2019 IEEE 58th Conference on Decision and Control (CDC)
Palais des Congrès et des Expositions Nice Acropolis
Nice, France, December 11-13, 2019

Robust Stabilization of Resource Limited Networked Control Systems Under Denial-of-Service Attack

Niladri Sekhar Tripathy, Mohammadreza Chamanbaz and Roland Bouffanais

***Abstract*— In this paper, we consider a class of denial-of-service (DoS) attacks, which aims at overloading the communication channel. On top of the security issue, continuous or periodic transmission of information within feedback loop is necessary for the effective control and stabilization of the system. In addition, uncertainty—originating from variation of parameters or unmodeled system dynamics—plays a key role in the system's stability. To address these three critical factors, we solve the joint control and security problem for an uncertain discrete-time Networked Control System (NCS) subject to limited availability of the shared communication channel. An event-triggered-based control and communication strategy is adopted to reduce bandwidth consumption. To tackle the uncertainty in the system dynamics, a robust control law is derived using an optimal control approach based on a virtual nominal dynamics associated with a quadratic cost-functional. The conditions for closed-loop stability and aperiodic transmission rule of feedback information are derived using the discrete-time Input-to-State Stability theory. We show that the proposed control approach withstands a general class of DoS attacks, and the stability analysis rests upon the characteristics of the attack signal. The results are illustrated and validated numerically with a classical NCS batch reactor system.**

I. Introduction

The range of applications of Cyber-Physical Systems (CPSs)—e.g. power systems, intelligent vehicles, civil infrastructure, aerospace, retail supply chains, connected medical devices—has vastly expanded beyond the realm of large-scale public infrastructures. The presence of a communication medium combined with a tight integration of various subsystems make most of these applications safety-critical. Therefore, both CPSs and Networked Control Systems (NCSs) are broadly exposed to cyber-threats and cyber-vulnerabilities which may affect the functionality of physical processes at their core. These critical issues have spurred new lines of research at the interface between cyber-security and control theory [1], [2]. For instance, the effects and containment of cyber-attacks on control systems, which affect the availability and integrity of sensor and actuator information have been studied in [3], [4]. Recently, Teixira et. al. [4] described different characteristics of cyber-attacks and defined an attack space to analyze the effect of cyber-attacks on closed-loop dynamics. Cyber-attacks can be broadly classified into two categories: Denial-of-Service (DoS) attacks and deception attacks [5]. This paper is concerned with DoS attacks and their effects on dynamical systems. DoS attacks primarily affect the transmission medium within the feedback loop and cause irregular exchanges and losses of information [6], [7]. As this is one of the most reachable attack patterns in the attack space, many researchers have studied its effects both theoretically and experimentally [8]–[11].

Beyond inherent security issues present in NCSs, the exchange of feedback information over the shared communication channel, be it continuous or periodic, consumes a significant portion of the available bandwidth. Recently, it has been shown that significant savings in the bandwidth and communication resources can be achieved by switching from periodic or continuous sampling to aperiodic sampling [12], [13]. Specifically, event-triggered control strategies have revealed drastic reductions in the use of network bandwidth within the feedback loop [14]–[18]. A central problem with classical event-triggered control is the need to have an accurate model of the system in order to devise appropriate event-triggering rules. In practice, system modeling inevitably simplifies the actual system's operations, and thereby introduces a certain level of inaccuracy. Recently, Tripathy et al. [17] have developed a robust event-triggered control algorithm based on aperiodic feedback so as to deal with the presence of uncertainty.

It is worth highlighting that there is a vast breadth of problems related to the issue of event-triggering control in the presence of DoS attacks, and with model uncertainty in NCSs. In event-triggered control, any new information is exchanged only when the stability criterion is violated, which implicitly assumes that the communication channel is available at the time of event generation. It is clear that any factor or event affecting the availability of the interconnecting network, such as a DoS attack for instance, has the potential to seriously hinder the underlying physical processes and overall operations of the NCS. In light of this, it appears timely to develop new event-triggering control strategies capable of ensuring the stability of the closed loop system subjected to DoS attacks characterized by their frequency and duration, while accounting for uncertainty of the NCS model.

In this paper, we propose an attack-resilient event-based robust control algorithm for discrete-time uncertain systems. Norm-bounded mismatched uncertainty is considered for the derivation of the robust control results. The primary goal of

Niladri Sekhar Tripathy, Mohammadreza Chamanbaz and Roland Bouffanais are with the Singapore University of Technology and Design, Singapore 487372, e-mail: (niladri.tripathy, chamanbaz, bouffanais@sutd.edu.sg)

This work was supported in part by the National Research Foundation (NRF), Prime Minister's Office, Singapore, under its National Cybersecurity R&D Programme (Award No. NRF2014NCR-NCR001-040) and administered by the National Cybersecurity R&D Directorate and MOE Tier 1 grant (T1MOE17001).

