SENSITIVITY ANALYSIS OF THE SEQUENTIAL TEST FOR DETECTING CYBER-PHYSICAL ATTACKS

Van Long Do[*], *Lionel Fillatre*[†], *and Igor Nikiforov*[*]

[*] University of Technology of Troyes
CNRS, ICD/LM2S, UMR 6281
10004 Troyes Cedex, France

[†] University Nice Sophia Antipolis
CNRS, I3S, UMR 7271
06900 Sophia Antipolis, France

ABSTRACT

This paper deals with the problem of detecting cyber-physical attacks on Supervisory Control And Data Acquisition (SCADA) systems. The discrete-time state space model is used to describe the systems. The attacks are modeled as additive signals of short duration on both state evolution and sensor measurement equations. The steady-state Kalman filter is employed to generate the sequence of innovations. Next, these independent random variables are used as entries of the Variable Threshold Window Limited CUmulative SUM (VTWL CUSUM) test. It has been shown that the optimal choice of thresholds with respect to (w.r.t.) the transient change detection criterion leads to the Finite Moving Average (FMA) test. The main contribution of this paper is a sensitivity analysis of the FMA test. This analysis is based on a numerical calculation of the probabilities of wrong decision under the variation of operational parameters. Theoretical results are applied to the detection of an attack scenario on a SCADA water network.

Index Terms— Transient change detection, Window Limited CUSUM test, FMA test, cyber-physical attacks, SCADA systems.

1. INTRODUCTION

The SCADA systems have been playing a vital role in various safety-critical infrastructures, including electric power grids, gas pipelines and water networks [1]. Modern SCADA systems become more and more vulnerable to cyber-physical attacks, not only on the physical infrastructures but also on the communication network and the control center. The Maroochy water breach [2], the pump burnout [3] or the Stuxnet virus [4] are some examples of recent cyber incidents targeting SCADA systems.

Three approaches have been considered for studying the security of SCADA systems against cyber-physical attacks: information technology (IT) approach, secure control approach and fault detection and isolation (FDI) approach. The IT approach is concerned with the authentication, access control or message integrity. In contrast, the secure control methods focus mainly on investigating the vulnerabilities of networked control systems for designing stealthy attacks which can partially or completely bypass traditional anomaly detectors [5, 6]. The FDI approach, on the other hand, exploits the analytical redundancy of the systems to detect the attacks [7, 8]. For example, the security of water canals against cyber attacks has been considered in [9], where a bank of unknown input observers is designed to detect and isolate the attacks. A comprehensive framework has been introduced in [10] to study the attack detection and identification problem.

Previously, cyber-physical attacks are considered as an action of infinite duration. In some practical situations, however, the adversary may prefer to perform his malicious attack within a short period due to limited resources. Moreover, for safety-critical applications, it is required to detect the attacks with the detection delay upper bounded by a prescribed value. For these reasons, we formulate the detection of attacks as the problem of detecting transient changes in stochastic-dynamical systems [11].

The sequential detection of transient signals in the independent Gaussian observations has been treated in [12, 13]. The optimality criterion involves the minimization of the worst-case probability of missed detection for a given value on the worst-case probability of false alarm within any time window of predefined length. A sub-optimal algorithm w.r.t. this criterion has been introduced. Pursuing the work started in [12, 13], the authors have considered the detection of transient changes in the discrete-time state space model (see [11]). The main idea is as follows. The steady-state Kalman filter is used to generate the sequence of innovations. These innovations are used as entries of the Variable Threshold Window Limited CUmulative SUM (VTWL CUSUM) test, which has been introduced in [12, 13], to detect the transient signals. Finally, the thresholds are chosen to optimize the VTWL CUSUM test w.r.t. the criterion defined in [12,13]. It has been shown that the optimal choice of variable thresholds w.r.t. the transient change detection criterion leads to the Finite Moving Average (FMA) test (see, [11–13] for more details).

The originality of this paper w.r.t. to previous works con-

This work received financial support from French National Research Agency (ANR) through the project SCALA

978-0-9928626-3-3/15/$31.00 ©2015 IEEE

sists in proposing a numerical method for estimating the error probabilities of the FMA test and investigating the sensitivity of the FMA test w.r.t. operational parameters, including the attack duration, the attack profiles, and the noise covariance matrices. The paper is organized as follows. The problem statement is given in section 2. The Kalman filter-based detection algorithms are designed in section 3. In section 4, a numerical method of the error probabilities calculation is introduced to study the sensibility of the FMA test. Examples of SCADA system are given in section 5. Some concluding remarks and perspectives are drawn in section 6.

