2015 IEEE 54th Annual Conference on Decision and Control (CDC)
December 15-18, 2015. Osaka, Japan

Event-Triggered Control over Unreliable Networks Subject to Jamming Attacks

Ahmet Cetinkaya, Hideaki Ishii, and Tomohisa Hayakawa

Abstract— **Event-triggered networked control of a linear dynamical system is investigated. Specifically, the dynamical system and the controller are assumed to be connected through a communication channel. State and control input information packets between the system and the controller are attempted to be exchanged over the network only at time instants when certain triggering conditions are satisfied. We provide a probabilistic characterization for the link failures which allows us to model random packet losses due to unreliability in transmissions as well as those caused by malicious jamming attacks. We obtain conditions for the almost sure stability of the closed-loop system, and we illustrate the efficacy of our approach with a numerical example.**

I. Introduction

One of the main challenges in networked control systems is that communication between plant and controller may not always be reliable. State measurement and control input packets may fail to be transmitted at times due to network congestion or errors in communication. In the literature, unreliability of a network is often characterized through random models for packet loss events [1]. For instance, in [2], [3], Bernoulli processes are used for modeling packet losses in a network. Furthermore, in [4], [5], packet loss events are characterized in a more general way by employing Markov chains. In these studies, a variety of control methods are proposed to ensure stability of networked control systems that face random packet losses.

More recently, cyber security has become a critical issue in networked control systems since the channels are nowadays connected via the Internet or wireless communications [6], [7]. Here, in addition to random losses, we consider communication effects due to jamming attacks initiated by malicious agents. Such attacks may block the communication link and effectively prevent transmission of packets between the plant and the controller. In a few recent works [8]–[11], networked control problems under malicious jamming attacks were investigated.

In this paper we explore feedback control of a discrete-time linear system over a network that is subject to both random packet losses due to unreliability of the communication channel and jamming attacks coming from an intelligent attacker. We employ an event-triggered control framework, where the plant and the controller attempt to exchange state and control input information packets only at times that correspond to event-triggering instants. Following the approach in [12], [13], we utilize Lyapunov-like functions to characterize the triggering conditions. The triggering conditions that we propose in this paper ensure that the value of a Lyapunov-like function of the state stays within certain limits. Packet exchanges are attempted only before the value of the Lyapunov-like function is predicted to exceed a certain level. In a successful packet exchange scenario, state measurements are sent from the plant to the controller, which computes a control input and sends it back to the plant. However, state measurement or control input packets may fail to be transmitted due to random packet losses and jamming attacks. We model random losses using a binary-valued *time-inhomogeneous* Markov chain. To characterize jamming attacks, we follow the approach of [10]. Rather than specifying predetermined patterns or distributions for the occurrences of jamming attacks, we allow jamming attacks to happen arbitrarily as long as the total number of packet exchange attempts that face jamming attacks are almost surely bounded by a certain ratio of the number of total packet exchange attempts.

We consider both the case where random packet losses and jamming attacks are independent and the case where the attacker may use information of past random packet losses in generating a jamming attack strategy. The main theoretical challenge in dealing with both of these cases stems from the fact that random losses and jamming attacks are of different nature and hence have different models. By utilizing a tail probability inequality for the sum of processes that represent random losses and jamming attacks, we show that a probabilistic characterization for the evolution of the total number of packet exchange failures allows us to deal with both cases. Based on this characterization, we obtain conditions for almost sure asymptotic stability of the closed-loop event-triggered networked control system. Furthermore, we present a numerical method for finding stabilizing feedback gains as well as parameters for the event-triggering mechanism.

The paper is organized as follows. In Section II, we describe the event-triggered networked control system under random and jamming-related packet losses. We provide sufficient conditions for almost sure asymptotic stability of the closed-loop control system in Section III and present an illustrative numerical example in Section IV. Finally, in Section V, we conclude the paper.

A. Cetinkaya and T. Hayakawa are with the Department of Mechanical and Environmental Informatics, Tokyo Institute of Technology, Tokyo 152-8552, Japan. ahmet@dsl.mei.titech.ac.jp, hayakawa@mei.titech.ac.jp

H. Ishii is with the Department of Computational Intelligence and Systems Science, Tokyo Insitute of Technology, Yokohama, 226-8502, Japan. ishii@dis.titech.ac.jp

This work was supported in part by Japan Science and Technology Agency under the EMS-CREST program.

We use a fairly standard notation in the paper. Specifically, we denote positive and nonnegative integers by $\mathbb{N}$ and $\mathbb{N}_0$, respectively. We write $\mathbb{R}$ for the set of real numbers, $\mathbb{R}^n$ for the set of $n \times 1$ real column vectors, and $\mathbb{R}^{n\times m}$ for the set of $n \times m$ real matrices. Moreover, $(\cdot)^{\mathrm{T}}$ denotes transpose, $\|\cdot\|$ denotes the Euclidean vector norm, and $\lfloor\cdot\rfloor$ denotes the largest integer that is less than or equal to its real argument. The notation $\mathbb{P}[\cdot]$ denotes the probability on a probability space $(\Omega, \mathcal{F}, \mathbb{P})$ with filtration $\{\mathcal{F}_i\}_{i\in\mathbb{N}_0}$.

