Wireless Networked Control Facing Combined Effects of Disturbance and Jamming Interference

Ahmet Cetinkaya, Hideaki Ishii, and Tomohisa Hayakawa

Abstract— **We explore the networked control problem under the effects of disturbance and jamming attacks. Specifically, we consider the scenarios where an insecure wireless communication channel is used for transmission of the control input packets from the controller to the plant. This channel is assumed to face jamming attacks and the likelihood of transmission failures on this channel depends on the power of the jamming interference signal emitted by an attacker. We show that the combined effects of the jamming attacks and the disturbance can cause instability even if the attacked system without disturbance is stable. Furthermore, we show that stability under jamming and disturbance can be achieved if the average jamming interference power is restricted in a certain way.**

I. Introduction

Information and communication technologies are becoming essential components of industrial control systems. For example, nowadays, wireless networks and the Internet are utilized for tranmission of measurement and control data packets. These communication technologies bring efficiency in connecting remotely located parts of a control system, but they can also make the system vulnerable against various types of cyber-attacks [1].

Among the types of attacks a control system may face, jamming attacks seem to be the easiest to achieve from the viewpoint of an attacker. A jamming attack is a Denial-of-Service attack where the attacker can effectively block packet transmissions on a wireless channel by emitting sufficiently strong interference signals [2], [3]. Jamming attacks can cause performance issues and instability in wireless networked control systems.

Recently, the effect of jamming attacks and other Denial-of-Service attacks that cause transmission failures in control systems have been investigated in several works (see, e.g., [4]–[11]). In these works, different approaches have been explored for modeling the attacks. For instance, the models in [4]–[8] allow the timing of attacks to be arbitrary as long as the total attack duration and the frequency of attacks satisfy certain conditions. Moreover, physical jamming attack models based on wireless communication theory are considered in [9]–[11]. In those physical models, the likelihood of the occurrence of a transmission failure is influenced by the strength of the jamming interference. In particular, a transmission failure at a certain time is more likely, if the power of the jamming interference signal at that time is large. In our previous work [12], we used such a physical model and considered a networked stabilization problem for the scenarios where the level of interference power used by the attacker at each time is unknown. The results in [12] indicate that stabilization can be achieved if the average interference power is bounded in the long run even if the power level can be very large at certain times.

In this paper our goal is to extend our previous work [12] to analyze the combined effects of *jamming attacks* and *disturbance* on the dynamics. When the system is subject to disturbance, jamming attacks can become more dangerous. The attacker may take advantage of the disturbance to cause instability even if the attacked system without disturbance is stable. Specifically, the attacker can cause the state norm to grow to arbitrarily large values, while keeping the jamming interference power below a threshold in the long run.

We show in this paper that stability under jamming and disturbance can be achieved if the average jamming interference power is restricted so that the wireless channel is not subject to long consecutive emissions of high powered interference signals. First, we investigate the case where the system is subject to bounded disturbance. Then, we explore the more general scenario where the distribution of the disturbance norm may have infinite support. For this scenario, we obtain an inequality for the first moment of state that is similar to inequalities used for characterizing noise-to-state stability in stochastic systems (e.g., [13], [14]). A key role in our analysis is played by a nondecreasing and concave function of the attacker's interference power that upper-bounds the transmission failure probability. Furthermore, the use of the first moment of the state in the analysis facilitates the investigation of cross product terms that involve the disturbance and the indicator process for transmission failures through induced matrix norms.

The paper is organized as follows. In Section II, we explain the wireless networked control problem under jamming attacks. Then in Section III, we discuss the stability of the system without disturbance and explain the combined effects of jamming interference and disturbance. We provide an analysis for the system with disturbance and jamming in Section IV, and finally we conclude the paper in Section V.

The notation used in the paper is fairly standard. Specifically, $\mathbb{N}$ and $\mathbb{N}_0$ respectively denote the set of positive and nonnegative integers. Moreover, $\|\cdot\|_2$ denotes the Euclidean

Ahmet Cetinkaya and Hideaki Ishii are with the Department of Computer Science, Tokyo Insitute of Technology, Yokohama, 226-8502, Japan. ahmet@sc.dis.titech.ac.jp, ishii@c.titech.ac.jp

Tomohisa Hayakawa is with the Department of Systems and Control Engineering, Tokyo Institute of Technology, Tokyo 152-8552, Japan. hayakawa@sc.e.titech.ac.jp

This work was supported in part by the JST CREST Grant No. JP-MJCR15K3 and by JSPS under Grant-in-Aid for Scientific Research Grant No. 15H04020.

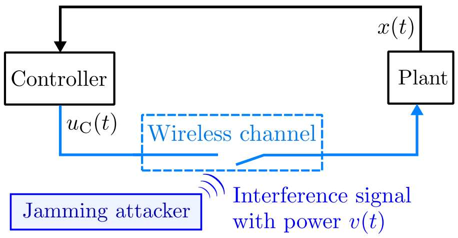

Fig. 1. Operation of networked control system under jamming attacks

norm. The notations $\lambda_{\min}(P)$ (resp., $\lambda_{\max}(P)$) denote the minimum (resp., maximum) eigenvalue of the Hermitian matrix P. We use $\mathbb{P}[\cdot]$ and $\mathbb{E}[\cdot]$ respectively denote the probability and the expectation on a probability space $(\Omega, \mathcal{F}, \mathbb{P})$.