2. SYSTEM AND ATTACK MODELS WITH OPTIMALITY CRITERION

The following discrete-time state space model is employed in this paper to describe an industrial SCADA system:

$$\begin{cases} x_{k+1} &= Ax_k + Bu_k + Fd_k + B_a a_k + w_k \\ y_k &= Cx_k + Du_k + Gd_k + D_a a_k + v_k \end{cases}, \quad (1)$$

where $x_k \in \mathbb{R}^n$ is the vector of system states, $u_k \in \mathbb{R}^m$ is the vector of control signals, $d_k \in \mathbb{R}^q$ is the vector of disturbances, $y_k \in \mathbb{R}^p$ is the vector of measurements, $a_k \in \mathbb{R}^s$ is the vector of attack signals, $w_k \in \mathbb{R}^n$ is the vector of process noises and $v_k \in \mathbb{R}^p$ is the vector of sensor noises; the matrices $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times m}$, $F \in \mathbb{R}^{n\times q}$, $C \in \mathbb{R}^{p\times n}$, $D \in \mathbb{R}^{p\times m}$, $G \in \mathbb{R}^{p\times q}$, $B_a \in \mathbb{R}^{n\times s}$ and $D_a \in \mathbb{R}^{p\times s}$ are assumed to be known. For the sake of simplicity, the control signals u_k and the disturbances d_k are assumed to be completely known. The process noises $w_k \sim \mathcal{N}(0, Q)$ and the sensor noises $v_k \sim \mathcal{N}(0, R)$ are assumed to be independent identically distributed (i.i.d.) zero-mean Gaussian random vectors with known covariance matrices Q and R. It is assumed also that the initial states $x_0 \sim \mathcal{N}(\overline{x}_0, P_0)$, where $\overline{x}_0$ and P_0 are known.

Suppose that the attacker performs his malicious action during a short period $\tau_a = [k_0, k_0 + L - 1]$, where k_0 is the unknown attack instant and L is the known attack duration. Then, the attack vector a_k is modeled as

$$a_k = \begin{cases} 0 & \text{if } k < k_0 \\ \theta_{k-k_0+1} & \text{if } k_0 \le k < k_0 + L \\ 0 & \text{if } k \ge k_0 + L \end{cases}, \quad (2)$$

where $\theta_1, \theta_2, \cdots, \theta_L \in \mathbb{R}^s$ are known attack profiles.

With the target of detecting transient changes in stochastic-dynamical systems, we use through this paper the optimality criterion introduced in [12, 13], involving the minimization of the following worst-case probability of missed detection:

$$\inf_{T\in C_\alpha}\left\{\overline{\mathbb{P}}_{\text{md}}(T; L) = \sup_{k_0\ge L} \mathbb{P}_{k_0}(T - k_0 + 1 > L | T \ge k_0)\right\}, \quad (3)$$

among all stopping times $T \in C_\alpha$ satisfying the worst-case probability of false alarm within any time window of predefined length m_α :

$$C_\alpha = \left\{T : \overline{\mathbb{P}}_{\text{fa}}(T; m_\alpha) = \sup_{l\ge L} \mathbb{P}_0\{l \le T < l + m_\alpha\} \le \alpha\right\}. \quad (4)$$

3. TRANSIENT CHANGE DETECTION ALGORITHMS

In this section, we design the VTWL CUSUM test and the FMA test based on the sequence of innovations generated by the steady-state Kalman filter with known parameters.

3.1. Model of transient changes in Kalman filter innovations

Seeking for simplicity, suppose that the steady-state Kalman filter is employed to generate the sequence of innovations. The steady-state Kalman gain K_∞ is calculated as

$$K_\infty = P_\infty C^T \left(CP_\infty C^T + R\right)^{-1}, \quad (5)$$

where P_∞ covariance matrix can be found by solving the following discrete-time algebraic Riccati equation:

$$P_\infty = AP_\infty A^T - AP_\infty C^T \left(CP_\infty C^T + R\right)^{-1} CP_\infty A^T + Q. \quad (6)$$

