Letter

A Novel Memory-Based Scheduling Protocol for Networked Control Systems Under Stochastic Attacks and Bandwidth Constraint

Hongchenyu Yang, Chen Peng, *Senior Member, IEEE*, and Zhiru Cao

Dear Editor,

In this letter, a novel memory-based scheduling protocol (MBSP) is investigated for networked control systems (NCSs) under bandwidth constraint and stochastic denial-of-service (DoS) attacks. First, considering the bandwidth constraint and that multiple sensors' channels may be attacked, a novel memory-based scheduling protocol is proposed to alleviate the pressure of signal transmission, which can dynamically allocate network sources according to different intensities of DoS attacks. Second, under the proposed MBSP, a stochastic impulse system model is established with consideration of network-induced delay and packet loss. Then, sufficient conditions for the existence of the desired controller gain and MBSP parameters are given to ensure the mean-square stability of the studied closed-loop system subject to DoS attacks. Finally, a simulation example is provided to verify the effectiveness of the proposed method.

NCSs are spatially distributed systems, where signal transmissions among system components are realized through a shared network. NCSs have been widely used in various fields, including power systems, industrial automation, offshore platform, and so on. However, due to the limited bandwidth of the shared communication network, there may exist some imperfect phenomena such as time delay and data loss, which could degenerate system performances and even make systems unstable. In an open network environment, communication channels are vulnerable to malicious cyber-attacks which could jeopardize NCSs and cause security problems seriously. Generally, deception attacks and DoS attacks are the two most common types of cyber-attacks. Given that DoS attacks occur most frequently and are extremely common, this work focuses mainly on dealing with DoS attacks from a defender's point of view.

To mitigate the pressure of band-limited network communication, lots of studies are devoted to researching proper communication strategies. As one of the most effective transmission strategies which are based on the necessity of communication, the event-triggered mechanism has received much attention during the past decades. However, most of these results take an assumption that all of control signals should be boxed into one data package. But in practical applications, the nodes of NCSs are distributively linked over a large physical extent. That is, only one packet to transmit is unrealistic. Therefore, the research on multiple packet transmission under network bandwidth constraint is indispensable. In view that nodes could preempt network resources from each other, it is unavoidable for the node collision phenomena during multiple packet transmission. To solve this problem, scheduling protocols have been presented to decide which node to gain access to the communication network under multi-channel transmissions. Generally, there are three main types of multi-channel scheduling: Round-Robin (RR) scheduling, try-once-discard (TOD) scheduling, and stochastic scheduling.

Related work: Recently, a time-delay approach has been discussed to solve the stabilization problem of NCSs [1] and [2]. In [2], an analysis and comparison between Bernoulli and Markovian stochastic protocols have been made and sufficient exponential stability conditions have been derived for the studied impulsive delayed system with multiple sensor nodes. Besides, the hybrid system method has been employed to analyze NCSs with variable delays

under TOD communication protocol in [3], where a partial exponential stabilization criterion of the hybrid system with time delay has been derived. By utilizing the above three protocols to orchestrate the signal transmission, the stabilization of discrete-time NCSs has been studied in [4] which are provided with uncertain and variable parameters. However, most of these results rarely consider the network security problem, which is one of the most urgent problems to be solved today. Therefore, how to schedule system nodes when NCSs are attacked is one of the topics worth studying.

It is well-known that DoS attacks have been widely researched in the past several years [5] and [6]. As discussed in [5], for the case that DoS attacks block the signal transmission of a single communication channel periodically, an event-triggered control method based on state-observer has been presented to realize remote control and observation of the attacked system. In [6], the input-to-state stabilization problem of cyber-physical systems based on multi-channel communication has been addressed under arbitrary DoS attacks of which the feature is characterized by frequency and duration. In [7], each successful transmission interval has been divided into two kinds of time intervals to discuss according to whether attacks exist, and the switching-like event-triggered transmission mechanism has been presented to cope with intermittent DoS attacks so as to accomplish the expected system performances. From the energy-constrained attacker perspective, a stochastic DoS attack energy minimization problem has been solved in [8], where the minimum stochastic attack energy cost could be used to estimate the behavior of the synergetically working sensor network effectively. As mentioned above, most results are based on either a single transmission channel or multiple transmission channels not taking the intensity of DoS attacks into account. Few researchers have studied the scheduling scheme that considers the intensity of DoS attacks under multiple packet transmissions, which stimulates this work.