978-1-7281-1398-2/19/$31.00 ©2019 IEEE

this work is to analyze the effect of DoS attacks on a discrete-time uncertain network controlled system, and to characterize the relationship between frequency and duration of the attack signal and closed-loop stability. The Input-to-State Stability (ISS) theory is applied to derive the transmission rule and on/off periods of DoS attack signal. The key contributions of this paper are listed below:

- We derive and propose a resilient event-based robust control law, within the optimal control framework, that is capable of dealing with both the occurrence of repeated DoS attacks and model uncertainty.
- We establish the upper bound of acceptable duration and frequency of DoS attacks, for which the ISS stability of the uncertain discrete-time systems is guaranteed with event-triggered feedback.
- The numerical results obtained with a NCS model for a batch reactor system provide an illustration of the proposed approach and also validate its effectiveness.

Notations and Definitions: The Euclidean norm of a vector $x \in \mathbb{R}^n$ is denoted by $\|x\|$. The symbols I denote the identity matrix of appropriate dimension. The maximum (resp. minimum) eigenvalue of a symmetric matrix $P \in \mathbb{R}^{n\times n}$ is $\lambda_{\max}(P)$ (resp. $\lambda_{\min}(P)$). A continuous function f: $\mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is said to be class $\mathcal{K}_\infty$ if it is strictly increasing, $f(0) = 0$ and $f(s) \to \infty$ as $s \to \infty$. A function $f : \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is a class $\mathcal{K}$ function, if it is continuous, strictly increasing and $f(0) = 0$. A continuous function $\beta(r, s) : \mathbb{R}_{\geq 0} \times \mathbb{R}_{\geq 0} \to \mathbb{R}_{\geq 0}$ is a $\mathcal{KL}$ function, if it is a class $\mathcal{K}$ function with respect to r for a fixed s, and it is strictly decreasing with respect to s when r is fixed [19]. For any given time interval $[0, k)$ where $k > 1$, $T_{\text{off}}(k)$ denotes the total duration of DoS attack over $[0, k)$. The ratio $\frac{T_{\text{off}}(k)}{k}$ represents the rate of unavailability of the communication channel following the DoS attack. The variable $N_{\text{off}}(k)$ represents the frequency of DoS attack in the time interval $[0, k)$ i.e. it means that $N_{\text{off}}(k)$ off-to-on transitions are present in the attack signal during which communication is impossible. The definitions detailed below are used to establish the theoretical results.

Definition 1 (Input-to-State Stability [19]): A discrete-time system

$$x(k + 1) = Ax(k) + Bu(k), \tag{1}$$

is globally input-to-state stable (ISS) if it satisfies

$$\|x(k)\| \leq \beta(\|x(0)\|, k) + \gamma(\|u(k)\|), \tag{2}$$

for all admissible inputs $u(k)$ and for all initial values $x(0)$, with β a $\mathcal{KL}$ function, and γ a $\mathcal{K}_\infty$ one.

Definition 2 (ISS Lyapunov Function [19]): Assume system (1) is at steady state at the origin, that is $f(0, 0) = 0, \forall\, k > 0$. A positive function $V(x(k)) : \mathbb{R}^n \to \mathbb{R}$ is an Input-to-State Lyapunov function for (1) if there exists class $\mathcal{K}_\infty$ functions $\alpha_1, \alpha_2, \alpha_3$ and a class $\mathcal{K}$ function γ for all $x \in \mathbb{R}^n$ and $u \in \mathbb{R}^m$ satisfying the following conditions

$$\alpha_1(\|x(k)\|) \leq V(x(k)) \leq \alpha_2(\|x(k)\|), \tag{3}$$
$$V(k + 1) - V(k) \leq -\alpha_3(\|x(k)\|) + \gamma(\|u(k)\|). \tag{4}$$

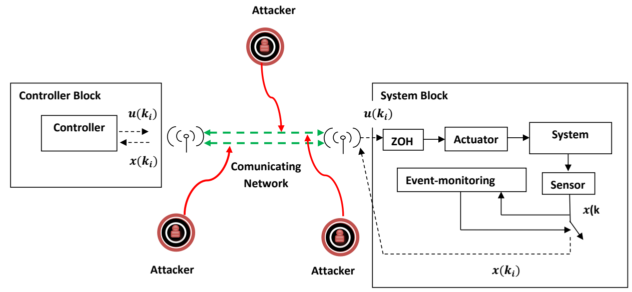

Fig. 1. Block diagram of proposed control technique under DoS attack

II. Problem Formulation and Preliminaries

A. Problem description

Consider a linear event-triggered system with model uncertainty mathematically represented by

$$x(k + 1) = \big(A + \Delta A(p)\big)x(k) + Bu(k_i), \quad \forall\, k \in [k_i, k_{i+1}),\ i \in \mathbb{N}, \tag{5}$$
$$u(k_i) = Kx(k_i) = K\{x(k) + e(k)\}, \tag{6}$$

where $x(k) \in \mathbb{R}^n$ and $u(k_i) \in \mathbb{R}^m$ are the system state and input vectors, respectively. The symbol k_i in (5) and (6) represents the i-th aperiodic sensing and actuation instant and $e(k) = x(k_i) - x(k), \forall k \in [k_i, k_{i+1})$. The unknown matrix $\Delta A(p) \in \mathbb{R}^{n\times n}$ represents the uncertainty due to the bounded variations of the system's parameter p and its effects on the nominal system matrix A. The variations of p are bounded by a known and possibly uncountable set Ω. In general, the uncertainty is either matched or mismatched [21]. For matched system, the uncertainty affects the system's dynamics via the input matrix, i.e. $\Delta A(p)$ is in the range space of matrix B. This assumption does not hold for mismatched systems. In this paper, the unknown matrix $\Delta A(p)$ is mismatched in nature and it is expressed as

$$\Delta A(p) = \underbrace{BB^+\Delta A(p)}_{\text{matched}} + \underbrace{(I - BB^+)\Delta A(p)}_{\text{mismatched}}. \tag{7}$$

