the data integrity. FMO [12][13] has been adapted to many applications such as fault detection [14], diagnosis [15] and hybrid system [16]. Based on these works, a FMO to predict and estimate packet losses is developed.

This paper is organized in four parts. First, the systems used here are presented and the system behaviour after packet loss is analysed. Secondly, the FMO used for measurement prediction and estimation is introduced. Thirdly, a method for recovering the system integrity using FMO is developed. Section IV provides numerical simulations to illustrate the recovering methods of packets losses and system measurement integrity.

II. FINITE MEMORY OBSERVER

The aim of this work is to demonstrate the ability of the FMO to respectively, estimate and predict correct values with or without data losses. The prediction can be used by the controller to continue working in a proper way or complementary to a subsequent diagnosis. For this reason, the FMO is formulated in a time vector collection form. Analysis of the prediction’s accuracy in function of packet loss behaviour is also studied. The effectiveness of using the previous prediction will also be treated.

In the next sections, the temporality of differential equations is used to formulate the FMO in a way concurring with packets losses and integrity losses.

A. Dynamic Finite Memory Observer

Given the linear state-space representation system defined by equation (1):

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) \\ y(t) = Cx(t) + v(t) \end{cases} \quad (1)$$

where, A , B , C are the state space representation matrices with appropriate dimensions. $x \in \mathbb{R}^n$ is the state vector, $u \in \mathbb{R}^m$ the input vector, $y \in \mathbb{R}^p$ the measurement vector and $v \in \mathbb{R}^p$ the gaussian noise measurement vector with $\mathbb{E}(v) = \mathbf{0}$ and $\mathbb{E}(v)\mathbb{E}^T(v) = R$.

State $x(t)$ at a time t can be expressed in function of a previous time state $t - t_0$, written $x(t - t_0)$ in (2).

$$x(t) = e^{At_0}x(t - t_0) + \int_{t-t_0}^t e^{A(t-\theta)}Bu(\theta)d\theta \quad (2)$$

Extracting $x(t - t_0)$ from (2), and multiplying by $e^{-A(t-t_0)}$ gives:

$$x(t - t_0) = e^{-At_0}x(t) - \int_{t-t_0}^t e^{A(t-t_0-\theta)}Bu(\theta)d\theta \quad (3)$$

The delayed measurement can be expressed in function of the current state by multiplying (3) by C and adding the noise measurement.

$$y(t - t_0) = Ce^{-At_0}x(t) - C \int_{t-t_0}^t e^{A(t-t_0-\theta)}Bu(\theta)d\theta + v(t - t_0) \quad (4)$$

Thus, the previous time measurement $y(t - t_0)$ is expressed in function of the current state $x(t)$. Let $Y_L(t)$ be the time t collection (or window) of data composed of previously available measurements (5). The window's length is size L and steady through time. The window contains the L last data's measurement collected and timestamped at time t . Let T be the time vector associated to $Y_L(t, T)$: $T = [t_0, t_1, \dots, t_{L-1}]$ with $t_0 < t_1 < \dots < t_{L-1}$.

Then, the window of available measurements with timestamp T used to estimate or predict a value at a time t is $Y_L(t, T)$:

$$Y_L(t, T) = \begin{pmatrix} y(t - t_0) \\ y(t - t_1) \\ \vdots \\ y(t - t_{L-1}) \end{pmatrix} \quad (5)$$

The equation (4) is applied to $Y_L(t, T)$ given the following system of equations (6).

$$\begin{cases} y(t - t_0) = Ce^{-At_0}x(t) - C \int_{t-t_0}^t e^{A(t-t_0-\theta)}Bu(\theta)d\theta \\ \quad + v(t - t_0) \\ y(t - t_1) = Ce^{-At_1}x(t) - C \int_{t-t_1}^t e^{A(t-t_1-\theta)}Bu(\theta)d\theta \\ \quad + v(t - t_1) \\ \vdots \\ y(t - t_{L-1}) = Ce^{-At_{L-1}}x(t) + v(t - t_{L-1}) \\ \quad - C \int_{t-t_{L-1}}^t e^{A(t-t_{L-1}-\theta)}Bu(\theta)d\theta \end{cases} \quad (6)$$

