The ability to detect the linear attack of WL-CUSUM and FMA algorithms

Duc Duong Nguyen[1,2], Minh Thuy Le[1], Thanh-Long Cung[1]
[1]Department of Automation Engineering, School of Electrical and Electronic Engineering, Hanoi University of Science and Technology, Hanoi, Vietnam
[2]Department of Control and Automation Engineering, Faculty of Electrical Engineering, University of Economics–Technology for Industries, Hanoi, Vietnam

Article Info

Article history:

Received Aug 18, 2022
Revised Sep 30, 2022
Accepted Oct 19, 2022

Keywords:

Finite moving average
Kullback-Leiber
Linear attack
Weighted likelihood ratio
WL-CUSUM

ABSTRACT

The problem of detecting linear attacks on industrial systems is presented in this paper. The object is attacked by linear attack is the wireless communication process from sensors to controller with simulated mathematical model (stochastic dynamical systems and random noises). The attack matrices are calculated to ensure that Kullback-Leiber (K-L) algorithm is passed. With these matrices, the window limited cumulative SUM (WL-CUSUM) algorithm and finite moving average (FMA) algorithm are utilized to detect the changes in the sequence of residuals generated from Kalman filter method and are appreciated the ability to detect the linear attack. The simulated results show that an appropriate range of threshold of the WL-CUSUM and FMA algorithm can be chosen to detect the linear attack in case the K-L method cannot detect. Moreover, tested results using the Monte Carlo simulation also show that the evaluation performance of the FMA detection algorithm is better than that of WL-CUSUM, CUSUM, and Chi-squared (Chi2).

Corresponding Author:

Thanh Long Cung
Department of Automation Engineering, School of Electrical and Electronic Engineering
Hanoi University of Science and Technology
Dai Co-Viet street, Hai-Ba-Trung district, Hanoi, Vietnam
Email: long.cungthanh@hust.edu.vn

1. INTRODUCTION

Distributed control systems (DCS) are widely used in a lot of fields of industry, such as electric power grids, chemical factories, paper or food factories. It is very important to retain the good operation of data processing, data collection and secureing the data integrity in such systems. The operation of DCS depends on communication networks because of their geographically dispersed characteristics. So it can attack DCS at a lot of points [1]–[13]. From 2017, in [5]–[7], [10] initiated a type which changed the data transmitted from sensors to controllers in a DCS. The attack is a typical cyber/physical attack and proven to be very dangerous. Some attack detection algorithms, such as Chi-squared (Chi2) algorithm in several cases or Kullback-Leiber (K-L) algorithm in any case [5], [6] and traditional abrupt change detection algorithms can be passed. It can attack any system during a short period due to the resources limit, leading to the change in the parameter of short duration. Therefore, it is necessary to check algorithms to detect dangerous attack on short signals (transient change) before they disappear.

This paper focus on the detection of linear attack in DCS. Detecting linear attack is a kind of the fault detection and isolation (FDI) problem. FDI detects whether faults have appeared and identify the types of the faults from systems states under the affection of random noises. It consists of two steps, that is generating and evaluating residual. The residuals are first generated by using Kalman filter. These residuals, then, are evaluated by detection algorithms, such as finite moving average (FMA), window limited cumulative SUM (WL-CUSUM), CUSUM, Chi2, and fixed-size sample (FSS). These algorithms are applied in case the expectation and the variance of the system are known when occur abnormal changes. Besides, we can use weighted likelihood ratio (WLR), generalized likelihood ratio (GLR) in case the expectation and the variance of the system are unknown when there are abnormal changes. In our paper, the attacked object by linear attack is a wireless communication process from sensors to controller as shown in Figure 1.

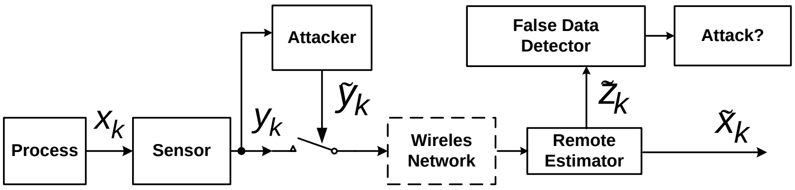


Figure 1. Diagram describing the linear attack’s position

Inherited our published research results [14], [15], in this paper we compare WL-CUSUM, FMA, CUSUM, and Chi2 algorithms on the linear attack detection ability, to confirm the effectiveness of these algorithms. The Chi2 algorithm only utilizes the data before an unusual alteration, while the data both after and before an unusual alteration is utilized by the CUSUM, WL-CUSUM, and FMA [16]. The next parts of the paper are arranged as follows: the section 2 presents a general view of the linear attack, K-L, CUSUM and Chi2 detection algorithms. WL-CUSUM and FMA detection algorithms are shown in the section 3. Discussions on application of WL-CUSUM and FMA are shown in section 4 and section 5 presents some conclusions and our future works.

2. LINEAR ATTACK, K-L, CUSUM AND CHI-SQUARED DETECTION ALGORITHMS

Perpending a DCS with the linear attack point presented in Figure 1, which impacts the wireless transmission data at the output of sensor [5]. Input signal and the relationship between input and output of the sensors can be performed as in (1) [5].

$$x_{k+1} = Ax_k + \omega_k;\ y_k = Cx_k + v_k \tag{1}$$

Where: $x_k \in \mathbb{R}^n$is the process states; $y_k \in \mathbb{R}^m$is the sensor’s output signal; $\omega_k \in \mathbb{R}^n$, $\omega_k \sim N(0, Q)$ is white noise acted on state variable; $v_k \in \mathbb{R}^m, v_k \sim N(0, R)$ is gaussian noise, white noise that acted on sensors; $R > 0$; $Q \geq 0$ are covariance matrices of white noise; $\hat{x}_k^-, \tilde{x}_k$ are estimations of the remote estimator’s state when not assaulted and having assaulted , respectively; $A \in \mathbb{R}^{nxn}, C \in \mathbb{R}^{m\times m}$ are system matrices; $\bar{P}$ is the estimation of the covariance at steady state; $k \in N$ is the index of each variable.