II. Networked Control Under Jamming Attacks

In this paper, we consider the networked control problem of a discrete-time linear plant with a static state feedback controller. As illustrated in Fig. 1, a wireless communication channel is used for transmission of control input packets from the controller to the plant. This channel is assumed to be subject to transmission failures at certain times due to interference caused by the jamming signal of an attacker.

In the networked control operation, at each time step t, the controller computes a control input using the state information and attempts to transmit it on the wireless channel. If the transmission is successful, then the transmitted control input is applied at the plant side. If, on the other hand, there is a transmission failure, then the control input at the plant side is set to 0. In this setting, the dynamics of the plant is given by

$$x(t+1) = Ax(t) + (1 - l(t))Bu_{\mathrm{C}}(t) + w_{\mathrm{P}}(t), \qquad (1)$$

where $x(t) \in \mathbb{R}^n$ is the state, $u_{\mathrm{C}}(t) \in \mathbb{R}^m$ is the control input that is attempted to be transmitted by the controller to the plant at time t, $w_{\mathrm{P}}(t) \in \mathbb{R}^n$ is the disturbance vector, and $l(t) \in \{0, 1\}$ represents the transmission status (with $l(t) = 1$ indicating failure and $l(t) = 0$ indicating success). Moreover, $A \in \mathbb{R}^{n \times n}$ is the unstable system matrix and $B^{n \times m}$ is the input matrix.

In this paper, the likelihood of a transmission failure at time t depends on the power of the jamming interference signal at that time. If the interference power is large, then it is more likely that there is a transmission failure. In particular, with $v(t) \in [0, \infty)$ denoting the jamming interference power at time t, the failure indicator $l(t)$ in (1) is given by

$$l(t) \triangleq \mathbb{1}[r(t) \leq p(v(t))], \quad t \in \mathbb{N}_0, \qquad (2)$$

where, $p \colon [0, \infty) \to [0, 1]$ is a Borel-measurable, nondecreasing function, and $r(0), r(1), \ldots$ are independent random variables that are distributed uniformly in $[0, 1]$. Furthermore $\{r(t) \in [0, 1]\}_{t \in \mathbb{N}_0}$ and $\{v(t) \in [0, \infty)\}_{t \in \mathbb{N}_0}$ are assumed to be mutually independent processes. Notice that for a fixed scalar ϑ, $p(\vartheta) \in [0, 1]$ represents the conditional probability of a transmission failure given that the jamming interference power is set to ϑ. In particular, (2) implies

$$\begin{aligned} \mathbb{P}[l(t) = 1 | v(t) = \vartheta] &= \mathbb{P}[r(t) \leq p(\vartheta) | v(t) = \vartheta] \\ &= \mathbb{P}[r(t) \leq p(\vartheta)] = p(\vartheta). \end{aligned}$$

Observe that, if $v(t)$ is large so that $p(v(t))$ is close to 1, then it becomes more likely that $r(t) \leq p(v(t))$, and hence by (2), a transmission failure is likely to occur. Note also that transmission failures at different times are *conditionally independent* given the interference powers at those times. Namely, for every $t_1 < t_2 < \cdots < t_k$, $k \in \mathbb{N}$,

$$\begin{aligned} &\mathbb{P}[l(t_1) = 1, \ldots, l(t_k) = 1 | v(t_1) = \vartheta_1, \ldots, v(t_k) = \vartheta_k] \\ &= \prod_{i=1}^{k} \mathbb{P}[l(t_i) = 1 | v(t_i) = \vartheta_i] = \prod_{i=1}^{k} p(\vartheta_i). \end{aligned}$$

The characterization in (2) enables us to describe security and reliability properties of different wireless channel models by utilizing different p functions. For instance, to describe the additive white Gaussian noise channel with quadrature amplitude modulation scheme considered in the work [11], p can be selected as

$$p(\vartheta) = 2Q\Big(\sqrt{c\frac{\xi}{\vartheta + \sigma}}\Big), \qquad (3)$$

where $Q(y) \triangleq \frac{1}{\sqrt{2\pi}} \int_y^\infty e^{-\frac{s^2}{2}} \mathrm{d}s$, $\xi \in (0, \infty)$ and $\sigma \in (0, \infty)$ are constants associated respectively with the transmission power and the power of the channel noise, and $c \in (0, \infty)$ is a constant associated with the parameters of the communication protocol. Notice that the term $\frac{\xi}{\vartheta + \sigma}$ in (3) corresponds to Signal to Interference plus Noise Ratio (SINR), which is an indicator of the quality of a wireless channel [15]. Even if there is no attack at time t (i.e., $v(t) = \vartheta = 0$), there may still be a transmission failure due to channel noise $\sigma > 0$, since $p(0) > 0$.