The matrix B^+ represents the left-pseudo inverse of input matrix B, i.e. $B^+ = (B^TB)^{-1}B^T$. The unknown state perturbation matrix $\Delta A(p)$ is bounded by a known matrix F which is defined as

$$\Delta A(p)^T \Delta A(p) \leq \epsilon \frac{F}{2}, \tag{8}$$

where the scalar ϵ is a design parameter. The block diagram of the proposed controlled system is shown in Fig. 1. According to (5), the control and sensing actions are executed at each event-triggering instant k_i. However, when DoS interruptions affect the communication medium, the control and sensing actions are prevented from being executed. For simplicity, in this paper we assume that DoS attack equally affects the control and measurement channels. As expected, in the presence of DoS attacks, the data cannot be transmitted to or received from the communication channel.

Problem Statement: Design robust event-triggered state feedback control law (6) that stabilizes system (5) in the presence of DoS attacks and mismatched uncertainty (7).

Proposed Solution: A two-step solution to this control problem is proposed. First, a robust controller is designed to handle uncertainty and then, a transmission rule for sensing and actuation is derived to tackle DoS effects and limited availability of communication channel. To derive the robust controller gain, an emulation-based approach is adopted from [17]. That means, the controller is designed excluding the influence of the network, and then some conditions are derived to deal with network constraints. In [17], Tripathy et. al. derived the robust controller gain matrices within the optimal control framework, which is discussed next.

B. Optimal Control Approach for Robust Controller Design

The optimal control solution for a virtual system

$$x(k+1) = Ax(k) + Bu(k) + \alpha(I - BB^{+})v(k), \tag{9}$$

which minimizes a modified cost function

$$J(k) = \frac{1}{2}\sum_{k=0}^{\infty}\Big\{x(k)^T(Q+F)x(k) + u(k)^T R_1 u(k) + v(k)^T R_2 v(k)\Big\}, \tag{10}$$

is robust for the original systems (5) in the presence of uncertainty defined in (7). Here, α is a scalar and $Q \geq 0$, $R_1 > 0$, $R_2 > 0$ are matrices. The system (9) has two control inputs u and v, which are denoted as stabilizing and virtual inputs respectively. The importance of virtual input v is discussed in Remark 1. To design the robust controller gains for (5), the optimal control problem for (9) and (10) is solved adopting the method proposed in [17], [22] and results are presented as a Lemma below.

Lemma 1: Suppose there exist a scalar $\epsilon > 0$ and positive definite solution $P > 0$ of the following Riccati equation

$$A^T\big\{P^{-1} + BR_1^{-1}B^T + \alpha^2(I - BB^{+})R_2^{-1} (I - BB^{+})^T\big\}^{-1}A - P + Q + F = 0, \tag{11}$$

and

$$(\epsilon^{-1}I - P) > 0. \tag{12}$$

If the optimal control inputs $u = Kx$ and $v = Lx$ for (9) and (10) are selected as

$$K = -R_1^{-1}B^T\big\{P^{-1} + BR_1^{-1}B^T + \alpha^2(I - BB^{+})R_2^{-1}(I - BB^{+})^T\big\}^{-1}A, \tag{13}$$

$$L = -\alpha R_2^{-1}(I - BB^{+})^T\big\{P^{-1} + B^T R_1^{-1}B + \alpha^2(I - BB^{+})R_2^{-1}(I - BB^{+})^T\big\}^{-1}A, \tag{14}$$

where the gain matrices K and L satisfy the following matrix inequality

$$Q_1 = (Q + K^T R_1 K + L^T R_2 L + M^T P^{-1} M) - A_c^T\big(P^{-1} - \epsilon I\big)^{-1}A_c > 0, \tag{15}$$

with $A_c = A + BK$ and

$$M = \{P^{-1} + BR_1^{-1}B^T + \alpha^2(I - BB^{+})R_2^{-1}(I - BB^{+})^T\}^{-1}A, \tag{16}$$

then, the matrix K is the robust controller gain for (5).

The detailed proof of Lemma 1 can be found in [17]. In the next section, the gain matrices K and L are used to derive the transmission instant.

Remark 1: The virtual system (9) has two control inputs $u = Kx$ and $v = Lx$. The virtual input v is used for handling the mismatched uncertainty even though v is not used directly to stabilize the uncertain system (5). However, v indirectly helps to design the robust controller gain K by satisfying the inequality (15).

III. Main results

In this section, we consider a class of DoS attacks and present an event-triggering rule robustly stabilizing the closed loop system in the presence of model uncertainty and DoS attack. In particular, we assume that the DoS attack holds the following assumptions.