The proofs of the results are omitted due to limitation in space, but can be found in [14].

II. Event-Triggered Networked Control

In this section we provide the mathematical model for the event-triggered networked control system. We then present a characterization of a network that faces random packet losses and packet losses caused by jamming attacks.

A. Event-Triggered Control System

Consider the linear dynamical system

$$x(t+1) = Ax(t) + Bu(t), \quad x(0) = x_0, \quad t \in \mathbb{N}_0, \quad (1)$$

where $x(t) \in \mathbb{R}^n$ and $u(t) \in \mathbb{R}^m$ denote the state and the control input; furthermore, $A \in \mathbb{R}^{n\times n}$ and $B^{n\times m}$ are the state and input matrices, respectively.

In this paper, we use the event-triggering framework (see [13] and the references therein), where the control input is only updated when a certain triggering condition is satisfied. The triggering condition is checked at each time step at the plant side.

In the networked operation setting, the plant and the controller are connected through a communication channel and attempt to exchange information packets at times corresponding to event-triggering instants. We consider the case where packets are transmitted without delay, but they may get lost. In a successful packet exchange scenario, at a certain time instant, measured plant states are transmitted to the controller, which generates a control input based on the received state information and sends a packet containing the control input information to the plant. The transmitted control input is applied at the plant side. In the case of an unsuccessful packet exchange attempt, either the measured state packet or the control input packet may get dropped, and in such cases control input at the plant side is set to 0.

We use $\tau_i \in \mathbb{N}_0, i \in \mathbb{N}_0$, to denote the time instants at which packet exchanges between the plant and the controller are attempted. To characterize these time instants we utilize a quadratic Lyapunov-like function $V\colon \mathbb{R}^n \to [0,\infty)$ given by $V(x) \triangleq x^{\mathrm{T}}Px$, where $P > 0$. Letting $\tau_0 = 0$, we describe τ_i, $i \in \mathbb{N}$, and control input $u(t)$ applied to the plant by

$$\tau_{i+1} \triangleq \min\Big\{t \in \{\tau_i+1, \tau_i+2, \ldots\}\colon t \geq \tau_i + \theta \text{ or } V(Ax(t)+Bu(\tau_i)) > \beta V(x(\tau_i))\Big\}, \quad (2)$$

$$u(t) \triangleq (1-l(i))\,Kx(\tau_i),\ t \in \{\tau_i, \ldots, \tau_{i+1}-1\}, \quad (3)$$

for $i \in \mathbb{N}_0$, where $\beta \in (0,1)$, $\theta \in \mathbb{N}$, and $\{l(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ is a binary-valued process that characterizes success or failure of packet exchange attempts. When $l(i) = 0$, packet exchange attempt at time τ_i is successful and the piecewise-constant control input at the plant side is set to $u(\tau_i) = Kx(\tau_i)$, where $K \in \mathbb{R}^{m\times n}$ denotes the feedback gain. On the other hand, the case $l(i) = 1$ indicates that either the packet sent from the plant or the packet sent from the controller is lost at time τ_i. Again, in such cases, control input at the plant side is set to 0.

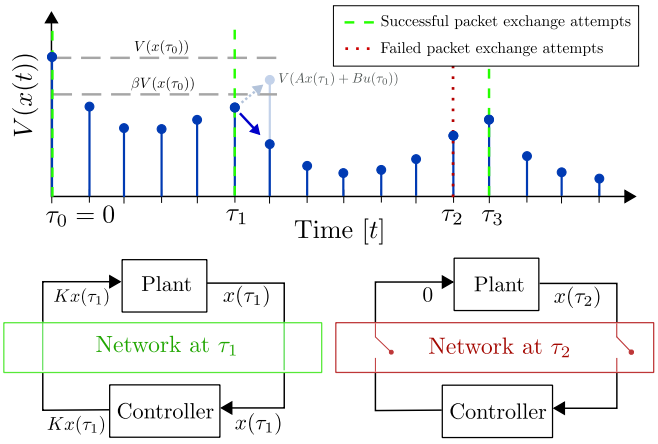

Fig. 1. Networked control system operation

The triggering condition (2) involves two parts. The part characterized by $V(Ax(t)+Bu(\tau_i)) > \beta V(x(\tau_i))$ ensures that after a successful packet exchange attempt at τ_i, the value of the Lyapunov-like function $V(\cdot)$ stays below the level $\beta V(x(\tau_i))$ until the next packet exchange attempt. Furthermore, the triggering condition $t \geq \tau_i + \theta$ ensures that two consecutive packet exchange attempt instants are at most θ steps apart, that is, $\tau_{i+1} - \tau_i \leq \theta$, $i \in \mathbb{N}_0$. Although the specific value of θ does not affect the results developed below, the boundedness of packet exchange attempt intervals guarantees that τ_i (and hence $V(x(\tau_i))$) are well-defined for each $i \in \mathbb{N}$. In practice, the value of θ can be selected considering how frequent the plant state is desired to be monitored by the controller side.

