International Journal of Control, Automation, and Systems VV(X) (YYYY) 1-11
http://dx.doi.org/10.1007/s12555-xxx-xxxx-x
ISSN:1598-6446 eISSN:2005-4092
http://www.springer.com/12555

DIDoS: Disturbance-Induced Denial-of-Service Attack in Cyber-Physical Systems

Sangjun Kim , Sanghoon Lee , and Kyung-Joon Park*

Abstract: Event-triggered control (ETC) in a cyber-physical system (CPS) is an efficient aperiodic control strategy that generates control packets only when a control-triggering condition is satisfied. However, the CPS with ETC introduces a new point of vulnerability. A well-designed disturbance signal can unnecessarily trigger control events and the resulting excessive packet exchanges can destabilize the physical systems due to network saturation. In this paper, we propose a novel CPS attack vector entitled the disturbance-induced denial of service (DIDoS) attack, which has the following key characteristics: DIDoS cannot be mitigated by a conventional network security method such as a firewall. Unlike most cyber-physical attacks, DIDoS does not require knowledge of physical system dynamics. Under DIDoS, a disturbance signal into a single physical system can saturate the whole network and destabilize all the physical systems connected to the network. We study the relationship between the network delay and the stability of physical systems under DIDoS. We derive a stability condition under a time-varying network delay and quantitatively describe network saturation under DIDoS with an IEEE 802.11 wireless network model. Our simulation results show that DIDoS can saturate the network and destabilize all the physical systems.

Keywords: Cyber-physical systems, Cyber-physical security, Denial of service, Networked control system, Event-triggered control.

1. INTRODUCTION

A cyber-physical system (CPS) converges physical processes in the real world and control software in the cyber world, with communication networks tightly connecting these two realms [1,2]. As communication technology advances, networks can now connect large numbers of physical systems to their controllers in real time [3]. In particular, wireless networking in CPSs offers advantages in terms of maintenance cost, mobility, and connectivity [2].

Nevertheless, introducing a network also exposes the CPS to externally launched cyber-physical attacks [4]. A cyber-physical attack interferes with the interaction between a physical system and its computing counterpart through data tampering or intentional exhaustion of network resources [5,6]. Such attacks damage the network by exploiting vulnerabilities, causing malfunctions or even destabilising the physical systems. For example, most control-theoretic attacks-including zero-dynamics, pole-dynamics, covert, and replay attacks-tamper with sensor measurements or control inputs using knowledge of the system model [7]. Denial-of-service (DoS) attacks, on the other hand, disrupt communication between the physical and computing domains [8]; the resulting delay and packet loss degrade performance or even destabilize the plants [9, 10].

Event-triggered control (ETC) has been introduced to CPS as an efficient way to use network resources [11]. ETC is an aperiodic strategy that transmits control packets only when a specified triggering condition is satisfied [12]. Compared with conventional periodic control, ETC significantly reduces per-plant network utilization, allowing more plants to share the same network. Its aperiodic nature also mitigates malicious packet-dropping attacks [13], while lower utilization provides tolerance against delay-inducing attacks such as packet flooding.

However, ETC introduces a new vulnerability from the attackers' perspective. A carefully crafted disturbance signal can trigger unnecessary control events and markedly increase network delay [14]. These extra packets consume limited bandwidth, and the problem is exacerbated when a single controller manages many physical systems-a disturbance affecting one plant can saturate the entire network and degrade control performance for all plants.

In this paper, we propose a novel cyber-physical attack vector termed the disturbance-induced denial-of-service (DIDoS) attack. Whereas conventional CPS attacks focus on data manipulation or packet delivery interruption on the network, DIDoS injects a disturbance into the physical system itself and exhausts bandwidth through ETC's triggering mechanism. The key characteristics of DIDoS are as follows:

- To the best of our knowledge, the proposed DIDoS

S. Kim is with the Center for R&D Investment Planning, Korea Institute of Science & Technology Evaluation and Planning (KISTEP), Eumseong 27740, South Korea (e-mail: ksj@kistep.re.kr). S. Lee and K.-J. Park are with the Department of Electrical Engineering & Computer Sciences, DGIST, Daegu 42988, South Korea (e-mail: leesh2913@dgist.ac.kr, kjp@dgist.ac.kr). * Corresponding author.

attack is the first cyber-physical attack targeting the CPS network by exploiting the intrinsic nature of ETC.
- Unlike DoS attacks, the proposed DIDoS attack cannot be mitigated by a conventional network security method such as a firewall.
- DIDoS does not require any knowledge of physical system dynamics while most cyber-physical attacks such as zero-dynamics attack, pole-dynamics attack, and covert attack require knowledge of physical system dynamics.
- DIDoS is more serious than most of existing cyber-physical attacks because all the physical systems connected to the network can be destabilized even when only a single physical system is under attack.

We consider a CPS with ETC, where one computing system controls multiple physical systems through a wireless network. For quantitative analysis, we specify the network protocol as IEEE 802.11 that is widely used in practice. We analyze the control performance degradation and state divergence of the physical systems with respect to the number of physical systems being attacked. We derive a stability condition under a time-varying network delay and quantitatively describe network saturation under DIDoS with an IEEE 802.11 wireless network model.

The rest of this paper is organized as follows. In Section 2, we present related studies on the conventional DoS attack and a networked control system (NCS) with an uncertain communication channel. Section 3 provides preliminary information on ETC systems and IEEE 802.11 wireless networks. In Section 4, we present the stability conditions of the NCS against network delay, and we analyze the mechanisms of the DIDoS attack. In Section 5, we provide simulation results to demonstrate the effectiveness of DIDoS. Finally, we conclude this paper in Section 6.

2. RELATED WORK

Cyber-physical security covers a wide range of multidisciplinary studies including control theory, networks, and software. Hence, here we only provide the most-related studies. Comprehensive surveys on cyber-physical security can be found in [15–17]. In this section, we first specify our interest in physical systems, and provide the modeling and physical impact of DoS attacks. Then, we introduce CPS designs that ensure the stability of the physical systems considering packet drops and network delays.

2.1. Denial of Service (DoS)

DoS attacks cause packet drops [18] and additional network delays [19], which can catastrophically damage physical systems. In terms of control theory, the DoS attack is modeled as stochastic packet drops under two constraints: average duration and frequency, which are physical restrictions on DoS attack devices [11]. To maximize the impact of the DoS attack on an NCS, an optimal DoS attack strategy is proposed in [20] targeting a linear time-invariant (LTI) system from an energy-constrained attacker. An analysis of performance degradation from communication jamming is provided in [21] for communication-based train control systems. The intentional packet drops from communication jamming increases the journey times of all trains in the network.