Assumption 1: [DoS attack rate] There exist scalars $\eta_1, c_1, c_2 \in \mathbb{R}$ such that

$$\frac{T_{\text{off}}(k)}{k} \leq \frac{2\ln(\eta_1) - \ln(c_1)}{\ln(c_2) - \ln(c_1)}, \qquad \forall\, k > 1. \tag{17}$$

where $c_1 < \eta_1 < 1$ and $c_2 > 1$.

Assumption 2: [DoS frequency] Let T_a be the average time between two consecutive attacks and suppose scalar η_2 satisfies $1 > \eta_2 > \eta_1$. Then, the frequency of DoS attack for an interval $[0, k)$ is upper bounded by

$$\frac{N_{\text{off}}(k)}{k} \leq T_a, \tag{18}$$

where $T_a = \frac{2(\ln(\eta_2) - \ln(\eta_1))}{\ln(\lambda_{\max}(P)/\lambda_{\min}(P))}$.

Assumptions 1 and 2 imply some restrictions on the nature of the DoS attack in terms of duration and frequency of attack. For the sake of the analysis, we limit our study to the class of DoS signals satisfying both Assumptions 1 and 2. Owing to the occurrence of DoS attack disrupting the communication channel, the transmission of information at time instant k_i may be influenced.

To prove the stability of the closed-loop system (5) and to design an event-triggering rule that can withstand model uncertainty in the presence of DoS attacks, the following two cases are considered. First, we establish the stability results and derive an event-triggering condition in the absence of any DoS attack. Second, to circumvent the DoS-related effects, we derive some conditions that the attack signal must satisfy for our event-triggering approach to be effective. Before stating the main theorem, the following two lemmas adopted from [17], [20] are introduced which are instrumental to prove the main results.

Lemma 2: Suppose there exists a positive definite solution $P > 0$ of (11) and a scalar $\epsilon > 0$. Then if $(\epsilon^{-1}I - P) > 0$, the following holds

$$\hat{X}^T P\hat{W} + \hat{W}^T P\hat{X} + \hat{W}^T P\hat{W} \leq \hat{X}^T(\epsilon^{-1}I - P)^{-1}\hat{X} + \epsilon^{-1}\hat{W}^T\hat{W}, \quad (19)$$

where $\hat{X}$ and $\hat{W}$ are two matrices with appropriate dimensions.

Lemma 3: Let $P > 0$ be a solution of (11) and the gain matrices K and L be computed using (13) and (14), respectively. Using (13) and (14) the following holds

$$A^T(P^{-1} + BR^{-1}B^T + \alpha^2(I - BB^+)R_2^{-1}(I - BB^+)^T)^{-1}A = K^T R_1 K + L^T R_2^T L + M^T P^{-1} M, \quad (20)$$

where matrix M is defined in (16).

The main results of this paper are stated in the following theorem.

Theorem 1: Suppose there exist scalars $\sigma \in (0, 1)$ and $\epsilon > 0$ which satisfy (8) and (12) and let the controller gain matrices derived from (13) and (14). Consider any DoS signal for which Assumptions 1 & 2 hold. If (15) holds and the control input (6) is actuated based on the following event-triggering sequence

$$k_0 = 0, k_{i+1} = inf\Big\{k \in \mathbb{N} | k \geq k_i \wedge (\mu\|x\|^2 - \|e\|^2) \leq 0\Big\}, \quad (21)$$

with

$$\mu = \frac{\sigma\lambda_{\min}^2(Q_1)}{4\|(A_c^T PBK)\|^2 + 2\lambda_{\min}(Q_1)\|K^T B^T(P^{-1} - \epsilon I)BK\|}, \quad (22)$$

then, the event-triggered control law (6) ensures the ISS of the system (5) in the presence of uncertainty (7) and DoS attacks.

The proof of Theorem 1 is divided into two cases discussed below.

Case 1. No DoS attack has occurred: Here, we assume that the communication medium is perfect for data transmission, without any jamming within the channel. Therefore, any attempts in updating the control inputs will be successful. That means, whenever an event is generated, the transmission of sensor and control information are not interrupted and the control law is actuated immediately. The stability criteria and aperiodic transmission rule of information in the absence of any DoS attack are reported below for this particular case.

Case 2. A DoS attack has occurred: Here, we suppose that the attacker successfully compromises the effectiveness of the communication medium, thereby preventing feedback loops from operating from time to time. If the channel is not available to update the control actions, it may affect the closed-loop stability and sensing and actuation instants. In this case, we study the effect of attacks and model uncertainty in system's stability and propose a criterion guaranteeing the stability of the closed-loop system in the presence of DoS attacks satisfying Assumptions 1 and 2.