We remark that the case where the interference power is constant (i.e., $v(t) = \vartheta^*$, $t \in \mathbb{N}_0$, for some fixed deterministic scalar ϑ^*) corresponds to Bernoulli-type packet losses (see [16]–[18]) with packet loss probability $p(\vartheta^*)$. In this paper, we follow the problem setting in our previous work [12] and explore the scenarios where the attacker can jam the network with different interference powers at different times.

III. Combined Effects of Disturbance and Jamming Interference on Networked Control

In this section, we investigate the networked stabilization of the plant (1) through a state-feedback controller, where the control input transmitted by the controller is given by

$$u_{\mathrm{C}}(t) = Kx(t) + w_{\mathrm{C}}(t), \quad t \in \mathbb{N}_0, \qquad (4)$$

where $K \in \mathbb{R}^{m \times n}$ denotes the feedback gain, and $w_{\mathrm{C}}(t) \in \mathbb{R}^m$ is used for describing malicious or nonmalicious disturbances on the control input. Notice that the effects of state-measurement noise can also be represented through the process $\{w_{\mathrm{C}}(t)\}_{t \in \mathbb{N}_0}$. Specifically, if the state measurement is noisy, then the control input is given by $K\tilde{x}(t)$, where

$\tilde{x}(t) = x(t) + \eta(t)$ is the measured state and $\eta(t) \in \mathbb{R}^n$ represents the measurement noise. This situation is represented through (4) by setting $w_{\mathrm{C}}(t) \triangleq K\eta(t)$.

With $w(t) \triangleq w_{\mathrm{P}}(t) + (1 - l(t))w_{\mathrm{C}}(t)$, the closed-loop networked control system (1), (4) becomes

$$x(t+1) = Ax(t) + (1 - l(t))BKx(t) + w(t), \ t \in \mathbb{N}_0. \quad (5)$$

In what follows, we first investigate the stability of (5) in the disturbance-free case ($w(t) = 0$, $t \in \mathbb{N}_0$). Then we discuss how a strategic jamming attacker can take advantage of the disturbance to prevent stabilization.

A. Stabilization in the Disturbance-Free Case

For the case without disturbance ($w(t) = 0$, $t \in \mathbb{N}_0$), our previous work [12] shows that stabilization can be achieved if the long run average jamming interference power is bounded by a sufficiently small scalar. In particular, the jamming characterization in [12] allows the interference power $v(t)$ to arbitrarily change at each time t as long as it satisfies the following assumption.

Assumption 3.1: There exist scalars $\overline{\kappa} \geq 0$ and $\overline{v} \geq 0$ such that

$$\mathbb{P}\big[\sum_{i=0}^{t-1} v(i) \leq \overline{\kappa} + \overline{v}t\big] = 1, \quad t \in \mathbb{N}. \quad (6)$$

Here, $\overline{v} \geq 0$ is an asymptotic upper-bound on the average interference power (i.e., $\limsup_{k\to\infty} \frac{1}{k}\sum_{t=0}^{k-1} v(t) \leq \overline{v}$). Notice that if p in (2) is a concave function, then $p(\overline{v})$ can be utilized in the stability analysis as an upper bound on the long run average number of transmission failures. On the other hand, if p is not concave, then a concave function that upper-bounds p can be used for the same purpose. To this end, we utilized in [12] a continuous, nondecreasing, and concave function $\hat{p}\colon [0,\infty) \to [0,1]$ such that

$$\hat{p}(v) \geq p(v), \quad v \in [0,\infty). \quad (7)$$

As discussed in [12], $\hat{p}$ satisfying (7) always exists. Moreover, it is shown in [12] that

$$\limsup_{t\to\infty} \frac{1}{t}\sum_{i=0}^{t-1} l(i) \leq \hat{p}(\overline{v}). \quad (8)$$

In other words, the average number of transmission failures is upper bounded in the long run by $\hat{p}(\overline{v})$. The inequality (8) was used in [12] for establishing stability of the closed-loop system (5) in the case without disturbance. The analysis in [12] indicates that if $\overline{v}$ is sufficiently small, then the closed-loop system is asymptotically stable almost surely, implying $\mathbb{P}[\lim_{t\to\infty} \|x(t)\|_2 = 0] = 1$.

In addition to almost sure asymptotic stability, moment stability of the networked control system can also be analyzed under Assumption 3.1. In particular, the following result provides a condition under which the first-moment of the state ($\mathbb{E}[\|x(t)\|_2]$) converges to zero at a geometric rate. In presentation of this result, we utilize induced matrix norms (see Section 5.6 in [19]). Specifically, for a given matrix $M \in \mathbb{R}^{n\times n}$, let $\|M\|$ denote the induced matrix norm defined by $\|M\| \triangleq \sup_{x\in\mathbb{R}^n\setminus\{0\}} \frac{\|Mx\|}{\|x\|}$, where $\|\cdot\|$ on the right-hand side denotes a vector norm on $\mathbb{R}^n$.