The dimensional expression of (6) is:

$$Y_L(t, T) = W_L(T)x(t) - \Phi_L(t, T) + V_L(t, T) \quad (7)$$

with,

$$W_L(T) = \begin{pmatrix} Ce^{-At_0} \\ Ce^{-At_1} \\ \vdots \\ Ce^{-At_{L-1}} \end{pmatrix}, V_L(t, T) = \begin{pmatrix} v(t - t_0) \\ v(t - t_1) \\ \vdots \\ v(t - t_{L-1}) \end{pmatrix}$$

$$\Phi_L(t, T) = \begin{pmatrix} C \int_{t-t_0}^t e^{A(t-t_0-\theta)}Bu(\theta)d\theta \\ C \int_{t-t_1}^t e^{A(t-t_1-\theta)}Bu(\theta)d\theta \\ \vdots \\ C \int_{t-t_{L-1}}^t e^{A(t-t_{L-1}-\theta)}Bu(\theta)d\theta \end{pmatrix}.$$

Given $Z_L(t, T) = Y_L(t, T) + \Phi_L(t, T)$,

$$Z_L(t, T) - V_L(t, T) = W_L(T)x(t). \quad (8)$$

P_L is the covariance matrix of the Gaussian noise component $V_L(t, T)$:

$$P_L = \mathbb{E}[V_L(t, T)V_L^T(t, T)] \quad (9)$$

with

$$P_L = \begin{pmatrix} R & 0 & \dots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \dots & 0 & R \end{pmatrix}$$

The solution of the equation (8), $\hat{x}_L(t|T)$ is obtained using the least square method [15]:

$$\hat{x}_L(t|T) = (W_L^T(T)P_L^{-1}W_L(T))^{-1}W_L(T)^T P_L^{-1}Z_L(t, T) \quad (10)$$

Choosing $\Omega_L^{-1} = (W_L^T(T)P_L^{-1}W_L(T))^{-1}$ simplified the form of (10).

The estimation error and its variance are ([15],[17]):

$$\mathbb{E}(\hat{y}(t) - y(t)) = 0 \quad var(\hat{y}(t) - y(t)) = \Omega_L^{-1} \quad (11)$$

III. PROBLEMATIC OF SYSTEM WITH MEASUREMENT PACKET LOSSES

Next, the temporality of differential equations to formulate FMO (Finite Memory Observer) is applied on systems with packet losses.

The model of a network control system subjected to losses of packets presented by [1] is used. This model allows the use of a set number of successive packet losses. Given system subject to network disturbances is defined as:

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) \\ y(t) = Cx(t) + v(t) & \text{if } \phi = 1 \\ y(t) = \text{empty} & \text{if } \phi = 0 \end{cases} \quad (12)$$

where the boolean variable $\phi = 1$ when the packet is received, and $\phi = 0$ when the packet is not received. The variation of ϕ can be modelled by a Markov chain (Fig. 2) where the probability of the state of the next packet reception state is only determined by the current packet reception state. Using this model, the probability of a certain number of successive packets losses can be computed using the stationary distribution of the Markov chain.

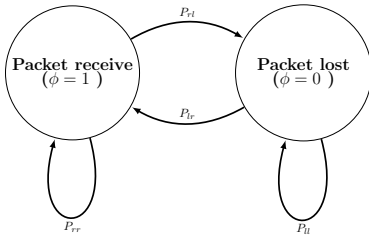


Fig. 2: Behaviour of measurement packet loss

Then, this paper studies the behaviour of the values estimated using the observer in the case of packet losses.