Operation of the event-triggered networked control system is illustrated in Fig. 1. The triggering condition (2) is checked at the plant side at each step $t \in \mathbb{N}_0$. At times $t = \tau_i$, $i \in \mathbb{N}$, the triggering condition is satisfied and packet exchanges between the plant and the controller are attempted. For this example, packet exchange is attempted at time $t = \tau_1$, since $V(Ax(t) + Bu(\tau_0)) > \beta V(x(\tau_0))$. At this time instant, the plant and the controller successfully exchange state and control input packets over the network, and as a result, control input on the plant side is updated to $Kx(\tau_1)$. Note that packet exchange attempts are not always successful, and may fail due to loss of packets in the network. For instance, the packet exchange attempt at time τ_2 fails for the case of Fig. 1. In this case, the control input at the plant side is set to 0 at time τ_2, which results in an unstable behavior. A packet exchange is attempted again at the very next time step τ_3, since the triggering condition is also satisfied at that instant.

Remark 2.1: The event-triggering framework we describe

above requires a plant-side mechanism for checking the triggering condition (2) at each time step. If the overall practical setup of the process does not allow placing such a mechanism at the plant side, following the self-triggering control approach described in [15], we can use a decision mechanism at the controller side. In this case, packet exchange times are decided at the controller side based on the state information obtained at previously successful packet exchange attempts.

B. Characterization of a Network with Random Packet Losses and Packet Losses Caused by Jamming Attacks

Packet transmission failures in a network may have different reasons. Packet losses caused by network congestion may be accurately described using stochastic models [16]. However, only stochastic models would not be enough to characterize packet losses if the communication channel is subject to jamming attacks of a malicious agent. In what follows we characterize the effects of certain stochastic and jamming-related packet loss models in a unified manner by investigating dynamical evolution of the total number of packet exchange failures.

First, we define a nonnegative integer-valued process $\{L(k) \in \mathbb{N}_0\}_{k\in\mathbb{N}}$ by

$$L(k) \triangleq \sum_{i=0}^{k-1} l(i), \quad k \in \mathbb{N}. \tag{4}$$

Note that $L(k)$ denotes the total number of *failed* packet exchange attempts during the time interval $[0, \tau_{k-1}]$.

Assumption 2.1: There exist scalars $\rho \in [0,1]$, $\gamma_k \in [0,\infty)$, $k \in \mathbb{N}$, such that

$$\mathbb{P}[L(k) > \rho k] \leq \gamma_k, \quad k \in \mathbb{N}, \tag{5}$$

$$\sum_{k\in\mathbb{N}} \gamma_k < \infty. \tag{6}$$

Note that conditions (5) and (6) provide a probabilistic characterization of the evolution of the total number of packet exchange failures through scalars $\rho \in [0,1]$, $\gamma_k \in [0,\infty)$, $k \in \mathbb{N}$. A closely related characterization for packet dropouts in a communication link is presented in [3]; the scalar ρ in (5) corresponds to the notion *dropout rate* discussed there.

The following result is a direct consequence of Borel-Cantelli lemma (see [17]) and it shows that under Assumption 2.1, the long run average of the total number of failed packet exchanges is upper bounded by ρ.

Lemma 2.2: If there exist scalars $\rho \in [0,1]$, $\gamma_k \in [0,\infty)$, $k \in \mathbb{N}$, such that (5), (6) hold, then $\limsup_{k\to\infty} \frac{L(k)}{k} \leq \rho$, almost surely.

It is important to note that for any packet loss model, Assumption 2.1 is trivially satisfied with $\rho = 1$, and $\gamma_k = 0, k \in \mathbb{N}$, since $L(k) \leq k$. On the other hand, as illustrated in the following, for certain random and jamming-related packet loss models, ρ can be obtained to be strictly smaller than 1.

