entropy

Review

An Overview on Denial-of-Service Attacks in Control Systems: Attack Models and Security Analyses

Ahmet Cetinkaya [1,*], Hideaki Ishii [1] and Tomohisa Hayakawa [2]

[1] Department of Computer Science, Tokyo Institute of Technology, Yokohama 226-8502, Japan; ishii@c.titech.ac.jp

[2] Department of Systems and Control Engineering, Tokyo Institute of Technology, Tokyo 152-8552, Japan; hayakawa@sc.e.titech.ac.jp

[*] Correspondence: ahmet@sc.dis.titech.ac.jp; Tel.: +81-45-924-5216

Received: 29 January 2019; Accepted: 19 February 2019; Published: 22 February 2019

Abstract: In this paper, we provide an overview of recent research efforts on networked control systems under denial-of-service attacks. Our goal is to discuss the utility of different attack modeling and analysis techniques proposed in the literature for addressing feedback control, state estimation, and multi-agent consensus problems in the face of jamming attacks in wireless channels and malicious packet drops in multi-hop networks. We discuss several modeling approaches that are employed for capturing the uncertainty in denial-of-service attack strategies. We give an outlook on deterministic constraint-based modeling ideas, game-theoretic and optimization-based techniques and probabilistic modeling approaches. A special emphasis is placed on tail-probability based failure models, which have been recently used for describing jamming attacks that affect signal to interference-plus-noise ratios of wireless channels as well as transmission failures on multi-hop networks due to packet-dropping attacks and non-malicious issues. We explain the use of attack models in the security analysis of networked systems. In addition to the modeling and analysis problems, a discussion is provided also on the recent developments concerning the design of attack-resilient control and communication protocols.

Keywords: networked control; cyber-security; denial-of-service; jamming attacks; probabilistic failure models; stability analysis; resilient control systems; multi-agent systems

1. Introduction

Many industrial control systems rely on information and communication technologies for their operation. In particular, wireless networks and the Internet are becoming key components of control systems, since they can be utilized in the transmission of measurement and control data to remote locations. As the Internet of Things is becoming more popular, the use of wireless technologies in control systems is expected to increase even more. These new developments are bringing efficiency to control systems, but they are also expected to introduce several vulnerabilities. A major concern is that cyber-attackers may be able to exploit the vulnerabilities in control systems that are utilized in power grids, transportation, water distribution, and many other services that are important for the society. To prevent financial losses and environmental damages that may be caused by disruption of those services, it is critical to assess and improve the security of existing control systems and develop new systems that are resilient against cyber attacks.

Various cyber-security issues of networked control systems and detection/mitigation approaches for those issues have been discussed in [1–8]. As pointed out in those works, attackers targeting vulnerable networked control systems may be able to change the contents of measurement and control packets. There may even be cases where attackers can inject false data into the system without being detected. These attacks require the attacker to be knowledgeable on the communication protocol as well as the system dynamics. On the other hand, attackers who have limited information on the control system may resort to denial-of-service (DoS) attacks that prevent delivery of control and measurement data packets. Networked control system under DoS attacks can face severe performance issues.

Our goal in this paper is to provide an overview of attack-modeling and security analysis approaches in recent works that explore networked control systems subject to DoS attacks. To this end, we look at the control, estimation, and consensus problems and discuss different DoS attack models utilized by researchers for addressing those problems. DoS attacks can take different forms in different network settings. In this paper, we focus on packet drop attacks by malicious nodes in multi-hop networks, and jamming attacks in wireless channels.

In multi-hop networks such as wireless ad hoc networks, remotely located nodes can transmit data packets to each other with the help of intermediate nodes that act as routers. It is typically assumed that all nodes obey the routing protocols in the network; however, in reality, a network can face packet drops by malicious nodes [9,10]. For instance, in *blackhole* DoS attacks, a malicious node first falsely introduces itself to other nodes as if it is part of the shortest path to a set of remote nodes. Then, many unsuspecting nodes in the network attempt to send all packets addressed to those remote nodes through the malicious node, which in fact drops all packets instead of forwarding them. Furthermore, in *grayhole* attacks, malicious nodes act normal and follow the standard routing protocols for certain periods of time to avoid being detected. The authors in [9–13] discussed both malicious and non-malicious packet dropping issues in ad hoc networks and presented several attack detection and mitigation approaches.