Problem statement: In Fig. 1, consider the linear system

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

where $x(t) \in \mathbb{R}_x$, $y(t) \in \mathbb{R}_y$, $u(t) \in \mathbb{R}_u$ are state, measurement output and control input. A, B and C have suitable dimensions. For system (1), consider the cost function

$$J = \int_0^{+\infty} [x^T(t)\bar{M}x(t) + u^T(t)\bar{N}u(t)]dt \tag{2}$$

where $\bar{M}$ and $\bar{N}$ are given symmetric matrices. Denote sampling instant as s_q satisfying that $0 = s_0 < s_1 < \cdots < s_q < \cdots$, $s_{q+1} - s_q \leq \bar{s}$,

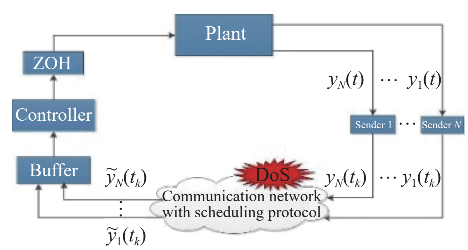

Fig. 1. NCSs subjected to stochastic DoS attacks under MBSP.

Corresponding author: Chen Peng.

Citation: H. C. Yang, C. Peng, and Z. R. Cao, "A novel memory-based scheduling protocol for networked control systems under stochastic attacks and bandwidth constraint," *IEEE/CAA J. Autom. Sinica*, vol. 10, no. 5, pp. 1336–1339, May 2023.

The authors are with the School of Mechatronic Engineering and Automation, Shanghai University, Shanghai 200444, China (e-mail: yhchenyu@163.com; c.peng@shu.edu.cn; zhiru_cao@163.com).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/JAS.2023.123162

$\lim_{q\to+\infty} s_q = +\infty$, $q \in \mathbb{Z}_+$, where $\bar{s}$ is the maximum allowable transfer interval. The measurement of the ith sensor is $y_i(s_q) = C_i x^i(s_q)$, $i = 1,\ldots,N$, in which $x^i(s_q)$ is the state corresponding to $y_i(s_q)$ and there are N sensor nodes in the system. Thus, $y(s_q) = col\{y_1(s_q),\ldots, y_N(s_q)\}$, $C = col\{C_1,\ldots,C_N\}$.

In an open network environment, packet dropout, cyber-attacks and network-induced delay are inevitable. Denote the sequence after packet loss by$\{t_k\} \subseteq \{s_q\}$, that is, only at sampling instants $\{t_k\}$, the input of the controller can be updated. We assume that the network-induced delay $\eta_k \in [\eta_1, \bar{\eta}_2]$. For the convenience of description, let $\iota_k = t_k + \eta_k$, $\iota_{k+1} = t_{k+1} + \eta_{k+1}$. In this work, DoS attacks are assumed to follow a Bernoulli distribution:

$$\gamma_k^i = \begin{cases} 1, & \text{no DoS attacks} \\ 0, & \text{with DoS attacks} \end{cases} \tag{3}$$

where $\mathbb{E}\{\gamma_k^i\} = Prob\{\gamma_k^i = 1\} = \theta_k^i$.

In the following, we apply an independent identically distributed (i.i.d) stochastic protocol for the network transmission, which prescribes that only one node gets access to be transmitted at instants $\{t_k\}$. Under i.i.d protocol, let $\chi_k \in \{1,\ldots,N\}$ be the active output node at t_k. The selection of χ_k is independent of the previously chosen node and is assumed to be i.i.d with a known invariable β_k^i,

$$Prob\{\chi_k = i\} = \beta_k^i,\ \ i = 1,\ldots,N,\ \ \beta_k^i \geq 0,\ \textstyle\sum_{i=1}^N \beta_k^i = 1.$$

The updating law of controller input $\tilde{y}_i(t_k)$ is described as

$$\tilde{y}_i(t_k) = \begin{cases} y_i(t_k), & i = \chi_k \\ \tilde{y}_i(t_{k-1}), & i \neq \chi_k. \end{cases} \tag{4}$$

Moreover, the controller keeps its control input signal as constant till new data arriving, that is, for $t \in [\iota_k, \iota_{k+1})$,

$$\tilde{y}(t) = \tilde{y}(t_k) = col\{\tilde{y}_1(t_{k-1}),\ldots, y_{\chi_k}(t_k),\ldots,\tilde{y}_N(t_{k-1})\}.$$