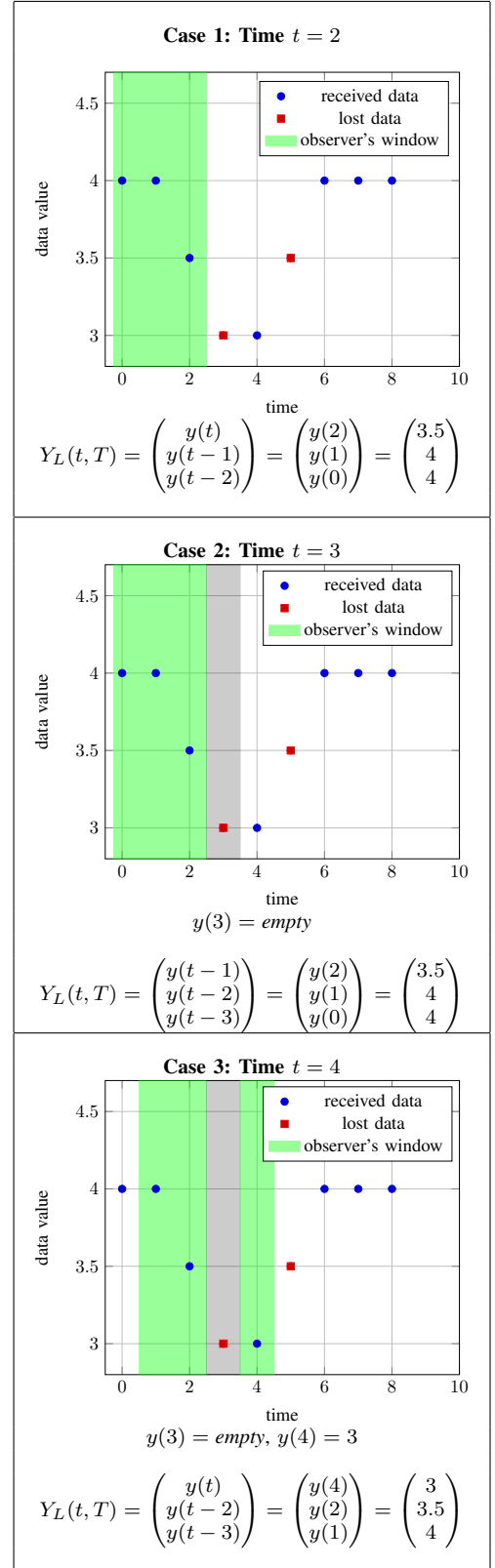
This section presents the strategy of FMO dynamic estimation based on previously received data, as well as the dynamic of the observer's matrix computed using measurements.

Table I represents the behaviours of the FMO's structure in a three packet loss scenario example. In the first case, at time $t = 2$ the FMO window (green area) of size $L = 3$ is composed of three data received previously (with $T = [0, 1, 2]^T$). The FMO estimates the system state at $t = 2$.

In the second case, the measurement at $t = 3$ is lost so that $y(3)$ is empty and the data window of the observer has to use the "old" measurements with timestamp $T = [1, 2, 3]^T$. In this case, the observer will provide a prediction of the measurement at $t = 3$ (grey zone). The dynamical structure of the FMO will take into account only the timestamp of the available data as present in the associate table, which means that the measurements contained in the window will not be updated.

Finally, the measurement data corresponding to timestamp ($t = 4$) is received from the system. The data at $t = 3$ previously predicted (in the grey area) and considered

TABLE I: Dynamical structure of FMO for a specific scenario of packet loss



continuously non available will be ignored. The measurement window of the FMO will be updated by adding the new

data and deleting the oldest data so that $T = [0, 2, 3]^T$. The numerical structure of the FMO changes in accordance with the numerical values of the measurement and associated timestamp.

The evolution of the T vector packet of the FMO is:

$$T = \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}^T \Rightarrow \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}^T \Rightarrow \begin{pmatrix} 0 \\ 2 \\ 3 \end{pmatrix}^T \Rightarrow \begin{pmatrix} 0 \\ 1 \\ 3 \end{pmatrix}^T \Rightarrow \begin{pmatrix} 0 \\ 1 \\ 2 \end{pmatrix}^T \dots \quad (13)$$

IV. PROBLEMATIC OF MEASUREMENT INTEGRITY LOSS

Besides the situation of packet loss where no data is received, the proposed FMO-based strategy can also be applied to ensure diagnostic of system functioning with data received but modified also called integrity loss. After packet loss, integrity loss is one of the biggest causes of the insecurity of network control systems. Today, integrity modification by external attacks is a major security issue (CIA - Confidentiality Integrity Availability, Fig. 3), leading to abnormal functioning of network systems and risk for industrial plants.