1) Random Losses: To characterize random packet losses in the communication channel, we utilize time-inhomogeneous Markov chains. Specifically, let $\{l_{\mathrm{R}}(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ be an $\mathcal{F}_i$-adapted time-inhomogeneous Markov chain characterized by initial distributions $\vartheta_q \in [0,1]$, $q \in \{0,1\}$, and time-varying transition probabilities $p_{q,r}\colon \mathbb{N}_0 \to [0,1]$, $q,r \in \{0,1\}$, such that

$$\mathbb{P}[l_{\mathrm{R}}(0) = q] = \vartheta_q, \ q \in \{0,1\},$$
$$\mathbb{P}[l_{\mathrm{R}}(i+1) = r | l_{\mathrm{R}}(i) = q] = p_{q,r}(i), \ q,r \in \{0,1\}, \ i \in \mathbb{N}_0.$$

The state $l_{\mathrm{R}}(i) = 1$ indicates that the network faces random packet losses at time τ_i, and hence the packet exchange attempt at τ_i results in failure. Note that in this characterization, the event that a packet exchange attempt fails depends on the states of previous packet exchange attempts. Furthermore, transition probabilities between success ($l_{\mathrm{R}}(i) = 0$) and failure ($l_{\mathrm{R}}(i) = 1$) states of packet exchange attempts are time-dependent. For instance, the probability of packet exchange failure at time τ_{i+1} is given by $p_{l_{\mathrm{R}}(i),1}(i)$.

It is important to note that the time-inhomogeneous Markov chain characterization of random packet losses generalizes the Bernoulli and *time-homogeneous* Markov chain models that are often used in the literature.

2) Jamming Attacks : For jamming attacks coming from an intelligent attacker, a model capturing the attack strategy of a malicious agent has been proposed in [10]. In that study, the sum of the length of attack durations is assumed to be bounded by a certain ratio of total time.

We follow the approach of [10] for modeling packet exchange failures due to a jamming attack. Specifically, let $\{l_{\mathrm{J}}(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ denote the state of jamming attacks. The state $l_{\mathrm{J}}(i) = 1$ indicates that the network is subject to a jamming attack at time τ_i. We consider the case where the number of packet exchange attempts that face jamming attacks are upper bounded almost surely by a certain ratio of the total number of packet exchange attempts, that is, $\{l_{\mathrm{J}}(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ satisfies

$$\mathbb{P}\big[\sum_{i=0}^{k-1} l_{\mathrm{J}}(i) \leq \kappa + \frac{k}{\tau}\big] = 1, \quad k \in \mathbb{N}, \tag{7}$$

where $\kappa \geq 0$ and $\tau > 1$. In this characterization, among k packet exchange attempts, at most $\kappa + \frac{k}{\tau}$ of them are affected by jamming attacks. The ratio $\frac{1}{\tau}$ corresponds to the notion *jamming rate* discussed in [18]. Note that when $\kappa = 0$, (7) implies $l_{\mathrm{J}}(i) = 0$, $i \in \{0,\ldots,\lfloor\tau\rfloor\}$, almost surely. Scenarios that involve possible jamming attacks during the first few packet exchange attempts can be modeled by setting $\kappa > 0$. Note that the characterization in (7) does not require $l_{\mathrm{J}}(i)$, $i \in \mathbb{N}_0$, to follow a particular distribution. In fact, $l_{\mathrm{J}}(\cdot)$ may be generated in a deterministic fashion, or it may involve randomness.

3) Combination of Random and Jamming-Related Losses: In order to model the case where the network is subject to both random losses and malicious jamming attacks, we

define $\{l(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ by

$$l(i) = \begin{cases} 1, & l_{\mathrm{R}}(i) = 1 \text{ or } l_{\mathrm{J}}(i) = 1, \\ 0, & \text{otherwise}, \end{cases} \quad i \in \mathbb{N}_0, \tag{8}$$

where $\{l_{\mathrm{R}}(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ is a time-inhomogeneous Markov chain characterizing random packet losses (see Section II-B.1) and $\{l_{\mathrm{J}}(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ satisfying (7) is a binary-valued process that characterizes jamming attacks (see Section II-B.2).

Proposition 2.3 below provides a range of values for $\rho \in (0,1)$ that satisfy Assumption 2.1 in the case that the network under consideration faces both random packet losses and jamming attacks.

Proposition 2.3: Consider the packet loss indicator process $\{l(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ given by (8) where $\{l_{\mathrm{R}}(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ and $\{l_{\mathrm{J}}(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ are mutually independent. If there exist scalars $p_0, p_1 \in (0,1)$ such that

$$p_{q,1}(i) \leq p_1, \tag{9}$$

$$p_{q,0}(i) \leq p_0, \quad q \in \{0,1\}, \quad i \in \mathbb{N}_0, \tag{10}$$

$$p_1 + \frac{p_0}{\tau} < 1, \tag{11}$$

hold, then for all $\rho \in (p_1 + \frac{p_0}{\tau}, 1)$, there exist $\gamma_k \in [0,\infty)$, $k \in \mathbb{N}$, that satisfy (5), (6).