Furthermore, the flooding-type DoS attack causes network delays in order to degrade control performance or destabilize physical systems. The stability of the physical system under network delays is analyzed for static delays [22] and time-varying delays [23], respectively. In particular, the analysis in [23] shows that the delay bound of the NCS depends on the controller design. In [24], an empirical study is conducted on the behavior of an unmanned aerial vehicle (UAV) against a massive packet-flooding attack that causes packet transmission delays. From the intentional delays caused by the attacker, control command packets cannot reach the UAV system within the deadline constraint. Consequently, the UAV system enables the fail-safe mode and hovers at a standstill with missions uncompleted.

2.2. Secure NCS Design

ETC is one of the typical control strategies to mitigate the physical impact of cyber-physical attacks. A control gain design method is proposed in [25], which guarantees the stability of the ETC system against packet losses from uncertain communication channels and DoS attacks. The control gain is determined by system dynamics, average dropped-packet duration, and event-triggering conditions. Hence, the event-triggering condition and controller gain need to be tuned in order to stabilize a physical system under a DoS attack. In [5], a novel event-triggering strategy for ETC systems is proposed to mitigate data-tampering based cyber-physical attacks on a network. The authors in [5] show that cyber-physical attacks increase network traffic, and under such attacks, the proposed ETC strategy provides better control than a conventional ETC strategy.

In addition to theoretical control methods, network designs for the NCS can also reduce the impact of cyber-physical attacks. A transmission period selection method for sensor traffic is proposed in [26] for a periodic NCS with multiple physical systems. The proposed method, which is formulated as a convex optimization problem, simultaneously considers network delays in an IEEE 802.11 wireless network as well as control costs from network traffic. Also, a delay mitigation strategy against a massive flooding attack with user datagram protocol (UDP) packets is proposed in [27]. The software-defined networking (SDN) technique identifies and eliminates the useless packet flows generated by the attacker, and guarantees

a low-level delay and packet loss rate, despite the UDP flooding.

3. PRELIMINARIES ON EVENT-TRIGGERED CONTROL IN NETWORKED CONTROL SYSTEM

This section reviews event-triggered control (ETC) in networked control systems (NCSs). An NCS is a feedback loop that exchanges sensor data and control commands over a shared network [26, 28, 29]. We outline the ETC trigger, which curtails the bandwidth wasted by periodic sampling, and then present an IEEE 802.11 model that links network delay to the number of plants and their packet rates.

3.1. Event-Triggered Control Systems

We consider a CPS consisting of the physical system, network, and computing system illustrated in Fig. 1. We model the physical system as a linear time-invariant (LTI) system in a continuous-time domain, which is described as follows:

$$\dot{x}(t) = Ax(t) + B(u(t) + w(t)), \tag{1}$$

where $x(t) \in \mathbb{R}^n$ is the state of the physical system with n dimensions; $A \in \mathbb{R}^{n\times n}$ is the system matrix, $B \in \mathbb{R}^n$ is the input matrix, $u(t) \in \mathbb{R}$ is the control input signal, and $w(t) \in \mathbb{R}$ is the disturbance. For LTI system (1), we assume that the matrix pair (A,B) is controllable, which means that there always exists a control input signal $u(t)$ that can transfer the state $x(t)$ of the physical system to any given value in a finite time.

Exchanging control-related data such as the physical state and control input signals in the physical system is conducted by sampling the physical state $x(t)$ with a proper transmission period t_s in the discrete-time domain. Therefore, we consider a discretization model of the physical system (1) with a zero-order hold (ZOH) as follows:

$$\begin{aligned} x(k+1) &= A_d x(k) + B_d(u(k) + w(k)), \\ u(k) &= -Kx(k), \end{aligned} \tag{2}$$

where $K \in \mathbb{R}^{1\times n}$ is the control gain of the controller in the computing system. We assume that the control gain K is appropriately selected to stabilize the physical system (1) such as to make $A_d - B_d K$ a Schur matrix [30].

Event-triggered control is an aperiodic control method that exchanges control-related information only when certain events occur. For every transmission period t_s, the physical system checks an event policy, $\Phi(k)$, and transmits the physical state $x(k)$, through the network if the physical system satisfies the event policy at time k, as illustrated in Fig. 1. The event policy $\Phi(k)$ involves two conditions: the packet transmission period and transition

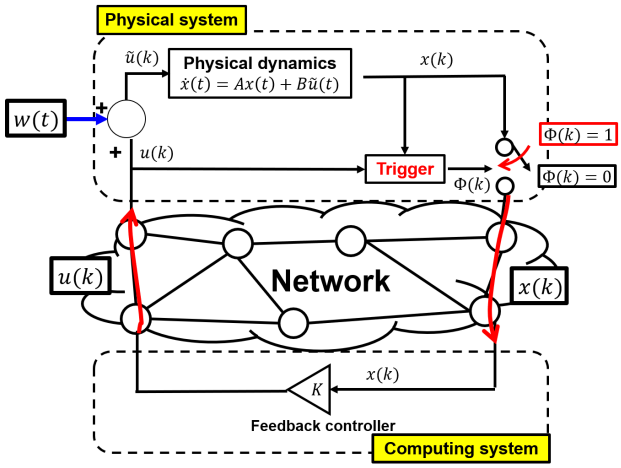


Fig. 1. Structure of an event-triggered control system.

of the physical state $x(k)$. We consider an event policy as follows:

$$\begin{aligned} \eta_{i+1} \triangleq min\{k \in \{\eta_i + 1, \eta_i + 2, \cdots\} : k \geq \eta_i + \theta \\ or\ V(Ax(k) + Bu(\eta_i)) > \beta V(x(\eta_i))\}, \end{aligned} \tag{3}$$

where η is the time instant when an event is triggered, $\theta \in \mathbb{N}$ is the packet transmission period, and $\beta \in (0,1)$. In addition, we consider a quadratic Lyapunov function $V(x(k)) \triangleq x^T(k)Px(k)$ as an event-generating condition from transition of the physical state $x(k)$.

The condition $t \geq \eta_i + \theta$ indicates that the physical system sends the physical state $x(k)$ at least once every θh if there is no physical issue for event generation regarding the transition of the physical state $x(k)$. The condition $V(Ax(k) + Bu(\eta_i)) > \beta V(x(\eta_i))$ shows event generation from transition of the physical state, where the value of $V(Ax(k) + Bu(\eta_i))$ remains less than the value of $\beta V(x(\eta_i))$ until the next event-time instant, η_{i+1}, from the time η_i, of successful reception of the control input signal $u(\eta_i)$.

3.2. Modeling of the IEEE 802.11 Protocol

In this section, we consider the network as a queueing system in a similar manner as the one in network-control co-design in [26], where a computing system and N physical systems are connected through the network. From a viewpoint of the network, each physical system as well as the computing system is a communication node that transmits packets. The nodes adopt the IEEE 802.11 wireless network standard, configuring the feedback control loops between the computing system and the multiple physical systems. We assume relaxed NCS conditions that all communication nodes always have packets to send and packet transmissions by each node are independent.