In addition to packet-dropping attacks, networked controls systems may also suffer from DoS attacks in the form of jamming of wireless transmissions. Specifically, a jamming attacker can prevent transmission of packets by emitting strong interference signals to a wireless channel [14,15]. It is mentioned in [15] that jamming devices can target various wireless technologies including GPS, mobile communications, and Wi-Fi. Jamming attacks can become a major concern for control systems, since they are easy to launch. The work in [16] illustrates that off-the-shelf hardware with wireless capabilities can be used for generating jamming attacks on wireless networks that use the popular IEEE 802.11 protocol. Jamming attacks can target both the physical layer and the medium access control (MAC) layer of the protocol. In the case of physical-layer attacks, the jamming attacker is not even required to follow the wireless protocol. By simply emitting strong interference signals, the jamming attacker can cause a decrease in the Signal to Interference plus Noise Ratio (SINR), which in turn prevents the receiver to detect transmitted packets [16]. In the case of MAC-layer attacks, both the packet sender and the jamming attacker operate on the same channel; the jamming attacker's goal is to cause packet collisions [16]. Under jamming attacks, packets transmitted to the receiver may get corrupted and fail cyclic redundancy checks (CRC) used in the protocol. Note that, in wireless networks, jamming attacks and packet-dropping attacks by malicious nodes can also coexist.

Recently, DoS attacks have been investigated in the context of feedback control, state estimation, and multi-agent consensus problems. To tackle these problems, researchers have proposed several approaches for characterizing the occurrences of attacks. In particular, some of the works in the literature present models that take into account the energy constraints that an attacker may have. In another line of research, optimal attack strategies are investigated through game-theoretic frameworks and worst-case attack scenarios are studied. In this paper, we give an overview of both lines of research. In addition, we also discuss probabilistic modeling approaches that attempt to capture the effects of both malicious DoS attacks and non-malicious reasons of transmission failures. Such approaches are needed, as attacks may not be the only source of transmission failures in networks. Typically, networks may face non-malicious link errors, channel noise, and congestions caused by genuine network users [17,18]. In this paper, we discuss the utility of different modeling approaches in analyzing system security in control, estimation, and consensus problems. Furthermore, we present recent developments in the design of attack-resilient control and communication protocols.

We note that there are several review articles that discuss various aspects of denial-of-service attacks from the viewpoint of information technologies. In particular, denial-of-service attacks in sensor networks are investigated in [19]. A discussion of defense mechanisms against denial-of-service attacks is provided in [20]. Distributed denial-of-service attacks and potential approaches of mitigating their effects are explored in [21,22]. Additionally, an overview of a set of control-theoretical methods as well as techniques from information technologies to mitigate jamming attacks is presented in [23], and, furthermore, a survey of articles concerned with DoS and false data injection attacks in control systems for the smart grid is provided in [24]. Differently from previous works, we present an overview of DoS attacks in networked control systems with a special emphasis on probabilistic modeling and analysis approaches.

We organize the rest of our paper into five sections. In Section 2, we introduce control problems subject to DoS attacks and provide an overview of the literature that explore those problems. In Section 3, we discuss several deterministic, game-theoretical and optimization-based attack-modeling approaches. Moreover, in Section 4, we discuss recent developments in probabilistic approaches to modeling of networks that face denial-of-service attacks and also non-malicious issues. We then present a set of recently developed attack-resilient control and communication techniques in Section 5. Finally, we conclude the paper in Section 6.

We use fairly standard notation in the paper. Specifically, nonnegative and positive integers are, respectively, denoted by $\mathbb{N}_0$ and $\mathbb{N}$. Furthermore, the notation $\mathbb{P}[\cdot]$ represents the probability on a probability space $(\Omega, \mathcal{F}, \mathbb{P})$, and, moreover, $\mathbb{E}[\cdot]$ represents the expectation. We use the notations $\vee$ and $\wedge$ to, respectively, denote the "or" and "and" operations on binary numbers. Moreover, we denote the Lebesgue measure of a set $S \subset \mathbb{R}$ by $|S|$.

2. An Overview of Literature on Denial-of-Service in Control Systems

In this section, we present an overview of the recent literature that investigates DoS attacks in: (1) networked control; (2) state estimation, and (3) multi-agent consensus problems. We provide a general outlook on the problem settings and discuss a range of subproblems. These problem settings provide a basis for the more detailed discussions on attack models and security analysis techniques presented in Sections 3 and 4.

2.1. Networked Control Problem

In the networked control problems depicted in Figure 1, the plant and the controller are remotely located entities that exchange data packets over a network that is subject to DoS attacks in the form of jamming and malicious packet-dropping. Such DoS attacks cause failures in the transmission of packets between the plant and the controller. Below, we discuss the networked control problem in both the discrete-time and the continuous-time settings.

