2018 European Control Conference (ECC)
June 12-15, 2018. Limassol, Cyprus

Secure estimation and attack detection in cyber-physical systems with switching attack

Dina Martynova* and Ping Zhang*

Abstract— **Cyber attacks on cyber-physical systems bring new challenges to existing methods of fault detection and fault tolerant estimation. In this paper, an approach is proposed for the secure state estimation in cyber-physical systems with switching attacks. The attack signal causes a switch in the system behaviour. We consider only two system modes, nominal mode and attacked mode. As the switching sequence is unknown, information coming from IT cybersecurity layer is used to guide the switching signal of the observer mode. The residual signal provided by the switched observer also influences the switching signal of the observer. The stability of the resulting estimation error dynamics is proven. An example is given to illustrate the advantage of the proposed approach over two other switching observer schemes.**

I. INTRODUCTION

The quality of state estimate influences the control performance. A recent trend in the process control is a change from isolated systems to fully interconnected systems. This trend makes Industrial Control Systems (ICS) similar to traditional Information Technology (IT) systems. That makes ICS vulnerable to cyber threats. After a local network is connected with global Internet, a physical access to devices on the plant is no longer a requirement to harm a system.

The ability of hackers to destroy physical equipment was demonstrated by a labour experiment in 2007 [1]. After this explicit demonstration of possible consequences of a cyber attack on ICS, a new challenge for a control society was established. A connection between cyber and physical worlds is highlighted in the new term Cyber-Physical System (CPS). The biggest difference between classic control systems and CPS is a trust in communication networks to transmit measurements and control packets, which allows the possibility of attacks against physical plants.

In the past few years, secure estimation despite a cyber attack has been considered. An estimation of a scalar state when a subset of available measurements is under adversary control can be found in [2]. The work provides the optimal estimator when the attacker can manipulate less than half of the measurements. The authors have also shown that if more than half measurements are under attack then the optimal worst-case estimator should ignore all measurements and be based solely on the apriori information of the system state distribution. The case when less than half the measurements are attacked has been also considered in [3]. The idea of the work is to combine the local estimate into a more secure state estimate by a minimization problem. An objective function characterizes the influence of the error caused by the noise and the error caused by the adversary injected bias. Secure estimation of a vector state despite an attack in the plant has been considered in [4]. The maximum number of attacks that can be detected and corrected has been provided. The number of attacked sensors is assumed to be constant. An algorithm for state estimation using a moving horizon approach during an attack was proposed in [4]. The method has been extended to scenarios in which the set of nodes under attack can change over time in [5]. The proposed approach was applied to systems subjected to a random and bounded noise in [6].

There are several ways to model a cyber attack on a CPS. A cyber attack can be modelled explicitly as manipulated control input signals or manipulated measurements, [7]. Another way to model the CPS under cyber attacks is to differentiate between nominal and attacked system modes and the attack signal caused a switch between different modes. Then the system under attack can be modelled by Markov jump systems [8] or hidden Markov models [9]. When the cyber attack is considered as a signal that changes the system dynamics from nominal to the attacked one, then the attack signal can be viewed as a switching signal that defines system mode. Nominal mode then corresponds to an attack-free case, while one or several attacked modes correspond to different attack scenarios. Such point of view brings the topic on cyber security to a well-established area of switched systems. There are papers which consider the switching sequence (the sequence that determines system mode) as an unknown parameter (see, [10]–[14]). Such works do not implicitly consider a cyber attack but still can be applied to the detection of cyber attacks.

In this work, we also consider a CPS as a hybrid system. A cyber attack induces a change in the system dynamics. The system is described by a set of different modes, one of them corresponds to the nominal system behaviour and another corresponds to a cyber attack on the system. When the cyber attack occurs, the system switches from the nominal mode to the attacked mode.

The field of computer science provides also some approaches to detect a security threat. Different Intrusion Detection Systems (IDSs) have been reviewed in [15]. Despite many differences between traditional IT cyber security and CPS security highlighted in [16], the IDS can be integrated into the control procedure. The example of such combination is given in [17]. The authors introduced overall CPS as a system with multiple layers, namely, physical layer, control layer, communication layer, network layer, supervisory layer, and management layer. The interaction between different

*The authors are with Institute for Automatic Control, University of Kaiserslautern, Kaiserslautern 67663, Germany martyn@rhrk.uni-kl.de, pzhang@eit.uni-kl.de

layers occurs due to the hybrid nature of the system. The state of the cyber system causes a structural transition in the physical part of the system.