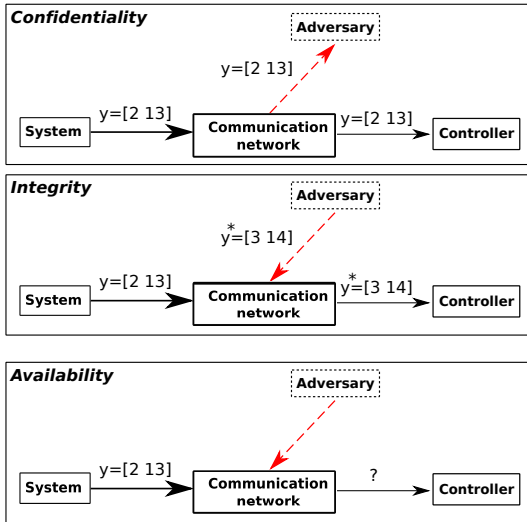


Fig. 3: Cyberattacks on a communication network [18]

Data integrity loss can cause serious consequences ([19], [20] [21]).

In this case, the output data y is modified over the communication network. The modification of the measurement is represented by a variable $\psi(t)$ added to the output:

$$y^*(t) = y(t) + \psi(t) \quad (14)$$

where $\psi(t) = 0$ when the received data is correct; otherwise, the received data has been modified by attack on the network. The value and variation of ψ is bound to the attack method [22] and [23].

Given a modification of y at each instant t , after reception of a new measurement $y(t)$ ($t = t_0$), the difference (residual) between $y(t)$ and its FMO estimation $\hat{y}(t)$ using the previous data collection $Y_L(t, T)$, $T = \{t_1, \dots, t_L\}$ is computed.

If the residual gets out of the previously set interval, a modification on measurement is detected.

Only data previously checked by the detection tool are used to guarantee the quality of prediction ($\hat{x}(t), \hat{y}(t)$).

V. NUMERICAL SIMULATIONS

In this section, the estimation-prediction accuracy of FMO in different packet loss and integrity loss scenarii is illustrated.

A. System studied

Given the following four tank system ([24], [25], [26]) (Fig. 5): the system is controlled by a decentralized LQG controller while measurement are communicated through a network.

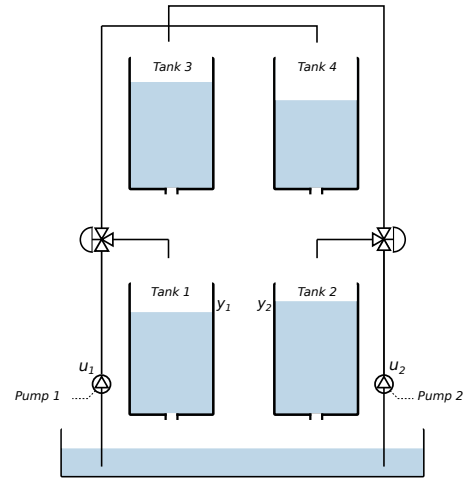


Fig. 4: Quadruple tank system

The linear state space representation of the system is given by (1):

$$\begin{cases} \dot{x}(t) = Ax(t) + Bu(t) \\ y(t) = Cx(t) + v(t) \end{cases}$$

where

$$A = \begin{pmatrix} -\frac{1}{12} & 0 & 0 \\ 0 & 0 & 1 \\ 0 & -0.05 & -0.7 \end{pmatrix}, B = \begin{pmatrix} 1 \\ 0 \\ 0.1 \end{pmatrix},$$

$$C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$$

$$y(t) = \begin{cases} y_1(t) = \text{Level in tank 1} \\ y_2(t) = \text{Level in tank 2} \end{cases}$$

$x \in \mathbb{R}^2$ is the state vector, $u \in \mathbb{R}$ the input vector, $y \in \mathbb{R}^2$ the measurement vector and $v \in \mathbb{R}^2$ the noise measurement vector with $\text{var}(v) = 0.1$. The simulation is built using a continuous time representation and the measurements are discretized at sampling time $T_s = 0.1s$.

