Neurocomputing 000 (2017) 1–8

Contents lists available at ScienceDirect

Neurocomputing

journal homepage: www.elsevier.com/locate/neucom

Resilient control of networked control systems with stochastic denial of service attacks

Hongtao Sun[a], Chen Peng[a,*], Taicheng Yang[a], Hao Zhang[a], Wangli He[b]

[a] Department of Automation, School of Mechatronic Engineering and Automation, Shanghai University, Shanghai, China
[b] The Key Laboratory of Advanced Control and Optimization for Chemical Processes, Ministry of Education, East China University of Science and Technology, Shanghai 200237, China

ARTICLE INFO

Article history:
Received 13 June 2016
Revised 14 February 2017
Accepted 23 February 2017
Available online xxx

Keywords:
Networked control systems
DoS attacks
Markovian process
Resilient control

ABSTRACT

This paper focuses on resilient control of networked control systems (NCSs) under the denial of service (DoS) attacks characterized by a Markov process. Firstly, based on the game between attack strategies and defense strategies, the packet dropouts induced by DoS attacks are modeled as a Markov process. Secondly, an NCS under DoS attacks is modeled as a Markovian jump linear system. Then, by use of the Lyapunov theory and the derived NCS model, four theorems are given for the system stability analysis and controller design. Finally, a numerical example is used to illustrative the effectiveness of proposed method.

1. Introduction

Networked control systems (NCSs) have received an increasing attention in the past decades. At present, NCSs have been widely applied in industrial processes, electric power networks, intelligent transportation and so on [1,2,3,4,27,28]. With the growing of the NCSs, network, as a critical element in an NCS, is vulnerable to cyber-threats which can menace the control systems [5,10]. In the presence of network attacks or unreliable links, the separation design of the security and control is no longer available. Therefore, the co-design of NCSs under consideration of network attacks and control scheme is extremely urgent [6,7].

A most common network attack is so-called denial of service (DoS). DoS attacks usually prevent the information exchange through a large volume invalid data to deliberately consume the network resources. Control problems in the presence of network attacks have been discussed in some recent works, such as [8,9,11,12,25,26]. On the one hand, an attacker would try it best to degrade the performance of the NCSs. In the scenario that DoS occurred during the data transmission between sensor and remote estimator with energy constraints, an optimal attack schedules that to maximize the expected average estimation error is studied in [9]. Considering the limitation of attackers, a feedback controller that maximize a given function subjected to safety and power constraints is designed for a class of DoS attack models in [13]. A two-player zero-sum stochastic game is formulated to model the dynamic interactions between a jammer (attacker) and a sensor transmitter (defender) in [14]. On the other hand, the stability of NCS should be guaranteed when attack occurred from the perspective of controller design. For a signal-input remote control system, a control strategy with placing poles method is studied under the periodic DoS attack in [8]. Under a certain condition of frequency and duration of DoS, the input-to-state stability for the closed loop is analyzed in [11]. A hidden Markovian model which is used to describe the attacker jams the control packets stochastically and the stability problem are investigated in [15]. However, there are few works focus on the stochastic consecutive packets dropout. These issues motivate the current study.

Generally, the attacker's purpose is to prevent the updating of control signal for the DoS attacks. That is to say, packet dropouts would occur due to the DoS attacks and then induce the instability of the control systems by denying the communication of control signal. Traditionally, the robust control strategies that only consider the worst case of QoS (Quality of Service) are often used to stabilize the NCSs. However, these robust controllers are deemed to lack of flexibility and adaptability. So, more flexible control strategies with the consideration of the concrete behaviors of packets dropout should be designed. Contributions to this topic have been reported in [17–20]. The stability and its controller design with both arbitrary and Markovian packet losses are established via a packet-loss depended Lyapunov approach in [16]. For a class of continuous-time and discrete-time Markovian jump linear system (MJLS) with partly unknown transition probabilities, the

* Corresponding author.
E-mail address: c.peng@shu.edu.cn (C. Peng).

http://dx.doi.org/10.1016/j.neucom.2017.02.093
0925-2312/

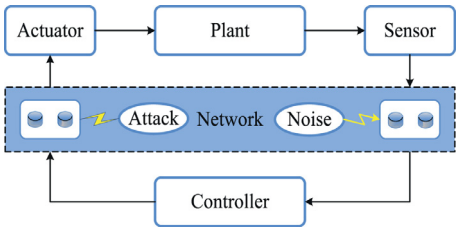

Fig. 1. An NCS under DoS attacks and stochastic noise.

stability and stabilization problems are investigated in [18]. Without the knowledge of all transition probabilities, packet-loss-dependent switching controllers which considered both the packet-loss and time delay are designed in [19]. However, network attacks are ignored in the above mentioned works.

The objective of this paper is to design a resilient control strategy to tackle the DoS attacks problem for a class of NCSs. Different from the single robust controller, we aim to find a group of controllers to deal with varying degrees of DoS attacks. In fact, the packet dropouts can be seen as the results of game between attack and defense. However, these results are stochastic and can be described as a Markov process. The main contributions of the paper can be summarized as:

(a) Due to the stochastic game between both sides of attack and defense, the packet dropouts induced by DoS attacks is modeled as a Markov process with full or part transition probabilities, and an MJLS model is well constructed to describe the networked control systems with the stochastic noises. It is convenient for us to design the resilient controller for the studied system under the DoS attacks; and
(b) By use of the proposed MJLS model, a stability criterion and a stabilization criterion are established for the system under consideration with the stochastic DoS attacks and stochastic noise. Since the full transition probabilities are not needed, the designed control scheme is resilient to the DoS attacks.