The main contribution of this paper is to provide a state estimation method by combining two approaches, one of them is an IDS-based method, where no knowledge of system model is necessary and the other method is a residual based method, where the main idea is to evaluate the difference between measured and expected output.

The rest of the work is organized as follows: In Section II the problem is formulated, the model of the plant is described and stability of switched systems is recalled. A switched observer is described in Section III. In Section IV the proposed method is presented. Advantages of the proposed approach are shown in Section V. An illustrative example is given in Section VI. Section VII includes concluding remarks.

II. PROBLEM FORMULATION

A. Model of plant under a switching attack

The system under a cyber attack can be modelled as a switched system and the cyber attack is a switching signal that changes the system description between a nominal model and an attacked plant model, as shown in Fig. 1.

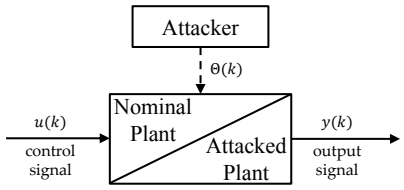

Fig. 1. Cyber attack is represented as a change of the mode in the system

Hence, a discrete-time system under switching attacks can be modelled by

$$\begin{aligned} x(k+1) &= A_{\Theta(k)}x(k) + B_{\Theta(k)}u(k) + w(k) \\ y(k) &= C_{\Theta(k)}x(k) + v(k). \end{aligned} \tag{1}$$

where k is the time index, $x(k) \in \mathbb{R}^n$ is the state vector, $u(k) \in \mathbb{R}^m$ is the control input vector, $y \in \mathbb{R}^l$ is the measured output vector, w is the process noise and v is the measurement noise. It is assumed that w and v are two mutually independent Gaussian white noises. The matrices A, B, C are appropriately dimensioned real constant matrices. $\Theta(k)$ represents the influence of the unknown attack. For the sake of clarity, we consider the system with two modes, thus, $\Theta(k) \in \{0,1\}$. $\Theta(k) = 0$ corresponds to the nominal system behaviour and $\Theta(k) = 1$ corresponds to the attacked mode.

B. Stability of switched systems

Recall now the well-known conditions for the stability of switched systems given in [18] (see Theorem 6 therein).

Lemma 1: The switched discrete-time system

$$x(k+1) = Q_{\sigma(k)}x(k),\ k \in \mathbb{Z}^+,\ Q_{\sigma(k)} \in \{Q_1, Q_2, \ldots, Q_N\}$$

with the state $x \in \mathbb{R}^n$, $Q_1 \in \mathbb{R}^{n\times n}, \ldots, Q_N \in \mathbb{R}^{n\times n}$, is asymptotically stable under arbitrary switching, if and only if there exists a finite integer m such that

$$||Q_{i_1}Q_{i_2}\cdots Q_{i_m}||_\infty < 1 \tag{2}$$

for all m-tuple $Q_{i_j} \in \{Q_1, Q_2, \ldots, Q_N\}$, where $j = 1, \ldots, m$.

C. Problem formulation

The main purpose of this paper is a secure state estimation that is able to provide a good estimate of the states despite a cyber attack on the system and cyber attack detection.

III. SWITCHED OBSERVER

A. Basic idea

For the state estimation purpose an observer can be implemented. As the plant changes its dynamic under a cyber attack, an observer should switch its parameters as well. The switching signal of the switched observer is an estimation of the unknown attack signal.

The first approach to detect a cyber attack, in other words, estimate the system mode, is to use the Intrusion Detection System (IDS) established by computer science (see [15]). Though the IDS provides some information about the mode of the system, there is no guarantee of estimation quality using this method. The IDS provides information about cyber attacks in the system by analyzing communication profiles in the network (see, for example, [19]).

Another approach to estimate the system mode is a residual based approach. The residual signal is the difference between the system output and its estimated value with respect to a system model, so the mode of the plant can be identified when the residual signal deviates from zero. The method has some limitations that will be discussed below.

The proposed approach is a combination of advantages of the above two methods.