Memory-based scheduling protocol: As Fig. 2 depicts, for the case that the channel has no transmission permission, if NCSs are attacked, the attack will not affect the system, and the historical information stored in the buffer can be still used. When the channel has permission to transmit, if $\gamma_k^i = 1$, $y_i(t_k)$ is transmitted to the controller side; if $\gamma_k^i = 0$, $\tilde{y}_i(t_{k-1})$ is used by the controller. In a word, DoS attacks affect only the active sensor node at instant t_k. And when DoS attacks occur, the control input keeps constant with the previous measurement. Therefore, under MBSP, the available control input is

$$\tilde{y}(t_k) = \begin{cases} col\{\tilde{y}_1(t_{k-1}),\ldots, y_{\chi_k}(t_k),\ldots,\tilde{y}_N(t_{k-1})\}, & \gamma_k^i = 1 \\ col\{\tilde{y}_1(t_{k-1}),\ldots,\tilde{y}_{\chi_k}(t_{k-1}),\ldots,\tilde{y}_N(t_{k-1})\}, & \gamma_k^i = 0. \end{cases}$$

That is, under MBSP, the input of controller can be $\tilde{y}(t_k) = col\{\tilde{y}_1(t_{k-1}),\ldots,\gamma_k^i y_{\chi_k}(t_k) + (1-\gamma_k^i)\tilde{y}_{\chi_k}(t_{k-1}),\ldots,\tilde{y}_N(t_{k-1})\}$.

Two random variables γ_k^i, χ_k are introduced to build a connection between scheduling process and DoS attack process. The intensity of DoS attacks is described with θ_k^i. The smaller the value is, the more frequently the attack occurs, and vice versa. MBSP can dynamically allocate network sources according to different intensities of DoS attacks, so as to be used to relieve the pressure of network communication under multiple packet transmissions.

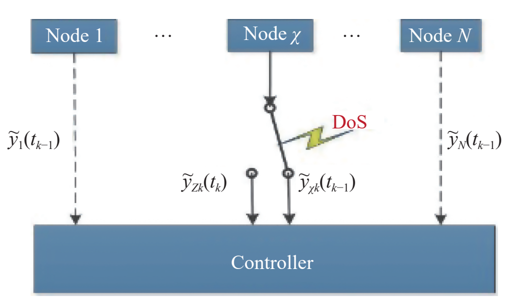

Fig. 2. Memory-based scheduling protocol.

Stochastic impulsive system model: Define $\tilde{x}^i(t_{k-1})$ is the state vector corresponding to $\tilde{y}_i(t_{k-1})$ of the ith sensor. Consider state errors $e_i(t) = \tilde{x}^i(t_{k-1}) - x^i(t_k)$ to describe the control input, so as to build a bridge between attack and scheduling parameters. Thus,

$$\tilde{y}(t) = \sum_{i=1}^N (1-\gamma_k^i) I_i C_i e_i(t) + Cx(t_k) + \sum_{i=1, i\neq\chi_k}^N \gamma_k^i I_i C_i e_i(t)$$

where $I_i = col\{\underbrace{0,\ldots,0}_{i-1}, I, \underbrace{0,\ldots,0}_{N-i}\}$.

Next, we introduce an output feedback controller

$$u(t) = K\tilde{y}(t),\ \iota_k \leq t \leq \iota_{k+1} \tag{5}$$

where K is the controller gain to be designed. The controller is

$$u(t) = \sum_{i=1}^N (1-\gamma_k^i) K I_i C_i e_i(t) + KCx(t_k) + \sum_{i=1, i\neq\chi_k}^N \gamma_k^i K I_i C_i e_i(t).$$

Let $\eta(t) = t - t_k$ for $t \in [\iota_k, \iota_{k+1})$, then

$$\eta_1 \leq \eta_k \leq \eta(t) \leq t_{k+1} - t_k + \eta_{k+1} \leq \eta_2$$

Define the following indicator functions:

$$\lambda_k^i = \begin{cases} 1, & \chi_k = i, \\ 0, & \chi_k \neq i, \end{cases} \quad i = 1,\ldots,N$$

where $\mathbb{E}\{\lambda_k^i\} = Prob\{\chi_{t_k} = i\} = \beta_k^i$.