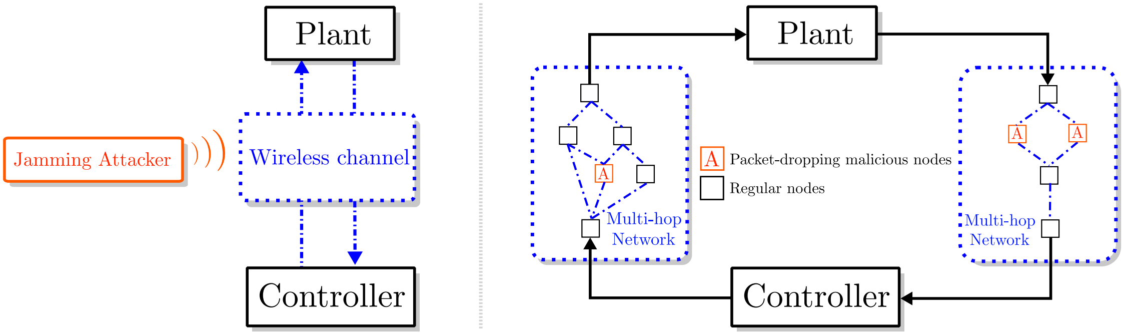

Figure 1. Operation of networked control system under denial-of-service attack: (**Left**) wireless networked control system facing jamming attacks; and (**Right**) multi-hop networked control system that faces packet-dropping attacks by malicious nodes in the networks.).

2.1.1. Discrete-Time Setting

We first look at the networked control problem of a discrete-time linear plant described by

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

$$y(t) = Cx(t), \tag{2}$$

where $x(t) \in \mathbb{R}^n$, $u(t) \in \mathbb{R}^m$, and $y(t) \in \mathbb{R}^h$, respectively, denote the state, the input, and the output vectors of the plant. Moreover, $A \in \mathbb{R}^{n\times n}$, $B \in \mathbb{R}^{n\times m}$, and $C \in \mathbb{R}^{h\times n}$, respectively, denote the state, the input, and the output matrices representing the dynamics.

In the state-feedback networked control problem, sensors located at the plant side measure the state $x(\cdot)$ and transmit it to the controller, which then computes a control input and transmits it back to the plant. In the output-feedback setting, the sensors measure and transmit the output $y(\cdot)$.

State-feedback networked control problem under DoS attacks is discussed in our previous works [25–27]. In those works, the system without control is considered to be unstable (i.e., A has eigenvalues that are outside the unit circle of the complex plane); moreover, the goal is to achieve stabilization of the zero solution $x(t) \equiv 0$ by means of designing suitable control and communication rules. It is also assumed there that the network does not induce delay in transmissions, but packets may fail to be delivered due to attacks. In [28], we further generalized the setting so that delays can also be taken into account.

In the control frameworks in [25–28], the input $u(t)$ that is applied to the plant is set to 0 when there is a failure in the transmission of the state measurement or the control input data. This is one of the most common approaches in the networked control literature that deals with transmission failures (e.g., Kellett et al. [29], Hespanha et al. [30], Gupta et al. [31], Okano and Ishii [32]). In the setup in [25–28], acknowledgement messages are not needed, since a packet exchange failure is known to the plant by the absence of an incoming control input. This in turn allows UDP-like communication protocols discussed in [33] to be used for the practical implementation of the networked operation.

In [26,27], we assumed that packet exchanges take place at every time step. On the other hand, in [25], we developed event-based communication (transmission) rules. In the event-based approach, packet exchanges are attempted between the plant and the controller at times $t_0, t_1, t_2, \ldots \in \mathbb{N}_0$ (with $t_i < t_{i+1}$). These times are decided based on certain event-triggering conditions. The triggering conditions proposed in [25] guarantee that the state stays within certain level sets in between consecutive transmission attempt times, and packet exchange attempts are triggered only before the state is predicted to leave a predefined level set. A more detailed explanation to this event-triggering setup is given in Section 5.1.1.

In the event-based setting in [25], the control input $u(t)$ applied to the plant is given by

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

where $K \in \mathbb{R}^{m\times n}$ denotes the feedback gain matrix and $\{l(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ is a binary-valued process that is used for indicating success/failure of packet exchange attempts. Specifically, $l(i) = 0$ indicates that the packet exchange attempt at time t_i is successful, whereas $l(i) = 1$ indicates that either the packet sent from the plant or the packet sent from the controller failed to be delivered at time t_i. If there are many packet exchange failures, the overall system can become unstable. This is because, when there is a failure, the system is governed by the unstable open-loop dynamics.