B. IDS based switched observer

We describe a cyber attack as a kernel process $\Theta(k)$ of the hidden Markov model (HMM) and the IDS information as an observation sequence $\hat{\Theta}(k)$ of the HMM. In order to estimate the system state, an observer is used. When both the nominal system description and the attacked system description are known, a switched observer can be used. IDS signal can be considered as a switching signal of the following switched observer

$$\begin{aligned} \hat{x}(k+1) &= A_{\hat{\Theta}(k)}\hat{x}(k) + B_{\hat{\Theta}(k)}u(k) + L_{\hat{\Theta}(k)}(y(k) - \hat{y}(k)) \\ \hat{y}(k) &= C_{\hat{\Theta}(k)}\hat{x}(k) \end{aligned} \tag{3}$$

where $\hat{\Theta}(k) \in \{0,1\}$ is an attack estimate provided by the IDS, when IDS estimates the mode at time k as the nominal mode then $\hat{\Theta}(k) = 0$, when IDS estimates the mode at time k as the attacked mode then $\hat{\Theta}(k) = 1$. k is the time index, $\hat{x}(k) \in \mathbb{R}^n$ is an estimation of the state vector and $\hat{y} \in \mathbb{R}^l$ is the estimation of the output vector. Matrices L_0 and L_1 are observer feedback gain matrices of the switched observer in the nominal mode and in the attacked mode, respectively.

Fig. 2 shows the switched observer when the switching of the observer is triggered by the IDS signal.

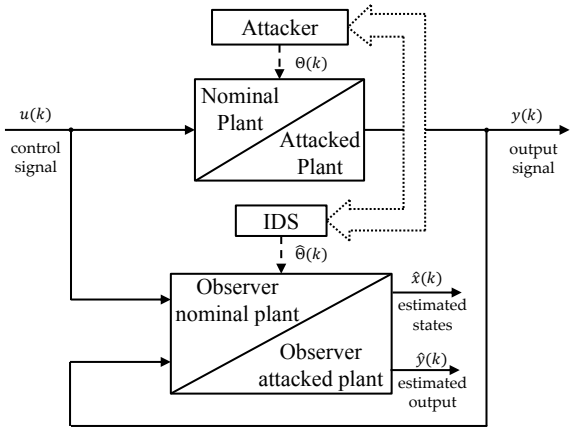

Fig. 2. Switched observer based on IDS signal

C. Residual based switched observer

Because the IDS algorithm is provided by third parties, it is difficult to know beforehand how good the detection quality would be. The main question that arises in this work whether it is it possible to improve the state estimation quality by a combination of IDS information with one that is provided by the system itself, so-called residual based estimation. Observer in each mode has a residual signal

$$r(k) = y(k) - \hat{y}(k). \tag{4}$$

The residual signal carries information about correspondence of the system mode to the current mode of the observer. The residual signal can be a basis of the residual based estimation in the idea that residual signal should be close to zero when the mode of the observer coincides with the mode of the plant. Details of such statement are evaluated by analyzing the change in the residual signal caused by a mode change.

D. Threshold to detect a cyber attack

When the residual signal (4) is used to determine which observer mode of the switched observer is now to use, the threshold for the residual signal should be calculated.

In this section we consider the system (1) without noise, i.e. $w = v = 0$, the noise will be taken into account in Section IV. Assume that an attack happens at time $k = p$ and system will change its state space representation from the nominal mode (A_0, B_0, C_0) to the attacked mode (A_1, B_1, C_1), namely

$$\begin{aligned} x(p) &= A_0 x(p-1) + B_0 u(p-1) \\ y(p-1) &= C_0 x(p-1) \end{aligned} \tag{5}$$

and

$$\begin{aligned} x(p+1) &= A_1 x(p) + B_1 u(p) \\ y(p) &= C_1 x(p), \end{aligned} \tag{6}$$

The observer, meanwhile, remains in the nominal mode, i.e.

$$\begin{aligned} \hat{x}(p) = A_0 \hat{x}(p-1) + B_0 u(p-1) + L_0 (y(p-1) - \hat{y}(p-1)) \\ \hat{y}(p-1) = C_0 \hat{x}(p-1) \end{aligned} \tag{7}$$

To show the basic idea of threshold selection, assume also that before an attack the observer state and the plant state are equal, i.e. $\hat{x}(p-1) = x(p-1)$. Then the observer output and the plant output are equal too, i.e. $\hat{y}(p-1) = y(p-1)$.

Consequently, at the moment of the attack (i.e. at the time $k = p$), the state estimate equals to the plant state $\hat{x}(p) = x(p)$.

Furthermore, two cases should be considered. Let $J_{0\to1}$ denote the threshold for the residual signal when the system changes from mode 0 to mode 1.