When having not attacked, it is easy to write the estimation of sensor output bias as in (2) [5], [17].

$$z_k = y_k - C\hat{x}_k^-;\ z_k \sim N(0; \Sigma);\ \Sigma = C\bar{P}C^T + R;\ E\left[z_i, z_j^T\right] = 0\ \forall i \neq j \tag{2}$$

Where $E\left[z_i, z_j^T\right]$ is the expected residual components z_k. When having attacked, the sensor’s output signal is modified, and be described as in (3).

$$\tilde{y}_k = \tilde{z}_k + C\tilde{x}_k^- \tag{3}$$

The K-L detection is founded on the fundamental of computing the difference between two strings of accidental values and be described as in (4)) [5], [18].

$$D(\tilde{z}_k||z_k) = \int f_{\tilde{z}_k}(\chi)\, log\frac{f_{\tilde{z}_k}(\chi)}{f_{z_k}(\chi)} d\chi \tag{4}$$

Where $f_{\tilde{z}_k}(\chi)$ and $f_{z_k}(\chi)$ are the density functions of $\tilde{z}_k$and z_k. When D is higher than a threshold δ, the data is considered as being attacked, which expressed in (5).

$$D(\tilde{z}_k||z_k) \leq \delta \rightarrow \text{not assaulted} \qquad D(\tilde{z}_k||z_k) > \delta \rightarrow \text{assaulted} \tag{5}$$

Where δ is the K-L algorithm's detection threshold.

Based on [5], through the influence of linear attack, the signals of sensor are changed into, as shown in (3) and (6).

$$\tilde{z}_k = T_k z_k + b_k \tag{6}$$

Where $T_k \in \mathbb{R}^{m\times m}$ is linear attack matrix; $b_k \sim N(0, \Gamma_k)$ is Gaussian random variable. The linear attack can pass the K-L detection test when attack matrices T_k, Γ_k can be determined and satisfied (7) [5].

$$\begin{cases} \min\limits_{(T_k)} Tr(C\bar{P}\bar{P}C^T\Sigma^{-1}T_k) \\ \begin{bmatrix} \tilde{\Sigma} & T_k \\ T_k^T & \Sigma^{-1} \end{bmatrix} \leq 0 \end{cases} ;\Gamma_k = \tilde{\Sigma}_k - T_k\Sigma T_k^T \tag{7}$$

Based on the convex plan principle of Karush-Kuhn-Tucker, the relationship of two thresholds μ and δ is expressed in (8) [5].

$$\mu\left(\frac{1}{2}Tr\left(\Sigma^{-1}\tilde{\Sigma}_k\right) - \frac{m}{2} + \frac{1}{2}log\frac{|\Sigma|}{|\tilde{\Sigma}_k|} - \delta\right) = 0 \tag{8}$$

Where $\mu > 2\min\limits_{1\leq i\leq m}\lambda_i$ and $\lambda_1, \lambda_2, \ldots, \lambda_m$ are the eigenvalues of $K^TK\Sigma$; $K$is the Kalman coefficient matrix, $Tr\left(\Sigma^{-1}\tilde{\Sigma}_k\right)$ is the matrix's trace $\Sigma^{-1}\tilde{\Sigma}_k$. So, for each value δ of the K-L algorithm, the appropriate linear attack matrices T_k, Γ_k is always found to pass the K-L test. In this case, the residuals from remote estimator (Kalman filter) can be rewritten as (9).

$$z_k \sim \begin{cases} N(0, \Sigma_0) & if\ 1 \leq k < k_0\ or\ k \geq k_0 + L, \text{when non-attacked} \\ N(0, \Sigma_1) & if\ k_0 \leq k < k_0 + L, \text{when attacked} \end{cases} \tag{9}$$

Where Σ_0, Σ_1matrices, calculated as (10).

$$\Sigma_0 = \Sigma = C\bar{P}C^T + R;\ \Sigma_1 = T_k\Sigma T_k^T + \Gamma_k \tag{10}$$

Under the influence of the linear attack, the covariance of system's residual is clearly changed. Other attacks often change the mean. It shows how the linear attack is dangerous. According to [14], [15], [19], the Chi2 algorithm is different from the K-L algorithm in that it applies the quadratic form of z_k value strings to test the significant deviation between of the error's wanted value z_k and the covariance. The Chi2 procedure is described as (11).

$$T_{CHI2} = min\left(k: \sum_{i=k-J+1}^{k} z_i^T\, \Sigma^{-1} z_i \geq h\right) \tag{11}$$

According to [19]–[22], CUSUM algorithm differs from K-L and Chi2 algorithms in that it puts the theory of Wald into sequential analysis to analyze checked data's anomalies. The CUSUM procedure is described as (12).

$$T_{CS} = min\left\{k \geq 1: \max_{1\leq i\leq k} S_i^k \geq h\right\};\ S_i^k = \sum_{t=i}^{k} ln\frac{f_{\theta_1}(x_t)}{f_{\theta_0}(x_t)} \tag{12}$$

3. WL-CUSUM AND FMA DETECTION ALGORITHMS

3.1. WL-CUSUM detection algorithm

WL-CUSUM algorithm is a special case of CUSUM algorithm. The behavior of the log-likelihood ratio (LLR) $\{S_L^k\}_{k\geq L}$ is introduced in Figure 2(a). It is easy to see that before the change point k_0 and after the change point $k_0 + L - 1$, the mean derivative of the LLR is negative, while between k_0 and $k_0 + L - 1$ it is positive. The stopping time is described as in (13) [17], [23], [24].

$$T_{WL} = min\left\{k \geq L: \max_{k-L+1\leq i\leq k} S_i^k \geq h\right\};\ S_i^k = \sum_{t=i}^{k} ln\frac{f_{\theta_1}(x_t)}{f_{\theta_0}(x_t)} \tag{13}$$

where S_i^k is the LLR, h is a chosen threshold.