An IEEE 802.11 node first senses the medium; if busy,

it defers. When idle, it draws a back-off counter $BC \in [0, CW_{\min} - 1]$, with the contention window CW initially set to $CW_{\min}$. While the channel remains idle, BC decrements each slot and freezes whenever activity resumes. The node transmits as soon as $BC = 0$.

We denote the packet collision probability for node n as p_n, which is the probability transmission will fail due to simultaneously transmission by other nodes. From [31], the average back-off window of node n is given by

$$\bar{W}_n = \frac{1 - p_n - p_n(2p_n)^m}{1 - 2p_n} \frac{CW_{min}}{2}, \tag{4}$$

where, p_n is the packet-collision probability, $\mathrm{CW}_{\min}$ is the initial contention window, and $m = \log_2(\mathrm{CW}_{\max}/\mathrm{CW}_{\min})$ is the maximum back-off stage defined by the IEEE 802.11 back-off procedure. By (4), the collision probability of node n is derived as follows:

$$p_n = 1 - \prod_{\substack{i=1 \\ i \neq n}}^{N} \left(1 - \rho_i \frac{1 - 2p_i}{1 - p_i - p_i(2p_i)^m} \frac{2}{CW_{min}}\right). \tag{5}$$

Also, the packet service time $1/\mu_n$ of node n, where μ_n is the service rate of node n, is derived as follows:

$$\frac{1}{\mu_n} = \sum_{\substack{i=1 \\ i \neq n}}^{N} \rho_i \left[T_{S_i} + T_{C_i} \frac{p_i}{2(1 - p_i)}\right] + \bar{W}_n + T_{S_n} + T_{C_i} \frac{p_n}{2(1 - p_n)}, \tag{6}$$

where T_{S_i} and T_{C_i} are the average time for successful packet transmission and the packet collision time for node i in the unit of back-off slots, respectively. From (6), we can get the network utilization $\rho_n = \lambda_n/\mu_n$ of node n as follows:

$$\rho_n = \sum_{\substack{i=1 \\ i \neq n}}^{N} \lambda_n \rho_i \left[T_{S_i} + T_{C_i} \frac{p_i}{2(1 - p_i)}\right] + \lambda_n \left[\bar{W}_n + T_{S_n} + T_{C_i} \frac{p_n}{2(1 - p_n)}\right], \tag{7}$$

where λ_i is the transmission rate of node i. By numerically solving a system of $2N$ equations (5) and (7), we can derive a solution to the $2N$ unknowns p_n and ρ_n, $n = 1, \cdots, N$.

4. ANALYSIS OF THE DIDOS ATTACK

This section first derives the maximum delay that preserves stability, then introduces the disturbance-induced denial-of-service (DIDoS) attack in an IEEE 802.11 NCS. Instability stems from two coupled effects: (i) time-varying network delay, which directly degrades control performance, and (ii) event-triggered control (ETC), whose trigger depends on the plant state $x(k)$ and can be forced by external disturbances. A carefully crafted disturbance fires ETC at every step, flooding the network with sensor packets. The resulting bandwidth saturation lengthens delay beyond the allowable bound, ultimately destabilising all connected plants.

4.1. Allowable Delay Bound for Stability

An NCS suffers network delays in the packet exchange process, which can degrade the control performance or even destabilize the physical systems. Typically, the NCS has intrinsic time-varying network delays. Consequently, the stability of the NCS can be analyzed by using the maximum allowable delay bound, which provides a stability region for the physical system.

The delay bound is set by plant dynamics, sampling period, controller gain, and-under ETC-the trigger rule (3). Using the framework in [23], we compute this bound and evaluate stability with $w(k) = 0$ to isolate how the chosen gain dictates delay tolerance.

To consider the time-varying network delay in the control system (2), we assume that the network delay, τ_{net}, is bounded by $\underline{d} := \lfloor \tau_{min}/t_s \rfloor$ and $\bar{d} := \lceil \tau_{max}/t_s \rceil$, where τ_{min} and τ_{max} are the minimum and maximum values, respectively. We denote the time instant t_j^k as follows:

$$\begin{aligned} t_j^k = min\{ & max\{0, \tau_{k+j-\bar{d}} + (j - \bar{d})t_s\}, \\ & max\{0, \tau_{k+j-\bar{d}+1} + (j - \bar{d} + 1)t_s\}, \cdots, \\ & max\{0, \tau_{k-\bar{d}} - \underline{d}t_s\}, t_s \}, \end{aligned}$$

where $0 = t_0^k < \cdots < t_j^k < t_{j+1}^k < \cdots < t_{\bar{d}-\underline{d}+1}^k = t_s$. From the time instant t_j^k, we present the discrete-time NCS model (2), considering the network delay as follows:

$$x(k+1) = A_d x(k) + \sum_{j=0}^{\bar{d}-\underline{d}} \int_{t_s - t_{j+1}^k}^{t_s - t_j^k} e^{As} ds B u(k + j - \bar{d}). \tag{8}$$

Because of the network delay τ_{net}, the NCS model (8) reflects how the current physical state $x(k)$ depends on not only the current control input signal $u(k)$, but also the previous state and control input signals. We introduce the ξ dynamics, which is defined as $\xi(k) = \left[x(k)^T, u(k-1)^T, \cdots, u(k-\bar{d})^T\right]^T$, in the state-space form in order to describe the state $x(k)$ by considering the previous states and control input signals as follows:

$$\xi(k+1) = \tilde{A}(\boldsymbol{t}^k)\xi(k) + \tilde{B}(\boldsymbol{t}^k)u(k), \tag{9}$$

where

$$\tilde{A}(\boldsymbol{t}^k) = \begin{bmatrix} A_d & \tilde{M}_{\bar{d}-1} & \tilde{M}_{\bar{d}-2} & \cdots & \tilde{M}_0 \\ 0 & 0 & 0 & \cdots & 0 \\ 0 & I & 0 & \cdots & 0 \\ \vdots & & \ddots & & \cdots \\ 0 & 0 & 0 & I & 0 \end{bmatrix},$$

$$\tilde{B}(\boldsymbol{t}^k) = \begin{bmatrix} \tilde{M}_{\bar{d}}^T & I & 0 & \cdots & 0 \end{bmatrix}^T, \boldsymbol{t}^k = \begin{bmatrix} t_1^k, \cdots, & t_{\tilde{d}}^k, \end{bmatrix}$$

$$\tilde{M}_j = \begin{cases} \int_{t_s - t_{j+1}^k}^{t_s - t_j^k}, e^{As} ds B & \text{if } 0 < j < \bar{d} - \underline{d} \\ 0, & \text{otherwise.} \end{cases}$$

To analyze the feasible stability region for the time-varying network delay τ_{net} in the NCS, we introduce linear combinations of matrices in the Jordan form into the discrete-time NCS model (9). The system matrix A of the physical system (1) is described in the Jordan form $A = QJQ^{-1}$, where $J = diag(J_1, \cdots, J_p)$ is the real Jordan form with p distinct real eigenvalues or pairs of complex eigenvalues, and Q is a matrix generated by eigenvectors. Each Jordan block, $J_{\tilde{i}}$, has real Jordan blocks $J_{\tilde{i},\tilde{j}}$, where $j = 1, \cdots, g_{\tilde{i}}$ with the geometric multiplicity $g_{\tilde{i}}$.

