Kybernetika

Yabing Huang; Jun Zhao

Switched Stackelberg game analysis of false data injection attacks on networked control systems

Kybernetika, Vol. 56 (2020), No. 2, 261–277

Persistent URL: `http://dml.cz/dmlcz/148300`

SWITCHED STACKELBERG GAME ANALYSIS OF FALSE DATA INJECTION ATTACKS ON NETWORKED CONTROL SYSTEMS

Yabing Huang, Jun Zhao

This paper is concerned with a security problem for a discrete-time linear networked control system of switched dynamics. The control sequence generated by a remotely located controller is transmitted over a vulnerable communication network, where the control input may be corrupted by false data injection attacks launched by a malicious adversary. Two partially conflicted cost functions are constructed as the quantitative guidelines for both the controller and the attacker, after which a switched Stackelberg game framework is proposed to analyze the interdependent decision-making processes. A receding-horizon switched Stackelberg strategy for the controller is derived subsequently, which, together with the corresponding best response of the attacker, constitutes the switched Stackelberg equilibrium. Furthermore, the asymptotic stability of the closed-loop system under the switched Stackelberg equilibrium is guaranteed if the switching signal exhibits a certain average dwell time. Finally, a numerical example is provided to illustrate the effectiveness of the proposed method in this paper.

Keywords: networked control systems, false data injection attacks, switched systems, switched Stackelberg games, switched Stackelberg equilibrium

Classification: 91A50, 91A65, 91A80

1. INTRODUCTION

The recent advances of sensing, wireless communication, and computing technologies have boosted the emergence of networked control systems, where the communication network acts as the transmission medium of information flows among various system components including sensors, controllers and actuators. The main advantage of these networked control systems is that the tight coordination of communication network and physical processes and components offers greater autonomy, efficiency, functionality, reliability, and adaptability [3], thus promising great application potential in a wide range of fields including military, factory, industrial process automation and home automation.

The introduction of communication networks in networked control systems provides a flexible two-way communication among the various spatially distributed system components such as sensors, controllers and actuators [8], while also renders certain levels of network-induced constraints such as data losses [2, 28], communication delays [25],

DOI: 10.14736/kyb-2020-2-0261

intermittent sampling/transmission periods [5, 7, 27], and random network topologies [6, 31, 34] inevitable during the analysis and synthesis of the networked control system. Up until now, there are several available systematic reviews on dealing with such network-induced constraints. We refer the interested readers to the recent surveys [32, 33] for detailed discussions on the modeling and methodologies. On the other hand, the openness and vulnerability of the communication network may be exploited intentionally by malicious adversaries such that the information flow through the communication network can be deliberately falsified and manipulated, which makes the security issue of networked control systems fundamentally significant. In this regard, some typical malicious attacks such as deception attacks [9, 11, 29] and denial-of-service (DoS) (or jamming) attacks [12, 13, 15] have been widely explored and their impacts on the system performance have been qualitatively assessed by assuming different attack models and attack strategies. As a powerful tool handling multi-player decision making processes, the concept of noncooperative games has been introduced to deal with the competition between the networked controllers and the sophisticated attacker in the cyber-world. The remote state estimation under DoS attacks was considered in [13], where a Markov game framework was proposed to model the interaction between the sensor and the attacker. In [15], both the sensor and the attacker were modelled as the directly opposed players participating in a zero-sum game, and the Nash equilibrium was constructed under the energy constraint for both players.

Apart from the prominent Nash games which models simultaneous decision making process, Stackelberg games [1], which have superiority in modelling sequential decision making processes, have been introduced to analyze the security of networked control systems as well. A static Stackelberg game in [14] modelled the interactive decision-making procedure between the defender and the attacker, where the defender attempts to allocate defense resources to defend against the false data injection attack launched by the malicious attacker. In [37], a dynamic Stackelberg game was proposed in the resilient control problem for discrete-time linear systems, and sufficient conditions are established for the stability of the closed-loop system corresponding to the Stackelberg equilibrium. However, the above mentioned works consider scenarios of non-switched dynamics only. It is worth mentioning that the system dynamics may be scheduled according to a certain external switching mechanism, which complicates the evolution of system states but also breeds some interesting features that any subsystem does not have. As a result, switched systems has evolved into a mushrooming avenue of research, and a fruitful collection of literatures on various topics have proliferated, including stability [19, 23, 36], input-to-state stability [17, 18, 24], small-gain theorem [20, 21], L_2 gain [26] and dissipativity [35], which motivates this study on switched Stackelberg games.

In this paper, the security problem of single-loop networked control systems is considered where the plant and the controller are spatially distributed and the information exchange is implemented via an unsafe communication network. The dynamics of state evolution are modeled as switched linear systems in discrete time, which offers a step forward in modelling much sophisticated scenarios. The main contributions of this paper can be then summarized as follows:

- A two-layer switched Stackelberg dynamic game is formulated to model the competitive interaction between the controller and the attacker who can launch false data injection attacks. Furthermore, the switched Stackelberg equilibrium is constructed to quantitatively evaluate the performance of both players.

- By making use of the average dwell time concept, the switches between subsystems are restricted not to occur too frequently in the average sense. The asymptotic stability of the closed-loop systems under the switched Stackelberg equilibrium is guaranteed if the switching signal satisfies a certain average dwell time constraint.

The remainder of this paper is structured as follows. In Section 2, the networked control systems with switched dynamics are described before formulating the switched Stackelberg game. Section 3 presents the construction of the switched Stackelberg equilibrium in a receding horizon manner. Specifically, an assumption is made for the seeking of the switched Stackelberg strategy. Section 4 provides the main result concerning the asymptotic stability of the closed-loop systems under the switched Stackelberg equilibrium. Finally, an illustrative example presented in Section 5 validates the correctness of the proposed method and some concluding remarks are given in Section 6.

2. PROBLEM FORMULATION

2.1. Dynamics of a switched networked control system

Consider the remotely-controlled system whose dynamics are described by the following switched linear time invariant system in discrete time

$$x(t+1) = A_{\sigma(t)}x(t) + B_{\sigma(t)}u(t), \tag{1}$$

where $x(t) \in R^n$ is the system state, $u(t) \in R^m$ is the control input and $\sigma(t) \in \mathcal{M} := \{1, \ldots, M\}$ is the switching signal orchestrating the activation modes among the M subsystems.