Considering a system $X = [x_1, x_2, \ldots x_k]^T \sim N(\mu, \Sigma)$ and supposing that $X \sim N(\eta, \Sigma_0)$ when non-attacked, and $X \sim N(\eta, \Sigma_1)$ when attacked. This system is described in (14).

$$x_k \sim \begin{cases} N(\eta, \Sigma_0) & if\ 1 \le k < k_0\ or\ k \ge k_0 + L \\ N(\eta, \Sigma_1) & if\ k_0 \le k < k_0 + L \end{cases} \tag{14}$$

In this case, the WL CUSUM's statistic decision values g_k are calculated according to (15), (16) [17], [23]:

$$g_k = \max_{k-L+1 \le i \le k} S_i^k \ge h = \begin{cases} g_{k-1} + s_k \text{ if } g_{k-1} + s_k > 0\ and\ k \ge L \\ 0 \text{ if } g_{k-1} + s_k < 0\ or\ k < L \end{cases} \tag{15}$$

$$s_k = \frac{1}{2} ln \frac{det\,\Sigma_0}{det\,\Sigma_1} - \frac{1}{2}(x - \mu)^T [\Sigma_1^{-1} - \Sigma_0^{-1}](x - \mu) \tag{16}$$

The stopping time of WL-CUSUM test T_{WL} is satisfied (17) [20].

$$T_{WL} = min(k \ge L: g_k \ge h) \tag{17}$$

3.2. FMA detection algorithm

The FMA is an algorithm that, for each time instant $k \ge 1$, accomplishes a check between the alternative assumption *H₁* and the null assumption *H₀*, according to the block of L observations $x_{k-L+1}, \dots, x_k$ (Figure 2(b)). For the time $k + 1$, it shifts one step by erasing the last observation x_{k-L+1} and using the novel one x_{k+1} to make block of the observations $x_{k-L+2}, \dots, x_{k+1}$ [11], [12], [17], [23], [25]. The attack warning time of the FMA test is satisfied as (18).

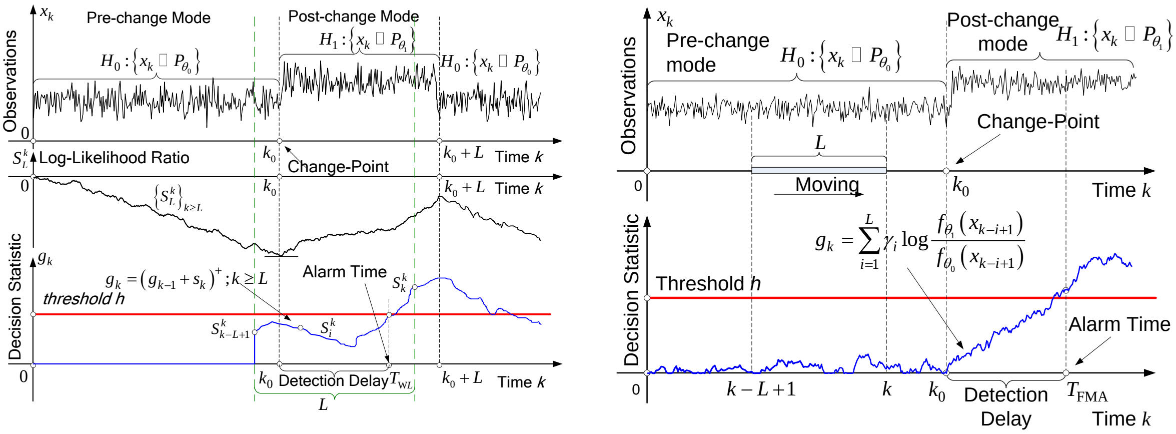
$$T_{FMA} = min\left\{k \ge L: g_k = \gamma_i \sum_{i=i}^{L} ln \frac{f_{\theta_1}(x_{k-i+1})}{f_{\theta_0}(x_{k-i+1})} \ge h\right\} \tag{18}$$

where h is a chosen threshold and $\gamma_i > 0$, for $i = 1,\dots,L$ are any weights for causal filters or predefined coefficients. Assume that coefficients $\gamma_i = \gamma$ for $i = 1,\dots,L$, we have (19).

$$g_k = \gamma \sum_{i=i}^{L} ln \frac{f_{\theta_1}(x_{k-i+1})}{f_{\theta_0}(x_{k-i+1})} = \sum_{t=k-L+1}^{k} \gamma ln \frac{f_{\theta_1}(x_t)}{f_{\theta_0}(x_t)} = \sum_{t=k-L+1}^{k} S_t^k \tag{19}$$

In the case (change in covariance) described in (12), the FMA test's g_k values are calculated by (19), (20).

$$S_t^k = \frac{1}{2}\gamma \left\{ln \frac{det\,\Sigma_0}{det\,\Sigma_1} - (x_t - \mu)^T [\Sigma_1^{-1} - \Sigma_0^{-1}](x_t - \mu)\right\} \tag{20}$$



(a) (b)

Figure 2. Describe detection procedure (a) WL-CUSUM and (b) FMA [20]

4. APPLICATION AND DISCUSSION

In this paper, to evaluate the linear attack detection ability of the FMA and WL-CUSUM algorithms, we use the same model of a MIMO system with two sensors, which has been published by Guo *et al.* [5]. Based on [5], we have the object's discrete state model in (1) with following data:

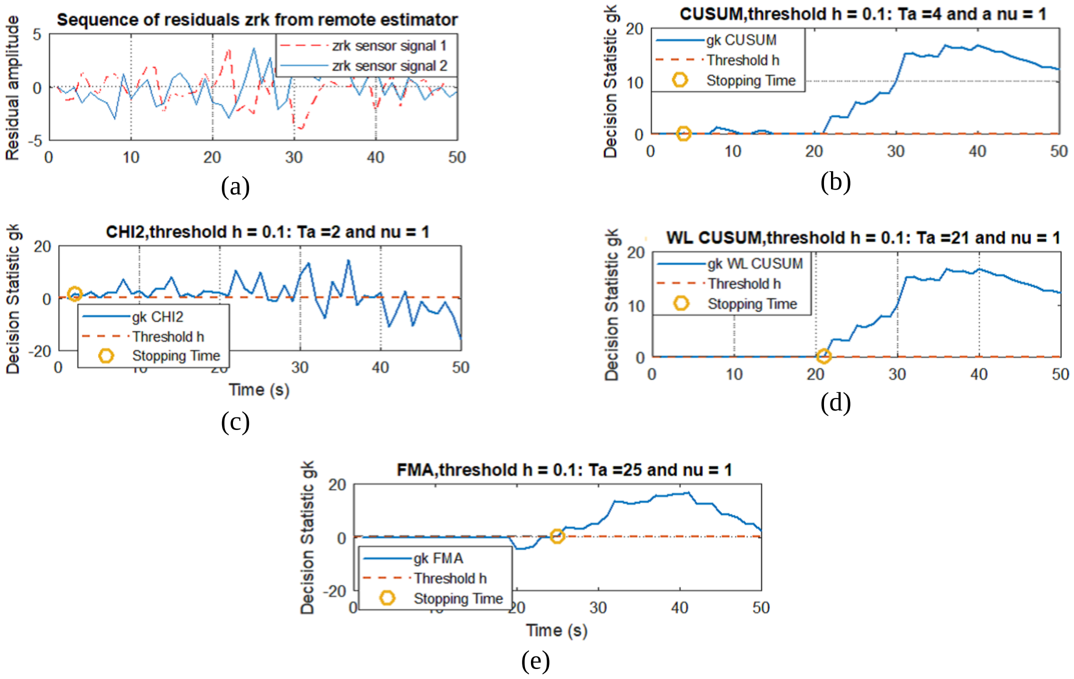
$$A = \begin{bmatrix} 0.7 & 0.2 \\ 0.05 & 0.64 \end{bmatrix}; C = \begin{bmatrix} 0.5 & -0.8 \\ 0 & 0.7 \end{bmatrix}; Q = \begin{bmatrix} 0.5 & 0 \\ 0 & 0.7 \end{bmatrix}; R = \begin{bmatrix} 1 & 0 \\ 0 & 0.8 \end{bmatrix}$$

Simulation data is used to evaluate the applicability of the algorithms. We check the possibility of the existence of threshold h, so that the two algorithms can detect attacked data, in case the K-L algorithm cannot. In (8) shows the correlation of two thresholds μ and δ in the K-L algorithm. According to the dissection in [5], [15], we choose δin the value pattern $\delta \in [0; 2.544]$.

$$\delta = \begin{cases} 0 & \equiv \delta_0 \\ 0.5 & \equiv \delta_1 \\ 1.0 & \equiv \delta_2 \\ 1.5 & \equiv \delta_3 \end{cases} \Rightarrow \mu = \begin{cases} \infty & \equiv \mu_0 \\ 1.2923 & \equiv \mu_1 \\ 1.1305 & \equiv \mu_2 \\ 1.0638 & \equiv \mu_3 \end{cases}; \delta = \begin{cases} 2.0 & \equiv \delta_4 \\ 2.5 & \equiv \delta_5 \\ 2.544 & \equiv \delta_6 \end{cases} \Rightarrow \mu = \begin{cases} 1.02627 & \equiv \mu_4 \\ 1.0019 & \equiv \mu_5 \\ 1.0 & \equiv \mu_6 \end{cases}$$

By applying MATLAB's CVX toolbox to solve (7), we obtain the linear attack's matrices $T_{k0} \div T_{k6}; \Gamma_{k0} \div \Gamma_{k6}$ so that linear attack overcomes the K-L algorithm. To appraise the materiality of FMA and WL-CUSUM (with the coefficient $\gamma = 1$), the authors perpend the circumstance of linear attack overcoming the K-L test at a small threshold $\delta = \delta_1 = 0.5$. We establish the emulation dataset (50 s) with linear attack appearing in the value pattern from 20 s to 40 s to check Chi2, CUSUM, WL-CUSUM and FMA test. At the detection threshold of these tests *h=0.1*, using (7), (8), (11), (12), (14)-(17) to compute attack's stopping time T_a, we obtained graphs that illustrated in Figure 3. Four tests are implemented on a sequence of residuals from remote estimator (Figure 3(a)). The obtained results show that the linear attack is detected by the WL-CUSUM test at $T_{WL} = 21\ s, nu = 1$, (correctly detected), (Figure 3(d)) and FMA test detected linear attack at $T_{FMA} = 25s, nu = 1$, (correctly detected), (Figure 3(e)). However, the CUSUM and Chi2 test obtain false alarm points, because they have $nu = 1$, $T_{CUSUM} = 4\ s$ (Figure 3(b)); $T_{CHI2} = 2\ s$ (Figure 3(c)) and they are not within the period of linear attack.

With threshold value *h=5.3*, the authors similarly acquire simulation graphs as shown in Figure 4. All tests are implemented on a sequence of residuals from remote estimator as indicated in the Figure 4(a). Simulation results show that FMA and CUSUM test have $T_{FMA} = 22\ s$ (Figure 4(e)), $T_{CUSUM} = 21\ s$ (Figure 4(d)), $nu = 1$, (correct detection). However, the Chi2 and WL-CUSUM have $T_{CHI2} = 4s$, (Figure 4(b)), $T_{WL} = 0, nu = 0$ (false detection) (Figure 4(c)). On the whole, to appraise linear attack detection over time interval $k_0\ k_0 + L)$ of each test, we use the worst-case probability of false alarm P_{fa}, the probability of missed detection P_{md} and correct detection probability P_d as shown in Figure 5.