A window length $L = 5$ FMO is placed near the controller and receives the system data from the network as does the controller (Fig. 5).

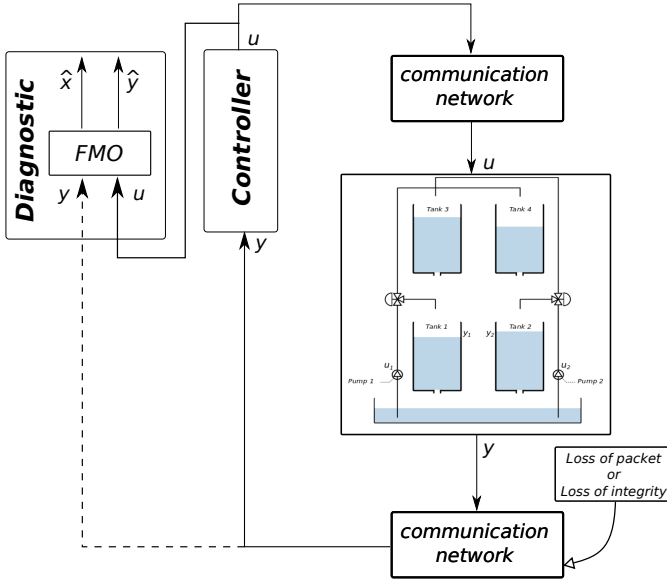


Fig. 5: Locations of FMO and controller around the quadruple tank system

B. Scenario of packet loss

First, the evolution of the FMO estimations with different packet loss behaviours is presented. Moreover, the propagation of this event corresponding to Table I is described.

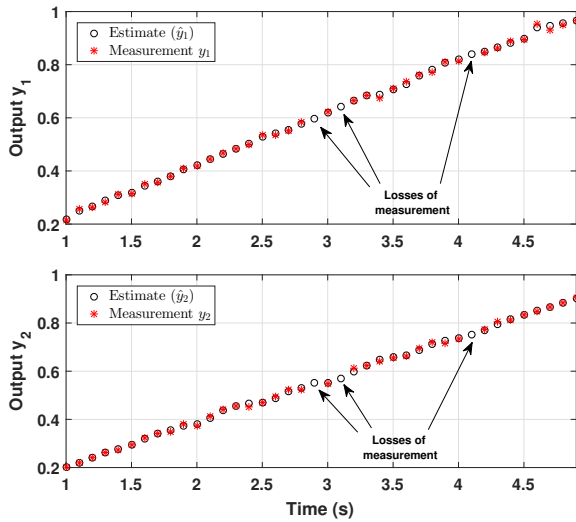


Fig. 6: Original measurement and estimation with and without packet loss

Fig. 6 shows the evolution of received measurements and their estimations. Packet losses on both measurements are observed at $t = 2.9s$, $t = 3.1s$ and $t = 4.1s$. When measurement packets are lost, the FMO tool is able to provide correct estimations and keep the system working correctly and continuously. Moreover, the FMO formulation is able to dynamically adapt its structure to realize correct estimation - prediction (Fig. 7).

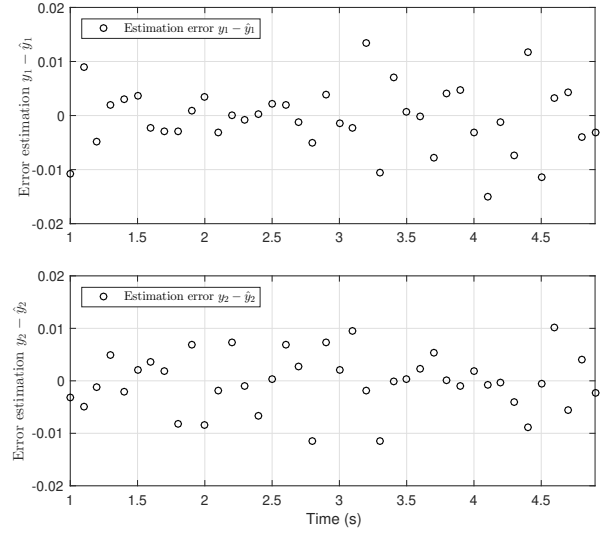


Fig. 7: Estimation error

C. Scenario of integrity loss

During the simulation a modification of output integrity occurs from $t = 1.1s$ to $t = 1.4s$