2.2. Corrupted control input under false data injection attacks

The architecture of the remote control framework for the concerned system (1) under attacks is illustrated in Figure 1. In this paper, our focus is laid on the network communication channel between the remote controller and the actuator as the control sequence $\{u(t)\}_{t\in\mathbb{R}}$ calculated by the suitable control law may be maliciously falsified by an adversary via injecting some spurious signals into the desired control sequences when they are transmitted over the network. More specifically, the system state $x(t)$ of (1) is sampled at every sampling instant $t \in \mathbb{Z}$ and then fed into a remotely located controller. Then the control input $u(t)$ is generated consequently and transmitted back to the plant through a communication network, which closes the control loop. Meanwhile, there exists an attacker locating between the controller and the actuator, which means the attacker decides his attack input after he observes the control input generated by the remotely located controller. Moreover, the attacker corrupts the control input by injecting some false data as follows

$$u_c(t) = u(t) + u_a(t) \tag{2}$$

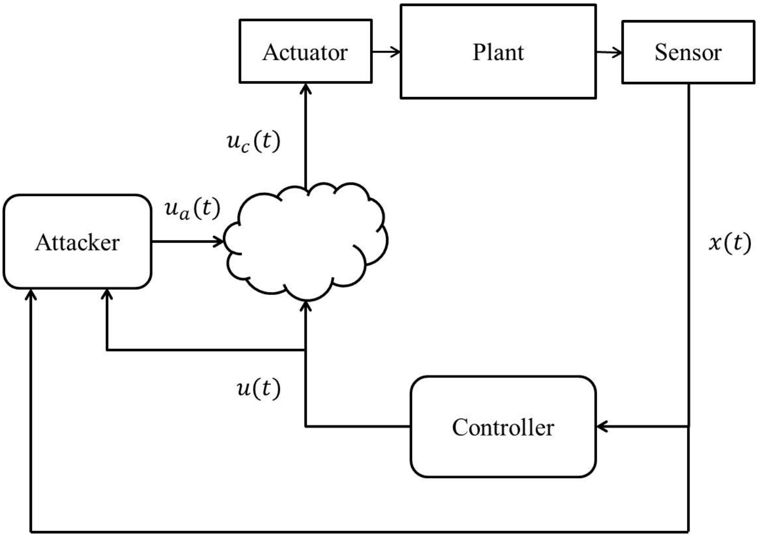

Fig. 1. The architecture of a corrupted networked control system in the presence of a malicious attacker-

where $u(t)$ is the desired control input calculated by the control law and also observed by the attacker at current instant, $u_a(k)$ is the spurious attack input signal, and $u_c(k)$ is the corrupted control input which is received and implemented by the actuator.

In the following, it is assumed that the attacker pursues two partly conflicted objectives: (1) being an malicious assailant, the attacker seeks to destabilize the system by steering the system state as far away from the origin as possible, which can be quantitatively described by the maximization of the distance between the origin to the state of next sampling instant; (2) being a rational adversary, the attacker takes into account the cost of launching the attack injection, namely, incorporating the energy of the injected false data $\|u_a(k)\|^2$. Then the objective of the attacker can be translated mathematically into a minimization problem which serves as the guideline during the strategy conducting process of the attacker:

$$\begin{aligned}(\mathcal{P}^a):\quad \min_{u_a(t)\in R^m}\quad & J^a(\sigma(t),x(t),u(t),u_a(t)) := -x^T(t+1|t)Q_{\sigma(t)}x^T(t+1|t)\\ &\qquad\qquad + u_a^T(t)R^a_{\sigma(t)}u_a(t)\\ \text{s.t.}\quad & x(t+1|t) = A_{\sigma(t)}x(t) + B_{\sigma(t)}(u(t)+u_a(t))\end{aligned}$$

where $Q_i \geq 0, R_i^a > 0, \forall i \in \mathcal{M}$. The solution is parameterized by $(\sigma(t), x(t), u(t))$ and denoted as $u_a^*(t) := \mathrm{BR}^a(\sigma(t), x(t), u(t)) : \mathcal{M} \times R^n \times R^m \to R^m$.

As for the controller, a conventional linear quadratic functional over finite horizon is considered as the cost functional to be minimized, whose mathematical interpretation, denoted as $J^u(\sigma(t), x(t), u(t))$, will be discussed fully in Section 3. The solution of this minimization process is denoted as $u^*(t) := \mathrm{BR}(\sigma(t), x(t))$.

It is worth mentioning that the system matrices $(A_i, B_i), \forall i \in \mathcal{M}$ are the common knowledge availabe to both the controller and the attacker. Moreover, the switch signal and the system state $(\sigma(t), x(t))$ are available in real time. At any stage, the controller and the attacker solve their own minimization problems, respectively, only after collecting the current value of $(\sigma(t), x(t))$.

2.3. Framework of switched Stackelberg game

The competition between the controller and the attacker is modelled as a switched Stackelberg game whose players act in rather a sequential manner than the simultaneous way in Nash games. Therefore, the asymmetric roles of these two players lead to a hierarchical structure of the decision making procedure. On the one hand, the controller is modelled as the leader according to his superior role compared with the attacker and is located at the high level of this hierarchy, thus has full information including the cost function of the attacker and takes his action first. On the other hand, the attacker, located on the data route between the controller and the actuator, is modelled as the follower who is unaware of the cost function of the controller but makes his own decision after he observes the action of the controller.

Remark 2.1. The notations "leader" and "follower" adopted here are to differentiate the asymmetric information structures and the sequential order of decision making between these two players, which are distinct from that in the field of multi-agent systems.

Remark 2.2. The objective of the attacker can have specific physical significances under certain circumstances, such as maximizing the signal-to-interference-and-noise ratio (SINR) [13], minimizing the cost for launching an attack [14]. Therefore, the controller can realize the cost function of the attacker based on these features in real-life situations. On the other hand, the controller can attain the information about the cost function of the attacker with the help of the statistical characteristics based on the history information.

The switched Stackelberg equilibrium, as the solution of the switched Stackelberg game formulated above is defined as below.

Definition 2.3. (*Switched Stackelberg Equilibrium*) A pair of strategies $(u^*(t), u_a^*(t)), t = 0, 1, \dots, \infty$, is called a switched Stackelberg equilibrium if the following inequalities hold:

$$\begin{cases} u_a^*(t) \in \mathrm{BR}^a(\sigma(t), x(t), u^*(t)) \\ \text{and} \\ \max\limits_{u_a(t) \in \mathrm{BR}^a(\sigma(t), x(t), u^*(t))} J^u(\sigma(t), x(t), u^*(t))) \\ \qquad \le \max\limits_{u_a(t) \in \mathrm{BR}^a(\sigma(t), x(t), u(t))} J^u(\sigma(t), x(t), u(t))). \end{cases} \tag{3}$$

The definition of switched Stackelberg equilibrium above is an extension of the conventional Stackelberg equilibrium, see more information in [1] and [22]. Even though the switching signal in this paper is not a design freedom but an external input/disturbance, the introduction of switched dynamics still makes a step further to model much sophisticated circumstances.