(a)

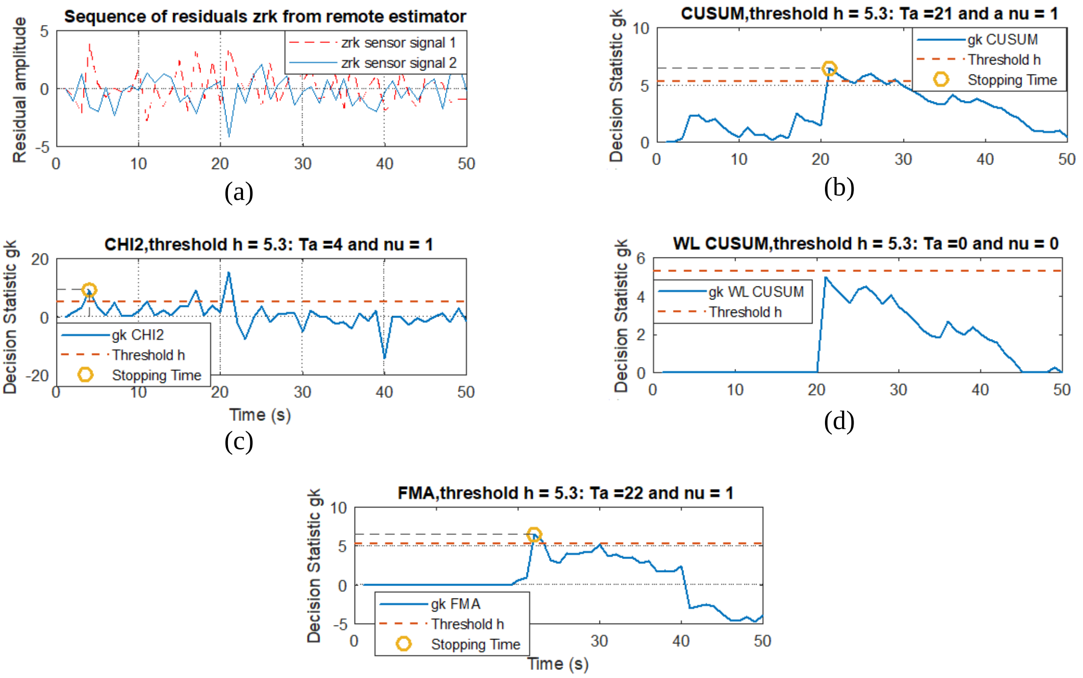
(b)

(c)

(d)

(e)

Figure 3. Linear attack detection with threshold $\delta = 0.5$ and $h = 0.1$ on (a) a sequence of residuals from remote estimator, using (b) CUSUM, (c) CHI2, (d) WL CUSUM and (e) FMA algorithms



(a) (b) (c) (d) (e)

Figure 4. Linear attack detection with threshold δ =0.5 and h=5.3 on (a) a sequence of residuals from remote estimator, using (b) CUSUM, (c) CHI2, (d) WL CUSUM and (e) FMA algorithms

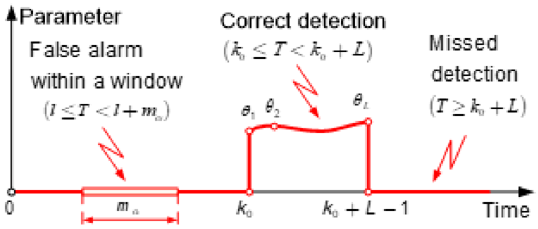


Figure 5. Transient change detection criterion [17]

"False alarm": the alteration is found before it happens $(T < k_0)$. The false alarm rate can be evaluated by P_{fa} within a time window m_α of anticipated length l and threshold α illustrated in (21) [17], [20], [23]:

$$P_{fa}(T, m_\alpha) = P_{fa} = \underset{l\geq 1}{sup} P_0[(l \leq T \leq l + m_\alpha) \leq \alpha] \qquad (21)$$

"Missed detection": the alteration is detected after its disappearance, or the change is never revealed. The missed detection rate is evaluated by the probability of missed detection illustrated in (22) [17], [20], [23]:

$$P_{md}(T, L) = P_{md} = \underset{k_0\geq L}{sup} P_{k_0}(T - k_0 + 1 > L | T \geq k_0) \qquad (22)$$

according to [16], [17], [26], the Monte-Carlo estimation of $\bar{P}_{fa}$ and $\bar{P}_{md}$ is computed as in (23):

$$\bar{P}_{fa} = \frac{1}{nS}\sum_{k=1}^{nS} nu(k), k \leq k_0;\ \bar{P}_{md} = \frac{1}{nS}\sum_{k=1}^{nS} nu(k);\ k > k_0 + L - 1 \qquad (23)$$

Graphs in Figures 6-8 show that, the linear attack overcoming K-L at thresholds δ can be detected by the Chi2, CUSUM, WL-CUSUM, and FMA algorithms (thanks to the low false alarm probability P_{fa} and low missed detection probability P_{md} of these algorithms). Secondly, Figures 7(a), 7(b), 8(a), 8(b) show that, the FMA and WL-CUSUM algorithms are much better than the traditional nonparametric Chi2 detector (under the same check situations, missed detection probability and P_{fa} of the Chi2 algorithm is larger than those of the WL-CUSUM and FMA algorithms). This issue can be explained that the Chi2 algorithm does not consider the transient change profiles of signals while the other algorithms can develop this necessity information. Thirdly, given an adequate level of P_{fa} (from 10^{-5} to 10^{0}), P_{md} of the FMA algorithm is smaller than that of the CUSUM, WL-CUSUM, Chi2 algorithms. In other words, the FMA algorithm's detection ability is more superior than detection ability of the other algorithms.