The rest of this paper is organized as follows: In Section 2, a MJLS model for the studied system is formulated under consideration of the DoS attacks and the feedback noise; In Section 3 , stochastic stability and stabilization criteria under network attacks are derived with the full and partial-known transition probabilities; The following Section 4 shows the numerical simulations to verify the given results; The last Section 5 concludes this paper.

2. Problem formulation

In this section, the secure control of discrete-time linear system is formulated as a Markov jumping system under consideration of the DoS attacks.

A typical scenario of an NCS under the DoS attacks and the stochastic feedback noise is depicted in Fig. 1. The plant dynamic model is given as:

$$\dot{x}(t) = Ax(t) + Bu(t) \tag{1}$$

where $x(t) \in \Re^n$ is the state vector; $u(t) \in \Re^m$ is the control input; A, B are constant matrices with appropriate dimensions.

Suppose the control signal $u(t)$ is hold by a zero-order-holder with a sampling period T_0. Then the discrete-time model of (1) can be represented as

$$x_{\gamma_0}(k+1) = G_{\gamma_0}x(k) + H_{\gamma_0}u(k) \tag{2}$$

where $G_{\gamma_0} = e^{AT_0}, H_{\gamma_0} = B\int_0^{T_0} e^{A\tau}d\tau$ and γ_0 represents that there is no DoS attack.

In an ideal network state, the sensor and control signal can be updated every T_0 time. However, due to the vulnerability of network, the transmission of sensor or control signal is often blocked by an attacker that may cause the denial of service. Consider the scenario that there is an attacker between controller and actuator, and denote γ_i as the subsystem that there are i-consecutive packets dropout for γ_i subsystem. Then, these i-consecutive packets cannot be received by the actuator, and the actuator generates an input that is based on the most recently received control signal until the end of attacks. An control signal update example can be seen in Fig. 2.

When the control packets are jammed, the varying sampling period method [21,22] can be adopted to obtain the discrete-time systems. So, if there are i-consecutive packet dropouts, in this case, the discrete-time system model can be written as:

$$x_{\gamma_i}(k+1) = G_{\gamma_i}x(k) + H_{\gamma_i}u(k) \tag{3}$$

where $G_{\gamma_i} = e^{A(\gamma_i+1)T_0}, H_{\gamma_i} = B\int_0^{(\gamma_i+1)T_0} e^{A\tau}d\tau$. The subsystem γ_i jumps to the subsystem γ_j satisfying a Markov transition probability for all $i, j \in S$. Similar to [15,16], suppose the i take values in set $S = \{1, 2, \ldots, M\}$, where M represents the energy constraint of DoS attacks, and suppose that the attacker adopt attack strategies $A = \{a_1, a_2, \ldots, a_M\}$ and the defender adopt defend strategies $D = \{d_1, d_2, \ldots, d_M\}$, the results between attack and defense which indicated by packet dropouts $S = \{1, 2, \ldots, M\}$ can be seen as stochastic satisfying the following transition probabilities:

$$p_{ij}(a_i, d_j) = Pr(\gamma_j(k+1) = j|\gamma_i(k) = i) \tag{4}$$

where the $p_{ij}(a_i, d_j)$ represents that packet dropouts shift from i to j if attacker adopt attack strategy a_i and the defender adopt defend strategy d_j. Hereafter, the $p_{ij}(a_i, d_j)$ will be denoted as p_{ij} for simplicity. shown In what follows, two cases about the transition probability matrix are considered:

(I) Full transition probability matrix are known as listed in (5), which means that all games behaviors can be obtained completely

$$P = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1M} \\ p_{21} & p_{22} & \cdots & p_{2M} \\ \vdots & \vdots & \vdots & \vdots \\ p_{M1} & p_{M2} & \cdots & p_{MM} \end{pmatrix} \tag{5}$$

where $p_{ij} \geq 0$ and $\sum_{j=1}^{M} p_{ij} = 1$; and

(II) Partial transition probability matrix are known, as shown in (6), which represents that only partial games behavior can be known a priori,

$$P = \begin{pmatrix} p_{11} & p_{12} & \mathcal{X} & \cdots & p_{1M} \\ \mathcal{X} & p_{22} & p_{23} & \cdots & \mathcal{X} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ p_{M1} & \mathcal{X} & \mathcal{X} & \cdots & p_{MM} \end{pmatrix} \tag{6}$$

where p_{ij} are known transition probabilities as in (5) and $\mathcal{X}$ are unknown transition probabilities.

To make the proposed method more suitable for practical engineering, similar to [23], the controller considering the uncertain system state is designed as:

$$u(k) = K_{\gamma_i}diag[1 + v_{k1}, 1 + v_{k2}, \ldots, 1 + v_{kn}]x(k) \tag{7}$$

where v_{ki} is independent Gaussian white noise with $E[v_{ki}] = 0$, $E[v_{ki}^2] = \sigma^2$ and $E[v_{ki}v_{kj}] = 0$.

Integrating the Eqs. (3) and (7), we have

$$x_{\gamma_i}(k+1) = (G_{\gamma_i} + H_{\gamma_i}K_{\gamma_i}diag[1 + v_{k1}, 1 + v_{k2}, \ldots, 1 + v_{kn}])x(k) \tag{8}$$

Please cite this article as: H. Sun et al., Resilient control of networked control systems with stochastic denial of service attacks, Neurocomputing (2017), http://dx.doi.org/10.1016/j.neucom.2017.02.093