Remark 2.4. Different from the simultaneous decision making characterized by the well-known Nash equilibrium [1, 4], the Stackelberg equilibrium discussed here has the advantage of handling the sequential decision making process due to the asymmetric information structures of all players. The Stackelberg equilibrium also safeguards each player against any attempt by the other to deviate, but in a sequential manner. To be detailed, the leader has no better choice than to adopt his Stackelberg strategy, then, he has no incentive to cheat since he knows that his control action is continuously monitored by the follower; the follower has no better choice than to react according to his Stackelberg strategy either, since the Stackelberg strategy of the follower is the best response to the Stackelberg strategy of the leader. In this sense the Stackelberg strategy is also an equilibrium point.

3. RECEDING-HORIZON CONTROL LAW

In this section, the cost functional of the controller will be clarified first. In contrast to the myopic behavior of the attacker, a receding horizon manner is adopted in the decision making process of the controller. Specifically, an accumulation of running cost over a moving fixed-horizon window is adopted as the guideline of the controller, where the size of the window bounds the size of this optimization problem. Compared with that of the attacker, the cost function of the controller reflects the preference for long-term "average" effects over just instantaneous effects.

3.1. Virtual attacker

The best response of the attacker is defined as a one-step function due to the myopic nature, which makes it impossible to make use of this best response directly in the optimization of the controller. Therefore, a virtual attacker is introduced to imitate the myopic pattern of the attacker over the same horizon with that of the controller, so that the corresponding best response is an attack sequence of the same length with the horizon of the controller. The best response of the virtual attacker, instead of the one-step best response of the attacker, is the reaction predicted by the controller to construct the optimal control input.

Given the information including $\sigma(t) \in \mathcal{M}$, $x(t)$ and a sequence of N future inputs $\mathbf{u}(t) := [u(t|t), u(t+1|t), \dots, u(t+N-1|t)]$, the sequence of states $\mathbf{x}(t) := [x(t), x(t+1|t), \dots, x(t+N-1|t), x(t+N|t)]$ depends on the control input sequence of the virtual attacker accordingly and can be predicted using recursively the model, where the positive integer N is the prediction horizon. The objective of the virtual attacker is to construct his optimal solution $\mathbf{u}_{\text{vir}}(t) := [u_{\text{vir}}(t|t), u_{\text{vir}}(t+1|t), \dots, u_{\text{vir}}(t+N-1|t)]$, where $u_{\text{vir}}(t+\tau|t)$ can be obtained by solving the stage-wise quadratic program repeatedly for $0 < \tau < N-1$.

$$\begin{aligned}
(\mathcal{P}^{\text{vir}}): \quad \min_{u_{\text{vir}}(t+\tau|t) \in R^m} \quad & J^{\text{vir}}(\sigma(t), x(t), \mathbf{u}(t)) := -x^T(t+\tau+1|t) Q_{\sigma(t)} x(t+\tau+1|t) \\
& \qquad + u_{\text{vir}}^T(t+\tau|t) R^a_{\sigma(t)} u_{\text{vir}}(t+\tau|t) \\
\text{s.t.} \quad & x(t+\tau+1|t) = A_{\sigma(t)} x(t+\tau|t) + B_{\sigma(t)} u(t+\tau|t) \\
& \qquad + B_{\sigma(t)} u_{\text{vir}}(t+\tau|t), \quad \tau = 0, 1, \dots, N-1, \\
& x(t|t) = x(t),
\end{aligned}$$

and the solution is denoted as $\mathbf{u}_{\mathrm{vir}}(t) := \mathrm{BR}^{\mathrm{vir}}(\sigma(t), x(t), \mathbf{u}(t))$.

Remark 3.1. The introduction of a moving fixed-horizon window makes it possible to get rid of the dependence on the future information of the switching sequence. As in the field of conventional optimal control of switched systems, take the well-known two-stage framework proposed in [30] for example, where the optimizing variables include both the control law and the switching signal. During the design process of the control law, a full knowledge of the parameterized switching signal, including the mode sequence and the parameterized switching instants, is needed *a priori* so that the optimal control problem of switched systems degenerates into a conventional optimal control of piecewise dynamic systems which can be handled with the aid of Pontryagin's Maximum Principle and Dynamic Programming. The dependence on the switching signal over the whole optimization horizon, makes it pretty challenging to extend the two-stage framework from finite horizon case to infinite horizon case. On the contrary, only the current value of switching signal $\sigma(t)$ instead of the full knowledge is needed in this receding horizon technique, which alleviates the computational burden and also offers an opportunity to take not only optimality but also stability into consideration.

3.2. Controller

Once $\mathrm{BR}^{\mathrm{vir}}(\sigma(t), x(t), \mathbf{u}(t))$ is determined, the strategy constructing process of the controller can be transformed into the N-horizon minimax problem:

$$
\begin{aligned}
(\mathcal{P}^u_{\mathrm{minimax}}): \quad \min_{\mathbf{u}(t)} \max_{\mathbf{u}_{\mathrm{vir}}(t)} \quad J^u(\sigma(t), x(t)) := \sum_{\tau=0}^{N-1} \Big(& x^T(t+\tau|t) Q_{\sigma(t)} x(t+\tau|t) \\
& + u^T(t+\tau|t) R_{\sigma(t)} u(t+\tau|t) \Big) \\
& + x^T(t+N|t) Q^f_{\sigma(t)} x(t+N|t) \\
\text{s.t.} \quad x(t+\tau+1|t) = A_{\sigma(t)} x(t+\tau|t) & + B_{\sigma(t)} u(t+\tau|t) \\
& + B_{\sigma(t)} u_{vir}(t+\tau|t), \quad \tau = 0, 1, \ldots, N-1, \\
x(t|t) = x(t), & \\
\mathbf{u}_{\mathrm{vir}}(t) \in \mathrm{BR}^{\mathrm{vir}}(\sigma(t), x(t), \mathbf{u}(t))). &
\end{aligned}
$$

Since the design of the weighting matrices in the cost function is a kind of freedom, the appropriate choices will simplify the construction of the optimal solution.