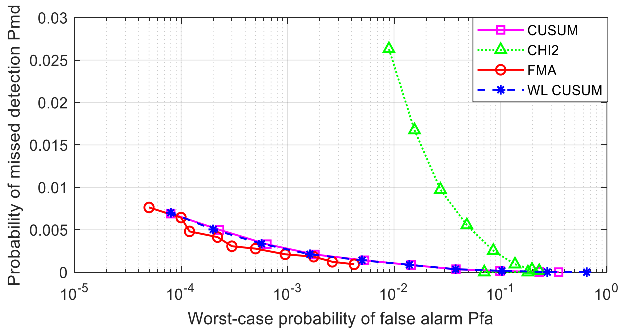
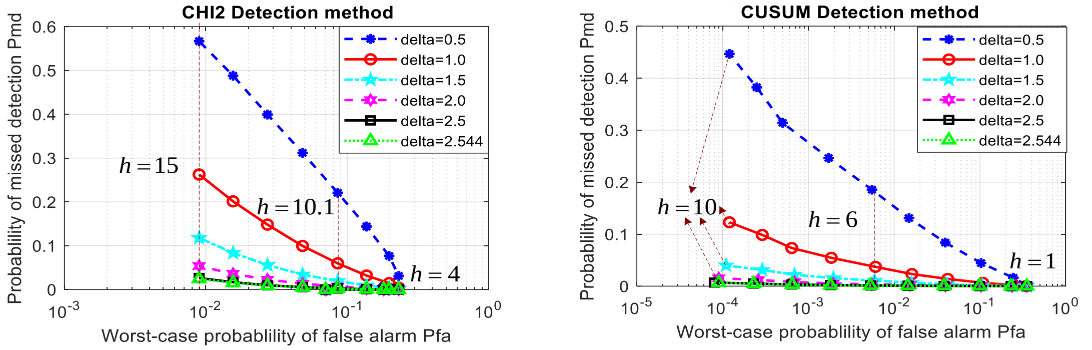
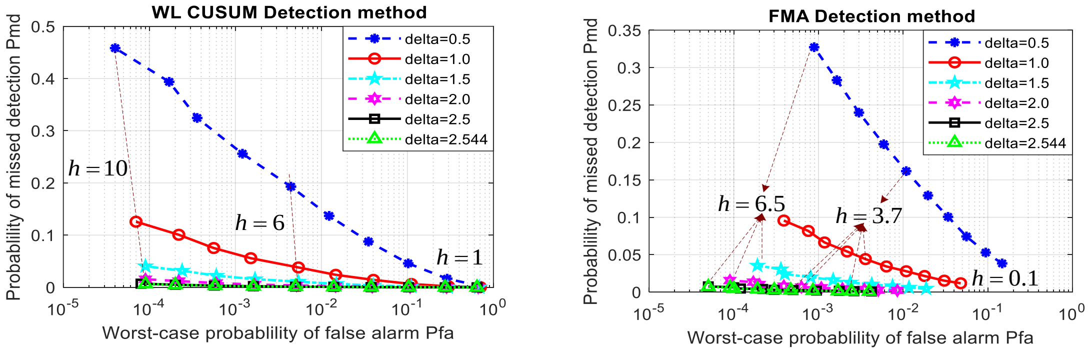


Figure 6. Statistical performance comparison among some detection algorithms with thresholds h when K-L is overcome with threshold $\delta = 2.5$ by 10^5 Monte Carlo simulation



(a) (b)

Figure 7. Statistical performance detecting linear attack with some thresholds δ (a) Chi2 detection algorithm and (b) CUSUM detection algorithm



(a) (b)

Figure 8. Statistical performance detecting linear attack test with some thresholds δ (a) WL-CUSUM detection algorithm and (b) FMA detection algorithm

Some further tests are conducted on FMA algorithm to evaluate its robustness with respect to some parameters, including the attack duration and the coefficients. The Figure 9 shows P_{md} which is presented as a function of P_{fa} for dissimilar values of true attack duration $\bar{L} = \{12, 16, 20\} \leq L = 20$, with the coefficient $\gamma = 1$. For $\bar{L} \leq L$, P_{fa} subordinates especially on the $\bar{L}$. The smaller the putative true attack duration $\bar{L}$, the higher P_{fa}. Besides, when $\bar{L}$ is reduced, P_{md} is changed. In other words, both of P_{fa} and P_{md} are sensitive to the true attack duration $\bar{L}$. The issue can be clarified by the fact that small attack duration $\bar{L}$ leads to small changes in the observable distribution, thus raising P_{fa} and changing P_{md}. With different values of coefficient $\gamma = \{0.6, 0.7, 0.8, 0.9, 1.0, 1.1, 1.2, 1.3, 1.4, 1.5\}$, when using the true attack duration $\bar{L} = L = 20$, and the threshold $\delta = 2.5$, we have results as shown in Figure 10. The probability of missed detection P_{md} is presented as a function of P_{fa} for the magnitude of change from 60% to 150% and the "shape" of the change is changed as shown in Figure 10(a). Figure 10(b) shows that error probabilities (P_{md} and P_{fa}) are presented as a function of coefficients γ. The higher the coefficient γ, the smaller the probability of missed detection P_{md} for the change of threshold h from 0.1 to 8.0 as shown in Figure 10(c). And in the same case, Figure 10(d) shows that the higher the coefficient γ, the higher the probability of false alarm P_{fa} but the changes are rather small. The issue can be clarified by the fact that small coefficients γ lead to small changes in the observable distribution, thus abating P_{md} and raising P_{fa} (with each threshold h).