Proposition 3.1: Consider the closed-loop networked control system (1), (4) for the case where $w(t) = 0$, $t \in \mathbb{N}_0$. Suppose that the attacker's interference power process $\{v(t) \in [0,\infty)\}_{t\in\mathbb{N}_0}$ satisfies Assumption 3.1. Assume

$$(1 - \hat{p}(\overline{v}))\|A + BK\| + \hat{p}(\overline{v})\|A\| < 1. \quad (9)$$

Then the closed-loop system (1), (4) is first-moment geometrically stable, that is, there exist $\overline{\mu} \geq 0$ and $\overline{\theta} \in (0,1)$ such that

$$\mathbb{E}[\|x(t)\|_2] \leq \overline{\mu}\overline{\theta}^t\|x_0\|_2, \quad t \in \mathbb{N}. \quad (10)$$

In Proposition 3.1, the scalar $\overline{\theta}$ represents the rate of convergence of the first moment, and it depends on $\hat{p}(\overline{v})$ as well as the scalars $\|A + BK\|$ and $\|A\|$, which are associated with the closed-loop and the open-loop dynamics. In particular, $\overline{\theta}$ is a linear function of the left-hand side of (9). As a result, if the bound $\overline{v}$ on the long run average jamming interference power is small, then $\overline{\theta}$ is also small, indicating faster convergence of the first-moment. We note that geometric convergence of the first-moment also implies that the state converges to the origin almost surely (i.e., $\mathbb{P}[\lim_{t\to\infty} \|x(t)\|_2 = 0] = 1$).

B. Destabilizing Effects of Disturbance and Jamming Interference

So far we investigated the stability of the closed-loop networked control system (1), (4) for the case without disturbance. Proposition 3.1 indicates that if $\overline{v}$ in Assumption 3.1 is sufficiently small, then stability can be achieved. We now look at the case with disturbance. We observe that in this case, jamming attacks can become considerably more dangerous. Even if the disturbance is very small and the attacker has very limited jamming resources, there still exist attack strategies that can *destabilize* the system while satisfying Assumption 3.1 with very small $\overline{v}$. We illustrate this idea in the following example.

Example 3.1: Consider a scalar networked control system (1), (4) with $x_0 > 0$, $A + BK \in [0,1)$, $A > 1$, and constant disturbance $w(t) = w^* > 0$, $t \in \mathbb{N}_0$. Suppose that the conditional probability p of transmission failures is a strictly increasing function (e.g., p given by (3)). For this networked control system setup, an attacker can wait for a sufficiently long duration and then attack for a duration with a sufficiently large interference power so that the state norm grows to large values but the average interference power does not go above $\overline{v}$. In particular, for any $\overline{v} > 0$, $x_0 > 0$, $z > 0$, and $\rho \in (0,1)$, the attack strategy

$$v(t) \triangleq \begin{cases} v^*, & t \in \{\tau_1, \ldots, \tau_1 + \tau_2 - 1\}, \\ 0, & \text{otherwise}, \end{cases} \quad (11)$$

with $v^* \triangleq p^{-1}(\rho^{\frac{1}{\tau_2}}) + 1$, $\tau_1 \triangleq \lfloor \frac{\max\{v^* - \overline{v}, 0\}\tau_2}{\overline{v}} \rfloor + 1$, $\tau_2 \triangleq \lfloor \max\{\log_A(z/w^*), 0\} \rfloor + 1$ guarantees that Assumption 3.1 is satisfied and the state exceeds the value z with probability larger than ρ at time $\tau \triangleq \tau_1 + \tau_2$, i.e., $\mathbb{P}[x(\tau) > z] > \rho$. To show this, first we define the event $E(\tau_1, \tau_2) \in \mathcal{F}$ by

$$E(\tau_1, \tau_2) \triangleq \big\{\omega \in \Omega \colon l(t) = 1, t \in \{\tau_1, \ldots, \tau_1 + \tau_2 - 1\}\big\}.$$

This is the event that all packet transmissions during $t \in \{\tau_1, \ldots, \tau_1 + \tau_2 - 1\}$ fail. By (11), we have $\mathbb{P}[E(\tau_1, \tau_2)] = p^{\tau_2}(v^*)$. Now, since $x_0 > 0$, $A > 1$, and $w^* > 0$, we obtain $x(t) \geq w^*$, $t \in \mathbb{N}$. Therefore,

$$\begin{aligned}\mathbb{P}[x(\tau) > z] &\geq \mathbb{P}[x(\tau) > z \,|\, E(\tau_1, \tau_2)]\mathbb{P}[E(\tau_1, \tau_2)] \\ &\geq \mathbb{P}[A^{\tau_2} x(\tau_1) + \sum_{i=0}^{\tau_2 - 1} A^i w^* > z \,|\, E(\tau_1, \tau_2)] p^{\tau_2}(v^*) \\ &\geq \mathbb{P}[A^{\tau_2} w^* > z \,|\, E(\tau_1, \tau_2)] p^{\tau_2}(v^*) > 1 \cdot \rho^{\frac{\tau_2}{\tau_2}} = \rho.\end{aligned}$$

Furthermore, the attack strategy (11) satisfies Assumption 3.1 with $\overline{\kappa} = 0$, because $\tau_1 \geq \frac{\max\{v^* - \overline{v}, 0\}\tau_2}{\overline{v}} \geq \frac{(v^* - \overline{v})\tau_2}{\overline{v}}$, and thus, $\sum_{i=0}^{\tau-1} v(i) = v^* \tau_2 \leq \overline{v}(\tau_1 + \tau_2) = \overline{v}\tau$.