Assumption 1. The weight matrices Q_i and R^a_i in the cost function of the attacker satisfy the following inequalities:

$$
R^a_i - B^T_i Q_i B_i > 0, \quad \forall i \in \mathcal{M}. \tag{4}
$$

The maximization problem of the virtual control jammer is actually a series of pointwise maximizing, then it can be solved in a divide-and-conquer manner. The maximizing problem can be transformed into the equivalent version

$$\begin{aligned}
&\min_{u_{\mathrm{vir}}(t+\tau|t)\in R^m} \quad -\Big(A_{\sigma(t)}x(t+\tau|t)+B_{\sigma(t)}u(t+\tau|t)+B_{\sigma(t)}u_{\mathrm{vir}}(t+\tau|t)\Big)^T\cdot Q_{\sigma(k)}\\
&\qquad\cdot\Big(A_{\sigma(t)}x(t+\tau|t)+B_{\sigma(t)}u(t+\tau|t)+B_{\sigma(t)}u_{\mathrm{vir}}(t+\tau|t)\Big) \\
&\qquad+u_{\mathrm{vir}}^T(t+\tau|t)R^a_{\sigma(t)}u_{\mathrm{vir}}(t+\tau|t)
\end{aligned} \tag{5}$$

$$\begin{aligned}
&=\min_{u_{\mathrm{vir}}(t+\tau|t)\in R^m} \quad -\Big(A_{\sigma(t)}x(t+\tau|t)+B_{\sigma(t)}u(t+\tau|t)\Big)^T Q_{\sigma(k)}\\
&\qquad\cdot\Big(A_{\sigma(t)}x(t+\tau|t)+B_{\sigma(t)}u(t+\tau|t)\Big)\\
&\qquad-2u_{\mathrm{vir}}^T(t+\tau|t)B^T_{\sigma(t)}Q_{\sigma(t)}\Big(A_{\sigma(t)}x(t+\tau|t)+B_{\sigma(t)}u(t+\tau|t)\Big)\\
&\qquad+u_{\mathrm{vir}}^T(t+\tau|t)\Big(R^a_{\sigma(t)}-B^T_{\sigma(t)}Q_{\sigma(t)}B_{\sigma(t)}\Big)u_{\mathrm{vir}}(t+\tau|t).
\end{aligned} \tag{6}$$

By taking advantage of Assumption 1 on positive definiteness, the equivalent maximizing problem is strictly convex which admits a unique solution

$$\begin{aligned}
u_{\mathrm{vir}}(t+\tau|t)=&(R^a_{\sigma(t)}-B^T_{\sigma(t)}Q_{\sigma(t)}B_{\sigma(t)})^{-1}B^T_{\sigma(t)}Q_{\sigma(k)}\\
&\cdot(A_{\sigma(t)}x(t+\tau|t)+B_{\sigma(t)}u(t+\tau|t)),
\end{aligned} \tag{7}$$

therefore indicating the uniqueness of the best response $\mathrm{BR}^{\mathrm{vir}}(\sigma(t),x(t),\mathbf{u}(t))$.

It is worth mentioning that due to the uniqueness of the best response of the attacker with respect to the decision of the controller, the N-horizon minimax problem $\mathcal{P}^u_{\mathrm{minimax}}$ can be equivalently transformed into a simplified version $\mathcal{P}^u_N$ by discarding the max-operator and substituting the unique best response of the attacker

$$\begin{aligned}
(\mathcal{P}^u_N):\quad &\min_{\mathbf{u}(t)}\quad \sum_{\tau=0}^{N-1}\Big(x^T(t+\tau|t)Q_{\sigma(t)}x(t+\tau|t)+u^T(t+\tau|t)R_{\sigma(t)}u(t+\tau|t)\Big)\\
&\qquad\qquad+x^T(t+N|t)Q^f_{\sigma(t)}x(t+N|t)\\
&\text{s.t.}\quad x(t+\tau+1|t)=(I+S_{\sigma(t)})(A_{\sigma(t)}x(t+\tau|t)+B_{\sigma(t)}u(t+\tau|t))\\
&\qquad\qquad:=\bar{A}_{\sigma(t)}x(t+\tau|t)+\bar{B}_{\sigma(t)}u(t+\tau|t),\quad 0\le\tau\le N-1,\\
&\qquad x(t|t)=x(t),
\end{aligned}$$

where $S_{\sigma(t)}:=B_{\sigma(t)}(R^a_{\sigma(t)}-B^T_{\sigma(t)}Q_{\sigma(t)}B_{\sigma(t)})^{-1}B^T_{\sigma(t)}Q_{\sigma(t)}$.

Clearly, $\mathcal{P}^u_N$ is a typical linear quadratic regulator problem parameterized by the current value of the switching signal $\sigma(t)$. For any instant t, the optimal control sequence $\mathbf{u}^*(t)$ can be solved with the aid of the conventional finite horizon optimal control theory:

$$u^*(t+\tau|t)=-(\bar{B}^T_{\sigma(t)}P^{\tau+1}_{\sigma(t)}\bar{B}_{\sigma(t)}+R_{\sigma(t)})^{-1}\bar{B}^T_{\sigma(t)}P^{\tau+1}_{\sigma(t)}\bar{A}_{\sigma(t)}x(t+\tau|t),\quad \tau=0,\dots,N-1, \tag{8}$$

and the corresponding value function at instant t is

$$V_{\sigma(t)}(x(t)) = x^T(t)P^0_{\sigma(t)}x(t), \tag{9}$$

where the matrices $P^\tau_{\sigma(t)}, \tau = 0, \dots, N-1$ satisfy the matrix difference Riccati equations

$$P^\tau_{\sigma(t)} = \bar{A}^T_{\sigma(t)}\left[P^{\tau+1}_{\sigma(t)} - P^{\tau+1}_{\sigma(t)}\bar{B}_{\sigma(t)}\left(\bar{B}^T_{\sigma(t)}P^{\tau+1}_{\sigma(t)}\bar{B}_{\sigma(t)} + R_{\sigma(t)}\right)^{-1}\bar{B}^T_{\sigma(t)}P^{\tau+1}_{\sigma(t)}\right]\bar{A}_{\sigma(t)} + Q_{\sigma(t)}, \tag{10}$$

with the terminal condition

$$P^N_{\sigma(t)} = Q^f_{\sigma(t)}. \tag{11}$$

The first component of the obtained optimal solution $\mathbf{u}^*(t)$ is applied to the system which is denoted as the receding-horizon control law, i. e.,

$$\begin{aligned} u^{\mathrm{RH}}(t) = u^*(t|t) &= -(\bar{B}^T_{\sigma(t)}P^1_{\sigma(t)}\bar{B}_{\sigma(t)} + R_{\sigma(t)})^{-1}\bar{B}^T_{\sigma(t)}P^1_{\sigma(t)}\bar{A}_{\sigma(t)}x(t) && (12)\\ &:= K^{\mathrm{RH}}_{\sigma(t)}x(t). && (13)\end{aligned}$$

Remark 3.2. The time-invariance of the subsystem dynamics leads to the time-invariance of the corresponding difference Riccati equations with respect to different sampling instants, as a result the constant gain matrix of the receding horizon control law for each subsystem can be calculated off-line.