In this work, variables γ_k^i and λ_k^i are mutually independent. The stochastic impulsive system model is written as

$$\dot{x}(t) = Ax(t) + BKCx(t-\eta(t)) + \sum_{i=1}^N (1-\lambda_k^i\gamma_k^i) BKI_iC_ie_i(t) \tag{6}$$

and state errors update in the form

$$e_i(\iota_{k+1}) = (1-\lambda_k^i\gamma_k^i)e_i(t_k) + x^i(t_k) - x^i(t_{k+1}). \tag{7}$$

The initial of state $x(t)$ is to be $\psi(t)$, $t \in [\iota_0 - \eta_2, \iota_0]$, $\psi(0) = x_0$, and $\psi(t)$ is a continuous function on $t \in [\iota_0 - \eta_2, \iota_0]$. Define

$$\pi_k^i = \lambda_k^i\gamma_k^i = \begin{cases} 1, & Prob\{\pi_k^i = 1\} = \beta_k^i\theta_k^i \\ 0, & Prob\{\pi_k^i = 0\} = 1 - \beta_k^i\theta_k^i \end{cases}$$

where $\mathbb{E}\{\pi_k^i\} = \alpha_k^i = \beta_k^i\theta_k^i$. Therefore, (6) can be rewritten as

$$\dot{x}(t) = Ax(t) + BKCx(t-\eta(t)) + \textstyle\sum_{i=1}^N (1-\pi_k^i) BKI_iC_ie_i(t) \tag{8}$$

where $e_i(t) = (1-\pi_k^i)e_i(t_k) + x^i(t_k) - x^i(t_{k+1})$, $t \in [\iota_k, \iota_{k+1})$.

The scheduling protocol proposed in this work differs from the existing stochastic protocols, such as [2] and [9], which integrates DoS attack parameters. When occurring cyber-attacks, MBSP is used to defend cyber-attacks and choose the active node. When $\theta_k^i = 1$, there is no DoS attacks. The situation degenerates into the case in [2].

Main results:

Theorem 1: Under the proposed MBSP, for given matrices A, B, C, K, $\bar{M} > 0$, $\bar{N} > 0$ and scalars η_1, η_2, α_k^i, $i = 1,\ldots,N$, if there exist matrices $M_1 > 0$, $M_2 > 0$, $Z > 0$, $N_1 > 0$, $N_2 > 0$, and $G_i > 0$, $S_i > 0$, $T_i > 0$, $i = 1,\ldots,N$ with compatible dimensions such that

$$\Theta_i = \begin{bmatrix} (\eta_2-\eta_1)T_i - \alpha_k^i S_i & * \\ (1-\alpha_k^i)S_i & S_i - G_i \end{bmatrix} < 0,\ \ i = 1,\ldots,N \tag{9}$$

$$[\Pi_{ef}]_{e,f=1,\ldots,4} < 0,\ \ \Pi_{11} = [\Upsilon_{pq}]_{p,q=1,\ldots,8} \tag{10}$$

$$\Upsilon_{11} = A^T Z + ZA + M_1 - 4N_1,\ \ \Upsilon_{42} = -2N_2,\ \ \Upsilon_{43} = -2N_2^T$$

$$\Upsilon_{22} = -M_1 + M_2 - 4N_1 - 4N_2,\ \ \Upsilon_{44} = -8N_2,\ \ \Upsilon_{51} = 6N_1$$

$$\Upsilon_{81}^T = col\{(1-\alpha_1)ZBKI_1C_1,\ldots,(1-\alpha_N)ZBKI_NC_N\}$$

$$\Pi_{22} = \Delta_i = \text{diag}\{-N_1, -N_2, -G_1, \ldots, -G_N\},\ \Upsilon_{33} = -M_2 - 4N_2$$

$$\Pi_{41} = col\{\Phi, \overline{N}\Phi_1', \overline{N}\Phi_{21}', \ldots, \overline{N}\Phi_{2N}'\},\ \Phi = [M, 0, \ldots, 0]$$

$$\Pi_{21} = col\{\eta_1 N_1 \Phi_1, (\eta_2 - \eta_1) N_2 \Phi_1, \Omega_1, \ldots, \Omega_N\},\ \Upsilon_{21} = -2N_1$$

$$\Pi_{31} = col\{\Xi_1, \ldots, \Xi_N\}, \Pi_{33} = \text{diag}\{\Delta_1, \ldots, \Delta_N\},\ \Upsilon_{41} = C^T K^T B^T Z$$