Notice that for the wireless networked control system depicted in Figure 1 (left), transmission failures happen due to *jamming attacks* [26]. For *multi-hop* networked control systems (Figure 1, right), packets are attempted to be transmitted over *multi-hop networks*, and packet exchange failures happen due to drops by one or more of the malicious nodes in the network [27].

It is also important to note that the strategy used by the attackers essentially determine which packet exchanges fail. Most of the works in the literature consider the problem where the strategy of the attacker is not known a priori. Typically, certain deterministic or probabilistic models are considered to characterize how frequent the attacks happen. In Sections 3 and 4, we discuss such characterizations.

In the state-feedback control problem, Amin et al. [34] explored finite-horizon optimal control of a discrete-time linear plant under DoS attacks where timings of DoS can be random or arbitrary given that the total number of attacks in the horizon is bounded. Lai et al. [35] considered scenarios where a bound on the number of consecutive DoS attacks is known. Furthermore, in [26,36,37], we investigated the effects of jamming attacks by exploring physical wireless channel models based on Signal to Interference plus Noise Ratio (SINR).

In addition to the state-feedback control, the discrete-time output-feedback control problem has also been considered by taking into account the effects of DoS attacks. Specifically, Cetinkaya et al. [38], Wakaiki et al. [39] and Liu et al. [40] considered observer-based control ideas. In particular, Cetinkaya et al. [38] and Liu et al. [40] developed event-triggered controllers. The difficulty in the event-triggered output-feedback control problem is that the state information cannot be used for control purposes and for characterizing the event-triggering conditions. Observer-based quantized output-feedback control problem is investigated in [39], where a quantizer with dynamically varying ranges is utilized and sufficient convergence conditions are obtained. In addition to those results, optimal output-feedback control problem was considered by Zhang et al. [41] and Befekadu et al. [42] for systems with DoS attacks and noisy measurements. Furthermore, in [43], a game-theoretical approach is taken for an output-feedback networked control problem over multiple-channels that are subject to jamming attacks.

For discrete-time multi-hop networked control systems, there are several results (see, e.g., Cetinkaya et al. [27], Smarra et al. [44], D'Innocenzo et al. [45], D'Innocenzo et al. [46]). The multi-hop network characterization in our work [27] is based on a probabilistic approach that takes into account both non-malicious and malicious failures in the network (see Section 4.2). On the other hand, Smarra et al. [44], D'Innocenzo et al. [45] and D'Innocenzo et al. [46] utilized a different characterization where the information flow in the network for a given scheduling and routing protocol is characterized through difference equations. For this network setup, Smarra et al. [44] proposed methods for designing network weights as well as controller and observer gains by taking into account potential packet losses. Moreover, D'Innocenzo et al. [45] and D'Innocenzo et al. [46] proposed methods for detecting and isolating malicious nodes that intentionally delay packets or stop forwarding them. In addition, malicious nodes that inject false data can also be handled within the framework of [45,46].

2.1.2. Continuous-Time Setting

In [47,48], researchers considered event-based remote control of a plant described by a linear continuous-time system

$$\dot{x}(t) = Ax(t) + Bu(t), \quad x(0) = x_0, \quad t \geq 0, \tag{4}$$

$$y(t) = Cx(t). \tag{5}$$

The state of the plant is measured at times $t_0, t_1, t_2, \ldots \in [0, \infty)$ and transmitted on the network to the controller. The control input applied at the plant side is kept constant between each successful transmission over the network. In particular, the input $u(t)$ at the plant-side is given by

$$u(t) = Kx(t_{k(t)}), \tag{6}$$

where $k(t)$ denotes the index of the last successful transmission time. Notice that, in the control framework in [47,48], the control input at the plant side is not set to 0, when control data packet transmissions fail.

The framework developed in [47] allows resilient control update mechanisms. As we discuss further in Section 5.1.1, the intervals between consecutive transmission attempt times $t_0, t_1, t_2, \ldots$ are designed to depend on the presence/absence of attacks. For instance, if the transmission attempt at time

t_k faces an attack, then the next transmission is attempted shortly afterwards, whereas, if the attempt at time t_k is successful, the next attempt can be made after a longer duration. Similar resilient control setups are provided in the discrete-time setting in [25,38].

In [47,48], researchers provide a stability analysis approach for the closed-loop state-feedback control system in Equations (4) and (6) by utilizing bounds on the average duration and the frequency of DoS attacks. The characterization of attacks through average duration and frequency bounds is further discussed in Section 3.1.