From the Jordan form, we rewrite the discrete-time NCS model (9) into linear combinations of matrices as follows:

$$\begin{aligned} \xi(k+1) = & \left(F_0 + \sum_{i=1}^{\nu} \sum_{j=1}^{\bar{d}-\underline{d}} \alpha_i(t_j^k) F_{i,j} \right) \xi(k) \\ & + \left(G_0 + \sum_{i=1}^{\nu} \sum_{j=1}^{\bar{d}-\underline{d}} \alpha_i(t_j^k) G_{i,j} \right) u(k), \end{aligned} \tag{10}$$

where F_0, G_0, $F_{i,j}$, $G_{i,j}$, $i = 1, \cdots, \nu$, and $j = 1, \cdots, \bar{d} - \underline{d}$ are constant matrices, and $\alpha_i(t_j^k)$ is a time-varying function that depends on eigenvalues ofthe matrix A for the physical system (1). The parameter ν is defined as $\nu = \sum_{\tilde{i}=1}^{p} max_{\{j=1,\cdots,g_{\tilde{i}}\}}(dim\, J_{\tilde{i},\tilde{j}})$. More details on the linear matrix combination representation (10) and the time-varying function $\alpha_i(t_j^k)$ are described in [23].

Because the time varying network delay τ_{net} has an infinite number of cases in the range of $[\tau_{min}, \tau_{max}]$, the linear combination form of the NCS model (10) has an infinite number of conditions for the time-varying function $\alpha_i(t_j^k)$, which makes it formidable to check the feasibility of the delay bound in real time. To solve the feasible stability region problem in a finite time, we formulate the linear combination terms for F_i and G_i in the NCS model (10) as a convex set as follows:

$$\begin{aligned} \mathcal{H}_{FG} = \Bigg\{ & \left(F_0 + \sum_{i=1}^{\nu} \sum_{j=1}^{\bar{d}-\underline{d}} \alpha_{i,j} F_{i,j}, G_0 + \sum_{i=1}^{\nu} \sum_{j=1}^{\bar{d}-\underline{d}} \alpha_{i,j} G_{i,j} \right) : \\ & \alpha_{i,j} \in \left\{ \underline{\alpha}_{i,j}, \bar{\alpha}_{i,j} \right\}, i = 1, \cdots, \nu, j = 1, \cdots, \bar{d} - \underline{d} \Bigg\}, \end{aligned} \tag{11}$$

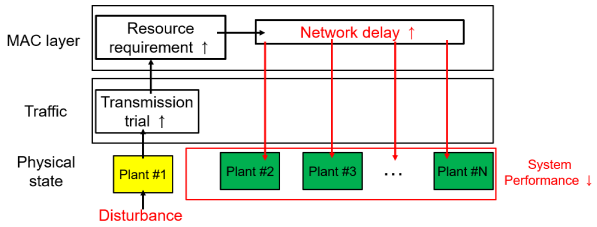


Fig. 2. Structure of a wireless networked control system with multiple physical systems.

where $\bar{\alpha}_{i,j} := max_{t_j^k \in [t_{min}^k, t_{max}^k]} \alpha_i(t_j^k)$ and $\underline{\alpha}_{i,j} := min_{t_j^k \in [t_{min}^k, t_{max}^k]} \alpha_i(t_j^k)$, with time instants

$$t_{j,min} = \begin{cases} \tau_{min} - \underline{d} t_s & \text{if } j = \bar{d} - \underline{d} \\ 0, & \text{if } 1 \le j < \bar{d} - \underline{d}, \end{cases}$$

$$t_{j,max} = \begin{cases} t_s, & \text{if } 1 < j \le \bar{d} - \underline{d} \\ \tau_{max} - \underline{d} t_s & \text{if } j = 1. \end{cases}$$

Here, set $H_F := \left\{ F_0 + \sum_{i=1}^{\nu} \sum_{j=1}^{\bar{d}-\underline{d}} \alpha_{i,j} F_{i,j} \right\}$ and $H_G := \left\{ G_0 + \sum_{i=1}^{\nu} \sum_{j=1}^{\bar{d}-\underline{d}} \alpha_{i,j} G_{i,j} \right\}$ have $2^{\nu(\bar{d}-\underline{d})}$ matrices.

From [23], it is known that the stability of the NCS can be verified by finding a positive definite matrix P that satisfies the following bilinear matrix inequalities (BMIs):

$$\begin{pmatrix} P & (H_F - H_G \bar{K})^T P \\ P(H_F - H_G \bar{K}) & P \end{pmatrix} > 0, \tag{12}$$

where $\bar{K} := \begin{bmatrix} K\, 0_{1,\bar{d}} \end{bmatrix}$. If such a matrix P exists, the NCS in (8) is globally asymptotically stable under any network delay within $\tau_{net} \in [\tau_{min}, \tau_{max}]$. In most practical CPS applications, the feedback gain K is designed off-line and then regarded as a fixed constant; under this setting, (12) becomes a standard linear matrix inequality (LMI) in the single variable P, which can be solved efficiently with guaranteed global optimality.

4.2. Network Saturation due to Disturbances

External disturbances perturb the plant state $x(t)$, forcing ETC to fire more often (Fig. 2). These extra packets saturate the limited bandwidth, elongating delay-a disturbance-induced DoS (DIDoS). The ensuing latency degrades control quality and can ultimately destabilise every plant on the network.

From the triggering function (3), we formulate the DIDoS attack as a co-existence problem between periodic control systems and ETC systems. First, we only consider a physical system suffering from disturbances in the worst packet-generation case. If a physical system undergoes proper disturbances that trigger the logic $V(Ax(k) + Bu(\tau_i)) > \beta V(x(\tau_i))$, then the compromised physical system generates the physical state packets in every trans-

mission period t_s. Therefore, in the worst case, the compromised physical system can be regarded as a periodic control system with the period of t_s.