Proof: [Proof of Theorem 1] **Case 1.** Let there exists an ISS Lyapunov function $V(k) = x^T Px$. Using (5), $\Delta V = [V(k+1) - V(k)]$ is computed as

$$\Delta V = x^T[A_c^T PA_c + A_c^T P\Delta A + \Delta A^T PA_c + \Delta A^T P\Delta A]x + x^T A_c^T PBKe + x^T\Delta A^T PBKe + e^T K^T B^T PA_c x + e^T K^T B^T P\Delta Ax + e^T K^T B^T PBKe - x^T Px,$$

where $A_c = A + BK$. The above equality is simplified using Lemma 2 as

$$\begin{aligned} \Delta V \quad \leq \quad & x^T[A_c^T(P + P(\epsilon^{-1}I - P)^{-1}P)A_c - P \\ & + 2\epsilon^{-1}\Delta A^T\Delta A]x + x^T A_c^T PBKe \\ & + e^T K^T B^T PA_c x + e^T K^T B^T(P \\ & + P(\epsilon^{-1}I - P)^{-1}P)BKe. \end{aligned} \quad (23)$$

Using matrix inversion lemma and solution of Riccati equation from (11), inequality (23) is simplified as

$$\begin{aligned} \Delta V \leq\ & x^T[A_c^T(P^{-1} - \epsilon I)^{-1}A_c - (Q + F) - A^T(P^{-1} \\ & + BR^{-1}B^T + \alpha^2(I - BB^+)R_2^{-1}(I - BB^+)^T)^{-1}A \\ & + 2\epsilon^{-1}\Delta A^T\Delta A]x + x^T A_c^T PBKe + e^T K^T B^T PA_c x \\ & + e^T K^T B^T(P^{-1} - \epsilon I)^{-1})BKe. \end{aligned} \quad (24)$$

Using (8) and applying Lemma 3 to (24), we arrive at

$$\begin{aligned} \Delta V \leq\ & x^T[A_c^T(P^{-1} - \epsilon I)^{-1}A_c - Q - K^T R_1 K - L^T R_2 L \\ & - M^T P^{-1} M]x + \psi x^T x + \frac{1}{\psi}\|A_c^T PBK\|^2\|e\|^2 \\ & + e^T K^T B^T(P^{-1} - \epsilon I)^{-1})BKe, \end{aligned}$$

where ψ is a positive scalar. Furthermore, using (15), we can simplify above inequality to

$$\begin{aligned} \Delta V \leq & -x^T Q_1 x + \psi x^T x + \frac{1}{\psi}\|A_c^T PBK\|^2\|e\|^2 \\ & + \|K^T B^T(P^{-1} - \epsilon I)^{-1})BK\|\|e\|^2. \end{aligned}$$

Choosing $\psi = \frac{\lambda_{\min}(Q_1)}{2}$, the following is obtained

$$\Delta V \quad \leq \quad -\xi_1\|x(k)\|^2 + \xi_2\|e(k)\|^2, \quad (25)$$

where matrix Q_1 is defined in (15) and $\xi_1 = \frac{\lambda_{\min}(Q_1)}{2}$ and $\xi_2 = \Big(\frac{2(\|A_c^T PBK\|^2}{\lambda_{\min}(Q_1)} + \|K^T B^T(P^{-1} - \epsilon I)^{-1}BK\|\Big)$. Using Definitions 1 and 2, the inequality (25) ensures the ISS of (5). In the absence of any DoS attack, the event-triggering condition (21) is also derived using (25). In fact, the control inputs need to be actuated whenever the condition (21) is violated.

The Lyapunov function $V(x) = x^T Px$ satisfies (3) where $\alpha_1(\|x\|) = \lambda_{\min}(P)\|x\|^2$ and $\alpha_2(\|x\|) = \lambda_{\max}(P)\|x\|^2$. Now applying the event-triggering condition (21), the bound of ΔV can be written as

$$\Delta V(x) \leq -\frac{\xi_1}{\lambda_{\min}(P)}(1 - \sigma)V(x) \leq -\frac{\lambda_{\min}(Q_1)}{2\lambda_{\min}(P)}(1 - \sigma)V(x), \quad (26)$$

where $\sigma \in (0, 1)$ regulates the transmission of information over the network. The information exchange over the network has inverse relation with the selection of σ. This proves that the closed-loop system (5) is globally asymptotically stable with event-triggered feedback and model uncertainty. Using (26), following yields

$$V(k+1) \leq c_1 V(k) \tag{27}$$

where $c_1 = (1 - \frac{\lambda_{\min}(Q_1)}{2\lambda_{\min}(P)}(1-\sigma))$ and is always less than 1 as $V(x)$ is decreasing. The following Remark describes the growth of error e in between two consecutive events.

Remark 2: Inequality (26) signifies that the state of the uncertain system (5) will remain bounded. Since the state is bounded, the measurement error $e(k)$ is also bounded. Here, the variable $e(k)$ evolves based on the following difference equation

$$\begin{aligned} e(k+1) &= x(k_i) - x(k+1), \qquad (28)\\ &= (A + BK + \Delta A)e(k) + (I - (A + \Delta A + BK))x(k_i). \end{aligned}$$

The matrix ΔA is also bounded as the condition (8) holds $\forall\, p \in \Omega$. This proves that the error growth remains bounded in between two consecutive events.

Case 2: Suppose that a DoS attack occurs in the feedback channel at the instant $a_i \in [0,\ k)$, where $i \in \{0, \dots, m\}$ represents the i^{th} attack event, and this attack lasts for the duration k_{a_i} time units. The scalar m represents the number of attacks during $[0,\ k)$. Now, within this time interval k_{a_i}, if an event is not generated then the requirement of feedback channel is unnecessary and the measurement error will grow according to (28). The problem is more severe if any event occurs within k_{a_i} time duration. According to (21), a triggering event occurs only when the stability criterion (25) is violated. Therefore, the unavailability of the communication channel may destabilize the system. The effects of this DoS attack on the system's stability is considered and analyzed in what follows.