The attack strategy (11) can make the state grow arbitrarily large even if the upper bound $\overline{v}$ of the average interference power is very small. This attack strategy is effective, because even if the attacker initially waits for a long duration without attacking, the state never reaches a small neighborhood of zero due to the disturbance. Hence, after waiting for a while, the attacker can consecutively attack with high interference powers to cause many transmission failures and make the state norm grow to large values due to lack of control. In the next section, we show that stability under the combined effects of jamming and disturbance can be achieved if the average jamming interference power is further restricted in a certain way.

IV. Stabilization Under Jamming Interference and Disturbance

To ensure stability under both disturbance and jamming, the attacks need to be restricted in a way that high jamming interference powers at consecutive times are not allowed. To this end, we consider the following assumption.

Assumption 4.1: There exist scalars $\hat{\kappa} \geq 0$, $\hat{v} \geq 0$ such that

$$\mathbb{P}\big[\sum_{i=t_1}^{t_2 - 1} v(i) \leq \hat{\kappa} + \hat{v}(t_2 - t_1)\big] = 1, \tag{12}$$

for all $t_1, t_2 \in \mathbb{N}_0$ with $t_1 < t_2$.

Notice that (12) implies (6) (with $\overline{\kappa} = \hat{\kappa}$ and $\overline{v} = \hat{v}$), but the converse is not true. Assumption 4.1 is thus more restrictive than Assumption 3.1. In particular, under Assumption 4.1, the attacker can attack with a jamming interference power $v^* > \hat{v}$ consecutively for at most $\lfloor \hat{\kappa}/(v^* - \hat{v}) \rfloor$ time steps. As a result, under Assumption 4.1, the destabilizing attacks discussed in Example 3.1 are avoided.

Assumption 4.1 is related to other characterizations that describe malicious attacks in the literature. In particular, in the continuous-time deterministic denial-of-service attack characterization of [4], the number of attacks in a given time frame as well as the total duration of those attacks are bounded by certain ratios of the length of that time frame. Under that characterization, the maximum possible length of a continuous attack duration is bounded, which enables analysis of input-to-state stability under disturbance. The restriction on jamming through Assumption 4.1 is similar, since long consecutive emissions of high powered interference signals are not allowed. We note, however, that Assumption 4.1 allows the scenario where the channel is attacked at all times if the attacker's interference power for certain times is small. Notice that emission of interference signals in jamming attacks require energy [2], [3]. In this respect, Assumption 4.1 can describe the constraints of an attacker with limited energy resources.

A. Stabilization Under Jamming Interference and Bounded Disturbance

In what follows, we investigate the networked control system (5) for the case where the jamming attacks satisfy Assumption 4.1 and the disturbance is bounded. The analysis is then extended in Section IV-B to the case where the disturbance has finite second moments but its norm may not be bounded by a fixed scalar.

In this paper, we consider scenarios where the norm of the disturbance does not approach zero, and hence the state or its moments may not converge to the origin. Therefore, instead of exploring asymptotic stability, our goal here is to obtain conditions under which the first moment of the state stays bounded. To this end, let

$$\hat{A}(t) \triangleq l(t)A + (1 - l(t))(A + BK), \quad t \in \mathbb{N}_0,$$

and moreover, for every $t_1, t_2 \in \mathbb{N}_0$ with $t_1 \leq t_2$, let

$$F(t_2, t_1) \triangleq \begin{cases} \hat{A}(t_2), & t_1 = t_2, \\ \hat{A}(t_2) \cdots \hat{A}(t_1), & t_1 < t_2. \end{cases}$$

For the closed-loop system (5), we have

$$\begin{aligned} x(t) = F(t-1, 0)x_0 + \sum_{j=0}^{t-2} F(t-1, j+1) w(j) \\ + w(t-1), \quad t \in \mathbb{N}. \end{aligned}$$

Therefore, for any induced norm $\|\cdot\|$, it follows from the triangle inequality and the submultiplicativity property of the induced norm that

$$\begin{aligned} \|x(t)\| \leq \Big(\prod_{i=0}^{t-1} \|\hat{A}(i)\|\Big)\|x_0\| + \sum_{j=0}^{t-2} \Big(\prod_{i=j+1}^{t-1} \|\hat{A}(i)\|\Big)\|w(j)\| \\ + \|w(t-1)\|. \end{aligned}$$

Here, we have $\|\hat{A}(i)\| = l(i)\|A\| + (1 - l(i))\|A + BK\|$, $i \in \mathbb{N}_0$. Hence, by letting

$$\zeta_1 \triangleq \|A\| - \|A + BK\|, \quad \zeta_0 = \|A + BK\|, \tag{13}$$

we obtain for $t \in \mathbb{N}$,

$$\|x(t)\| \leq \Big(\prod_{i=0}^{t-1}(\zeta_1 l(i) + \zeta_0)\Big)\|x_0\| + \sum_{j=0}^{t-2}\Big(\prod_{i=j+1}^{t-1}(\zeta_1 l(i) + \zeta_0)\Big)\|w(j)\| + \|w(t-1)\|. \tag{14}$$