We consider an NCS with a feedback controller and N physical systems, where each physical system establishes a wireless connection to the controller as illustrated in Fig. 3. We assume that each communication node including physical systems and the feedback controller generates packets with an independent and identical probability distribution. In an attack-free environment, the physical system activates the triggering function at a rate of R_{ev}, which is calculated as follows:

$$R_{ev} = \lim_{k\to\infty} \frac{n_{ev}}{k}, \tag{13}$$

where k is the time step in the discrete time domain, and n_{ev} the activation number of the event-triggering function. We assume that the triggering rate R_{ev} is a constant value within the range of $(0,1]$. Therefore, the uncompromised physical systems have the transmission rate of $\lambda_u = R_{ev}/t_s$. Meanwhile, a compromised physical system transmits the state $x(t)$ in every transmission period t_s due to the violation of the triggering logic (3). Consequently, the compromised physical system has a transmission rate of $\lambda_c = 1/t_s$.

The controller sends only the control input $u(k)$ derived from the latest plant states; packet loss and processing delay are ignored. Hence its packet rate equals the aggregate plant rate,

$$\lambda_{con} = \frac{N_c + (N - N_c)R_{ev}}{t_s}, \tag{14}$$

where N_c is the number of compromised plants.

A DIDoS attack forces each compromised node to transmit every cycle, so both their rates and λ_{con} rise with N_c. Network behaviour is obtained by jointly solving the $2(N+1)$ nonlinear equations for collision probability p_i and utilisation ρ_i. If the controller's utilisation ρ_{con} exceeds a critical threshold, delay violates the stability bound (12), causing every plant state to diverge.

To design the DIDoS attack, the attacker maximizes the event generation rate R_{ev} of physical systems from the given event-triggering policy (3) by injecting disturbances $w(k)$. DIDoS does not require identification of the plant dynamics or precise model parameters: it is sufficient that the target employs an ETC rule of the form (3) and that the attacker can inject a bounded, persistent disturbance.

In deriving the closed-form optimizations and worst-case bounds that follow, we assume that the attacker already knows the physical system model (2), event-triggering policies (3), and network parameters (7). Well-generated disturbances $w(k)$ violate the event-triggering condition $V(Ax(k)+Bu(\eta_i)) > \beta V(x(\eta_i))$ (3) of N_c compromised physical systems in every time step k, which increases the network utilization ρ_{con} (14).

Unlike conventional network delay attack that overwhelm a link with external traffic [24], a DIDoS attack originates from the plant nodes themselves, so a firewall cannot simply drop the packets without disrupting control. Because these packets are integral to feedback, they must still traverse the network to keep compromised plants stable. Widening channel bandwidth could help, but practical limits in 802.11 slot size and standard-defined data rates restrict how much capacity can be added.

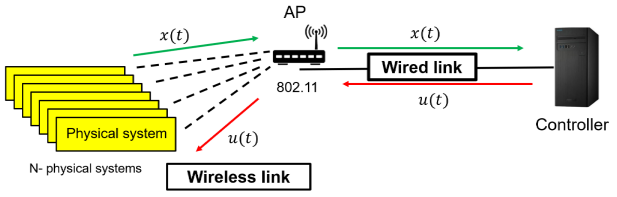


Fig. 3. The structure of the simulated wireless networked control system with multiple physical systems.

5. NUMERICAL STUDY

In this section, we show our simulation results on the impact of the proposed DIDoS attack.

5.1. Simulation Setup

In the simulation, we implement an NCS environment in NS-3 [32]. We consider an IEEE 802.11 wireless network connecting the computing system and multiple physical systems.

5.1.1 Network parameters

Figure 3 shows the simulated WLAN: an IEEE 802.11g (ERP-OFDM, 54 Mb/s) access point linked to 30 wireless plants and a controller that sits behind a high-capacity wired back-haul. Each plant sends its state every $t_s = 20$ ms in a 500-byte UDP packet; the controller immediately returns the full-state feedback input $u(k)$. The MAC uses the default slot time (20 µs) and contention-window limits ($CW_{\min} = 16$, $CW_{\max} = 1024$). All experiments run for 1000 s of simulated time. This idealized configuration intentionally excludes background traffic, channel fading, and node mobility so that the causal link between the injected disturbance, network saturation, and state divergence can be examined in isolation.

5.1.2 Physical system model

For the physical systems, we consider the well-known inverted pendulum control system, which is an inverted pendulum mounted to a cart. The goal of the control in this system is to balance the inverted pendulum by applying force to the cart.

Here, we use a second-order LTI model for the inverted

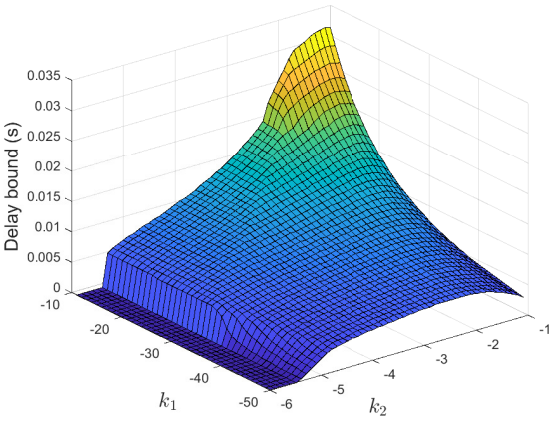


Fig. 4. The maximum allowable delay bound of an inverted pendulum with respect to the controller gain.

pendulum [33] as follows:

$$\dot{\mathbf{x}}(t) = \begin{bmatrix} 0 & 1 \\ \frac{(m+M)g}{Ml} & 0 \end{bmatrix} \mathbf{x}(t) + \begin{bmatrix} 0 \\ \frac{-1}{Ml} \end{bmatrix} (F(t) + w(t)), \quad (15)$$

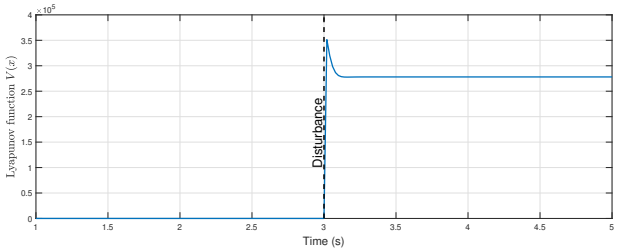
where $\mathbf{x}(\mathbf{t}) = \begin{bmatrix} \phi(t) & \dot{\phi}(t) \end{bmatrix}^T$ is the state vector of the inverted pendulum with $\phi(t)$ being the angle of the pendulum, $F(t)$ is the force applied to the cart, $\dot{\phi}(t)$ is the angle speed of the pendulum, m is the mass of the ball, M is the mass of the cart, l is the pendulum's length, and g is gravitational acceleration. In our simulation, we consider full-state feedback control, and the physical systems can measure and transmit the state $x(k)$ when the event-triggering function is activated.

We analyze the feasible stability region of the inverted pendulum model (15) with stability analysis (12) as illustrated in Fig. 4. We can verify in Fig. 4 that the maximum allowable delay bound depends on the controller gain K. We select the controller gain $K = [k_1\ k_2]$ so that the maximum allowable delay bound is 15 ms. If a certain physical system has a network delay greater than 15 ms, then the corresponding physical system becomes unstable.