As it follows from [7, 11], the innovations $\{r_k\}_{k\ge1}$ are independent Gaussian vectors with zero-mean under normal operation and with transient profiles $\phi_1, \cdots, \phi_L \in \mathbb{R}^p$ under the transient change. Let $\xi_1, \xi_2, \cdots \in \mathbb{R}^p$ be zero-mean i.i.d. Gaussian vectors satisfying $\xi_k \sim \mathcal{N}(0, J)$ where $J = CP_\infty C^T + R$. The model of the innovations is described by

$$r_k = \begin{cases} \xi_k & \text{if } k < k_0 \\ \phi_{k-k_0+1} + \xi_k & \text{if } k_0 \le k < k_0 + L \\ \tilde{\phi}_k + \xi_k & \text{if } k \ge k_0 + L \end{cases}, \quad (7)$$

where the transient profiles $\phi_1, \cdots, \phi_L \in \mathbb{R}^p$ are calculated from the attack profiles $\theta_1, \cdots, \theta_L$ (see [11]), and the latent profiles $\tilde{\phi}_k$, i.e. for $k \ge k_0 + L$, are of no interest.

Let $\mathcal{P}_{k_0}$ (resp. $\mathcal{P}_0 \triangleq \mathcal{P}_\infty$) and $\mathbb{E}_{k_0}$ (resp. $\mathbb{E}_0 \triangleq \mathbb{E}_\infty$) denote, respectively, the probability measures and the expectations when the innovations $r_1, r_2, \cdots$ follow the model (7). Let $r_{k-L+1}^k = \left[r_{k-L+1}^T, \cdots, r_k^T\right]^T \in \mathbb{R}^{Lp}$ be the concatenated vector of innovations, $\xi_{k-L+1}^k = \left[\xi_{k-L+1}^T, \cdots, \xi_k^T\right]^T \in \mathbb{R}^{Lp}$ be the concatenated vector of random noises and $\phi_{k-L+1}^k(k_0) \in \mathbb{R}^{Lp}$ be the concatenated vector of transient profiles, depending on the relative position between the change-point k_0 and the window $[k - L + 1, k]$ by the following relation:

$$\phi^k_{k-L+1}(k_0) = \begin{cases} [0]_0 & \text{if } k < k_0 \\ \begin{bmatrix} [0]_1 \\ \phi_1 \\ \vdots \\ \phi_{k-k_0+1} \end{bmatrix} & \text{if } k_0 \le k < k_0 + L \\ \tilde{\phi}^k_{k-L+1} & \text{if } k \ge k_0 + L \end{cases}, \tag{8}$$

where $[0]_0$ is the null vector of size Lp, $[0]_1$ is the null vector of size $[L-(k+k_0+1)]p$ and the post-change profiles $\tilde{\phi}^k_{k-L+1} \in \mathbb{R}^{Lp}$ are of no interest. From (7) and (9), the statistical model of r^k_{k-L+1} is described as

$$r^k_{k-L+1} \sim \mathcal{N}\left(\phi^k_{k-L+1}(k_0), \Sigma\right), \tag{9}$$

where $\Sigma = \text{diag}(J) \in \mathbb{R}^{Lp \times Lp}$ is a block-diagonal matrix formed of blocks J.

3.2. VTWL CUSUM algorithm and FMA detection rule

The stopping time T_{VTWL} of the VTWL CUSUM test, which was introduced in [11, 13], is defined as

$$T_{\text{VTWL}} = \inf\left\{k \ge L : \max_{k-L+1 \le i \le k} \left(S^k_i - h_{k-i+1}\right) \ge 0\right\}, \tag{10}$$

where $h_1, \cdots, h_L$ are chosen thresholds and S^k_i is the log-likelihood ratio (LLR) between $\mathcal{P}_i$ and $\mathcal{P}_0$, it is computed as

$$S^k_i = \left[\phi^k_{k-L+1}(i)\right]^T \left[\Sigma^{-1}\right] \left[r^k_{k-L+1} - \frac{1}{2}\phi^k_{k-L+1}(i)\right]. \tag{11}$$

The VTWL CUSUM algorithm (10)–(11) proceeds as follows. For each time index i from $k-L+1$ to k, the LLR S^k_i is calculated by (11). The LLR S^k_i is compared to each threshold h_{k-i+1} and the alarm time T_{VTWL} is raised if one of the LLRs is greater than or equal to its corresponding threshold. The thresholds $h_1, \cdots, h_L$ are considered as the tuning parameters for optimizing the VTWL CUSUM algorithm.