Note that in Proposition 2.3, $\{l_{\mathrm{R}}(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ and $\{l_{\mathrm{J}}(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ are assumed to be mutually independent processes. In other words, packet exchange attempt failures due to jamming attacks are assumed to be independent of packet exchange attempt failures due to random packet losses. This assumption would not be satisfied in the case that the malicious jamming attacker has information of the past random packet losses in the communication channel and utilizes this information in the attack strategy. Proposition 2.4 below deals with such cases.

Proposition 2.4: Consider the packet loss indicator process $\{l(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$. Suppose there exists a scalar $p_1 \in (0,1)$ such that (9) and

$$p_1 + \frac{1}{\tau} < 1, \tag{12}$$

hold. Then for all $\rho \in (p_1 + \frac{1}{\tau}, 1)$, there exist $\gamma_k \in [0,\infty)$, $k \in \mathbb{N}$, that satisfy (5), (6).

In comparison with Proposition 2.3, Proposition 2.4 provides a more restricted range of values for ρ that satisfy Assumption 2.1. The interpretation may be that the malicious jamming attacker is more knowledgeable and may use information of the past random packet losses in the attack strategy.

III. Conditions for Almost-Sure Asymptotic Stability of the Networked Control System

In this section, we investigate stability of the closed-loop event-triggered networked control system (1)–(3), which is a stochastic dynamical system due to probabilistic characterization of packet losses. Below we define almost sure asymptotic stability for stochastic dynamical systems.

Definition 3.1: The zero solution $x(t) \equiv 0$ of a stochastic system is *almost surely stable* if, for all $\epsilon > 0$ and $\bar{p} > 0$, there exists $\delta = \delta(\epsilon, \bar{p}) > 0$ such that if $\|x(0)\| < \delta$, then

$$\mathbb{P}[\sup_{t\in\mathbb{N}_0} \|x(t)\| > \epsilon] < \bar{p}. \tag{13}$$

Moreover, the zero solution $x(t) \equiv 0$ is *asymptotically stable almost surely* if it is almost surely stable and

$$\mathbb{P}[\lim_{t\to\infty} \|x(t)\| = 0] = 1. \tag{14}$$

In Theorem 3.2 below, we present sufficient conditions for almost sure asymptotic stability of the zero solution of the dynamical system (1)–(3).

Theorem 3.2: Consider the linear dynamical system (1). Suppose that the process $\{l(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ characterizing packet exchange failures in the network satisfies Assumption 2.1 with scalar $\rho \in [0,1]$. If there exist a matrix $K \in \mathbb{R}^{m\times n}$, a positive-definite matrix $P \in \mathbb{R}^{n\times n}$, and scalars $\beta \in (0,1)$, $\varphi \in [1,\infty)$ such that

$$\beta P - (A+BK)^{\mathrm{T}} P (A+BK) \geq 0, \tag{15}$$

$$\varphi P - A^{\mathrm{T}} P A \geq 0, \tag{16}$$

$$(1-\rho)\ln\beta + \rho \ln\varphi < 0, \tag{17}$$

then the event-triggered control law (2), (3) guarantees almost sure asymptotic stability of the zero solution $x(t) \equiv 0$ of the closed-loop system dynamics.

Theorem 3.2 provides a sufficient condition under which the event-triggered control law (2), (3) guarantees almost sure asymptotic stability of the linear dynamical system (1) for the case packet losses satisfy Assumption 2.1. Note that the scalars $\beta \in (0,1)$ and $\varphi \in [1,\infty)$ in conditions (15) and (16) characterize upper bounds on the growth of a Lyapunov-like function. Specifically, when a packet exchange attempt between the plant and the controller is successful at time τ_i, the condition (15) together with (2) guarantees that $V(x(\tau_{i+1})) \leq \beta V(x(\tau_i))$. On the other hand, if a packet exchange attempt between the plant and the controller is unsuccessful at time τ_i, it follows from (16) and (2) that $V(x(\tau_{i+1})) \leq \varphi V(x(\tau_i))$. If unsuccessful packet exchange attempts are sufficiently statistically rare (successful packet exchanges happen statistically frequently) such that condition (17) is satisfied, then the closed-loop system stability is guaranteed.

In the following, we outline a numerical method for designing the feedback gain $K \in \mathbb{R}^{m\times n}$, as well as the positive-definite matrix $P \in \mathbb{R}^{n\times n}$ and the scalar $\beta \in (0,1)$ used in the event-triggered control law (2), (3).