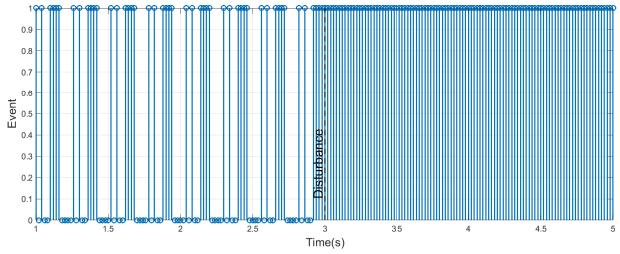
We measure the triggering rate of the inverted pendulum control system, $R_{ev} = 0.8$, with the ETC strategy by implementing an attack-free simulation. The transmission rates for the physical system λ_u and the compromised physical system λ_c are 0.04 and 0.05, respectively.

5.2. Simulation Results

In this section, we show the impact of the DIDoS attack, which degrades the control performance and destabilizes the physical systems. Our simulation result shows that the increased network delay by the DIDoS attack can affect the physical systems that is not directly attacked by DIDoS.



(a)



(b)

Fig. 5. Effect of constant disturbance in the viewpoint of event generation. (a) Lyapunov function. (b) Event generation in each time step.

5.2.1 Event-generation rate by constant disturbance

In this simulation, we assume that the attacker launches the wind gust to the inverted pendulum system (15), which applies a constant force to N_c compromised physical systems. Furthermore, we do not consider the energy constraint for the disturbance $w(k)$ of the attacker. Therefore, we can model the wind gust disturbance $w(k)$ on the inverted pendulum (15) as a constant value. A disturbance of sufficient magnitude keeps the Lyapunov function $V(x)$ from converging to zero and instead forces it to settle at a positive value, thereby violating the ETC condition (3) at every sampling instant.

Fig. 5 shows the numerical simulation results for constant disturbance on the ETC inverted pendulum system (15) in delay-free environment. Fig. 5(a) shows the Lyapunov function value of the ETC system (15) under constant disturbance. From the β parameter constraint in (3), the Lyapunov Function value $V(x)$ of the physical system must asymptotically converge to zero. However, due to the constant disturbance $w(k)$, the the Lyapunov Function value $V(x)$ converges to a certain positive, which always violates the event-triggering condition $V(Ax(k) + Bu(\eta_i)) > \beta V(x(\eta_i))$ in (3). As a result of the constant disturbance $w(k)$, the physical system generates events in every time step k as illustrated in Fig. 5(b). The additional events by the constant disturbance k increases the computing system-side network utilization ρ_{con}, which induces control performance degradation or destabilization.

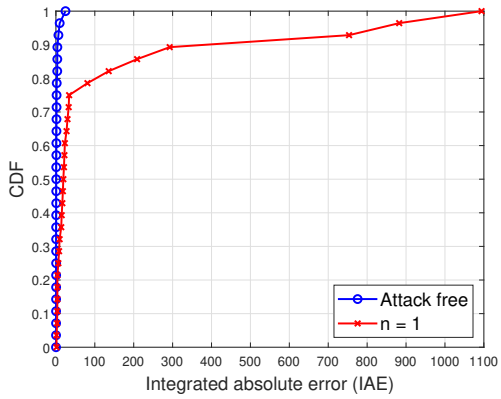


Fig. 6. Control performance degradation by the DIDoS attack.

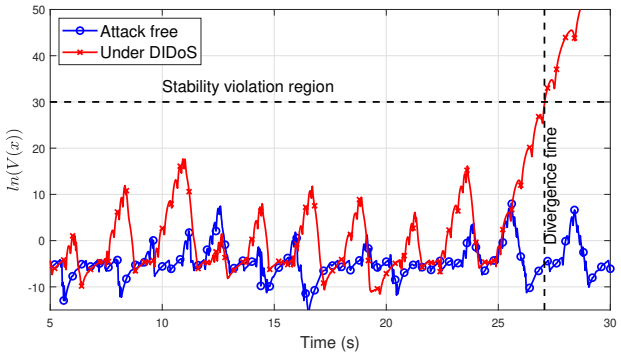


Fig. 7. The Lyapunov function and the divergence time of the inverted pendulum under the DIDoS attack.

5.2.2 Control performance degradation under DIDoS

If the attack-induced network delay does not exceed the maximum allowable delay bound, the stability of the physical systems is guaranteed. However, the increased network delay can deteriorate the control performance of the physical systems. In this simulation, we show the control performance degradation by the DIDoS attack when the attack-induced network delay does not exceed the stability condition of the physical systems.

The control performance is evaluated with the integrate absolute error (IAE), which is the integral of the absolute value of the error between the sensor measurement $y(t)$ and the position reference $y_r(t)$. A large value of the IAE indicates worse control performance. The IAE is calculated as follows:

$$IAE = \int_{t_a}^{t_f} |y(t) - y_r(t)|\, dt, \tag{16}$$

where t_a is the attack start time, and t_f is the end time of the simulation.

Fig. 6 illustrates the simulation results of the DIDoS attack when only one physical system is compromised. All physical systems on the network maintain stability because the attack-induced delay does not exceed the maximum allowable delay bound. However, the increased delay degrades the control performance of certain physical systems. When a physical system suffers from the DIDoS attack, packets generated by other physical systems experience longer network delays than an attack-free environment, which degrades the control performance as shown in Fig. 6. However, since the increased network delay is within the feasible range for stability, the physical systems remain stable.

5.2.3 Physical system disruption by the DIDoS attack

As more physical systems suffer from the DIDoS attack, network traffic increases because the increased number of the compromised physical systems generate more physical state packets, resulting in more consumption of the network bandwidth. In this simulation, we show that the DIDoS attack destabilizes physical systems. Furthermore, we show the relationship between the number of the compromised physical systems and the destabilization speed of the other physical systems.

To evaluate the speed of destabilization in the physical systems, we denote the divergence time as the last time that quadratic Lyapunov function $V(x)$ has a value under a certain threshold. Lyapunov function $V(x)$ represents the magnitude of the state $x(t)$. The divergence time is calculated as follows:

$$t_{div} = max\{t > t_a | ln(V(x(t))) < \varepsilon\}, \tag{17}$$

where ε is the stability violation threshold of the log scale Lyapunov function $ln(V(x))$. The threshold is selected as $\varepsilon = 30$.

Fig. 7 shows the log scale Lyapunov function $V(x)$ of a physical system in an attack-free situation and under the DIDoS attack. In the attack-free environment, the log scale Lyapunov function $ln(V(x))$ of the physical systems show bounded values without divergence. When the DIDoS attack is applied to physical systems, the log scale Lyapunov function $ln(V(x))$ diverges to infinity, and does not have a value less than the stability violation threshold ε.