The optimal choice of thresholds w.r.t. the criterion (3)–(4) has been considered in [11, 13]. It has been shown that the optimized VTWL CUSUM test (10)–(11) results in the following FMA test:

$$T_{\text{FMA}}(h_L) = \inf\left\{k \ge L : S^k_{k-L+1} \ge h_L\right\}, \tag{12}$$

where the threshold h_L is chosen for assuring an acceptable level of false alarms.

4. CALCULATION OF WRONG DECISION PROBABILITIES

In this section, we propose a numerical method for calculating the probabilities $\overline{\mathbb{P}}_{\text{md}}(T_{\text{FMA}}; L)$ and $\overline{\mathbb{P}}_{\text{fa}}(T_{\text{FMA}}; m_\alpha)$ for the FMA test given (12). This method can be used to study the sensitivity of the FMA test w.r.t. the operational parameters: attack duration L, attack profiles $\theta_1, \cdots, \theta_L$, noise covariances Q and R, respectively.

4.1. Formulas for error probabilities

From [12,13], we obtain the formulas for the worst-case probability of false alarm $\overline{\mathbb{P}}_{\text{fa}}$ and the worst-case probability of missed detection $\overline{\mathbb{P}}_{\text{md}}$ of the FMA test defined in (12) as

$$\overline{\mathbb{P}}_{\text{fa}}(m_\alpha, h_L) = 1 - \mathbb{P}_0\left(\bigcap_{k=L}^{L+m_\alpha-1} \left\{S^k_{k-L+1} < h_L\right\}\right), \tag{13}$$

$$\overline{\mathbb{P}}_{\text{md}}(L, h_L) = \sup_{k_0 \ge L} \frac{\mathbb{P}_{k_0}\left(\bigcap_{k=L}^{k_0+L-1} \left\{S^k_{k-L+1} < h_L\right\}\right)}{\mathbb{P}_{k_0}\left(\bigcap_{k=L}^{k_0-1} \left\{S^k_{k-L+1} < h_L\right\}\right)}. \tag{14}$$

The computation of $\overline{\mathbb{P}}_{\text{fa}}$ and $\overline{\mathbb{P}}_{\text{md}}$ is based on the numerical method for calculating the cumulative distribution function (c.d.f.) of the multivariate normal distribution, which was proposed in [14].

4.2. Calculation of expectations and covariances

Let $\overline{L}$ be the true attack duration, $\overline{\theta}_1, \cdots, \overline{\theta}_L$ be the true attack profiles, $\overline{Q}$ and $\overline{R}$ be the true covariances of process and sensor noises, respectively. Because the system is linear and the noises are Gaussian, to get (13) and (14) it is sufficient to calculate the expectations $\mathbb{E}_0\left[S^k_{k-L+1}\right]$, $\mathbb{E}_{k_0}\left[S^k_{k-L+1}\right]$ and the covariance $\sigma_{12} = \text{cov}\left(S^{k_1}_{i_1}, S^{k_2}_{i_2}\right)$ when the true values of operational parameters (i.e. $\overline{L}$, $\overline{\theta}_1, \cdots, \overline{\theta}_L$, $\overline{Q}$ and $\overline{R}$) are different from their putative values (i.e. L, $\theta_1, \cdots, \theta_L$, Q and R).

Under the pre-change probability measure $\mathcal{P}_0$, it follows from (8)–(9) that $\mathbb{E}_0\left[r^k_{k-L+1}\right] = 0$, leading to

$$\mathbb{E}_0\left[S^k_{k-L+1}\right] = -\frac{1}{2}\left[\phi^L_1(1)\right]^T \left[\Sigma^{-1}\right] \left[\phi^L_1(1)\right]. \tag{15}$$

Under the probability measure $\mathcal{P}_{k_0}$, we have $\mathbb{E}_{k_0}\left[r^k_{k-L+1}\right] = \overline{\phi}^k_{k-L+1}(k_0)$, where the concatenated vector of true transient profiles $\overline{\phi}^k_{k-L+1}(k_0)$ is formulated in the same manner as $\phi^k_{k-L+1}(k_0)$ in (8), with the putative transient profiles $\phi_1, \cdots, \phi_L$ replaced by the true transient profiles $\overline{\phi}_1, \cdots, \overline{\phi}_L$ which depend only on true values of $\overline{L}$ and $\overline{\theta}_1, \cdots, \overline{\theta}_L$, resulting in

$$\mathbb{E}_{k_0}\left[S^k_{k-L+1}\right] = \left[\phi^L_1(1)\right]^T \left[\Sigma^{-1}\right] \left[\overline{\phi}^k_{k-L+1}(k_0) - \frac{1}{2}\phi^L_1(1)\right]. \tag{16}$$