In this paper the threshold is defined as $|\hat{y}(t|T) - y(t)| > 3\sqrt{\max(\text{eig}(\Omega_L^{-1}))}$ with $\text{eig}(\Omega_L^{-1})$ the eigenvalues of Ω_L^{-1} , the received measurement $y(t)$ is considered modified, then estimated value $\hat{y}(t|T)$ replaces the received measurement.

Fig. 8 illustrates an attack on data integrity. Then, the FMO is able to detect measurement modification and compute an estimation of the attacked measurement.

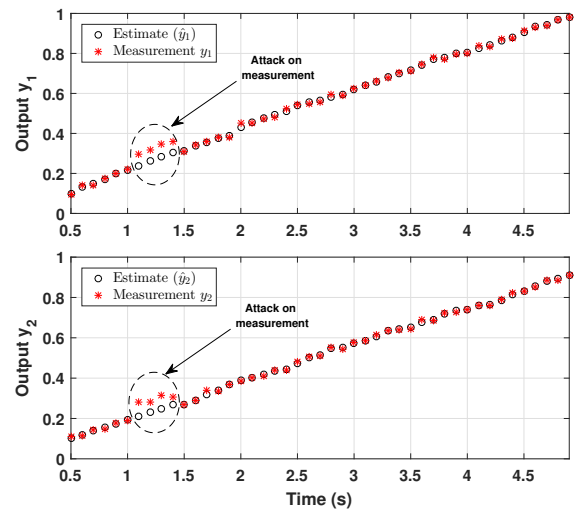


Fig. 8: Estimation error with and without packet loss

The different results presented in this section illustrate the ability of the FMO to predict data loss and modification. Moreover, the estimate error increases when a successive loss of packet happens but remains within an acceptable interval.

VI. CONCLUSIONS AND PERSPECTIVE

In this paper, a new formulation of a finite memory observer based on a finite collection of measurement is proposed to deal with packet loss and data integrity problems on network control systems.

This FMO is able to estimate and predict a system's state using an appropriate sliding window of measurements. A numerical simulation provides a correct estimation-prediction in the case of packet loss and data integrity loss. The simulation results confirm the ability of the FMO to detect the integrity and availability of data.

These two points are key aspects of the risk analysis for network control systems.

This paper confirms the efficiency of a FMO in the case of network system security breach.

Works in progress involve the computational simplification aspects and the use of this observer in real-time applications.