$$\Upsilon_{52} = 6N_1,\ \Upsilon_{55} = -12N_1,\ \Upsilon_{62} = 6N_2,\ \Upsilon_{64} = 6N_2,\ \Upsilon_{66} = -12N_2$$

$$\Upsilon_{73} = 6N_2,\ \Upsilon_{74} = 6N_2,\ \Upsilon_{77} = -12N_2,\ \Upsilon_{88} = \text{diag}\{-T_1, \ldots, -T_N\}$$

$$\Phi_1 = [A, 0, 0, BKC, 0, 0, 0, (1-\alpha_1)BKI_1C_1, \ldots, (1-\alpha_N)BKI_NC_N]$$

$$\Phi_1' = [0, 0, 0, KC, 0, 0, 0, (1-\alpha_1)KI_1C_1, \ldots, (1-\alpha_N)KI_NC_N]$$

$$\Phi_{2i} = [0, \ldots, 0, BKI_iC_i, 0, \ldots, 0],\ \Omega_i = \sqrt{\eta_2 - \eta_1} G_i \Phi_1$$

$$\Phi_{2i}' = [0, \ldots, 0, KI_iC_i, 0, \ldots, 0],\ \Lambda_{iv} = \sqrt{\eta_2 - \eta_1} G_v \Phi_{2i}$$

$$\Xi_i = \sqrt{\alpha_i(1-\alpha_i)} col\{\eta_1 N_1 \Phi_{2i}, (\eta_2 - \eta_1) N_2 \Phi_{2i}, \Lambda_{i1}, \ldots, \Lambda_{iN}\}$$

then system (8) is asymptotically mean-square stable and $\mathbb{E}\{J\} \leq J^* = \psi^T(0) Z \psi(0) + \int_{-\eta_2}^{-\eta_1} \int_{\upsilon}^{0} (\eta_2 - \eta_1) \dot{\psi}^T(\omega) N_2 \dot{\psi}(\omega) d\omega d\upsilon$

$$+ \int_{-\eta_1}^{0} \psi^T(\upsilon) M_1 \psi(\upsilon) d\upsilon + \int_{-\eta_1}^{0} \int_{\upsilon}^{0} \eta_1 \dot{\psi}^T(\omega) N_1 \dot{\psi}(\omega) d\omega d\upsilon$$

$$+ \int_{-\eta_2}^{-\eta_1} \psi^T(\upsilon) M_2 \psi(\upsilon) d\upsilon + \sum_{i=1}^{N} \int_{t_k}^{0} (\eta_2 - \eta_1) \sqrt{G_i} \dot{\psi}(\upsilon)^2 d\upsilon.$$

Proof: Define the Lyapunov functional candidate as

$$V(t) = \sum_{i=1}^{N} e_i^T(\iota_k) S_i e_i(\iota_k) + V_1(t) + V_2(t), V_1(t) = x^T(t) Z x(t)$$
$$+ \int_{-\eta_2}^{-\eta_1} \int_{t+\upsilon}^{t} (\eta_2 - \eta_1) \dot{x}^T(\omega) N_2 \dot{x}(\omega) d\omega d\upsilon$$
$$+ \int_{-\eta_1}^{0} \int_{t+\upsilon}^{t} \eta_1 \dot{x}^T(\omega) N_1 \dot{x}(\omega) d\omega d\upsilon$$
$$+ \int_{t-\eta_2}^{t-\eta_1} x^T(\upsilon) M_2 x(\upsilon) d\upsilon + \int_{t-\eta_1}^{t} x^T(\upsilon) M_1 x(\upsilon) d\upsilon$$
$$V_2(t) = \sum_{i=1}^{N} \int_{t_k}^{t} (\eta_2 - \eta_1) \sqrt{G_i} \dot{x}(\upsilon)^2 d\upsilon.$$

The detailed derivation process can refer to [9], which is omitted here due to the limited pages. ■