We evaluate the DIDoS attack with the minimum divergence time (17) for the physical systems in the network. Fig. 8 shows the minimum divergence time with respect to the number of compromised physical systems. When a single physical system is under the DIDoS attack, there is no t_{div} because the states for all the physical systems do not diverge. Therefore, we show the minimum divergence time of the physical systems when the number of compromised physical systems, N_c is greater than two.

As the number of compromised physical systems increases, the minimum divergence time is drastically decreased with respect to the number of compromised phys-

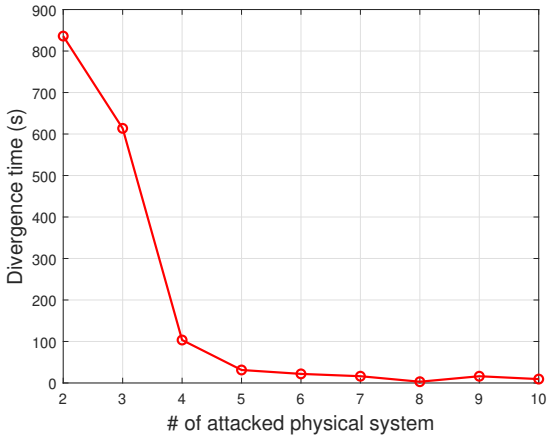


Fig. 8. Physical system divergence time.

ical systems as illustrated in Fig. 8. As the number of compromised physical systems increases, more packets are generated, which results in the increased network delay. Specifically, the increased network utilization ρ_i by the disturbances increases the network delay until it violates the stability condition (12). Therefore, the destabilization time of the uncompromised physical systems is accelerated by increasing the number of compromised physical systems. This pronounced reduction in t_{div} underscores the scalability of DIDoS: each additional compromised node amplifies network congestion and hastens divergence, causing the overall impact of the attack to grow super-linearly with N_c.

6. CONCLUSION

This paper introduces a new attack vector for ETC based CPSs: DIDoS attack. By injecting a disturbance of sufficient magnitude, the attacker forces compromised plants to generate state packets far more frequently, saturating the network, increasing delay, and ultimately destabilizing not only the disturbed plants but every plant that shares the network link. To characterize DIDoS, we derived a delay-dependent stability condition for CPS under time-varying network latency and modeled network saturation caused by DIDoS in an ETC system that operates over an IEEE 802.11 wireless link. Simulation results confirm that DIDoS severely degrades control performance and drives the physical plants to instability.

DIDoS shows that ETC-introduced precisely to save bandwidth-can paradoxically create a flood of feedback traffic and become an attack surface. Because the extra packets are indispensable for feedback, conventional firewalls cannot simply drop them, distinguishing DIDoS from traditional network-layer attacks. Future research should first address the detection of DIDoS. A practical approach is to analyze each node's inter-event time series in real time and flag trajectories whose empirical distributions deviate from the nominal ETC baseline. A second line of work concerns mitigation and adversarial refinement. Once a persistent disturbance is detected, the controller could raise the triggering ETC threshold, switch to a hybrid periodic/ETC schedule that caps per-node transmissions, or enforce a token-bucket rule at the MAC layer to reserve bandwidth. It demands tight network-control co-design. Conversely, investigating stealthier DIDoS variants, such as low-rate on-off disturbances that mimic process noise, will clarify the limits of these defenses and guide the development of more robust CPS deployments.

DECLARATIONS

Conflict of Interest

The authors declare that there is no competing financial interest or personal relationship that could have appeared to influence the work reported in this paper.

Authors' Contributions

Sangjun Kim conceived the research idea, designed the methodology and experimental procedures, conducted the experiments, collected the data, and prepared the initial manuscript draft. Sanghoon Lee carried out the statistical and numerical analyses. Kyung-Joon Park provided overall supervision of the research. All authors have read and approved the final manuscript.

Funding

This work was supported by the Institute of Information and Communications Technology Planning and Evaluation (IITP) Grant funded by Korean Government [Ministry of Science and ICT (MSIT)] under Grant RS-2024-00442085.

REFERENCES

[1] K.-J. Park, R. Zheng, and X. Liu. Cyber-physical systems: Milestones and research challenges. *Computer Communications*, 36(1):1–7, 2012.

[2] K.-J. Park, J. Kim, H. Lim, and Y. Eun. Robust path diversity for network quality of service in cyber-physical systems. *IEEE Transactions on Industrial Informatics*, 10(4):2204–2215, 2014.

[3] Derui Ding, Qing-Long Han, Zidong Wang, and Xiaohua Ge. Recursive filtering of distributed cyber-physical systems with attack detection. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 51(10):6466–6476, 2021.

[4] Yuchang Won, Buyeon Yu, Jaegeun Park, In-Hee Park, Haegeon Jeong, Jeanseong Baik, Kyungtae Kang, Insup Lee, Sang Hyuk Son, Kyung-Joon Park, and Yongsoon Eun. An attack-resilient CPS architecture for hierarchical control: A case study on train control systems. *Computer*, 51(11):46–55, 2018.

[5] Zhou Gu, Ju H. Park, Dong Yue, Zheng-Guang Wu, and Xiangpeng Xie. Event-triggered security output feedback control for networked interconnected systems subject to cyber-attacks. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 51(10):6197–6206, 2021.

[6] Sangjun Kim, Yongsoon Eun, and Kyung-Joon Park. Stealthy sensor attack detection and real-time performance recovery for resilient CPS. *IEEE Transactions on Industrial Informatics*, 17(11):7412–7422, 2021.

[7] Gyujin Na and Yongsoon Eun. A probing signal-based replay attack detection method avoiding control performance degradation. *International Journal of Control, Automation and Systems*, 20(11):3637–3649, 2022.

[8] Lisai Gao, Jingqi Fu, and Fuqiang Li. Output-based security control of ncss under resilient event-triggered mechanism and dos attacks. *International Journal of Control, Automation and Systems*, 19(4):1519–1527, 2021.

[9] Longyu Xu, Yong Chen, and Meng Li. Sliding mode resilient control for tod-based servo system under dos attack. *International Journal of Control, Automation and Systems*, 20(2):526–535, 2022.

[10] Bo-Chao Zheng, Lina Guo, Xiaoguang Liu, Zhou Gu, and Yangyang Zhao. Robust security control under denial-of-service jamming attacks: An event-triggered sliding-mode control approach. *International Journal of Control, Automation and Systems*, 20(12):3892–3902, 2022.

[11] Ahmet Cetinkaya, Hideaki Ishii, and Tomohisa Hayakawa. An overview on denial-of-service attacks in control systems: Attack models and security analyses. *Entropy*, 21(2):210, 2019.