REFERENCES

- [1] Jungers, R. M., Kundu, A., and Heemels, W. P. M. H. Observability and Controllability Analysis of Linear Systems Subject to Data Losses. *IEEE Transactions on Automatic Control*, 2018, 63(10), 3361–3376.
- [2] Jungers, R. M., Kundu, A., and Heemels, W. P. M. H. On observability in networked control systems with packet losses. In *53rd Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, 2015, (pp. 238–243).
- [3] Sahebsara, M., Chen, T., and Shah, S. L. Optimal H_∞ filtering in networked control systems with multiple packet dropouts. *Systems and control letters*, 2008, 57(9), 696–702.
- [4] Xue, B., Li, S., and Zhu, Q. Moving horizon state estimation for networked control systems with multiple packet dropouts. *IEEE Transactions on Automatic Control*, 2012, 57(9), 2360–2366.
- [5] Schenato, L., Sinopoli, B., Franceschetti, M., Poolla, K., and Sastry, S. S. Foundations of Control and Estimation Over Lossy Networks. *Proceedings of the IEEE*, 2007, 95(1), 163–187.
- [6] Sinopoli, B., Schenato, L., Franceschetti, M., Poolla, K., Jordan, M. I., and Sastry, S. S. Kalman Filtering With Intermittent Observations. *IEEE Transactions on Automatic Control*, 2004, 49(9).
- [7] Smith, S. C., and Seiler, P. Estimation with lossy measurements: jump estimators for jump systems. *IEEE Transactions on Automatic Control*, 2003, 48(12), 2163–2171.
- [8] Bemporad, A., Heemels, M., and Johansson, M. Networked Control Systems (Vol. 406), 2010. London: Springer London.
- [9] Gommans, T. M. P., Heemels, W. P. M. H., Bauer, N. W., and Wouw, N. van de. Compensation-based control for lossy communication networks. *International Journal of Control*, 2013, 86(10), 1880–1897.
- [10] Peng, C., Han, Q.-L., Yue, D. Communication-Delay-Distribution-Dependent Decentralized Control for Large-Scale Systems With IP-Based Communication Networks. *IEEE Transactions on Control Systems Technology*, 2013, 21(3), 820–830.
- [11] Chiuso, A., Fortuna, L., Frasca, M., Rizzo, A., Schenato, L., Zampieri, S. (Eds.). (2009). Modelling, Estimation and Control of Networked Complex Systems. Berlin, Heidelberg: Springer Berlin Heidelberg.
- [12] Medvedev, A. V., and Toivonen, H. T. A Continuous Finite-Memory Deadbeat Observer. In *American Control Conference*, 1992, pp 1800–1804.
- [13] Medvedev, A. State estimation and fault detection by a bank of continuous finite-memory filters. *International Journal of Control*, 1998, 69(4), pp 499–517.
- [14] Kratz, F., Bousghiri, S., and Mourot, G. A finite memory observer structure for robust residual generation. In *Proceedings of 32nd IEEE Conference on Decision and Control*, 1997, pp 1247–1249.
- [15] Graton, G., Kratz, F., Fantini, J. Finite Memory Observers for linear time-varying systems: Theory and diagnosis applications. *Journal of the Franklin Institute*, 2014, 351(2), 785–810.
- [16] Kajdan, R., Graton, G., Aubry, D., and Kratz, F. Fault detection of a non linear switching system using finite memory observer. *IFAC Proceedings Volumes*, 2006, 39(13), 992–997.
- [17] Graton, G., Fantini, J., Kratz, F. Finite Memory Observers for linear time-varying systems. Part II: Observer and residual sensitivity. *Journal of the Franklin Institute*, 2014, 351(5), 2860–2889.
- [18] A, Teixeira., KC, Sou., H, Sandberg., KH, Johansson. Secure Control Systems: A Quantitative Risk Management Approach. *IEEE Control Systems*, 2015, 35(1), 24–45.
- [19] Pan, K., Teixeira, A. M. H., Cvetkovic, M., Palensky, P. Combined data integrity and availability attacks on state estimation in cyber-physical power grids. In *2016 IEEE International Conference on Smart Grid Communications (SmartGridComm)*, 2016, 271–277. IEEE.
- [20] Kim, T. T., Poor, H. V. Strategic Protection Against Data Injection Attacks on Power Grids. *IEEE Transactions on Smart Grid*, 2011, 2(2), 326–333.
- [21] Mo, Y., Sinopoli, B. Integrity attacks on cyber-physical systems. In *Proceedings of the 1st international conference on High Confidence Networked Systems - HiCoNS '12*, 2012, 47. New York, New York, USA: ACM Press.
- [22] Yimeng Dong, Gupta, N., Chopra, N. On content modification attacks in bilateral teleoperation systems. In *2016 American Control Conference (ACC)*, 2016, 316–321. IEEE.
- [23] Liu, Y., Ning, P., Reiter, M. K. False data injection attacks against state estimation in electric power grids. *ACM Transactions on Information and System Security*, 2011, 14(1), 1–33.
- [24] Johansson, K. H. The quadruple-tank process: a multivariable laboratory process with an adjustable zero. *IEEE Transactions on Control Systems Technology*, 200, 8(3), 456–465.
- [25] Labibi, B., Marquez, H. J., Chen, T. Decentralized robust output feedback control for control affine nonlinear interconnected systems. *Journal of Process Control*, 2009, 19(5), 865–878.
- [26] Xiong, J., Lam, J. Stabilization of Networked Control Systems With a Logic ZOH. *IEEE Transactions on Automatic Control*, 2009, 54(2), 358–363.