The analysis approach in [47,48] does not require the strategy of the attacks to be known, and, moreover, the attacks can be time- or state-dependent. We also note that there are several works where periodic DoS attacks with unknown average duration and frequency are considered. In particular, Shisheh Foroush and Martínez [49] provided a detection-based control approach for periodic attacks, where the periodic strategy of the attacker can be learned so that transmission times are selected to avoid overlapping with the attack times.

In the case of *output-feedback* control problem, the utility of several different control frameworks under DoS attacks is investigated in [50–52]. As we further discuss in Section 5.1.1, Feng and Tesi [50] and Feng and Tesi [51] provided new architectures to limit the capabilities of attackers. Moreover, Lu and Yang [52] considered the case where multiple sensors make output measurements (ith sensor attempts to send the ith output measurement $y_i(t) = C_i x(t)$ over the ith channel).

In [53,54], the effect of DoS attacks on *nonlinear* systems is explored. Specifically, De Persis and Tesi [53] investigated the state-feedback control problem, and, moreover, Dolk et al. [54] explored dynamic event-based output-feedback controllers for stabilization. In [55], a linearization approach is developed for stabilizing nonlinear systems. There, it is mentioned that, when DoS attacks are sufficiently strong, the trajectories of the state may leave the linearization region, which may in turn cause instability due to the nonlinearity of the dynamics. For the case where the system dynamics involve unknown nonlinear functions, An and Yang [56] proposed adaptive controllers to guarantee boundedness of the state under DoS attacks.

Networked distributed control of a large-scale system is explored in [57]. There, the subsystems of the large-scale system utilize a shared network for the transmissions of their corresponding measurement and control input packets. To mitigate the effects of DoS, Feng et al. [57] proposed a transmission strategy that switches between event-based transmissions and a Round-robin protocol.

The performance of periodic and event-triggering networked control approaches under different types of jamming attacks was investigated in [58].

Additionally, frequency regulation problems in power networks under DoS attacks are considered in [59,60]. In both studies, the nodes in the power network are assumed to communicate over insecure communication channels that are subject to DoS attacks. In the problem formulation in [59], nonlinear dynamics are explored. Moreover, the researchers propose an event-based control approach in [60].

In [61], researchers considered networked control problem under DoS attacks and data-rate constraints, where state measurements are quantized through a dynamic quantization scheme.

We note that, among the different control approaches used for networked control systems under DoS attacks, event-triggered control (see, e.g., [25,38,48,54,58], and the references therein) appears to be the most commonly considered approach. We discuss the resiliency of event-triggering approaches against DoS attacks further in Section 5.1.1.

2.2. Networked State Estimation Problem

A remote state estimation problem over a network that is subject to DoS attacks is considered in [62]. There, the researchers explore a discrete-time linear plant given by

$$x(t+1) = Ax(t) + w(t), \tag{7}$$

$$y(t) = Cx(t) + v(t), \tag{8}$$

where $x(t) \in \mathbb{R}^n$ and $y(t) \in \mathbb{R}^h$, respectively, denote the state and output vectors; and $w(t) \in \mathbb{R}^n$ and $v(t) \in \mathbb{R}^h$, respectively, denote noises that are described by stochastic processes with zero-mean at each time instant t.

The networked state estimation framework in [62] is shown in Figure 2. In particular, a sensor at the plant side is assumed to be able to compute a local estimate $\hat{x}_S(t) \in \mathbb{R}^n$ based on output measurements $y(t)$. For this purpose, a Kalman filter is utilized. At certain time instants, the estimate $\hat{x}_S(t)$ is sent over a communication channel to a receiving node representing a *remote estimator*.

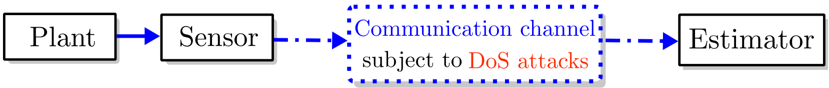

Figure 2. Operation of networked state estimation subject to DoS attacks.

As the receiving node may not have a direct access to the state estimate $\hat{x}_S(t)$ at all time instants, it keeps its own estimate $\hat{x}(t)$ of the state. If a new state estimate from the sensor is received, the receiving node sets its estimate value to the newly obtained value (i.e., $\hat{x}(t) = \hat{x}_S(t)$). In the case where there is no transmission or the transmission fails due to DoS attacks, the receiving node cannot obtain any information. In that case, previously available state estimate is used together with the plant dynamics to obtain a predicted value by setting $\hat{x}(t) = A\hat{x}(t-1)$.