- If $C_1 \neq C_0$, the change from one mode to another is immediately visible and the threshold $J_{0\to1}$ at time $k = p$ is set to

$$J_{0\to1}(p) = y(p) - \hat{y}(p) = (C_1 - C_0)\hat{x}(p). \tag{8}$$

- If $C_1 = C_0$, the fluctuation in the residual signal caused by changing mode is not immediately visible and can be visible only at the next step $k = p+1$. The threshold $J_{0\to1}$ at time $k = p+1$ is set to

$$\begin{aligned} J_{0\to1}(p+1) = y(p+1) - \hat{y}(p+1) = \\ C((A_1 - A_0)\hat{x}(p) + (B_1 - B_0)u(p)) \end{aligned} \tag{9}$$

$J_{1\to0}$ can be calculated in a similar manner. When $J_{0\to1}(p) \neq 0$ this value can be immediately used in the cyber attack detection algorithm, but if $J_{0\to1}(p) = 0$ as in the case when $C_1 = C_0$, the next value should be calculated and if it is not zero, it can be used to detect change from one mode to another.

Equation (9) shows the dependence on the threshold of the control signal $u(k)$. For example, if $(B_1 - B_0)u(p) = (A_0 - A_1)\hat{x}(p)$, then $J_{0\to1}(p+1) = 0$ and can not provide any useful information.

To overcome this disadvantage, the approach proposed in this paper combines both methods, IDS based as well as residual based switched observer.

IV. The proposed approach

In this section, an approach is proposed to combine the information of the IDS with the residual based method. To show the basic idea, we describe an algorithm of the proposed approach for the case when $C_1 = C_0$.

A. Algorithm of the proposed approach

Let $\hat{\Theta}(k)$ be the IDS signal and $\bar{\hat{\Theta}}(k)$ be the attack estimation got by proposed approach.

Given the plant model (1), the improved observer is described by the following algorithm.

Algorithm 1:

Step 1 Initialize $\hat{x}(k)$ and let $k = 0$.

Step 2 Calculate an estimated output for the current time k by

$$\hat{y}(k) = C_{\hat{\Theta}(k)} \hat{x}(k) \tag{10}$$

Note that the estimated output $\hat{y}(k)$ at time k depends indeed on the state $\hat{x}(k)$ that got in the previous step at time $k-1$.

Step 3 Calculate the residual signal $r(k)$ by (4).

Step 4 Compare the amplitude of the residual signal $r(k)$ with the amplitude of the residual signal on a previous step $r(k-1)$. If $|r(k)| > |r(k-1)| + \delta$, where

δ is a noise dependent uncertainty, then it could be concluded that the IDS signal does not coincide with the attack signal on the previous step, i.e. $\hat{\Theta}(k-1) \neq \Theta(k-1)$. The attack estimation signal, provided by proposed approach, $\bar{\hat{\Theta}}(k-1)$ could be estimated by minimizing the distance between the residual signal and thresholds of different modes

$$\bar{\hat{\Theta}}(k-1) = arg \min_{j=\{0,1\}} |r(k) - J_{\bar{\hat{\Theta}}(k-2)\to j}| \quad (11)$$

where j is the system mode at time $k-1$ and $\bar{\hat{\Theta}}(k-2)$ is the estimate of the system mode at $k-2$ got by proposed approach, $J_{0\to1}$ and $J_{1\to0}$ are given in Section III.D, $J_{0\to0} = J_{1\to1} = 0$. As will be shown at Step 6, the state estimate $\hat{x}(k)$ is calculated using the information of the IDS signal at the previous step. When the value of $\bar{\hat{\Theta}}(k-1)$ is different from $\hat{\Theta}(k-1)$, the state estimate at time k should be recalculated using the information of $\bar{\hat{\Theta}}(k-1)$. With the new value of $\hat{x}(k)$, a new estimate $\hat{y}(k)$ is also recalculated, i.e.

$$\begin{aligned}\hat{x}(k) = &A_{\bar{\hat{\Theta}}(k-1)}\hat{x}(k-1) + B_{\bar{\hat{\Theta}}(k-1)}u(k-1) + \\ &L_{\bar{\hat{\Theta}}(k-1)}(y(k-1) - \hat{y}(k-1)) \\ \hat{y}(k) = &C_{\bar{\hat{\Theta}}(k)}\hat{x}(k)\end{aligned} \quad (12)$$

Step 5 Calculate the estimated state $\hat{x}(k+1)$ at the next time point by

$$\hat{x}(k+1) = A_{\hat{\Theta}(k)}\hat{x}(k) + B_{\hat{\Theta}(k)}u(k) + L_{\hat{\Theta}(k)}(y(k) - \hat{y}(k)) \quad (13)$$

Step 6 Let $k = k+1$ and go to Step 2.