Lemma 3.3. Suppose Assumption 1 holds for all $i \in \mathcal{M}$. Then, $u^{\mathrm{RH}}(t) = K^{\mathrm{RH}}_{\sigma(t)}x(t)$ is the Stackelberg strategy of the controller, and $(u^{\mathrm{RH}}(t), \mathrm{BR}^a(\sigma(t), x(t), u^{\mathrm{RH}}(t))$ constitutes a switched Stackelberg equilibrium.

Proof. The proof can be trivially completed by verifying the inequalities in Definition 2.3, and is omitted here thereupon. □

The real-time running procedure can be summarized as the following iteration:
At any sample instant $t \geq 0$,

1. The sensor first samples and transmits the measurement of $x(t)$. Meanwhile, the current value of the switching signal $\sigma(t)$ is known by the controller and the attacker.
2. After receiving $x(t)$, the controller generates the receding horizon control input $u(t) = u^{\mathrm{RH}}(t)$ by solving the N-horizon linear quadratic optimal control problem $\mathcal{P}^u_N$, and sends it to the actuator through the communication channel.
3. The attacker corrupts $u(t)$ by adding $u_a(t) = \mathrm{BR}^a(\sigma(t), x(t), u(t))$.
4. The actuator receives and then implements the corrupted control input $u_c(t)$.
5. The system states evolve into that of next stage according to the currently activated system dynamics.

4. STABILITY ANALYSIS

In this section, the asymptotic stability of the closed-loop system is investigated under the switched Stackelberg equilibrium. Before going any further, the concept of average dwell time is introduced to characterize the feature of the switching signal in the time scale.

Definition 4.1. (*Average dwell time*) (Hespanha and Morse [10], Liberzon [16]) A switching signal $\sigma(t)$ has average dwell time τ_a if there exist scalar $N_0, \tau_a > 0$ such that the inequality

$$N_\sigma(T,t) \le N_0 + \frac{T-t}{\tau_a}, \quad \forall T \ge t \ge 0 \tag{14}$$

holds, where $N_\sigma(T-t)$ denotes the number of switches occuring in the interval $(t,T]$. N_0 characterizes the chattering bound which admits the possibility of some fast switches. As an extension of dwell time, the concept of average dwell time imposes a restriction of slow switching in the sense of average, i. e., τ_a timeslots must lie between two consecutive switches in average.

In the following, we will show that the closed-loop system under the switched Stackelberg equilibrium is asymptotically stable if the average dwell time of the switching signal σ satisfies an a priori bound.

Theorem 4.2. Suppose Assumption 1 holds for all $i \in \mathcal{M}$. If

$\Theta_i :=$

$$P_i^0 - \bar{A}_i^T \Big[I - P_i^1 \bar{B}_i (\bar{B}_i^T P_i^1 \bar{B}_i + R_i)^{-1} \bar{B}_i^T \Big] \cdot P_i^0 \cdot \Big[I - \bar{B}_i (\bar{B}_i^T P_i^1 \bar{B}_i + R_i)^{-1} \bar{B}_i^T P_i^1 \Big] \bar{A}_i > 0 \tag{15}$$

holds for all $i \in \mathcal{M}$, where P_i^0, P_i^1 satisfy the matrix difference Riccati equations (10) – (11) of the ith subsystem, and $\bar{A}_i$ and $\bar{B}_i$ are shorthands

$$\bar{A}_i = (I + S_i) A_i, \tag{16}$$

$$\bar{B}_i = (I + S_i) B_i, \tag{17}$$

$$S_i = B_i^T (R_i^a - B_i^T Q_i B_i)^{-1} B_i^T Q_i, \tag{18}$$

then, the closed-loop system, obtained by applying the switched Stackelberg equilibrium, is asymptotically stable if the switching signal σ satisfies the average dwell time constraint

$$\tau_a \ge \tau_a^* = -\frac{\ln \mu}{\ln(1-\alpha)}, \tag{19}$$

where $\alpha = \min_i \frac{\lambda_{\min}(\Theta_i)}{\lambda_{\max}(P_i^0)}$, and $\mu = \max_{i,j \in \mathcal{M}, i \ne j} \mu_{ij} = \max_{i,j \in \mathcal{M}, i \ne j} \frac{\lambda_{\max}(P_i^0)}{\lambda_{\min}(P_j^0)}$.

Proof. The positive definite value function of each subsystem is employed as the candidate Lyapunov function.

For any state $x \in R^n$, during the activation interval of each subsystem $i \in \mathcal{M}$, denote $x^+ := A_i x + B_i\big(u^{\mathrm{RH}} + \mathrm{BR}^a(i, x, u^{\mathrm{RH}})\big)$, then the evolution of the value function corresponding to the ith subsystem is

$$\begin{aligned} V_i(x^+) - V_i(x) =& x^T \bar{A}_i^T \Big[I - P_i^1 \bar{B}_i(\bar{B}_i^T P_i^1 \bar{B}_i + R_i)^{-1} \bar{B}_i^T\Big] \cdot P_i^0 \\ & \cdot \Big[I - \bar{B}_i(\bar{B}_i^T P_i^1 \bar{B}_i + R_i)^{-1} \bar{B}_i^T P_i^1\Big] \bar{A}_i x - x^T P_i^0 x \\ \leq& - \frac{\lambda_{\min}(\Theta_i)}{\lambda_{\max}(P_i^0)} \cdot V_i(x) \\ \leq& - \alpha V_i(x), \end{aligned}$$

from which we can get

$$V_i(x^+) \leq (1 - \alpha) \cdot V_i(x), \tag{20}$$

which indicates that exponential convergence of the value function according to each subsystem is guaranteed during the activation interval.

The value functions of any two instinct subsystems satisfy the following inequality

$$V_i(x) = x^T P_i^0 x \leq \lambda_{\max}(P_i^0) \leq \frac{\lambda_{\max}(P_i^0)}{\lambda_{\min}(P_j^0)} \cdot V_j(x) = \mu_{ij} \cdot V_j(x) \leq \mu V_j(x) \tag{21}$$

for $\forall i, j \in \mathcal{M}$ and all $x \in R^n$.