Li et al. [62] considered a finite horizon estimation problem, where $T \in \mathbb{N}$ denotes the horizon. In this problem, a performance indicator

$$J_\alpha(T) \triangleq \alpha \frac{1}{T} \sum_{t=1}^{T} \mathbb{E}[\|x(t) - \hat{x}(t)\|^2] + (1-\alpha)\mathbb{E}[\|x(T) - \hat{x}(T)\|^2] \tag{9}$$

with a scalar $\alpha \in [0,1]$ is used. By setting $\alpha = 1$, $J_\alpha(T) = J_1(T)$ represents the average estimation error variance, and by setting $\alpha = 0$, $J_\alpha(T) = J_0(T)$ corresponds to the final estimation error variance obtained at the end of the horizon.

In the problem formulation in [62], the sensor decides whether to transmit the data $\hat{x}_S(t)$ or not, and similarly the attacker decides whether to attack the channel or not at each time t. To identify the worst-case attack scenarios as well as the best transmission strategies, Li et al. [62] proposed game-theoretic characterizations, where the performance indicator $J_\alpha(T)$ is taken into account both by the sensor and the attacker. We explain these game-theoretic characterizations in a more detailed way in Section 3.2. In those characterizations, the number of transmissions by the sensor and the number of attacks by the attacker in a given horizon T are assumed to be constrained by certain scalars that are less than T. In [62], the optimal transmission and attack strategies are discussed for the case with constraints.

For scenarios where the sensor attempts transmission at each time step, closed-form optimal attack strategies that maximize $J_1(T)$ and $J_0(T)$ are obtained in [63,64]. The work in [63] also presents a variation of the problem of finding worst-case attack scenarios. In this variation, the attacker has additional constraints, which are proposed to explore strategies of an attacker that does not want to get detected by an intruder detection system.

The state estimation problem over wireless channels with SINR-based models have been discussed in [65,66]. Furthermore, Ding et al. [67] considered a network setup with multiple wireless channels. All three works explore game-theoretic and optimization-based analysis approaches. In particular, the sensor and the attacker are considered to be the players of a game. In the setting in [65,66], the players attempt to optimize not only the timing but also the signal and the interference power levels of transmissions and attacks. In the multi-channel estimation problem considered in [67], the sensor aims to optimally select the wireless channels that will be used to transmit packets, and, moreover, the attacker wants to optimally select the channels that will be blocked. For the state estimation problem with multiple sensors and multiple channels, the optimal strategies of the attacker are also discussed in [68].

We note that estimation problems under different attack types have also been studied. For instance, Guo et al. [69] investigated optimal false data injection attacks in state estimation problem. Furthermore, Guan and Ge [70] explored state estimation under jamming attacks as well as false data injections and developed a threshold-based detection method.

2.3. Multi-Agent Consensus Problem

The consensus problem for a multi-agent system under jamming attacks is considered in [71–73]. The multi-agent system in those works consists of n agents that possess scalar dynamics. In particular, the evolution of the ith agent's state is described by

$$\dot{x}^i(t) = u^i(t), \quad t \geq 0, \tag{10}$$

where $x^i(t) \in \mathbb{R}$ is the state and $u^i(t) \in \mathbb{R}$ is the local control input for agent i.

Inter-agent communication topology of the multi-agent system is characterized with an undirected graph $\mathcal{G} = (\mathcal{V}, \mathcal{E})$, where the nodes $\mathcal{V} = \{1, \ldots, n\}$ represent the agents and the edges $\mathcal{E} \subset \mathcal{V} \times \mathcal{V}$ represent the communication links between agents.

The goal in [71–73] is to develop control and communication rules to guarantee practical consensus under jamming attacks. In practical consensus, agents states $[\ x^1(t) \quad x^2(t) \quad \cdots \quad x^n(t)\ ]^{\mathrm{T}}$ converge to a vector $x^* \in \mathbb{R}^n$ that belongs to a consensus set $\mathcal{D}_\varepsilon$

$$\mathcal{D}_\varepsilon \triangleq \Big\{ x \in \mathbb{R}^n : \Big| \sum_{j \in \mathcal{N}^i} (x^j - x^i) \Big| < \varepsilon, \ i \in \mathcal{V} \Big\}, \tag{11}$$

where $\varepsilon > 0$ represents a predetermined required level of closeness between agents and $\mathcal{N}^i \subset \mathcal{V}$ denotes the neighbors of agent i, that is, the set of agents that share a communication link with agent i.