Theorem 2: Under the proposed MBSP, for given matrices A, B, C, $\bar{M} > 0$, $\bar{N} > 0$ and scalars $\zeta > 0$, η_1, η_2, α_k^i, $i = 1, \ldots, N$, if there exist $\tilde{M}_1 > 0$, $\tilde{M}_2 > 0$, $X > 0$, $\tilde{N}_1 > 0$, $\tilde{N}_2 > 0$, $G_i > 0$, $S_i > 0$, $T_i > 0$ and D, F with compatible dimensions such that (11) is solvable, where

$$mintr\left\{\sum_{i=1}^{N} G_i o_i\right\}$$
$$\text{s.t. } (9), (12) \text{ and } (13) \tag{11}$$

$$\left[\Pi_{ef}\right]_{e,f=1,\ldots,4} < 0, \Pi_{11} = \left[\Upsilon_{pq}\right]_{p,q=1,\ldots,8} \tag{12}$$

$$\begin{bmatrix} -\zeta I & (DC - CX)^T \\ DC - CX & -I \end{bmatrix} < 0,\ \begin{bmatrix} o_i & * \\ I & G_i \end{bmatrix} > 0 \tag{13}$$

$$\tilde{\Upsilon}_{11} = AX + XA^T + \tilde{M}_1 - 4\tilde{N}_1,\ \tilde{\Upsilon}_{22} = -\tilde{M}_1 + \tilde{M}_2 - 4\tilde{N}_1 - 4\tilde{N}_2$$

$$\tilde{\Upsilon}_{33} = -\tilde{M}_2 - 4\tilde{N}_2,\ \tilde{\Upsilon}_{21} = -2\tilde{N}_1,\ \tilde{\Upsilon}_{42} = -2\tilde{N}_2,\ \tilde{\Upsilon}_{44} = -8\tilde{N}_2$$

$$\tilde{\Upsilon}_{51} = 6\tilde{N}_1,\ \tilde{\Upsilon}_{52} = 6\tilde{N}_1,\ \tilde{\Upsilon}_{62} = 6\tilde{N}_2,\ \tilde{\Upsilon}_{64} = 6\tilde{N}_2,\ \tilde{\Upsilon}_{74} = 6\tilde{N}_2$$

$$\tilde{\Upsilon}_{55} = -12\tilde{N}_1,\ \tilde{\Upsilon}_{66} = -12\tilde{N}_2,\ \tilde{\Upsilon}_{73} = 6\tilde{N}_2,\ \tilde{\Upsilon}_{77} = -12\tilde{N}_2$$

$$\tilde{\Upsilon}_{81}^T = col\{(1-\alpha_1)BFC, \ldots, (1-\alpha_N)BFC\},\ \tilde{\Upsilon}_{41} = C^T F^T B^T$$

$$\tilde{\Pi}_{21} = col\left\{\eta_1 \tilde{\Phi}_1, (\eta_2 - \eta_1)\tilde{\Phi}_1, \tilde{\Omega}_1, \ldots, \tilde{\Omega}_N\right\},\ \tilde{\Upsilon}_{43} = -2\tilde{N}_2^T$$

$$\tilde{\Pi}_{22} = \tilde{\Delta}_i = \text{diag}\left\{-X\tilde{N}_1^{-1}X, -X\tilde{N}_2^{-1}X, -G_1^{-1}, \ldots, -G_N^{-1}\right\}$$

$$\tilde{\Pi}_{33} = \text{diag}\left\{\tilde{\Delta}_1, \ldots, \tilde{\Delta}_N\right\},\ \tilde{\Pi}_{31} = col\left\{\tilde{\Xi}_1, \ldots, \tilde{\Xi}_N\right\}$$

$$\tilde{\Pi}_{41} = col\left\{\tilde{\Phi}, \bar{N}\tilde{\Phi}_1', \bar{N}\tilde{\Phi}_{21}', \ldots, \bar{N}\tilde{\Phi}_{2N}'\right\},\ \tilde{\Phi} = [MX, 0, \ldots, 0]$$

$$\tilde{\Pi}_{44} = \text{diag}\left\{-\bar{M}, -\bar{N}, -\bar{N}, \ldots, -\bar{N}\right\},\ \tilde{\Upsilon}_{88} = \text{diag}\{-T_1, \ldots, -T_N\}$$

$$\tilde{\Xi}_i = \sqrt{\alpha_i(1-\alpha_i)} col\left\{\eta_1 \tilde{\Phi}_{2i}, (\eta_2 - \eta_1)\tilde{\Phi}_{2i}, \tilde{\Lambda}_{i1}, \ldots, \tilde{\Lambda}_{iN}\right\}$$

$$\tilde{\Omega}_i = \sqrt{\eta_2 - \eta_1}\tilde{\Phi}_1,\ \tilde{\Lambda}_{iv} = \sqrt{\eta_2 - \eta_1}\tilde{\Phi}_{2i},\ i, v = 1, \ldots, N$$