[12] Bing Li, Zidong Wang, and Qing-Long Han. Input-to-state stabilization of delayed differential systems with exogenous disturbances: The event-triggered case. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, 49(6):1099–1109, 2019.

[13] Ahmet Cetinkaya, Hideaki Ishii, and Tomohisa Hayakawa. Event-triggered control over unreliable networks subject to jamming attacks. In *Proceedings of the 54th IEEE Conference on Decision and Control (CDC)*, pages 4818–4823, 2015.

[14] Dan Liu and Guang-Hong Yang. Dynamic event-triggered control for linear time-invariant systems with l2-gain performance. *International Journal of Robust and Nonlinear Control*, 29(2):507–518, 2019.

[15] André Teixeira, Daniel Pérez, Henrik Sandberg, and Karl Henrik Johansson. Attack models and scenarios for networked control systems. In *Proceedings of the 1st international conference on High Confidence Networked Systems*, pages 55–64, 2012.

[16] Jairo Giraldo, David Urbina, Alvaro Cardenas, Junia Valente, Mustafa Faisal, Justin Ruths, Nils Ole Tippenhauer, Henrik Sandberg, and Richard Candell. A survey of physics-based attack detection in cyber-physical systems. *ACM Computing Surveys (CSUR)*, 51(4):1–36, 2018.

[17] Sangjun Kim and Kyung-Joon Park. A survey on machine-learning based security design for cyber-physical systems. *Applied Sciences*, 11(12):5458, 2021.

[18] Ahmet Cetinkaya, Hideaki Ishii, and Tomohisa Hayakawa. Analysis of stochastic switched systems with application to networked control under jamming attacks. *IEEE Transactions on Automatic Control*, 64(5):2013–2028, 2019.

[19] Thi Ngoc Diep Pham, Chai Kiat Yeo, Naoto Yanai, and Toru Fujiwara. Detecting flooding attack and accommodating burst traffic in delay-tolerant networks. *IEEE Transactions on Vehicular Technology*, 67(1):795–808, 2018.

[20] Heng Zhang, Peng Cheng, Ling Shi, and Jiming Chen. Optimal DoS attack scheduling in wireless networked control system. *IEEE Transactions on Control Systems Technology*, 24(3):843–852, 2015.

[21] Subhash Lakshminarayana, Jabir Shabbir Karachiwala, Sang-Yoon Chang, Girish Revadigar, Sristi Lakshmi Sravana Kumar, David KY Yau, and Yih-Chun Hu. Signal jamming attacks against communication-based train control: Attack impact and countermeasure. In *Proceedings of the 11th ACM Conference on Security & Privacy in Wireless and Mobile Networks*, pages 160–171, 2018.

[22] Wei Zhang, Michael S Branicky, and Stephen M Phillips. Stability of networked control systems. *IEEE Control Systems Magazine*, 21(1):84–99, 2001.

[23] Marieke B. G. Cloosterman, Nathan van de Wouw, W. P. M. H. Heemels, and Hendrik Nijmeijer. Stability of networked control systems with uncertain time-varying delays. *IEEE Transactions on Automatic Control*, 54(7):1575–1580, 2009.

[24] Young-Min Kwon, Jaemin Yu, Byeong-Moon Cho, Yongsoon Eun, and Kyung-Joon Park. Empirical analysis of MAVLink protocol vulnerability for attacking unmanned aerial vehicles. *IEEE Access*, 6:43203–43212, 2018.

[25] Ahmet Cetinkaya, Hideaki Ishii, and Tomohisa Hayakawa. Networked control under random and malicious packet losses. *IEEE Transactions on Automatic Control*, 62(5):2434–2449, 2017.

[26] Dohwan Kim, Yuchang Won, Seunghyeon Kim, Yongsoon Eun, Kyung-Joon Park, and Karl H Johansson. Sampling rate optimization for IEEE 802.11 wireless control systems. In *Proceedings of the 10th ACM/IEEE International Conference on Cyber-Physical Systems*, pages 87–96, 2019.

[27] Gao Shang, Peng Zhe, Xiao Bin, Hu Aiqun, and Ren Kui. FloodDefender: Protecting data and control plane resources under SDN-aimed DoS attacks. In *Proceedings of the IEEE INFOCOM 2017-IEEE Conference on Computer Communications*, pages 1–9, 2017.

[28] Sangjun Kim, Kyung-Joon Park, and Chenyang Lu. A survey on network security for cyber-physical systems: From threats to resilient design. *IEEE Communications Surveys & Tutorials*, 24(3):1534–1573, 2022.

[29] Sangjun Kim, Sanghoon Lee, and Kyung-Joon Park. Real-time controller reconfiguration for delay-resilient cyber-physical systems. *IEEE Access*, 10:101220–101228, 2022.

[30] Chi-Tsong Chen. *Linear System Theory and Design*. Oxford University Press, Inc., USA, 3rd edition, 1998.

[31] Omesh Tickoo and Biplab Sikdar. Modeling queueing and channel access delay in unsaturated IEEE 802.11 random access MAC based wireless networks. *IEEE/ACM Transactions on Networking*, 16(4):878–891, 2008.

[32] George F Riley and Thomas R Henderson. The ns-3 network simulator. In *Modeling and tools for network simulation*, pages 15–34. Springer, 2010.

[33] Wei Wu, Sven Reimann, Daniel Görges, and Steven Liu. Event-triggered control for discrete-time linear systems subject to bounded disturbance. *International Journal of robust and nonlinear control*, 26(9):1902–1918, 2016.

Sangjun Kim received the B.S. (2017) in Electronics Engineering from Pukyong National Univ. and the Ph.D. (2022) in EECS from DGIST, Korea. He served as a researcher on guided-weapon systems at KRIT (2022-2023) and is now Associate Research Fellow at KISTEP's Center for R&D Investment Planning. His interests include R&D budgeting and investment strategy.

Sanghoon Lee received the B.S. (2022) in the School of Undergraduate Studies at DGIST, Korea, in 2022. He is currently a Ph.D. candidate in the Department of Electrical Engineering and Computer Science at DGIST. His research interests include cyber-physical systems, Cyber-Physical AI, and their implementation with ROS 2

Kyung-Joon Park (Senior Member, IEEE) received the B.S. (1998) and M.S. (2000) degrees in electrical engineering and the Ph.D. degree (2005) in electrical engineering and computer science from Seoul National University, Seoul, South Korea. From 2005 to 2006, he was a Senior Engineer with Samsung Electronics, Suwon, South Korea. From 2006 to 2010, he was a Postdoctoral Research Associate with the Department of Computer Science, University of Illinois at Urbana-Champaign (UIUC), IL, USA. He is currently a Professor with the Department of Electrical Engineering and Computer Science, Daegu Gyeongbuk Institute of Science and Technology (DGIST), Daegu, South Korea. His research interests include cyber-physical systems, robot operating systems, and smart manufacturing.