For this problem formulation, Senejohnny et al. [71] and Kikuchi et al. [72] considered the attack setup shown on the left-hand side of Figure 3. In this setup, the jamming attacker can target all communication links at once. Specifically when there is an attack, none of the agents can communicate with each other. In the control approach in [71,72], each agent $i \in \mathcal{V}$ tries to communicate with its neighbors at certain times denoted by $t_0^i, t_1^i, \ldots$. Specifically, at time t_k^i, agent i sends a packet to its neighbors to request their states. In the case where there is no jamming attack at that time, all neighbors receive this packet and they respond by sending back their states. Those states are then used by agent i for constructing a ternary control input (i.e., $u^i(t) \in \{-1, 0, 1\}$) for achieving consensus.

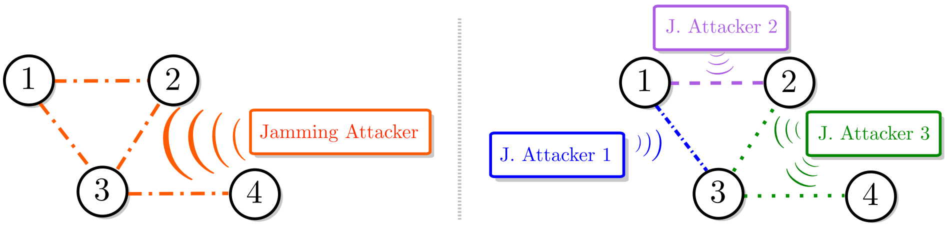

Figure 3. Multi-agent consensus in the presence of jamming attackers: (**Left**) single jamming attacker causes transmission failures on all inter-agent communication links; and (**Right**) multiple jamming attackers cause failures on different links).

For designing communication attempt times $t_0^i, t_1^i, \ldots$, Senejohnny et al. [71] used a self-triggering approach, where communication is attempted by each agent i only when a triggering condition holds. For achieving consensus, a restriction on the average duration and the average frequency on the attacks is imposed. These duration and frequency restrictions are discussed in Section 3.1, and they follow the attack characterization proposed by De Persis and Tesi [48]. It is shown in [72] that the restriction on the attack frequency can be removed when the agents utilize *randomization* in designing the communication attempt times. The utility of this randomization approach is further discussed in Section 5.2.1.

Recently, Senejohnny et al. [73] explored the multi-agent consensus problem under the attack setup shown in Figure 3 (right). In this setup, there are multiple jamming attackers that can target individual communication links.

We note that the consensus problem depicted in Figure 3 (left) is also explored for multi-agent systems with multi-dimensional dynamics in [74]. More recently, Nugraha et al. [75] considered a game-theoretical formulation of multi-agent systems under jamming attacks that can target individual links.

One of the key issues in studying the control, estimation, and consensus problems under denial-of-service attacks is that the attacker's actions cannot be known a priori. To account for the uncertainty in the way the attacks may be generated, researchers have proposed several modeling approaches. These approaches can be classified into three groups: (1) deterministic approaches; (2) game-theoretic, optimization-based approaches; and (3) probabilistic approaches. In Sections 3 and 4, we discuss these approaches in detail.

3. Deterministic and Game-Theoretical Approaches to Denial-of-Service Attack Modeling

In this section, we provide an overview of deterministic and game-theoretical approaches proposed in the literature for modeling denial-of-service attacks. We present several models and discuss their efficacy for addressing the networked control problems mentioned in Section 2.

3.1. Deterministic Attack Models with Average Duration and Frequency Constraints

In [47], the authors proposed a model that allows DoS attacks to happen in an arbitrary fashion as long as the total duration of attacks in a given time interval is upper-bounded by a deterministic function of the length of that interval.

In the continuous-time setting of this model, the timing of the attacks can be characterized as follows. First, two sequences $\{a_k \geq 0\}_{k\in\mathbb{N}_0}$ and $\{\tau_k \geq 0\}_{k\in\mathbb{N}_0}$ are used for denoting the starting times and durations of attack intervals. As we illustrate in Figure 4, the kth attack interval starts at time a_k and lasts for τ_k units of time. It is assumed that $a_{k+1} > a_k + \tau_k$ so that different attack intervals are not overlapping.

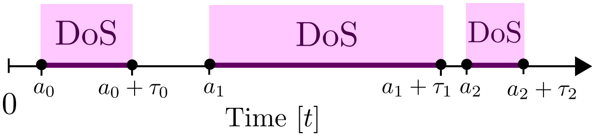

Figure 4. Sequence of DoS attack intervals. Transmission attempts that occur in any of the DoS attack intervals (represented with pink regions) fail.