The covariance σ_{12} between $S_{i_1}^{k_1}$ and $S_{i_2}^{k_2}$ is calculated by

$$\sigma_{12} = \left[\phi_{k_1-L+1}^{k_1}(i_1)\right]^T \left[\Sigma^{-1}\right] \left[\overline{\Sigma}_{12}\right] \left[\Sigma^{-1}\right] \left[\phi_{k_2-L+1}^{k_2}(i_2)\right],$$

where

$$\overline{\Sigma}_{12} = \mathbb{E}_0 \left[\begin{pmatrix} r_{k_1-L+1} \\ \vdots \\ r_{k_1} \end{pmatrix} \begin{pmatrix} r_{k_2-L+1}^T & \cdots & r_{k_2}^T \end{pmatrix} \right].$$

In such situations that $\overline{Q} \neq Q$ and/or $\overline{R} \neq R$, the Kalman filter is no longer optimal and the innovations are no longer independent. Hence, it is required to calculate $\mathbb{E}_0\left[r_{t_1} r_{t_2}^T\right]$, for $k_1 - L + 1 \leq t_1 \leq k_1$ and $k_2 - L + 1 \leq t_2 \leq k_2$. The calculation of $\mathbb{E}_0\left[r_k r_{k+l}^T\right]$, for $l \geq 0$, is given in Algorithm 1.

Algorithm 1 Calculation of the covariance $\mathbb{E}_0\left[r_k r_{k+l}^T\right]$.

1. Initialization: $\overline{P}_{0|-1} = P_\infty$ and $K = AK_\infty$, where K_∞ and P_∞ are given in (5)–(6).
2. Calculation of the true covariance $\overline{P}_{k+1|k}$:

$$\overline{P}_{k+1|k} = (A - KC)\,\overline{P}_{k|k-1}\,(A - KC)^T + \overline{Q} + K\overline{R}K^T.$$

3. If $(l = 0)$ then

$$\mathbb{E}_0\left[r_k r_k^T\right] = C\overline{P}_{k|k-1}C^T + \overline{R},$$

4. Else if $(l \geq 1)$ then

$$\mathbb{E}_0\left[r_{k+l} r_k^T\right] = CE_{k+l},$$

where E_{k+l} is computed recursively as

$$E_{k+l+1} = (A - KC)\,E_{k+l},$$

with initial value (i.e. $l = 1$)

$$E_{k+1} = A\overline{P}_{k|k-1}C^T - K\left(C\overline{P}_{k|k-1}C^T + \overline{R}\right).$$

5. APPLICATION AND NUMERICAL EXAMPLES

In this section, the proposed algorithms are applied to detect an attack scenario on a simple SCADA water network.

5.1. SCADA water distribution network

Consider a simple SCADA water network as shown in Fig. 1. The water network consists of two treatment plants W_1 and W_2, two reservoirs R_1 and R_2, a tank T_3, two pumps P_1 and P_2, two consumers d_1 and d_2, and several nodes and pipelines. Four pressure sensors S_1, S_2, S_3 and S_4 are equipped for measuring pressures at the reservoir R_1, at the reservoir R_2, at the tank T_3 and at the node N_4, respectively.

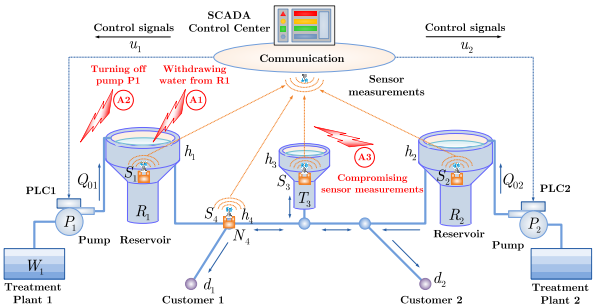


Fig. 1: The simple SCADA water distribution network.