A schematic description of the algorithm is given in Fig. 3.

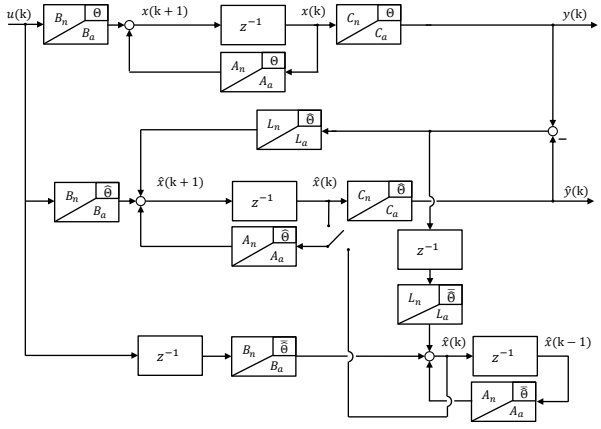

Fig. 3. Model of the switched observer when a switching signal is based on the proposed scheme

B. Selection of observer gains

To select observer gains of the switched observer in the proposed approach, the switched observer (3) can be analyzed. The stability condition of switched systems, introduced in Lemma 1, is given for arbitrary switching and switched observer of the proposed approach is actually the switched observer (3) with improved switching.

For the switched system (1) and the switched observer (3) a new variable is introduced

$$\bar{e}(k) = \begin{bmatrix} e(k) \\ x(k) \end{bmatrix} \quad (14)$$

The dynamic of the whole system would be

$$\bar{e}(k+1) = M_{\Theta(k),\bar{\hat{\Theta}}}\bar{e}(k) + \begin{bmatrix} B_{\Theta(k)} - B_{\bar{\hat{\Theta}}} \\ B_{\Theta(k)} \end{bmatrix} u(k) \quad (15)$$

where

$$M_{\Theta(k),\bar{\hat{\Theta}}} = \begin{bmatrix} A_{\bar{\hat{\Theta}}} - L_{\bar{\hat{\Theta}}}C_{\bar{\hat{\Theta}}} & A_{\Theta(k)} - A_{\bar{\hat{\Theta}}} - L_{\bar{\hat{\Theta}}}C_{\Theta(k)} + L_{\bar{\hat{\Theta}}}C_{\bar{\hat{\Theta}}} \\ 0 & A_{\Theta(k)} \end{bmatrix} \quad (16)$$

The error dynamic (15) has overall 4 possibilities under different values of $\Theta(k)$ and $\bar{\hat{\Theta}}$, as we consider a system with only two modes.

Now two observer gain matrices L_0 and L_1 should be selected for (3). The observer gains should be designed in such a way that (2) is satisfied for some m, where $Q_{\sigma(k)} = M_{\Theta(k),\bar{\hat{\Theta}}(k)}$, $Q_1 = M_{\Theta=0,\bar{\hat{\Theta}}=0}$, $Q_2 = M_{\Theta=0,\bar{\hat{\Theta}}=1}$, $Q_3 = M_{\Theta=1,\bar{\hat{\Theta}}=0}$, $Q_4 = M_{\Theta=1,\bar{\hat{\Theta}}=1}$, namely

$$\begin{aligned} Q_1 &= \begin{bmatrix} A_0 - L_0C_0 & 0 \\ 0 & A_0 \end{bmatrix} \\ Q_2 &= \begin{bmatrix} A_1 - L_1C_1 & A_0 - A_1 - L_1C_0 + L_1C_1 \\ 0 & A_0 \end{bmatrix} \\ Q_3 &= \begin{bmatrix} A_0 - L_0C_0 & A_1 - A_0 - L_0C_1 + L_0C_0 \\ 0 & A_1 \end{bmatrix} \\ Q_4 &= \begin{bmatrix} A_1 - L_1C_1 & 0 \\ 0 & A_1 \end{bmatrix} \end{aligned} \quad (17)$$

V. Advantages of proposed approach

A. Mode observability of switched systems

With an example from [20] one can see that two observable systems can give an unobservable switched system. Consider the one-dimensional linear system (1) with $\Theta(k) = \{1,2\}$, $n=1$, and $A_1 = A_2 = 0$, $B_1 = B_2 = 0$, and $C_1 = c_1 \neq 0$ $C_2 = c_2 \neq 0$, where $c_1 \neq c_2$. One can see that the initial state of each subsystem is observable, nevertheless, the initial state x_0 of subsystem one is indistinguishable with the initial state c_1x_0/c_2 of subsystem two.