By using (14), we can also obtain an upper-bound of the Euclidean norm of the state. Specifically, by Corollary 5.4.5 of [19], there exist $c_1 > 0$ and $c_2 > c_1$ such that

$$c_1\|y\| \leq \|y\|_2 \leq c_2\|y\|, \quad y \in \mathbb{R}^n. \tag{15}$$

Therefore, it follows from (14) that

$$\|x(t)\|_2 \leq \frac{c_2}{c_1}\Big(\prod_{i=0}^{t-1}(\zeta_1 l(i) + \zeta_0)\Big)\|x_0\|_2 + \frac{c_2}{c_1}\sum_{j=0}^{t-2}\Big(\prod_{i=j+1}^{t-1}(\zeta_1 l(i) + \zeta_0)\Big)\|w(j)\|_2 + \frac{c_2}{c_1}\|w(t-1)\|_2. \tag{16}$$

Notice here that the particular values of c_1 and c_2 depend on the choice of the vector norm that induces the matrix norm $\|\cdot\|$ used in (13). For example, in the case of Euclidean norm, (16) holds with $c_1 = c_2 = 1$. On the other hand, if $\|\cdot\|$ in (13) is induced by the vector norm $\|x\|_P \triangleq \sqrt{x^{\mathrm{T}}Px}$ with a positive definite matrix $P \in \mathbb{R}^{n\times n}$, then (16) holds with $c_1 = 1/\sqrt{\lambda_{\max}(P)}$ and $c_2 = 1/\sqrt{\lambda_{\min}(P)}$.

We utilize (16) to provide bounds on the first moment $\mathbb{E}[\|x(t)\|_2]$ of the state. In the following result, we consider the case where the disturbance is *bounded* and the jamming attacks satisfy Assumption 4.1.

Theorem 4.1: Consider the closed-loop networked control system (5). Suppose that the attacker's interference power process $\{v(t) \in [0,\infty)\}_{t\in\mathbb{N}_0}$ satisfies Assumption 4.1. Furthermore, suppose that there exists $\overline{w} \geq 0$ such that

$$\mathbb{P}[\|w(t)\|_2 \leq \overline{w}] = 1, \quad t \in \mathbb{N}. \tag{17}$$

If

$$(1 - \hat{p}(\hat{v}))\|A + BK\| + \hat{p}(\hat{v})\|A\| < 1, \tag{18}$$

then there exist $\hat{\mu} \geq 0$, $\hat{\theta} \in (0,1)$, and $\hat{d} \geq 0$ such that

$$\mathbb{E}[\|x(t)\|_2] \leq \hat{\mu}\hat{\theta}^t\|x_0\|_2 + \hat{d}\overline{w}, \quad t \in \mathbb{N}. \tag{19}$$

Theorem 4.1 shows that if jamming attacks satisfy Assumption 4.1 with a sufficiently small $\hat{v}$ such that (18) holds, then the first moment of the state stays bounded. Furthermore, the upper bound given in (19) is geometrically decreasing towards the constant $\hat{d}\overline{w}$, where $\overline{w}$ is an upper bound on the Euclidean norm of disturbance vector $w(t)$. Notice that the condition (18) of Theorem 4.1 and the condition (9) utilized in the disturbance-free case in Proposition 3.1 are in the same form, but they use different scalars $\hat{v}$ and $\overline{v}$ due to the difference of the jamming interference characterizations in Assumptions 3.1 and 4.1. We remark that for jamming attacks that satisfy both assumptions, we necessarily have $\overline{v} \leq \hat{v}$.

The proof of Theorem 4.1 is based on obtaining upper bounds for the expectation of terms on the right-hand side of (16). In this regard, the following lemmas are utilized for deriving bounds for the terms $\mathbb{E}[\prod_{i=0}^{t-1}(\zeta_1 l(i) + \zeta_0)]$ and $\mathbb{E}[\sum_{j=0}^{t-2}(\prod_{i=j+1}^{t-1}(\zeta_1 l(i) + \zeta_0))]$. Notice that the scalar $\hat{v} \geq 0$ from Assumption 4.1 and the concave function $\hat{p}$ satisfying (7) are essential in the derivation of these bounds.

Lemma 4.2: Suppose that the attacker's interference power process $\{v(t) \in [0,\infty)\}_{t\in\mathbb{N}_0}$ satisfies Assumption 4.1. Then for every $\alpha_1 \geq 0$, $\alpha_0 \geq 0$ that satisfy

$$\alpha_1\hat{p}(\hat{v}) + \alpha_0 < 1, \tag{20}$$

there exist scalars $\mu \geq 0$ and $\theta \in (0,1)$ such that

$$\mathbb{E}[\prod_{i=t_1}^{t_2-1}(\alpha_1 l(i) + \alpha_0)] \leq \mu\theta^{(t_2-t_1)}, \tag{21}$$

for $t_1, t_2 \in \mathbb{N}_0$ with $t_1 < t_2$.