Corollary 3.3: Consider the linear dynamical system (1). Suppose that the process $\{l(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ characterizing packet exchange failures in the network satisfies Assumption 2.1 with scalar $\rho \in [0,1]$. If there exist a matrix $M \in \mathbb{R}^{m\times n}$, a positive-definite matrix $Q \in \mathbb{R}^{n\times n}$, and

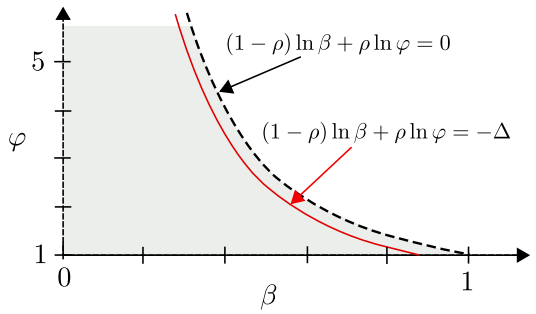

Fig. 2. Region for $\beta \in (0,1)$ and $\varphi \in [1,\infty)$ that satisfy (17) for $\rho = 0.4$

scalars $\beta \in (0,1)$, $\varphi \in [1,\infty)$ such that (17),

$$\begin{bmatrix} \beta Q & (AQ+BM)^{\mathrm{T}} \\ AQ+BM & Q \end{bmatrix} \geq 0, \tag{18}$$

$$\begin{bmatrix} \varphi Q & (AQ)^{\mathrm{T}} \\ AQ & Q \end{bmatrix} \geq 0, \tag{19}$$

hold, then the event-triggered control law (2), (3) with $P \triangleq Q^{-1}$ and $K \triangleq MQ^{-1}$ guarantees almost sure asymptotic stability of the zero solution $x(t) \equiv 0$ of the closed-loop system dynamics.

Proof: Using Schur complements (see [19]), we transform (18) and (19), respectively, into

$$\beta Q - (AQ+BM)^{\mathrm{T}} Q^{-1} (AQ+BM) \geq 0, \tag{20}$$

$$\varphi Q - (AQ)^{\mathrm{T}} Q^{-1} AQ \geq 0. \tag{21}$$

Now by multiplying both sides of inequalities (20) and (21) from left and right by Q^{-1}, we obtain (15) and (16) with $P = Q^{-1}$ and $K = MQ^{-1}$. Thus, the result follows from Theorem 3.2. □

Note that inequalities (18) and (19) are linear in $M \in \mathbb{R}^{m\times n}$ and $Q \in \mathbb{R}^{n\times n}$ for fixed $\beta \in (0,1)$ and $\varphi \in [1,\infty)$. In our method we seek feasible solutions M and Q for linear matrix inequalities (18) and (19) by iterating over a set of values for $\beta \in (0,1)$ and $\varphi \in [1,\infty)$ that satisfy (17). We do not need to search β and φ in the entire space characterized by (17). We restrict the search space and only check feasibility of (18) and (19) for larger values of β and φ that are close to the boundary of the search space identified by $(1-\rho)\ln\beta+\rho\ln\varphi = 0$. Specifically, we set $\Delta > 0$ as a small positive real number, and then we iterate over a set of values for β in the range $(0, e^{-\frac{\Delta}{1-\rho}}]$ to look for feasible solutions M and Q for linear matrix inequalities (18) and (19) with $\varphi = e^{-\frac{(1-\rho)\ln\beta+\Delta}{\rho}}$. In this approach, feasibility of (18) and (19) is checked only for $\beta \in (0,1)$, $\varphi \in [1,\infty)$ that are on the curve $(1-\rho)\ln\beta+\rho\ln\varphi = -\Delta$. We illustrate the curve $(1-\rho)\ln\beta+\rho\ln\varphi = -\Delta$ with solid red line in Fig. 2, where the dark shaded region corresponds to $\beta \in (0,1)$ and $\varphi \in [1,\infty)$ that satisfy (17). Note that picking smaller values for $\Delta > 0$ moves the curve towards the boundary identified by $(1-\rho)\ln\beta+\rho\ln\varphi = 0$. Also, there is no conservatism in *not* considering $\beta \in (0,1)$, $\varphi \in [1,\infty)$ such that $(1-\rho)\ln\beta+\rho\ln\varphi < -\Delta$. This is due to the fact that if there exist M and Q that satisfy (18) and (19) for values $\beta = \tilde{\beta}$ and $\varphi = \tilde{\varphi}$, then the same M and Q satisfy (18) and (19) also for larger values $\beta > \tilde{\beta}$ and $\varphi > \tilde{\varphi}$; moreover, for all $\tilde{\beta} \in (0,1)$, $\tilde{\varphi} \in [1,\infty)$ such that $(1-\rho)\ln\tilde{\beta}+\rho\ln\tilde{\varphi} < -\Delta$, there exist $\beta \geq \tilde{\beta}$ and $\varphi \geq \tilde{\varphi}$ such that $(1-\rho)\ln\beta+\rho\ln\varphi = -\Delta$.