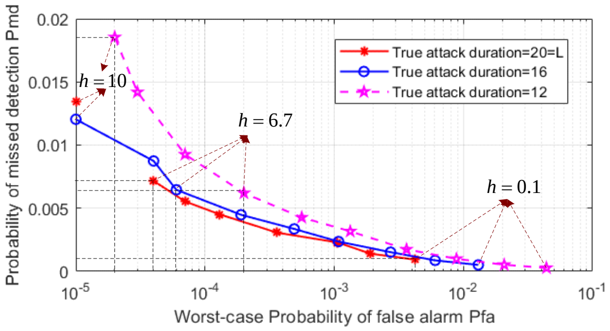
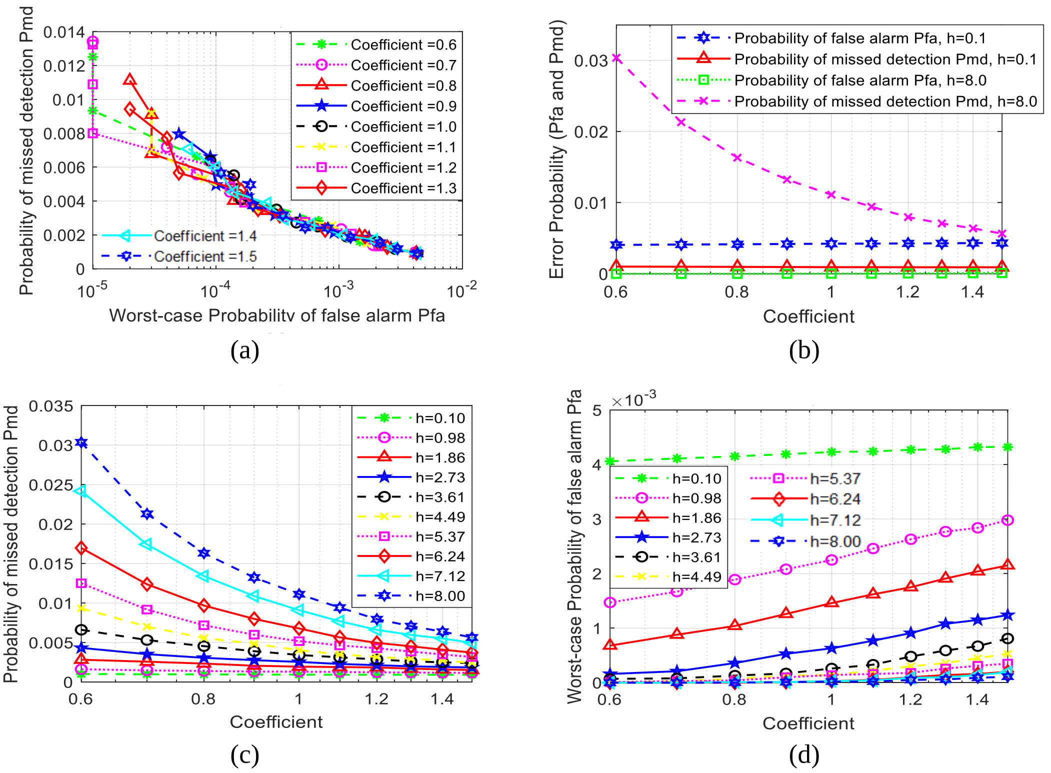


Figure 9. The FMA's sensitivity with relation to the attack duration



(a)

(b)

(c)

(d)

Figure 10. The FMA's sensitivity with relation to the coefficients, (a) Pfa_Pmd, (b) γ_Pfa and Pmd, and (c) γ_Pmd, and (d) γ_Pfa

5. CONCLUSION

This paper addresses the ability to detect the linear attack of WL-CUSUM and FMA algorithms when it passes the K–L algorithm. The tested object is described by the discrete-time state space model with unknown conditions and random noises. The traditional residual generation method (Kalman filter) is used. The WL-CUSUM and FMA algorithms use the sequence of residuals for ascertaining the stopping time at which the linear attack is detected. Simulation results on the tested object (the wireless communication process from sensors to controller) show that those algorithms outperform the traditional detectors (K-L and Chi2). These results also show that we can apply the WL-CUSUM or FMA algorithm as a back-end detection layer in a string of techniques which can be used to secure data integrity of industrial system. In addition, the analysis of simulation results also shows that the linear attack detection ability of the FMA algorithm is better than that of the Chi2, CUSUM, WL-CUSUM algorithms. The paper also analyses the influence of the coefficients and the true attack duration L to the ability to detect the linear attack of FMA algorithm. More profound mathematical research of these issues is an important perspective for the future study on the ability to detect the linear attack.

REFERENCES

[1] M. Lehto and P. Neittaanmäki, *Cyber security: Analytics, technology and automation*, vol. 78. Springer, 2015.

[2] S. East, J. Butts, M. Papa, and S. Shenoi, “A Taxonomy of Attacks on the DNP3 Protocol,” in *International Conference on Critical Infrastructure Protection*, 2009, pp. 67–81.

[3] R. L. Perez, F. Adamsky, R. Soua, and T. Engel, “Machine Learning for Reliable Network Attack Detection in SCADA Systems,” in *2018 17th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ 12th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)*, Aug. 2018, pp. 633–638. doi: 10.1109/TrustCom/BigDataSE.2018.00094.

[4] A. Hijazi, A. El Safadi, and J.-M. Flaus, “A Deep Learning Approach for Intrusion Detection System in Industry Network.,” in *BDCSIntell*, 2018, pp. 55–62.

[5] Z. Guo, D. Shi, K. H. Johansson, and L. Shi, “Worst-case stealthy innovation-based linear attack on remote state estimation,” *Automatica*, vol. 89, pp. 117–124, 2018.

[6] Z. Guo, D. Shi, K. H. Johansson, and L. Shi, “Optimal Linear Cyber-Attack on Remote State Estimation,” *IEEE Transactions on Control of Network Systems*, vol. 4, no. 1, pp. 4–13, Mar. 2017, doi: 10.1109/TCNS.2016.2570003.

[7] S. Wu, Z. Guo, D. Shi, K. H. Johansson, and L. Shi, “Optimal innovation-based deception attack on remote state estimation,” in *2017 American Control Conference (ACC)*, May 2017, pp. 3017–3022, doi: 10.23919/ACC.2017.7963410.

[8] D. Ding, Q.-L. Han, Y. Xiang, X. Ge, and X.-M. Zhang, “A survey on security control and attack detection for industrial cyber-physical systems,” *Neurocomputing*, vol. 275, pp. 1674–1683, 2018.

[9] D. -D. Nguyen, M.-T. Le, and T.-L. Cung, “Improving intrusion detection in SCADA systems using stacking ensemble of tree-based models,” *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 1, Art. no. 1, Feb. 2022, doi: 10.11591/eei.v11i1.3334.