Lemma 4.2 shows that under Assumption 4.1, $\mathbb{E}[\prod_{i=t_1}^{t_2-1}(\alpha_1 l(i) + \alpha_0)]$ with $\alpha_1 \geq 0$, $\alpha_0 \geq 0$ satisfying (20), converges to zero at a geometric rate. By using this lemma, we also obtain the following result.

Lemma 4.3: Suppose that the attacker's interference power process $\{v(t) \in [0,\infty)\}_{t\in\mathbb{N}_0}$ satisfies Assumption 4.1. Then for every $\alpha_1 \geq 0$, $\alpha_0 \geq 0$ that satisfy (20), there exists a scalar $d \geq 0$ such that

$$\sum_{j=0}^{t-2}\mathbb{E}\Big[\prod_{i=j+1}^{t-1}(\alpha_1 l(i) + \alpha_0)\Big] \leq d, \tag{22}$$

for $t \in \{2, 3, \ldots\}$.

By using Lemmas 4.2 and 4.3, we have

$$\mathbb{E}\big[\prod_{i=0}^{t-1}(\zeta_1 l(i) + \zeta_0)\big] \leq \mu\theta^t, \tag{23}$$

$$\sum_{j=0}^{t-2}\mathbb{E}\big[\prod_{i=j+1}^{t-1}(\zeta_1 l(i) + \zeta_0)\big] \leq d, \tag{24}$$

where $\mu \geq 0$, $\theta \in (0,1)$, and $d \geq 0$ are scalars that depend on ζ_1 and ζ_0 defined in (13). We use (23) and (24) to obtain an upper bound for the expectation of the right-hand side of (16), which we then utilize for showing (19) in Theorem 4.1. The details are omitted due to space limitations.

B. Stabilization Under Jamming Interference and Disturbance with Finite Second Moment

In the previous subsection, we considered the case where the Euclidean norm of the disturbance is bounded at each time almost surely by a scalar $\overline{w}$. Next, we investigate the scenarios where the disturbance may not be bounded by such a scalar. Our goal is to obtain a relation between the state and the disturbance similar to those used for establishing noise-to-state stability in stochastic systems (see, e.g., [13], [14]). Specifically, in the following result, we provide an upper bound for the first moment of the state by utilizing the second moment of the disturbance.

Theorem 4.4: Consider the closed-loop networked control system (5). Suppose that the attacker's interference power process $\{v(t) \in [0,\infty)\}_{t\in\mathbb{N}_0}$ satisfies Assumption 4.1. Furthermore, suppose $\mathbb{E}[\|w(t)\|_2^2] < \infty$, $t \in \mathbb{N}_0$. If

$$(1-\hat{p}(\hat{v}))\|A+BK\|^2 + \hat{p}(\hat{v})\|A\|^2 < 1, \qquad (25)$$

then there exist $\hat{\mu} \geq 0$, $\hat{\theta} \in (0,1)$, and $\hat{f} \geq 0$ such that

$$\mathbb{E}[\|x(t)\|_2] \leq \hat{\mu}\hat{\theta}^t\|x_0\|_2 + \hat{f} \max_{i\in\{0,\ldots,t-1\}} (\mathbb{E}[\|w(i)\|_2^2])^{\frac{1}{2}}, \quad (26)$$

for $t \in \mathbb{N}$.

Theorem 4.4 shows that if the jamming attacks satisfy Assumption 4.1 with a sufficiently small $\hat{v}$ such that (25) holds, then the first moment of the state satisfies the bound given in (26). The proof of this result relies on certain upper bounds for the expectation of the terms on the right-side of (16). In particular, we use Schwarz's and Jensen's inequalities (see [20]) to obtain

$$\begin{aligned}&\mathbb{E}\Big[\Big(\prod_{i=j+1}^{t-1}(\zeta_1 l(i)+\alpha_0)\Big)\|w(j)\|_2\Big]\\&\quad\leq \Big(\mathbb{E}\big[\big(\prod_{i=j+1}^{t-1}(\zeta_1 l(i)+\zeta_0)\big)^2\big]\Big)^{\frac{1}{2}}(\mathbb{E}[\|w(j)\|_2^2])^{\frac{1}{2}}\end{aligned}$$

and $\mathbb{E}[\|w(t-1)\|_2] \leq \big(\mathbb{E}[\|w(t-1)\|_2^2]\big)^{\frac{1}{2}}$. After noting that $\mathbb{E}\Big[\big(\prod_{i=j+1}^{t-1}(\zeta_1 l(i)+\zeta_0)\big)^2\Big] = \mathbb{E}\Big[\prod_{i=j+1}^{t-1}(\alpha_1 l(i)+\alpha_0)\Big]$ with $\alpha_1 \triangleq \zeta_1^2 + 2\zeta_1\zeta_0$ and $\alpha_0 \triangleq \zeta_0^2$, we show (26) by using Lemmas 4.2 and 4.3 together with (25).