The linearized model of the water network can be described in the discrete-time state space model (1), where $x_k = [h_1, h_2, h_3]^T \in \mathbb{R}^3$ is vector of system states; $u_k \in \mathbb{R}^2$ are the control signals sent to local controllers for regulating the flow rates Q_{01} and Q_{02} through the pump P_1 and P_2, respectively; $d_k \in \mathbb{R}^2$ are the consummation of customers; $y_k \in \mathbb{R}^4$ are the measurements of four sensors S_1, S_2, S_3 and S_4; the process noises $w_k \sim \mathcal{N}(0, Q)$ and the sensor noises $v_k \sim \mathcal{N}(0, R)$; the matrices $A \in \mathbb{R}^{3\times3}$, $B \in \mathbb{R}^{3\times2}$, $F \in \mathbb{R}^{3\times2}$, $C \in \mathbb{R}^{4\times3}$, $D \in \mathbb{R}^{4\times2}$, $G \in \mathbb{R}^{4\times2}$, $Q \in \mathbb{R}^{3\times3}$, and $R \in \mathbb{R}^{4\times4}$ (i.e. $n = 3, m = 2, p = 4, q = 2$).

For the demonstration purpose, let us consider an attack scenario where the attacker performs a coordinated attack by stealing water from the reservoir R_1, turning off the pump P_1 and compromising the measurements of sensors S_3 and S_4 during the attack period $\tau_a = [k_0, k_0 + L - 1]$, where k_0 is the unknown attack instant and L is the known attack duration. This attack scenario is motivated by a true attack on city water utility, as reported in [3]. The attack vector $a_k \in \mathbb{R}^8$ is designed by the attacker and by the covert attack strategy [6] which define matrices $B_a \in \mathbb{R}^{3\times8}$ and $D_a \in \mathbb{R}^{4\times8}$ (i.e. $s = 8$). The simulation parameters are omitted due to the paper limit.

5.2. Numerical examples

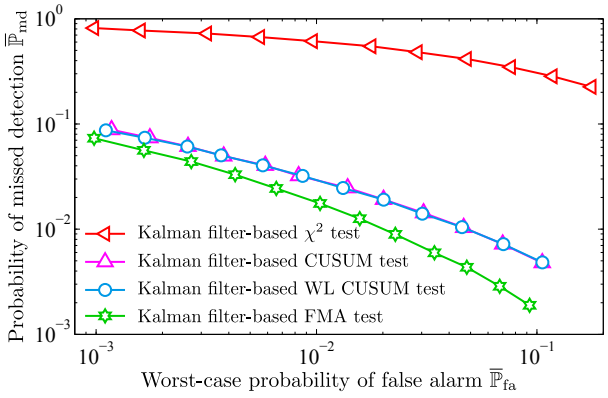
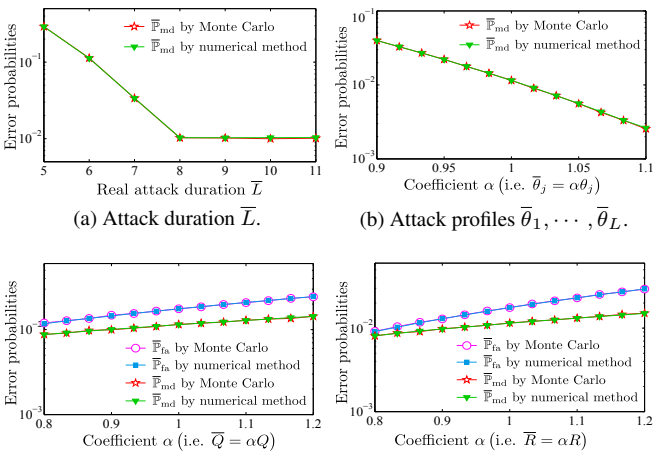


Fig. 2: Comparison between FMA test and classical tests.

Fig. 2 shows the comparison between the FMA test and three other competitors by using criterion (3) – (4). For a given value on the worst-case probability of false alarm, the worst-case probability of missed detection of the FMA test is smaller than that of the χ^2 test [5], the conventional CUSUM test and the WL CUSUM test given by (10) with the constant thresholds $h_1 = \cdots = h_L$.

The sensitivity of the FMA test w.r.t. operational parameters is shown in Fig. 3. It can be noticed that the numerical curves coincide perfectly with the Monte Carlo curves, thus validating the proposed numerical method.



(a) Attack duration $\overline{L}$. (b) Attack profiles $\overline{\theta}_1, \cdots, \overline{\theta}_L$.

(c) Process noise covariance $\overline{Q}$. (d) Sensor noise covariance $\overline{R}$.

Fig. 3: Robustness of FMA test w.r.t. operational parameters: comparison between Monte Carlo and numerical method.