then, system (8) is asymptotically mean-square stable. The controller gain is given by $K = FD^{-1}$ and $\mathbb{E}\{J\} \leq \tilde{J}^* = \psi^T(0) Z \psi(0) + \sum_{i=1}^{N} \int_{t_k}^{0} (\eta_2 - \eta_1) \sqrt{G_i} \dot{\psi}(\upsilon)^2 d\upsilon + \int_{-\eta_1}^{0} \psi^T(\upsilon)(\rho^2 \tilde{M}_1 - 2\rho X)\psi(\upsilon) d\upsilon + \int_{-\eta_2}^{-\eta_1} \psi^T(\upsilon)\left(\rho^2 \tilde{M}_2 - 2\rho X\right)\psi(\upsilon) d\upsilon + \int_{-\eta_1}^{0} \int_{\upsilon}^{0} \eta_1 \dot{\psi}^T(\omega)(\rho^2 \tilde{N}_1 - 2\rho X) \times \dot{\psi}(\omega) d\omega d\upsilon + \int_{-\eta_2}^{-\eta_1} \int_{\upsilon}^{0} (\eta_2 - \eta_1) \dot{\psi}^T(\omega)(\rho^2 \tilde{N}_2 - 2\rho X) \dot{\psi}(\omega) d\omega d\upsilon$.

An illustrative example: Suppose that the studied plant is a satellite system in [10]. There are three sensors to be used to measure state signals with $C_1 = [0, 1, 1, 0]$, $C_2 = [1, 0, 1, 1]$ and $C_3 = [0, 1, 0, 1]$ and $x(0) = col\{0.10, -0.18, -0.07, 0.04\}$ and the matrices of system (8) are given by

$$A^T = \begin{bmatrix} 0 & 0 & -0.09 & 0.09 \\ 0 & 0 & 0.09 & -0.09 \\ 1 & 0 & -0.04 & 0.04 \\ 0 & 1 & 0.04 & -0.04 \end{bmatrix},\ B^T = \begin{bmatrix} 0 & 0 & 1 & 0 \end{bmatrix}.$$

Case 1: Optimal choice of β_k^i for the attacked system under MBSP.

Utilizing the stepwise incremental algorithm similar to [9], given $\eta_1 = 0.02$, $\rho = 2$, $\theta_k^i = 0.5$, the optimal solution can be found as $\eta_2 = 0.2$, $\beta_k^i = [0.05, 0.55, 0.4]$ and the corresponding controller gain can be obtained as $K = [-0.0275, -1.7848, 0.8237]$. When $\rho = 1, 2$, [9] has no feasible results, while Theorem 2 in this work is solvable and we can reach the upper bound of delay is 0.25, 0.22. Furthermore, Fig. 3 depicts active sensor nodes, where activenode = 0 represents that stochastic DoS attacks occur, from which we can verify the effectiveness of main results.

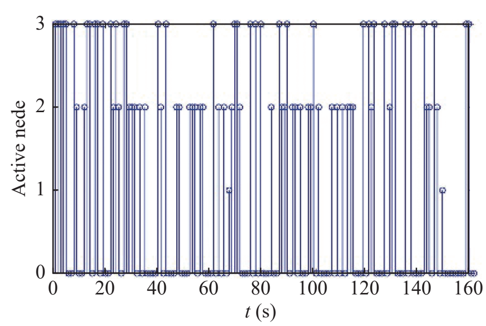

Fig. 3. Active sensor nodes under MBSP.

Case 2: Resilience of MBSP against different intensities of attacks.

Using the same parameter settings of Case 1, Fig. 4 depicts the control input under different intensities of DoS attacks. As Fig. 4 depicts, the proposed MBSP can resist different intensities of DoS attacks and make system stable finally.

Case 3: Comparison between MBSP and stochastic protocol in [2].

Using the same parameter settings of Case 1, state responses with the controller in [2] are shown in Fig. 5. Clearly, the controller of [2] cannot defend Dos attacks, which means that the proposed MBSP has significant advantages over the traditional stochastic protocol in [2] when NCSs are subjected to DoS attacks.