Several works have already defined observability for a switched system (see [12], [21] and citations therein). There are several different kinds of observability in switched systems:

- observability of the initial state,
- observability of the current state,
- switching time observability,
- mode observability.

In the following, the switching time observability will be considered. Actually, the object of the interest is to detect system mode, but for a case with two modes, the detection of the switching time always implies the detection

of mode, when the initial mode is known. Since switch time observability usually more relaxed, switch time observability would be considered.

The purpose of this section is to check when the switching time of the switched system could not be detected, in other words, which condition a switched system with two modes should satisfy so that its modes would be detectable in principle.

Before introducing a condition for observability recall the description of the system dynamics on a moving window that described by

$$y^{[\nu]}(k) = \mathscr{O}^{[\nu]} x(k-\nu) + \Gamma^{[\nu]} u^{[\nu]}(k) \tag{18}$$

where ν is the length of a moving window, and $\mathscr{O}^{[\nu]}$, $\Gamma^{[\nu]}$ are the correspondent matrices.

In [12] and [21] it is stated that the switched system (1) is switching time observable iff

$$rank\left[\mathscr{O}_i^{[2n]} - \mathscr{O}_j^{[2n]}\right] = n \tag{19}$$

and strong switching time observable iff

$$rank\begin{bmatrix}\mathscr{O}_i^{[2n]} - \mathscr{O}_j^{[2n]} & \Gamma_i^{[2n]} - \Gamma_j^{[2n]}\end{bmatrix} = n + rank(\Gamma_i^{[2n]} - \Gamma_j^{[2n]}) \tag{20}$$

where i and j represent different system modes and n is the system order.

To sum up, the residual signal can distinguish between two modes in the system (1) when the system satisfies (19). Moreover, the residual signal can distinguish between two modes for any control signal if the system satisfies (20). In other words, when the system satisfies (19) but does not satisfy (20), the switched observer with a switching signal based solely on the residual signal can not guarantee mode detectability for all possible control signals.

VI. EXAMPLE

An example is given in this section to illustrate the proposed approach. The switched observer got by the proposed approach is compared with the switched observer based only on IDS and the switched observer based on the residual signal.

The plant (1) is characterized by the matrices

$$A_0 = \begin{bmatrix}0.9050 & 0.0160\\ 0.0160 & 0.7048\end{bmatrix}, \quad A_1 = \begin{bmatrix}0.9050 & 0.0187\\ 0.0187 & 0.9706\end{bmatrix} \tag{21}$$

$$B_0 = \begin{bmatrix}0.0479\\ 0.0342\end{bmatrix}, \quad B_1 = \begin{bmatrix}0.0480\\ 0.0399\end{bmatrix}, \quad C_0 = C_1 = \begin{bmatrix}1 & 1\end{bmatrix}$$

The noise is generated as a zero mean Gaussian random variable with variance equal 0.05.

As the poles of the nominal plant are

$$eig(A_0) = \{0.9063,\ 0.7036\} \tag{22}$$

The observer gain is determined by the pole placement with

$$eig(A_0 - L_0 C) = \{0.4185,\ 0.6479\} \tag{23}$$

and the resulting observer gain is

$$L_0 = \begin{bmatrix}0.5827\\ -0.0393\end{bmatrix} \tag{24}$$

The poles of the plant in the attacked mode are

$$eig(A_1) = \{0.9000,\ 0.9756\} \tag{25}$$

so, the system is becoming slower and the proper observer gain is determined by the pole placement with

$$eig(A_1 - L_1 C) = \{0.8392,\ 0.7552\} \tag{26}$$

and the resulting observer gain is

$$L_1 = \begin{bmatrix}-0.0754\\ 0.3567\end{bmatrix} \tag{27}$$

It can be shown that chosen L_0 and L_1 satisfies (2) for $m = 9$ which confirms stability of the estimation error under arbitrary switching sequence.