It is clear that the probability of false alarm $\overline{\mathbb{P}}_{\text{fa}}$ is insensitive to both attack duration $\overline{L}$ and attack profiles $\overline{\theta}_1, \cdots, \overline{\theta}_L$. In contrast, the probability of missed detection $\overline{\mathbb{P}}_{\text{md}}$ depends heavily on these parameters. The larger the attack profiles, the smaller the probability of missed detection, as shown in Fig. 3b. The attack duration, on the other hand, impacts the probability of missed detection in a different way (see Fig 3a). For $\overline{L} \in \{5, 6, 7, 8\} \leq L = 8$, the probability of missed detection $\overline{\mathbb{P}}_{\text{md}}$ is a decreasing function of the true attack duration $\overline{L}$. However, the value of $\overline{\mathbb{P}}_{\text{md}}$ remains constant for $\overline{L} \in \{8, 9, 10, 11\} \geq L$ since any detection of attack with the delay greater than L is considered as missed.

The sensitivity of the FMA test w.r.t. the variances of random noises is presented in Fig. 3c and Fig. 3d, respectively. It can be concluded that $\overline{\mathbb{P}}_{\text{fa}}$ and $\overline{\mathbb{P}}_{\text{md}}$ are increasing functions of the multiplicative coefficient α, such that $\overline{Q} = \alpha Q$ and $\overline{R} = \alpha R$.

6. CONCLUSION

This paper has proposed a numerical method for estimating the probabilities of wrong decisions of the FMA test. This method is used to analyze the robustness of the FMA test w.r.t. some operational parameters, including the attack duration, the attack profiles, the process and sensor noise covariance matrices. This sensibility analysis is essential in evaluating the performances of the detection algorithm under the variation of the operational parameters.

REFERENCES

[1] Keith Stouffer, Joe Falco, and Karen Scarfone, "Guide to industrial control systems (ICS) security," *NIST special publication*, pp. 800–82, 2011.

[2] J. Slay and M. Miller, "Lessons learned from the maroochy water breach," *Critical Infrastructure Protection*, pp. 73–82, 2007.

[3] Kim Zetter, "Attack on city water station destroys pump," 2011, http://www.wired.com/threatlevel/2011/11/hackers-destroy-water-pump/.

[4] M. Brunner, H. Hofinger, C. Krauss, C. Roblee, P. Schoo, and S. Todt, "Infiltrating critical infrastructures with next-generation attacks," *Fraunhofer Institute for Secure Information Technology (SIT), Munich*, 2010.

[5] Y. Mo and B. Sinopoli, "Secure control against replay attacks," in *Communication, Control, and Computing, 2009. Allerton 2009. 47th Annual Allerton Conference on*. IEEE, 2009, pp. 911–918.

[6] Roy S Smith, "A decoupled feedback structure for covertly appropriating networked control systems," *Proc. IFAC World Congress*, pp. 90–95, 2011.

[7] Michèle Basseville and Igor V. Nikiforov, *Detection of abrupt changes: theory and application*, Prentice Hall Englewood Cliffs, 1993.

[8] Jie Chen and Ron J Patton, *Robust model-based fault diagnosis for dynamic systems*, Kluwer academic publishers, 1999.

[9] Saurabh Amin, *On Cyber Security for Networked Control Systems*, Ph.D. thesis, University of California Berkeley, 2011.

[10] Fabio Pasqualetti, *Secure Control Systems: A Control-Theoretic Approach to Cyber-Physical Security*, Ph.D. thesis, University of California, 2012.

[11] Van Long Do, Lionel Fillatre, and Igor Nikiforov, "Two sub-optimal algorithms for detecting cyber/physical attacks on scada systems," in *Proceedings of the X International Conference on System Identification and Control Problems (SICPRO'15)*, 2015.

[12] Blaise Kévin Guépié, Lionel Fillatre, and Igor Nikiforov, "Sequential detection of transient changes," *Sequential Analysis*, vol. 31, no. 4, pp. 528–547, 2012.

[13] Blaise Kévin Guépié, *Détection séquentielle de signaux transitoires : application à la surveillance d'un réseau d'eau potable*, Ph.D. thesis, Université de Technologie de Troyes, 2013.

[14] Alan Genz and Frank Bretz, "Comparison of methods for the computation of multivariate t-probabilities," *Journal of Computational and Graphical Statistics*, vol. 11, no. 4, pp. 950–971, 2002.