Notice that Theorem 4.4 is applicable to scenarios where the condition (17) of Theorem 4.1 may fail to hold. In particular, if the entries of the disturbance vector are random variables with distributions that have infinite support, then (17) does not hold. This is for example the case if $w(t)$ is normally distributed (i.e., $w(t) \sim \mathcal{N}(m,\Sigma)$ where $m \in \mathbb{R}^n$ and $\Sigma \in \mathbb{R}^{n\times n}$ is a positive-definite matrix). In such cases, Theorem 4.4 can be utilized. If $\mathbb{E}[\|w(t)\|_2^2] \leq \tilde{w}$ holds for all $t \in \mathbb{N}_0$ with a scalar $\tilde{w} \geq 0$, then it follows from (26) that $\limsup_{t\to\infty}\mathbb{E}[\|x(t)\|_2] \leq \hat{f}\tilde{w}^{\frac{1}{2}}$, indicating the boundedness of expected state norm in the long run.

We remark that although Theorem 4.4 is applicable to a wider range of scenarios in terms of the disturbance, the condition (25) concerning the upper bound $\hat{v}$ of the average jamming attack interference power is more restrictive than the condition (18) of Theorem 4.1. In particular, we have $\big((1-\hat{p}(\hat{v}))\|A+BK\| + \hat{p}(\hat{v})\|A\|\big)^2 < (1-\hat{p}(\hat{v}))\|A+BK\|^2 + \hat{p}(\hat{v})\|A\|^2$ for $\hat{p}(\hat{v}) \in (0,1)$ indicating that (25) implies (18), but not vice versa.

V. Conclusion

We investigated the networked stabilization problem over wireless channels that face jamming attacks with time-varying interference power. We explored the joint effects of jamming attacks and disturbance, and obtained conditions under which the first moment of the networked control system state stays bounded. Our results indicate that if the disturbance is known to be bounded, larger average jamming interference powers can be allowed.

References

[1] H. Sandberg, S. Amin, and K. H. Johansson, "Special issue on cyberphysical security in networked control systems," *IEEE Control Syst. Mag.*, vol. 35, no. 1, 2015.

[2] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *Proc. ACM Int. Symp. Mobile Ad Hoc Network. Comput.*, pp. 46–57, 2005.

[3] K. Pelechrinis, M. Iliofotou, and S. V. Krishnamurty, "Denial of Service attacks in wireless networks: The case of jammers," *IEEE Commun. Surveys Tuts.*, vol. 13, no. 2, pp. 245–257, 2011.

[4] C. De Persis and P. Tesi, "Input-to-state stabilizing control under Denial-of-Service," *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 2930–2944, 2015.

[5] C. De Persis and P. Tesi, "Networked control of nonlinear systems under Denial-of-Service," *Syst. Control Lett.*, vol. 96, pp. 124–131, 2016.

[6] H. Shisheh Foroush and S. Martínez, "On triggering control of single-input linear systems under pulse-width modulated DoS signals," *SIAM J. Control Optim.*, vol. 54, no. 6, pp. 3084–3105, 2016.

[7] A. Cetinkaya, H. Ishii, and T. Hayakawa, "Networked control under random and malicious packet losses," *IEEE Trans. Autom. Control*, vol. 62, no. 5, pp. 2434–2449, 2017.

[8] S. Feng and P. Tesi, "Resilient control under Denial-of-Service: Robust design," *Automatica*, vol. 79, pp. 42–51, 2017.

[9] 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. Autom. Control*, vol. 60, no. 10, pp. 2831–2836, 2015.

[10] H. Zhang, Y. Qi, J. Wu, L. Fu, and L. He, "DoS attack energy management against remote state estimation," *IEEE Trans. Control Netw. Syst.*, vol. 5, no. 1, pp. 383–393, 2018.

[11] 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.*, vol. 4, no. 3, pp. 632–643, 2017.

[12] A. Cetinkaya, H. Ishii, and T. Hayakawa, "Wireless control under jamming attacks with bounded average interference power," in *Proc. IFAC World Congr.*, pp. 8735–8740, Also, to appear, SIAM J. Control Optim., 2018., 2017.

[13] D. Mateos-Núñez and J. Cortés, "*p*th moment noise-to-state stability of stochastic differential equations with persistent noise," *SIAM J. Control Optim.*, vol. 52, no. 4, pp. 2399–2421, 2014.

[14] D. Zhang, Z. Wu, X.-M. Sun, and W. Wang, "Noise-to-state stability for a class of random systems with state-dependent switching," *IEEE Trans. Autom. Control*, vol. 61, no. 10, pp. 3164–3170, 2016.

[15] G. Shi and K. Li, *Signal Interference in WiFi and ZigBee Networks*. Springer, 2017.

[16] 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.

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

[18] D. E. Quevedo, J. Østergaard, and D. Nešić, "Packetized predictive control of stochastic systems over bit-rate limited channels with packet loss," *IEEE Trans. Autom. Control*, vol. 56, no. 12, pp. 2854–2868, 2011.

[19] R. A. Horn and C. R. Johnson, *Matrix Analysis*. Cambridge University Press, 1985.

[20] D. Williams, *Probability with Martingales*. Cambridge University Press, 2010.