In the simulation, the attack signal is generated as a Markov process with the state transition matrix

$$P = \begin{bmatrix}0.8 & 0.2\\ 0.1 & 0.9\end{bmatrix} \tag{28}$$

and the initial state

$$\Theta(0) = \begin{bmatrix}1\\ 0\end{bmatrix} \tag{29}$$

Note that the system (1) with coefficient matrices (21) satisfies (19) but does not satisfy (20). That means that the system is switching time observable, but not strong observable. This is because the system's transfer function has zeros and for some values of control signal the output can be equal to zero when the state vector is not a zero vector. As it was shown before for some values $u(k)$ thresholds from (9) could be equal to zero, that would make the residual based observer impossible to distinguish between system modes.

Fig. 4 shows control input u and system output y.

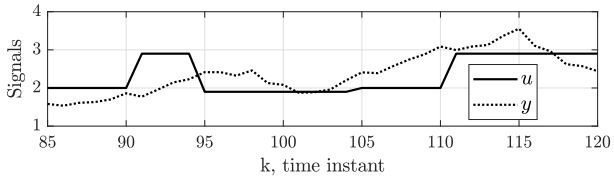

Fig. 4. Residual signals r for different estimation methods

Fig. 5 shows residual signals r provided by different estimation methods, namely the proposed switched observer given in Algorithm 1, the IDS based observer described in Section III.B, and the residual based switched observer. The residual based switched observer is got by the proposed approach, assuming the IDS signal is not available (i.e. $\hat{\Theta}(k) = 0$).

Fig. 6 shows the real attack signal and the estimated attack got by different methods. The attack signal is a binary signal and has only two values with 0 representing the nominal mode and 1 representing the attacked mode. Signals are spread over Signal axes for illustrative purposes. Table I gives the state estimation error $x - \hat{x}$ and the attack estimation error $\Theta - \hat{\Theta}$ evaluated by the l_2-norm for these three methods.

Both Fig. 4-6 and Table I show the better performance of the proposed approach over the other two methods.

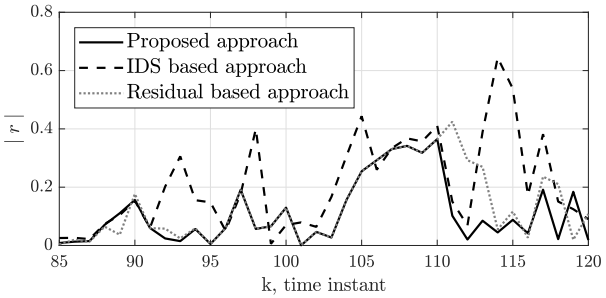

Fig. 5. State estimation error of the observers

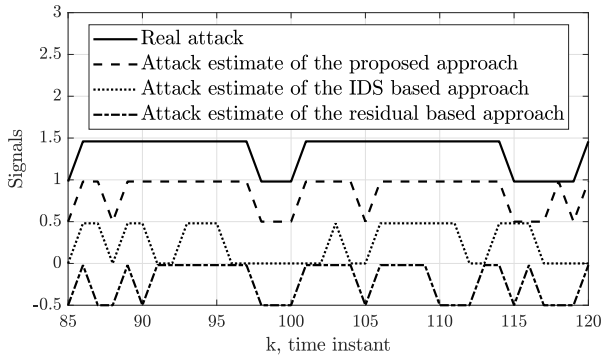

Fig. 6. Attack signal estimation for different methods

VII. CONCLUSIONS

Detection of cyber attacks in CPS can be carried out on two layers: IT level and application level. This paper proposes a method to combine two approaches working on different layers. A cyber attack is considered as a switching signal and the plant is described by a switched system. One mode of the system corresponds to the nominal plant behaviour without any attacks. Other modes correspond to the plant under switching attack. An attack estimation method working on the IT level is called an intrusion detection system (IDS) and decides about a presence of an attack by analyzing communication profiles of the data transmitted over the network. The proposed approach combines information coming from the IDS with a residual based observer. Such a policy is able to detect a cyber attack in different cases, for example, the residual based observer is unable to detect a cyber attack in the case of the unobservable switching signal and the IDS is not able to detect a malicious behaviour when an adversary is an approved system user. The proposed approach takes advantages of both methods. As shown in the simulation example, the performance of state estimation and attack detection has been improved. The proposed secure estimation algorithm can be extended to handle CPS under switching attacks with multiple attacked modes.

TABLE I

COMPARISON OF METHODS

	Proposed approach	IDS based approach	Residual based
Attack estimation error $\|\|\Theta-\hat{\Theta}\|\|_2$	10	15.6	12.6
State estimation error $\|\|x-\hat{x}\|\|_2$	5.9	16.9	7.1

REFERENCES

[1] M. Zeller, "Myth or reality - does the aurora vulnerability pose a risk to my generator?" *Proc. of the* 64^{th} *Annual Conference for Protective Relay Engineers*, pp. 130–136, 2011.