The switched value function $V_{\sigma(t)}(x(t))$ is employed to prove asymptotic stability of the resulted closed-loop system. Denote a sequence of switching instants as $\{\tau_0 = 0, \tau_1, \tau_2, \ldots, \tau_k, \tau_{k+1}, \ldots\}$. For any two switching instants τ_k, τ_{k+1}, the inequality is expressed as

$$\begin{aligned} V_{\sigma(\tau_{k+1})}(x(\tau_{k+1})) &\leq \mu V_{\sigma(\tau_k)}(x(\tau_{k+1})) \\ &\leq \mu \cdot (1 - \alpha)^{\tau_{k+1} - \tau_k} \cdot V_{\sigma(\tau_k)}(x(\tau_k)). \end{aligned} \tag{22}$$

Iterating this inequality from $k = 0$ to $k = N_\sigma(t, 0)$ yields

$$\begin{aligned} V_{\sigma(t)}(x(t)) &\leq \mu^{N_\sigma(t,0)} \cdot (1 - \alpha)^t \cdot V_{\sigma(0)}(x(0)) \\ &\leq \mu^{N_0 + \frac{t}{\tau_a}} \cdot (1 - \alpha)^t \cdot V_{\sigma(0)}(x(0)) \\ &= e^{(N_0 + \frac{t}{\tau_a}) \ln \mu + t \ln(1 - \alpha)} \cdot V_{\sigma(0)}(x(0)) \\ &= e^{N_0 \cdot \ln \mu + t \cdot \left(\ln(1 - \alpha) + \frac{\ln \mu}{\tau_a} \right)} \cdot V_{\sigma(0)}(x(0)). \end{aligned} \tag{23}$$

Since τ_a satisfies the lower bound

$$\tau_a \geq \tau_a^* = -\frac{\ln \mu}{\ln(1 - \alpha)},$$

we can draw the conclusion that $V_{\sigma(t)}(x(t))$ converges to zero as $t \to \infty$, which proves the asymptotic stability of the closed-loop system. □

Remark 4.3. For the sake of brevity, the weight matrix $Q_{\sigma(t)}$ in the cost function J^u is chosen as the same as that in the cost function J^a. There exists no difficulty in applying the previous method to the case of different weight matrix, therefore a different weight matrix can be adopted which will brings very few modifications.

5. AN ILLUSTRATIVE EXAMPLE

In this section, a numerical example is provided to validate the effectiveness of the derived result.

Consider a networked control system (1) consists of two linear subsystems whose system matrices are given as

$$A_1 = \begin{bmatrix} 1 & 0.8 \\ -0.7 & -0.5 \end{bmatrix}, B_1 = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, A_2 = \begin{bmatrix} -0.8 & -0.2 \\ 0.5 & 1 \end{bmatrix}, B_2 = \begin{bmatrix} 1 \\ 0 \end{bmatrix}.$$

The weight matrices in the cost functions J^u and J^a, corresponding to the controller and the attacker, respectively, are constructed as

$$Q_1 = \begin{bmatrix} 1 & 1 \\ 1 & 1.5 \end{bmatrix}, R_1^a = 8, R_1 = 10, Q_1^f = \begin{bmatrix} 1.5 & 0.8 \\ 0.8 & 2 \end{bmatrix},$$
$$Q_2 = \begin{bmatrix} 2 & 1 \\ 1 & 0.8 \end{bmatrix}, R_2^a = 10, R_2 = 8, Q_2^f = \begin{bmatrix} 2.5 & 1.5 \\ 1.5 & 1 \end{bmatrix}.$$

It is easy to confirm that Assumption 1 holds with the given system and weight matrices by simple calculation.

Hence, the switched Stackelberg strategy of the controller $u^*(t)$ can be achieved by solving the minimization problem $\mathcal{P}_N^u$ over finite horizon, and the resulting mode-dependent control gain matrices are

$$K_1^{\mathrm{RH}} = \begin{bmatrix} -0.2433 & -0.0777 \end{bmatrix}, K_2^{\mathrm{RH}} = \begin{bmatrix} 0.2405 & -0.1027 \end{bmatrix}.$$

Therefore, the switched Stackelberg strategy of the attacker can be obtained by substituting the Stackelberg strategy of the controller $u^*(t) = K_{\sigma(t)}^{\mathrm{RH}} x(t)$ into the best response of the attacker, which is also in the form of state feedback:

$$u_a^*(t) = \mathrm{BR}^a(\sigma(t), x(t), u^*(t)) := K_{\sigma(t)}^a x(t),$$

where the gain matrices are

$$K_1^a = \begin{bmatrix} 0.0746 & -0.0102 \end{bmatrix}, K_2^a = \begin{bmatrix} -0.0774 & 0.0493 \end{bmatrix}.$$

A conclusion can be made that the strategy pair $(u^*(t), u_a^*(t))$ is a switched Stackelberg equilibrium according to Lemma 3.3.

Furthermore, the average dwell time constraint of the stabilizing switching signal can be calculated by solving equation (19) along with equation (15), and a lower bound of this constraint is provided as

$$\tau_a^* = 22.17.$$

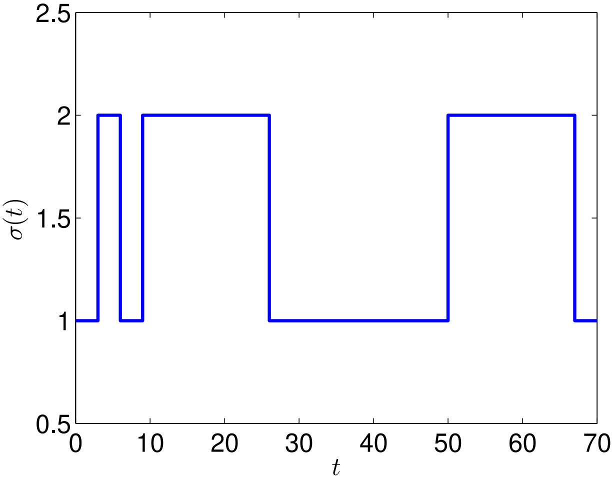

Fig. 2. A switching signal with average dwell time.

Then a prescribed switching signal provided in Figure 2 satisfies the average dwell time constraint in Theorem 4.2, which is then sufficient to guarantee the asymptotical stability of the closed-loop system under the switched Stackelberg equilibrium.

The resulting trajectory of the system states under the given switching signal and the switched Stackelberg equilibrium is portrayed in Figure 3, which vividly show the convergence of the system states to the origin point, therefore validates the asymptotic stability of the closed-loop dynamics.