IV. Numerical Example

In this section we present a numerical example to illustrate our results. Specifically, we consider (1) with

$$A \triangleq \begin{bmatrix} 1 & 0.1 \\ -0.5 & 1.1 \end{bmatrix}, \quad B \triangleq \begin{bmatrix} 0.1 \\ 1.2 \end{bmatrix}.$$

We use the event-triggering control law (2), (3) for stabilization of (1) over a network. We consider the case where the random packet losses in the network are characterized by the discrete-time Markov chain $\{l_{\mathrm{R}}(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ with initial distribution $\vartheta_0 = 0$, $\vartheta_1 = 1$, and transition probabilities $p_{0,1}(i) \triangleq 0.2 + 0.03\sin^2(0.1i)$, $p_{1,1}(i) \triangleq 0.2 + 0.03\cos^2(0.1i)$, and $p_{q,0}(i) = 1 - p_{q,1}(i)$, $q \in \{0,1\}$, $i \in \mathbb{N}_0$. Note that $\{l_{\mathrm{R}}(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ satisfies (9) and (10) with $p_1 = 0.23$ and $p_0 = 0.8$. Furthermore, the network is assumed to be subject to jamming attacks characterized with $\{l_{\mathrm{J}}(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ that is independent of $\{l_{\mathrm{R}}(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ and satisfies (7) with $\kappa = 2$ and $\tau = 5$.

Note that $p_1 + \frac{p_0}{\tau} < 0.4$. It follows from Proposition 2.3 that for $\rho = 0.4$, there exist $\gamma_k \in [0,\infty)$, $k \in \mathbb{N}$, such that (5) and (6) of Assumption 2.1 hold. Furthermore, matrices

$$Q = \begin{bmatrix} 0.618 & -2.119 \\ -2.119 & 28.214 \end{bmatrix}, \quad M = \begin{bmatrix} 0.202 & -20.405 \end{bmatrix},$$

and scalars $\beta = 0.55$, $\varphi = 2.4516$ satisfy (17), (18), (19). Hence, it follows from Corollary 3.3 that the event-triggered control law (2), (3) with $P = Q^{-1}$ and $K = MQ^{-1}$, guarantees almost sure asymptotic stabilization.

Fig. 3 shows 250 sample trajectories of the state norm $\|x(t)\|$ obtained with the same initial condition $x_0 = [1,\ 1]^{\mathrm{T}}$ and the event-triggering mechanism parameter $\theta = 1000$, but with different sample paths for $\{l_{\mathrm{R}}(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ and $\{l_{\mathrm{J}}(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$. Furthermore, in Fig. 4 we show a single sample trajectory of the Lyapunov-like function $V(x(t))$, and in Fig. 5 we show the corresponding sample trajectories for $l(\cdot)$, $l_{\mathrm{R}}(\cdot)$, and $l_{\mathrm{J}}(\cdot)$, indicating packet exchange attempt failures due to random packet losses and jamming attacks. Note that when packet exchange attempts fail due to a random loss or a jamming attack, the control input is set to 0. As a result, due to unstable dynamics of the uncontrolled system, the Lyapunov-like function $V(\cdot)$ may grow and take a larger value at the next packet exchange attempt instant. On the other hand, when a packet exchange attempt between the plant and the controller is successful, the control input at the plant side is updated. In this case $V(\cdot)$ is guaranteed to take a smaller value at the next packet exchange attempt instant, although it may not be monotonically decreasing. As implied by Corollary 3.3, the Lyapunov-like function $V(\cdot)$ eventually converges to zero (see Fig. 4).

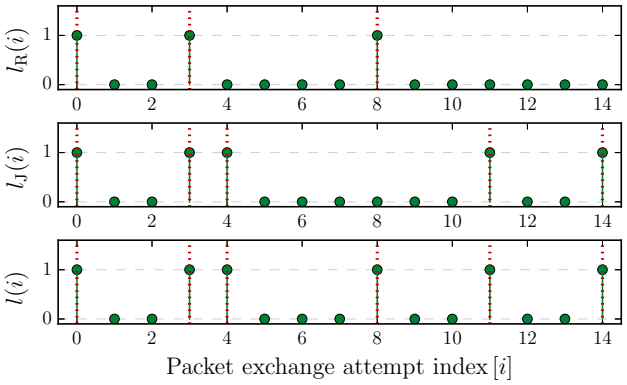

Fig. 5. Sample paths of $l_{\mathrm{R}}(\cdot)$, $l_{\mathrm{J}}(\cdot)$, and $l(\cdot)$