[10] D. Ye, B. Yang, and T.-Y. Zhang, “Optimal Stealthy Linear Attack on Remote State Estimation With Side Information,” *IEEE Systems Journal*, vol. 16, no. 1, pp. 1499–1507, Mar. 2022, doi: 10.1109/JSYST.2021.3063735.

[11] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, “Revealing stealthy attacks in control systems,” in *2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Oct. 2012, pp. 1806–1813, doi: 10.1109/Allerton.2012.6483441.

[12] S. Amin, A. A. Cárdenas, and S. S. Sastry, “Safe and Secure Networked Control Systems under Denial-of-Service Attacks,” in *Hybrid Systems: Computation and Control*, Berlin, Heidelberg, 2009, pp. 31–45, doi: 10.1007/978-3-642-00602-9_3.

[13] Y. Mo and B. Sinopoli, “Secure control against replay attacks,” in *2009 47th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*, Sep. 2009, pp. 911–918. doi: 10.1109/ALLERTON.2009.5394956.

[14] N. D. Duong, M. T. Le, and T. L. Cung, “Ability to detect the linear attack in industrial control systems by CUSUM method,” *Journal of Science & Techonology Techinical Universities*, pp. 14–20, 2020.

[15] N. D. Duong, M. T. Le, and C. T. Long, “Research on the ability to detect the Linear attack of the Chi-Squared method and the CUSUM method,” *Journal of Military Science and Technology*, no. 73, Art. no. 73, Jun. 2021, Accessed: Sep. 20, 2021. [Online]. Available: https://ojs.jmst.info/index.php/jmst/article/view/50

[16] D. -D. Nguyen and M.-H. Do, “Two Methods for Detecting the Linear Attack on SCADA Systems,” in *Advances in Engineering Research and Application*, Cham, 2022, pp. 929–940, doi: 10.1007/978-3-030-92574-1_95.

[17] V. L. Do, "Sequential detection and isolation of cyber-physical attacks on SCADA systems," Troyes, 2015.

[18] S. Kullback, *Information theory and statistics*. Courier Corporation, 1997.

[19] M. S. Nikulin, “Chi-squared test for normality,” in *Proceedings of the International Vilnius Conference on Probability Theory and Mathematical Statistics*, 1973, vol. 2, no. 1, pp. 119–122.

[20] M. Basseville and I. V. Nikiforov, *Detection of abrupt changes: theory and application*, vol. 104. prentice Hall Englewood Cliffs, 1993.

[21] R. H. Woodward and P. L. Goldsmith, *Cumulative sum techniques*. Imperial Chemical Industries Limited, 1964.

[22] B. K. Guépié, L. Fillatre, and I. Nikiforov, “Detecting a Suddenly Arriving Dynamic Profile of Finite Duration,” *IEEE Transactions on Information Theory*, vol. 63, no. 5, pp. 3039–3052, May 2017, doi: 10.1109/TIT.2017.2679057.

[23] L. Fillatre and I. Nikiforov, “Two sub-optimal algorithms for detecting cyber/physical attacks on scada systems,” in *SYSTEM IDENTIFICATION AND CONTROL PROBLEMS. SICPRO’15*, 2015, pp. 1144–1156.

[24] B. K. Guépié, L. Fillatre, and I. Nikiforov, “Sequential Detection of Transient Changes,” *Sequential Analysis*, vol. 31, no. 4, pp. 528–547, Oct. 2012, doi: 10.1080/07474946.2012.719443.

[25] A. G. Tartakovsky, N. R. Berenkov, A. E. Kolessa, and I. V. Nikiforov, “Optimal Sequential Detection of Signals With Unknown Appearance and Disappearance Points in Time,” *IEEE Transactions on Signal Processing*, vol. 69, pp. 2653–2662, 2021, doi: 10.1109/TSP.2021.3071016.

[26] C. Parloir and M. Kinnaert, “Performance evaluation of fault detection algorithms by monte carlo methods,” *IFAC Proceedings Volumes*, vol. 37, no. 21, pp. 597–602, 2004.

BIOGRAPHIES OF AUTHORS

Duc Duong Nguyen received his B.Eng (2009) and M.Sc (2011) degree in Control and Automation Engineering at Hanoi University of Science and Technology. From 2009 to 2012, he worked as a researcher at Hitech center-Hanoi University of Science and Technology. Since 2013, he has been working as a lecturer at the Faculty of Electrical Engineering, University of Economics–Technology for Industries. He is being a Ph.D student in Control and Automation Engineering, at Hanoi University of Science and Technology. His main research areas are intrusion detection in industrial information systems, DCS, SCADA systems, process control, and automation of production process. He can be contacted at email: ndduong86.ddt@uneti.edu.vn.

Minh Thuy Le received her engineer (2006), M.S (2008) degree in Electrical Engineering from Hanoi University of Science and Technology and Ph.D (2013) degree in Optics and Radio Frequency from Grenoble Institute of Technology, France. She is lecturer and also a Group leader of Radio Frequency group at Department of Instrumentation and Industrial Informatics (3I), School of Electrical and Electronic Engineering (SEEE), Hanoi University of Science and Technology (HUST). Her current interests include built-in antenna, antenna array, beamforming, metamaterials, indoor localization, RF energy harvesting, wireless power transfer, and wireless sensor network. She can be contacted at email: thuy.leminh@hust.edu.vn.

Thanh Long Cung received his B.Eng degree in Measurement and Automatic Control, in 2000, and his M.Sc degree in Measurement and Control Systems, in 2002, at Hanoi University of Science and Technology, Vietnam. He received his Ph.D degree in Electronics-Electrotechnique-Automation, in 2012, at Ecole Normale Superieure Paris-Saclay, France. He is currently a researcher/lecturer at the School of Electrical and Electronic Engineering, Hanoi University of Science and Technology. His research interests include electromagnetic non-destructive testing/evaluation, human emotion recognition, sensors, and signal processing. He can be contacted at email: long.cungthanh@hust.edu.vn.