Conclusions: In this work, a novel memory-based scheduling pro-

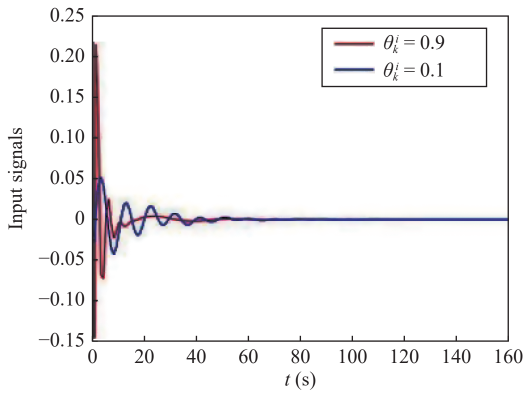

Fig. 4. Control input under $\theta_k^i = 0.9$, $\theta_k^i = 0.1$.

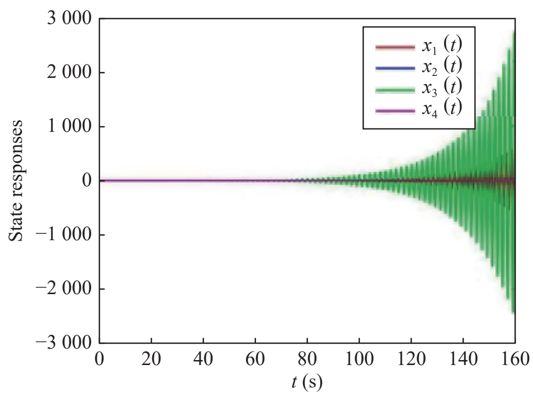

Fig. 5. State responses with the controller in [2].

tocol has been proposed for NCSs under multiple transmission channels and stochastic DoS attacks. First, MBSP has been proposed to alleviate the pressure of signal transmissions for NCSs and allocate network sources according to different intensities of DoS attacks dynamically. Second, further considering packet dropout and network-induced delay, a stochastic impulsive delayed system has been established. Then, by using time-delay methods, sufficient stability criteria and the guaranteed cost output feedback controller gain have been derived. Finally, an illustrative example has been provided to demonstrate the validity of the presented method. This work pays main attention to stochastic protocols. Future research will focus on how to optimally design other scheduling protocols when NCSs are attacked.

Acknowledgments: This work was supported in part by National Natural Science Foundation of China (62173218, 61833011) and the International Corporation Project of Shanghai Science and Technology Commission (21190780300).

References

[1] D. Freirich and E. Fridman, "Decentralized networked control of systems with local networks: A time-delay approach," *Automatica*, vol. 69, pp. 201−209, 2016.

[2] K. Liu, E. Fridman, and K. H. Johansson, "Networked control with stochastic scheduling," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 3071−3076, 2015.

[3] K. Liu, E. Fridman, and L. Hetel, "Network-based control via a novel analysis of hybrid systems with time-varying delays," in *Proc. IEEE Conf. Decis. Control*, 2012, pp. 3886−3891.

[4] M. Donkers, W. Heemels, D. Bernardini, A. Bemporad, and V. Shneer, "Stability analysis of stochastic networked control systems," *Automatica*, vol. 48, no. 5, pp. 917−925, 2012.

[5] V. Dolk, P. Tesi, C. De Persis, and W. Heemels, "Event-triggered control systems under denial-of-service attacks," *IEEE Trans. Control Netw. Syst.*, vol. 4, no. 1, pp. 93–105, 2016.

[6] A.-Y. Lu and G.-H. Yang, "Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial of service," *IEEE Trans. Autom. Control*, vol. 63, no. 6, pp. 1813−1820, 2017.

[7] C. Peng and H. Sun, "Switching-like event-triggered control for networked control systems under malicious denial of service attacks," *IEEE Trans. Autom. Control*, vol. 65, no. 9, pp. 3943−3949, 2020.

[8] Y. Zhang, L. Du, and F. L. Lewis, "Stochastic DoS attack allocation against collaborative estimation in sensor networks," *IEEE/CAA J. Autom. Sinica*, vol. 7, no. 5, pp. 1225−1234, 2020.

[9] J. Zhang, C. Peng, X. Xie, and D. Yue, "Output feedback stabilization of networked control systems under a stochastic scheduling protocol," *IEEE Trans. Cybern.*, vol. 50, no. 6, pp. 2851–2860, 2019.

[10] H. Gao, X. Meng, T. Chen, and J. Lam, "Stabilization of networked control systems via dynamic output-feedback controllers," *SIAM J. Control Optim.*, vol. 48, no. 5, pp. 3643−3658, 2010.