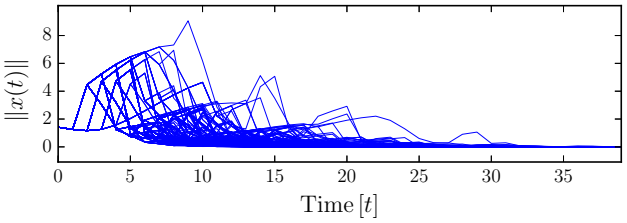

Fig. 3. Sample paths of the state norm

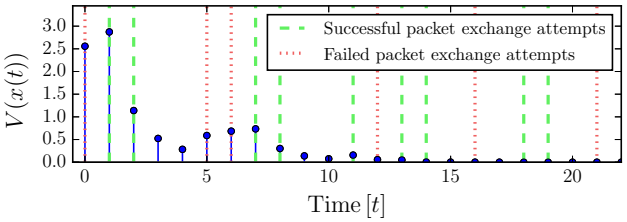

Fig. 4. A sample path of Lyapunov-like function $V(\cdot)$

V. Conclusion

In this paper, we explored event-triggered networked control of linear dynamical systems. We described a probabilistic characterization of the evolution of the total number of packet exchange failures in a network that faces random packet losses and jamming attacks. Based on this characterization, we obtained sufficient conditions for almost sure asymptotic stabilization of the zero solution and presented a method for finding a stabilizing feedback gain and parameters for our proposed event-triggered control framework. In the framework that we describe in the paper, the controller does not need the information whether the control input packets are successfully transmitted or lost. This type of acknowledgment messages would be useful to detect anomalies such as jamming attacks in the network. Future extensions include incorporating acknowledgement messages in the framework.

References

[1] J. P. Hespanha, P. Naghshtabrizi, and Y. Xu, "A survey of recent results in networked control systems," *Proc. IEEE*, vol. 95, no. 1, pp. 138–172, 2007.

[2] H. Ishii, "Limitations in remote stabilization over unreliable channels without acknowledgements," *Automatica*, vol. 45, no. 10, pp. 2278–2285, 2009.

[3] M. Lemmon and X. S. Hu, "Almost sure stability of networked control systems under exponentially bounded bursts of dropouts," in *Proc. 14th Int. Conf. HSCC*, (Chicago, IL), pp. 301–310, 2011.

[4] V. Gupta, N. C. Martins, and J. S. Baras, "Optimal output feedback control using two remote sensors over erasure channels," *IEEE Trans. Autom. Control*, vol. 54, no. 7, pp. 1463–1476, 2009.

[5] K. Okano and H. Ishii, "Stabilization of uncertain systems with finite data rates and Markovian packet losses," *IEEE Trans. Control Netw. Syst.*, vol. 1, pp. 298–307, 2014.

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

[7] "Special issue on cyberphysical security in networked control systems," *IEEE Control Syst. Mag.*, vol. 35, no. 1, 2015.

[8] S. Amin, A. A. Cardenas, and S. S. Sastry, "Safe and secure networked control systems under Denial-of-Service attacks," in *Proc. 12th Int. Conf. HSCC*, (San Francisco, CA), pp. 31–45, 2009.

[9] H. Shisheh-Foroush and S. Martínez, "On single-input controllable linear systems under periodic DoS jamming attacks," in *Proc. 2013 SIAM Conf. Contr. Appl.*, (San Diego, CA), 2013.

[10] C. De Persis and P. Tesi, "Resilient control under Denial-of-Service," in *Proc. 19th IFAC World Congress*, pp. 134–139, 2014.

[11] S. Liu, P. X. Liu, and A. El Saddik, "A stochastic game approach to the security issue of networked control systems under jamming attacks," *J. Franklin Inst.*, vol. 351, no. 9, pp. 4570–4583, 2014.

[12] M. Velasco, P. Martí, and E. Bini, "On Lyapunov sampling for event-driven controllers," in *Proc. Conf. Dec. Contr.*, (Shanghai, P. R. China), pp. 6238–6243, 2009.

[13] W. P. M. H. Heemels, M. C. F. Donkers, and A. R. Teel, "Periodic event-triggered control for linear systems," *IEEE Trans. Autom. Control*, vol. 58, no. 4, pp. 847–861, 2013.

[14] A. Cetinkaya, H. Ishii, and T. Hayakawa, "Event-triggered control over unreliable networks subject to jamming attacks," 2015. Online, `http://arxiv.org/abs/1503.06980`.

[15] W. P. M. H. Heemels, K. H. Johansson, and P. Tabuada, "An introduction to event-triggered and self-triggered control," in *Proc. IEEE Conf. Dec. Contr.*, (Maui, HI), pp. 3270–3285, 2012.

[16] E. Altman, K. Avrachenkov, and C. Barakat, "A stochastic model of TCP/IP with stationary random losses," *IEEE/ACM Trans. Networking*, vol. 13, no. 2, 2005.

[17] A. Klenke, *Probability Theory: A Comprehensive Course*. Springer-Verlag: London, 2008.

[18] L. Anantharamu, B. S. Chlebus, D. R. Kowalski, and M. A. Rokicki, "Medium access control for adversarial channels with jamming," in *Proc. 18th Int. Col. SIROCCO*, (Gdansk, Poland), pp. 89–100, 2011.

[19] D. Bernstein, *Matrix Mathematics: Theory, Facts, and Formulas*. Princeton University Press: Princeton, 2009.