[2] Y. Mo and B. Sinopoli, "Secure estimation in the presence of integrity attacks," *IEEE Trans. on Automatic Control*, vol. 60, no. 4, pp. 1145–1151, 2015.

[3] Y. Mo and E. Garone, "Secure dynamic state estimation via local estimators," *Proc. of the* 55^{th} *IEEE Conference on Decision and Control, Las Vegas, USA*, pp. 5073–5078, 2016.

[4] H. Fawzi, P. Tabuada, and S. Diggavi, "Secure estimation and control for cyber-physical systems under adversarial attacks," *IEEE Trans. on Automatic Control*, vol. 59, no. 6, pp. 1454–1467, 2014.

[5] Y. H. Chang, Q. Hu, and C. J. Tomlin, "Secure estimation based kalman filter for cyber-physical systems against adversarial attacks," *arXiv:1512.03853v2*, 2015.

[6] M. Pajic, P. Tabuada, I. Lee, and G. J. Pappas, "Attack-resilient state estimation in the presence of noise," *Proc. of the* 54^{th} *IEEE Conference on Decision and Control, Osaka, Japan*, pp. 5827–5832, 2015.

[7] A. Teixeira, I. Shames, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries," *Automatica*, vol. 51, pp. 135–148, 2015.

[8] N. Forti, G. Battistelli, L. Chisci, and B. Sinopoli, "Secure state estimation of cyber-physical systems under switching attacks," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 4979–4986, 2017.

[9] D. Shi, R. J. Elliott, and T. Chen, "On finite-state stochastic modeling and secure estimation of cyber-physical systems," *IEEE Trans. on Automatic Control*, vol. 62, no. 1, pp. 65–80, 2016.

[10] A. Alessandri, M. Baglietto, and G. Battistelli, "Luenberger observers for switching discrete-time linear systems," *International Journal of Control*, vol. 80, no. 12, pp. 1931–1943, 2007.

[11] M. Baglietto, G. Battistelli, and L. Scardovi, "Active mode observability of switching linear systems," *Automatica*, vol. 43, no. 8, pp. 1442–1449, 2007.

[12] E. Elhamifar, M. Petreczky, and R. Vidal, "Rank tests for the observability of discrete-time jump linear systems with inputs," *Proc. of the 2009 American Control Conference*, pp. 3025–3032, 2009.

[13] A. Alessandri, M. Baglietto, and G. Battistelli, "A maximum-likelihood kalman filter for switching discrete-time linear systems," *Automatica*, vol. 46, no. 11, pp. 1870–1876, 2010.

[14] M. Baglietto, G. Battistelli, and P. Tesi, "Stabilization and tracking for switching linear systems under unknown switching sequences," *Systems and Control Letters*, vol. 62, no. 1, pp. 11–21, 2013.

[15] H.-J. Liao, C.-H. R. Lin, Y.-C. Lin, and K.-Y. Tung, "Intrusion detection system: A comprehensive review," *Network and Computer Applications*, vol. 36, no. 1, pp. 16–24, 2013.

[16] A. A. Cárdenas, S. Amin, and S. Sastry, "Research challenges for the security of control systems," *Proc. of the* 3^{rd} *conference on Hot topics in security, HotSec*, pp. 1–6, 2008.

[17] Q. Zhu and T. Başar, "Robust and resilient control design for cyber-physical systems with an application to power systems," *Proc. of the* 50^{th} *IEEE Conference on Decision and Control and European Control Conference*, pp. 4066–4071, 2011.

[18] H. Lin and P. J. Antsaklis, "Stability and stabilizability of switched linear systems: A survey of recent results," *IEEE Trans. on Automatic Control*, vol. 54, no. 2, 2009.

[19] A. Terai, S. Abe, S. Kojima, Y. Takano, and I. Koshijima, "Cyber-attack detection for industrial control system monitoring with support vector machine based on communication profile," *IEEE European Symposium on Security and Privacy Workshops*, 2017.

[20] R. Vidal, A. Chiuso, S. Soatto, and S. Sastry, "Observability of linear hybrid systems," *International Workshop on Hybrid Systems: Computation and Control*, pp. 626–539, 2003.

[21] F. Küsters and S. Trenn, "Switch observability for switched linear systems," *Automatica*, vol. 87, pp. 121–127, 2018.