Within the interval $[0, k)$, some transmission attempts are not successful due to jamming. In other words, for the time duration $\left(k - \sum_{i=1}^{m} k_{a_i}\right)$, the channel is available for communication and for the remaining time, the channel is unavailable due to the DoS attack. The duration $\sum_{i=1}^{m} k_{a_i}$ is represented by $T_{\text{off}}(k)$. Then, at a_i, the growth of variable e is

$$e(k) = x(k_{i(a_i)}) - x(k), \tag{29}$$

where $x(k_{i(a_i)})$ represents the state of the system at the last successful control update up to a_i. At the moment of the attack, the condition (25) holds. That means

$$\|e(a_i)\| \leq \sqrt{\mu}\|x(a_i)\|, \quad x(k_{i(a_i)}) - x(a_i) \leq \sqrt{\mu}\|x(a_i)\|.$$

Using (29), the error $e(k)$ can be expressed as

$$\|e(k)\| \quad \leq \quad (1 + \sqrt{\mu})\|x(a_i)\| + \|x(k)\|. \tag{30}$$

The inequalities (30) and (25) can be used to compute ΔV as

$$\begin{aligned} \Delta V \quad &\leq \quad -\xi_1 \|x(k)\|^2 + \xi_2 \left((1+\sqrt{\mu})\|x(a_i)\| + \|x(k)\|\right)^2 \\ &\leq \quad \gamma \max\{V(x(k)), V(x(a_i))\}, \qquad (31) \end{aligned}$$

where $\gamma = \frac{\xi_2 (1+\mu)^2}{\lambda_{\min}(P)}$.

Let us consider the ith attack interval, i.e. $(a_i, a_i + k_{a_i})$. Using the comparison principle for discrete-time system presented in [23, Proposition 1], for $\tau \in (a_i, a_i + k_{a_i})$, (31) reduce to

$$V(x(\tau)) \leq c_2^{(\tau - k_{a_i})} V(x(a_i)), \tag{32}$$

where $c_2 = (1+\gamma) > 1$. Now, consider the consecutive time interval without any DoS attack, i.e. $(a_i + k_{a_i}, a_{i+1})$. Again, using comparison principle, [23, Proposition 1], for $\tau \in (a_i + k_{a_i}, a_{i+1})$, (27) reduces to

$$V(x(\tau)) \leq c_1^{(\tau - [a_{i+1} - (a_i + k_{a_i})])} V(x(a_i + k_{a_i})). \tag{33}$$

Therefore, whenever DoS signal blocks the communication channel, the system dynamics follows (32) and in the absence of DoS signal, it is governed by (33). Recalling that the number of off to on transitions of DoS attack within the interval $[0, k)$ is $N_{\text{off}}(k)$. With these ingredients in mind and combining (32) and (33), we get the following bound on $V(k)$

$$V(k) \leq \Xi^{N_{\text{off}}(k)} c_1^{(k - T_{\text{off}}(k))} c_2^{T_{\text{off}}(k)} V(x(0)) \tag{34}$$

where $\Xi = \lambda_{\max}(P)/\lambda_{\min}(P)$. Now, using (34) and (3), we obtain the following upper bound for the system's state

$$\|x(k)\| \leq \Xi^{\frac{1+N_{\text{off}}(k)}{2}} c_1^{\frac{(k - T_{\text{off}}(k))}{2}} c_2^{\frac{T_{\text{off}}(k)}{2}} \|x(0)\|. \tag{35}$$

To ensure the convergence of $x(k)$, the following two sub-cases are considered.

$\Xi = 1$: For a selection of $\Xi = 1$, inequality (35) reduces to

$$\|x(k)\| \leq c_1^{\frac{(k - T_{\text{off}}(k))}{2}} c_2^{\frac{T_{\text{off}}(k)}{2}} \|x(0)\|.$$

Now assume that there exists a scalar $1 > \eta_1 > c_1$ such that

$$c_1^{\frac{(k - T_{\text{off}}(k))}{2}} c_2^{\frac{T_{\text{off}}(k)}{2}} \leq \eta_1^k.$$

After simplification, the following is obtained

$$\frac{T_{\text{off}}(k)}{k} \leq \frac{2\ln(\eta_1) - \ln(c_1)}{\ln(c_2) - \ln(c_1)}. \tag{36}$$

$\Xi > 1$: For a selection of $\Xi > 1$, (35) reduces to

$$\|x(k)\| \leq \Xi^{\frac{1+N_{\text{off}}(k)}{2}} \eta_1^k \|x(0)\|. \tag{37}$$

Now, assume that there exists a scalar $1 > \eta_2 > \eta_1$ which simplifies (37) as

$$\Xi^{\frac{1+N_{\text{off}}(k)}{2}} \eta_1^k \leq \eta_2^k, \tag{38}$$

and thus $\|x(k)\| \leq \eta_2^k \|x(0)\|$. The inequity (38) is used to derive the DoS frequency as

$$\frac{N_{\text{off}}(k)}{k} \leq \frac{2(\ln(\eta_2) - \ln(\eta_1))}{\ln(\Xi)} = T_a,$$

where T_a is

$$T_a = \frac{2(\ln(\eta_2) - \ln(\eta_1)))}{\ln(\Xi)}, \tag{39}$$

which is defined in Assumption 2.