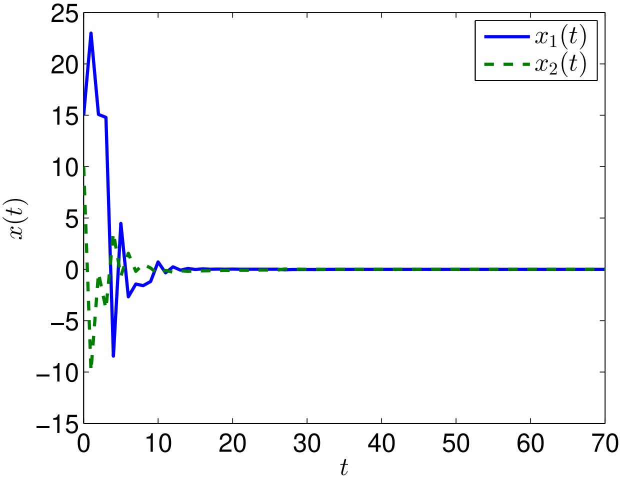

Fig. 3. Trajectory of the system states.

Moreover, the resulting actions of the switched Stackelberg equilibrium $(u^*(t), u_a^*(t))$ scheduled by this switching signal are illustrated in Figure 4 and Figure 5, respectively.

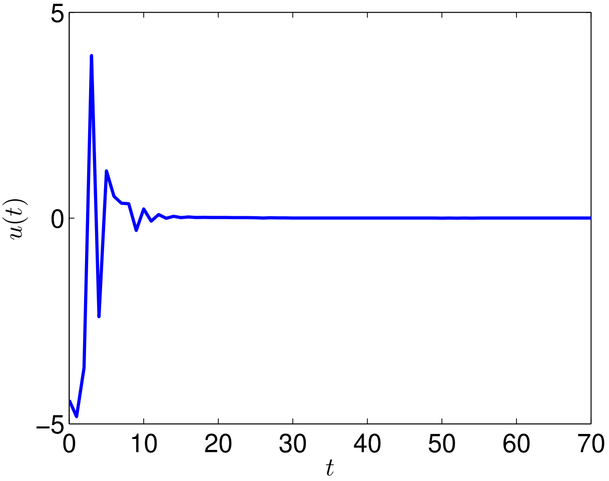

Fig. 4. The switched Stackelberg action of the controller.

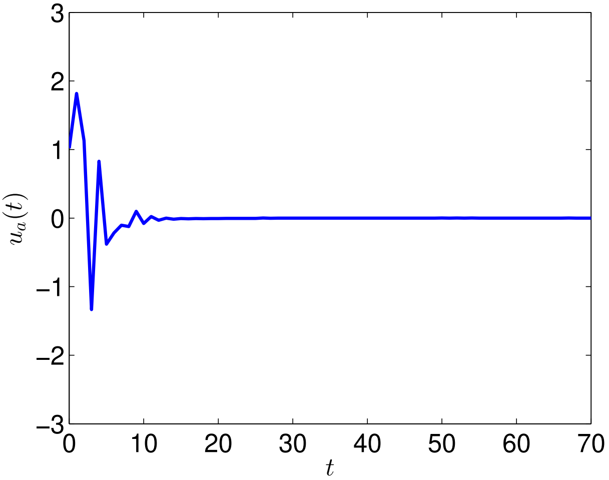

Fig. 5. The switched Stackelberg action of the attacker.

The attacker launches the false data injection attack based on the minimization of his cost function, which means that the attacker chooses his optimal solution based on the transmitted control input at every instant. However, due to the superior hierarchy in this coupled decision making process, the controller takes the reaction of the attacker into consideration and counteracts the potential attack in the generation of the control input $u(t)$. The asymmetric information structures make it possible for the controller to suppress the negative effects brought by the attacker and maintain the stability of the closed-loop system even with the presence of the malicious adversary.

6. CONCLUSION

In this paper, a game theoretic method was provided for the security problem of networked control systems. The definition of the switched Stackelberg equilibrium between the controller and the attacker was proposed before constructing the switched Stackelberg strategy of the controller in a receding-horizon manner. We showed that certain restriction posed on the weight matrices of the cost functions would simplify the equilibrium seeking procedure. Subsequently, with the obtained switched Stackelberg equilibrium, a sufficient condition is derived under which the asymptotic stability of the closed-loop system is maintained. Finally, a numerical example was presented and illustrated the effectiveness of the proposed method.

ACKNOWLEDGEMENT

This work was supported by the National Natural Science Foundation of China under Grant 61773098 and the 111 Project (B16009).

(Received September 11, 2019)

REFERENCES

[1] T. Basar and G. J. Olsder: Dynamic Noncooperative Game Theory. Siam, Philadelphia 1999. DOI:10.1137/1.9781611971132

[2] Y. Dong and J. Chen: Finite-time outer synchronization between two complex dynamical networks with on–off coupling. Int. J. Modern Phys. C. *26* (2015), 8, 1550095. DOI:10.1142/s0129183115500953

[3] D. Ding, Q.-L. Han, Z. Wang, and X. Ge: A survey on model-based distributed control and filtering for industrial cyber-physical systems. IEEE Trans. Ind. Inf. *15* (2019), 5, 2483–2499. DOI:10.1109/tii.2019.2905295

[4] J. Engwerda: LQ Dynamic Optimization and Differential Games. John Wiley and Sons, Chichester 2005.

[5] E. Garcia and P. Antsaklis: Model-based event-triggered control for systems with quantization and time-varying network delays. IEEE Trans. Automat. Control *58* (2013), 2, 422–434. DOI:10.1109/tac.2012.2211411

[6] X. Ge and Q.-L. Han: Consensus of multiagent systems subject to partially accessible and overlapping Markovian network topologies. IEEE Trans. Cybernet. *47* (2017), 8, 1807–1819. DOI:10.1109/tcyb.2016.2570860

[7] X. Ge, Q.-L. Han, and Z. Wang: A threshold-parameter-dependent approach to designing distributed event-triggered H_∞ consensus filters over sensor networks. IEEE Trans. Cybernet. *49* (2019), 4, 1148–1159. DOI:10.1109/tcyb.2017.2789296

[8] X. Ge, Q.-L. Han, X.-M. Zhang, L. Ding, and F. Yang: Distributed event-triggered estimation over sensor networks: A survey. IEEE Trans. Cybernet. *50* (2019), 3, 1306–1320. DOI:10.1109/tcyb.2019.2917179

[9] X. Ge, Q.-L. Han, M. Zhong, and X.-M. Zhang: Distributed Krein space-based attack detection over sensor networks under deception attacks. Automatica *109* (2019), 108557, 108557. DOI:10.1016/j.automatica.2019.108557

[10] J. P. Hespanha and A. S. Morse: Stability of switched systems with average dwell-time. In: Proc. 38th IEEE Conf. Decision Control 1999, pp. 2655–2660. DOI:10.1109/cdc.1999.831330

[11] L. Hu, Z. Wang, Q.-L. Han, and X. Liu: State estimation under false data injection attacks: Security analysis and system protection. Automatica *87* (2018), 176–183. DOI:10.1016/j.automatica.2017.09.028