From (35), if Assumptions 1 and 2 hold for the DoS attack signal, which are computed from (39) and (36), then $\|x(k)\|$ in (35) is bounded. This completes the proof. ■

IV. Simulation Results

This section validates the proposed robust control approach in the presence of DoS attacks with uncertainty in the system's dynamics using a numerical example. For the sake of numerical validation, we consider the classical networked control system corresponding to a batch reactor system [24] with two inputs and two outputs. To realize a stabilizing control law, the feedback control loop is closed by means of a wireless communication network. The control input is designed to tackle the aperiodic availability of feedback information in the presence of mismatched uncertainty.

We derive a discrete-time linearized model of a batch reactor system in the form of (5) from a continuous model with a sampling period $T = 0.05$. The matrices A and B are given by

$$A = \begin{bmatrix} 0.0690 & -0.0100 & 0.3355 & -0.2835 \\ -0.0290 & -0.2145 & 0 & 0.0338 \\ 0.0530 & 0.2135 & -0.3325 & 0.2945 \\ 0.0020 & 0.2135 & 0.0670 & 0.1050 \end{bmatrix},$$

and

$$B = \begin{bmatrix} 0 & 0.2840 & 0.0568 & 0.0568 \\ 0 & 0 & -0.1573 & 0 \end{bmatrix}^T.$$

The matrix ΔA is defined as $\Delta A = pI$ where variable p is the uncertain parameter with variations in the unit interval. To design the controller gains, the matrices $Q = 4I$, $R_1 = I$, $R_2 = I$ and variable $\epsilon = 0.01$ are selected. The scalar parameter σ is chosen to be 0.1. The simulation is carried out using MATLAB for a run time of 6 seconds with the initial state $x = \begin{bmatrix} -0.5 & -0.3 & 0.2 & -0.05 \end{bmatrix}^T$. The matrix $F = 2I$ and scalars $\eta_1 = 0.3$ and $\eta_2 = 0.95$ are selected such that the conditions (8), (15), (17) and (18) are satisfied. To obtain the controller gain matrices K and L, the Riccati equation (11) is solved leading to

$$K = \begin{bmatrix} -0.0710 & -0.9309 & -0.0356 & -0.1008 \\ 1.4597 & 0.1990 & 1.0212 & -0.5773 \end{bmatrix},$$

$$L = \begin{bmatrix} -0.0092 & 0.0057 & -0.0053 & 0.0092 \\ -0.0144 & 0.0174 & -0.0072 & 0.0215 \\ 0.0220 & -0.0104 & 0.0131 & -0.0193 \\ 0.0007 & -0.0166 & -0.0016 & -0.0142 \end{bmatrix}.$$

Figure 2 shows the convergence of the state x in spite of system's uncertainty and DoS attack on the communication channel. The attack signal is represented with the red color. The degradation of the system's performance following DoS attacks is apparent in Fig. 2. Table I shows the efficacy of the proposed control algorithm. The symbol u_{total} denotes the total number of transmissions of control inputs via the communication network. The quantities $\tau_{\min}$ and $\tau_{\max}$ represent the minimum and maximum duration of inter-event time respectively. The larger inter-event time, the improved savings in communication resources. The lower bound of attack duration, total DoS period and frequency are computed as $T_{\text{a}} = 0.1$ sec., $T_{\text{off}} = 1.53$ sec., $N_{\text{off}} = 12$. To generate the DoS signal we have used these bounds.

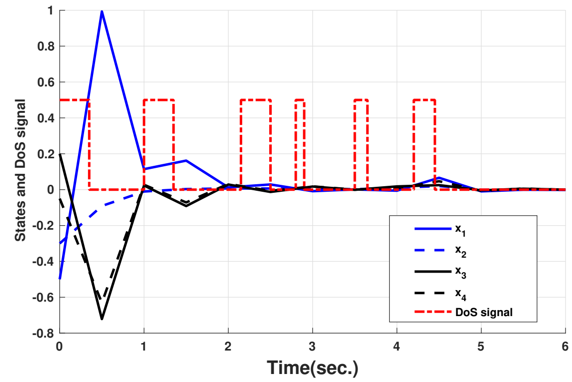

Fig. 2. Convergence of states in the presence of DoS attacks for $p = 0.5$.