[12] S. Hu, D. Yue, Q.-L. Han, X. Xie, X. Chen, and C. Dou: Observer-based event-triggered control for networked linear systems subject to denial-of-service attacks. IEEE Trans. Cybernet. *50* (2019), 5, 1952–1964. DOI:10.1109/tcyb.2019.2903817

[13] Y. Li, D. E. Quevedo, S. Dey, and L. Shi: SINR-based dos attack on remote state estimation: A game-theoretic approach. IEEE Trans. Control Netw. Syst. *4* (2017), 632–642. DOI:10.1109/tcns.2016.2549640

[14] Y. Li, D. Shi, and T. Chen: False data injection attacks on networked control systems: A Stackelberg game analysis. IEEE Trans. Automat. Control *63* (2018), 3503–3509. DOI:10.1109/tac.2018.2798817

[15] Y. Li, L. Shi, P. Cheng, J. Chen, and D. .E. Quevedo: Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach. IEEE Trans. Automat. Control *60* (2015), 2831–2836. DOI:10.1109/tac.2015.2461851

[16] D. Liberzon: Switching in Systems and Control. Birkhauser, Boston 2003. DOI:10.1007/978-1-4612-0017-8

[17] B. Liu, D. J. Hill, and Z. Sun: Input-to-state-kl-stability and criteria for a class of hybrid dynamical systems. Appl. Math. Comput. *326* (2018), 124–140. DOI:10.1016/j.amc.2018.01.002

[18] B. Liu, D. J. Hill, and Z. Sun: Input-to-state exponents and related iss for delayed discrete-time systems with application to impulsive effects. Int. J. Robust Nonlinear Control 28 (2018), 640–660. DOI:10.1002/rnc.3891

[19] L. Long: Stabilization by forwarding design for switched feedforward systems with unstable modes. Int. J. Robust Nonlinear Control *27* (2017), 4808–4824. DOI:10.1002/rnc.3832

[20] L. Long: Multiple Lyapunov functions-based small-gain theorems for switched interconnected nonlinear systems. IEEE Trans. Automat. Control *62* (2017), 3943–3958. DOI:10.1109/tac.2017.2648740

[21] L. Long and T. Si: Small-gain technique-based adaptive nn control for switched pure-feedback nonlinear systems. IEEE Trans. Cybernet. *49* (2019), 1873–1884. DOI:10.1109/tcyb.2018.2815714

[22] S. J. Rubio: On coincidence of feedback Nash equilibria and Stackelberg equilibria in economic applications of differential games. J. Optim. Theory Appl. *128* (2006), 203–220. DOI:10.1007/s10957-005-7565-y

[23] X.-M. Sun, G.-P. Liu, D. Rees, and W. Wang: Delay-dependent stability for discrete systems with large delay sequence based on switching techniques. Automatica *44* (2008), 2902–2908. DOI:10.1016/j.automatica.2008.04.006

[24] X.-M. Sun and W. Wang: Integral input-to-state stability for hybrid delayed systems with unstable continuous dynamics. Automatica *48* (2012), 2359–2364. DOI:10.1016/j.automatica.2012.06.056

[25] X. Sun, D. Wu, G. Liu, and W. Wang: Input-to-state stability for networked predictive control with random delays in both feedback and forward channels. IEEE Trans. Ind. Electron. *61* (2014), 3519–3526. DOI:10.1109/tie.2013.2278953

[26] X.-M. Sun, J. Zhao, and D. J. Hill: Stability and l2-gain analysis for switched delay systems: A delay-dependent method. Automatica *42* (2006), 1769–1774.

[27] X. Wang and M. Lemmon: Event-triggering in distributed networked control systems. IEEE Trans. Automat. Control *56* (2011), 3, 586–601. DOI:10.1109/tac.2010.2057951

[28] J. Wu and T. Chen: Design of networked control systems with packet dropouts. IEEE Trans. Automat. Control *52* (2007), 1314–1319. DOI:10.1109/tac.2007.900839

[29] S. Xiao, Q.-L. Han, X. Ge, and Y. Zhang: Secure distributed finite-time filtering for positive systems over sensor networks under deception attacks. IEEE Trans. Cybernet. *50* (2019), 3, 1220–1229. DOI:10.1109/tcyb.2019.2900478

[30] X. Xu and P. J. Antsaklis: Optimal control of switched systems based on parameterization of the switching instants. IEEE Trans. Automat. Control *49* (2004), 2–16. DOI:10.1109/tac.2003.821417

[31] K. You, Z. Li, and L. Xie: Consensus condition for linear multi-agent systems over randomly switching topologies. Automatica *49* (2013), 10, 3125–3132. DOI:10.1016/j.automatica.2013.07.024

[32] L. Zhang, H. Gao, and O. Kaynak: Network-induced constraints in networked control systems — A survey. IEEE Trans. Ind. Inf. *9* (2013), 1, 403–416. DOI:10.1109/tii.2012.2219540

[33] X.-M. Zhang, Q.-L. Han, and X. Yu: Survey on recent advances in networked control systems. IEEE Trans. Ind. Inf. *12* (2016), 5, 1740–1752. DOI:10.1109/tii.2015.2506545

[34] Y. Zhang and Y.-P. Tian: Consentability and protocol design of multi-agent systems with stochastic switching topology. Automatica *45* (2009), 5, 1195–1201. DOI:10.1016/j.automatica.2008.11.005

[35] J. Zhao and D. J. Hill: Dissipativity theory for switched systems. IEEE Trans. Automat. Control *53* (2008), 941–953. DOI:10.1109/tac.2008.920237

[36] J. Zhao, D. J. Hill, and T. Liu: tability of dynamical networks with non-identical nodes: A multiple V-Lyapunov function method. Automatica *47* (2011), 2615–2625. DOI:10.1016/j.automatica.2011.09.012

[37] M. Zhu and S. Martínez: Stackelberg-game analysis of correlated attacks in cyber-physical systems. In: Proc. Amer. Control Conf. 2011, pp. 4063–4068. DOI:10.1109/acc.2011.5991463

Yabing Huang, State Key Laboratory of Synthetical Automation for Process Industries, Northeastern University, Shenyang, 110819, P. R. China; College of Information Science and Engineering, Northeastern University, Shenyang 110819. P. R. China.
e-mail: yabing_huang@163.com

Jun Zhao, State Key Laboratory of Synthetical Automation for Process Industries, Northeastern University, Shenyang, 110819, P. R. China; College of Information Science and Engineering, Northeastern University, Shenyang 110819. P. R. China.
e-mail: zhaojun@ise.neu.edu.cn