TABLE I
Comparison of Event-Triggered vs. Periodic Feedback Control

Control Strategy	$\tau_{\max}$(sec.)	$\tau_{\min}$(sec.)	u_{total}
Periodic feedback control	0.05	0.05	120
Event-triggered control with DoS	0.93	0.05	37

V. Conclusion

In this paper, we investigated the robust stabilization of discrete-time mismatched uncertain systems in the presence of DoS attack. The primary contribution of this paper is an explicit characterization of the attack signal, namely DoS duration and frequency under which the mismatched system remains input-to-state stable with event-triggered feedback. The aperiodic use of feedback information significantly reduces the communication overhead over the transmission network. To handle the inherent uncertainty in the system's model, an optimal control approach based on a robust control technique has been considered. The proposed robust control approach translates the robust control problem into an optimal control one for a virtual system with a modified cost-functional. The optimal input for the virtual system is the robust solution for uncertain system. The proposed robust controller also ensures the stability of closed-loop system under a generic class of DoS attacks, for which the attack signal satisfies Assumptions 1 and 2. Beyond its effectiveness in overcoming the damaging effects of DoS attacks, the developed event-triggered control technique leads to significant savings in the channel bandwidth. The proposed control algorithm is illustrated and validated numerically using the classical NCS batch reactor model.

References

[1] Y. Mo, T. Kim, K. Brancik, D. Dickinson, H. Lee, A. Perrig, and B. Sinopoli, "Cyber-physical security of a smart grid infrastructure," *Proc. IEEE*, vol. 100, no. 1, pp. 195–205, 2012.

[2] A. Cárdenas, S. Amin, and S. Sastry, "Secure control: Towards survivable cyber-physical systems," *Int. Conf. Distrib. Comput. Syst. Workshops*, pp. 495-500, 2008.

[3] S. Sundaram and C. N. Hadjicostis, "Distributed function calculation via linear iterative strategies in the presence of malicious agents," *IEEE Trans. Autom. Control*, vol. 56, no. 7, pp. 1495–1508, 2010.

[4] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson, "Attack models and scenarios for networked control systems," *in Proc. 1st Int. Conf. High Confidence Networked Systems,* pp. 55–64. 2012.

[5] A. Teixeira, D. Pérez, H. Sandberg, and K. H. Johansson, "A secure control framework for resource-limited adversaries", *Automatica*, vol. 51, pp.135-148, 2015.

[6] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," *IEEE Network*, vol. 20, no. 3, pp. 41–47, 2006.

[7] D. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11b and other networks," *in Proc. 25th IEEE Commun. Soc. Military Commun. Conf.*, pp. 1075-1081, 2006.

[8] M. Zuba, Z. Shi, Z. Peng, and J. Cui, "Launching denial-of-service jamming attacks in underwater sensor networks," *ACM Int. Workshop on Underwater Networks*, DOI: 10.1145/2076569.2076581, 2011.

[9] H. Zhang, P. Cheng, L. Shi, J. Chen,"Optimal DoS attack scheduling in wireless networked control system", *IEEE Trans. Contr. Sys. Techn*, vol.24, no. 3, pp. 843-852, 2016.

[10] H. Zhang, P. Cheng, L. Shi, J. Chen, "Optimal denial-of-service attack scheduling with energy constraint", *IEEE Trans. Autom. Control*, vol. 60, no. 11, pp. 3023-3028, 2015.

[11] C. D. 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.

[12] L. Zhang and D. H. Varsakelis, "LQG control under limited communication", *44th IEEE Conf. on Decision and Control*, pp. 185-190, 2005.

[13] K. Astrom and B. Bernhardsson, "Comparison of Riemann and Lebesgue sampling for first order stochastic systems", *41st IEEE Conf. on Decision and Control*, pp. 2011-2016, 2002.

[14] P. Tabuada, "Event-triggered real-time scheduling of stabilizing control tasks", *IEEE Trans. on Autom. Control*, vol. 52, no. 9, pp. 1680-1685, 2007.

[15] S. Trimpe and R. D'Andrea, "Event-based state estimation with variance-based triggering", *51st IEEE Conf. on Decision and Control*, pp. 6583-6590, 2012.

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

[17] N. S. Tripathy, I. N. Kar, and K. Paul, "Stabilization of uncertain discrete-time linear system with limited communication", *IEEE Trans. Autom. Control*, vol. 62, no. 9, pp. 4727-4733, 2017.

[18] N. S. Tripathy, I. N. Kar, and K. Paul, "An event-triggered based robust control of robot manipulator", *International Conference on Control Automation Robotics and Vision*, pp. 425-430, 2014.

[19] H. K. Khalil, *Nonlinear Systems*, Prentice Hall, 3rd Edition, New Jersey, 2002.

[20] G. Garcia, J. Bernussou, and D. Arzelier, "Robust stabilization of discrete- time linear systems with norm-bounded time varying uncertainty", *Syst. Control Lett.*, vol. 22, pp. 327–339, 1994.

[21] I. R. Petersen, "Structural stabilization of uncertain systems: Necessity of the matching condition", *SIAM J. Control Optim.*, vol. 23, no. 2, pp. 286-296, 1985.

[22] D. S. Naidu, *Optimal Control Systems*. CRC press, India, 2009.

[23] G. Bitsoris, E. Gravalou, "Comparison principle, positive invariance and constrained regulation of nonlinear systems", *Automatica*, vol. 31, no. 2, pp. 217-222, 1995.

[24] D. Nešić, A. R. Teel, "Input-output stability properties of networked control systems", *IEEE Trans. Autom. Control*, vol. 49, no. 10, pp. 1650-1667, 2014.