This model fits well into scenarios with jamming, where the attacker may be emitting very strong jamming signals during the intervals $[a_k, a_k + \tau_k]$. Note that, when a packet transmission time t_j overlaps with any attack interval (i.e., $t_j \in \cup_{k\in\mathbb{N}_0}[a_k, a_k + \tau_k]$), then there will be a transmission failure at that time.

To model capabilities of the attacks, the notion of total attack duration is used. Specifically, for any time interval $[\tau, t] \subset [0, \infty)$, the set $\mathcal{A}(\tau, t) \subset [\tau, t]$ is used for denoting the times that the network faces DoS attacks, i.e.,

$$\mathcal{A}(\tau, t) \triangleq \cup_{k\in\mathbb{N}_0}[a_k, a_k + \tau_k] \cap [\tau, t], \tag{12}$$

and $|\mathcal{A}(\tau, t)|$ is used for denoting the total duration of the attacks in the same interval.

Note that, in the case where DoS attacks cover the entire time span, we have $|\mathcal{A}(0,t)| = t$ for all $t \geq 0$. In such cases, communication on a network is not possible, and hence, control, estimation, and consensus goals cannot be achieved over such networks.

Typically, attackers may have constraints that prevent them from attacking at all times. For instance, in the case of jamming attacks, emitting powerful interference signals is costly and attackers with limited energy resources cannot conduct attacks at all time instants. Note also that the constraints may be imposed by the attacker who wants to avoid being detected. Strategic attackers may want to keep away from attacking continuously at all times to avoid detection.

The model in [47] takes into account such constraints by considering the following assumption.

Assumption 1. *There exist scalars $\kappa_{\mathrm{D}} \geq 0$ and $\rho_{\mathrm{D}} \in [0,1)$ such that*

$$|\mathcal{A}(0,t)| \leq \kappa_{\mathrm{D}} + \rho_{\mathrm{D}} t, \quad t \geq 0. \tag{13}$$

It follows from Equation (13) that $\limsup_{t\to\infty} |\mathcal{A}(0,t)|/t \leq \rho_{\mathrm{D}}$. This indicates that the scalar ρ_{D} represents an upper-bound on the average ratio of attack durations in long intervals. If, for instance, $\rho_{\mathrm{D}} = 0.5$, then the total attack duration in the long run does not exceed 50% of the total time. In the case where the first attack interval starts at time $a_0 = 0$, Equation (13) implies a bound on the attack interval length τ_0 as $\tau_0 \leq \kappa_{\mathrm{D}}/(1-\rho_{\mathrm{D}})$. Thus, the scalar κ_{D} in Equation (13) can be selected for modeling initial capabilities of the attacker.

In [47,59], Assumption 1 is utilized in analyzing stability properties of networked control systems.

In [48], attackers with additional attack frequency constraints are considered. In particular, the following assumption characterizes attacks that have frequency constraints.

Assumption 2. *There exist scalars $\kappa_{\mathrm{F}} \geq 0$ and $\rho_{\mathrm{F}} \in [0,1)$ such that*

$$\mathcal{I}(0,t) \leq \kappa_{\mathrm{F}} + \rho_{\mathrm{F}} t, \quad t \geq 0, \tag{14}$$

where $\mathcal{I}(\tau,t) \in \mathbb{N}_0$ denotes the number of attack intervals in the time frame $[\tau,t]$.

The scalar ρ_{F} in Equation (14) provides an upper-bound on the frequency of attacks in the long run. To achieve stabilization of networked control systems with periodic transmissions, attack frequency needs to be bounded by a scalar ρ_{F} small enough. To see this, first consider periodic transmission attempts at every Δ units of time. A strategic attacker who knows the transmission period Δ can concentrate his/her attacks to pinpoint the periodic transmission times with attacks that have very short durations (which satisfy Assumption 1). Thus, for such settings, all transmission attempts may fail if $\rho_{\mathrm{F}} \geq \frac{1}{\Delta}$.

In [48], it is mentioned that Assumptions 1 and 2 do not suffice when one considers system dynamics with disturbance. This is because, under Assumptions 1 and 2, the attacker is allowed to attack continuously for arbitrarily long intervals as long as Equations (13) and (14) are satisfied. The attacker can achieve this by initially waiting for a long duration. This scenario is particularly dangerous for systems with disturbance, because even though the control packets may successfully be delivered in the initial attack-free period, the state never reaches zero due to disturbance. When the attack-free period ends, the attacker can attack continuously and cause the state to grow to very large values. To avoid such issues, De Persis and Tesi [48] proposed further restrictions of the average attack duration and the average attack frequency so that the maximum length of a continuous attack is bounded. These new restrictions are described by the inequalities

$$|\mathcal{A}(\tau,t)| \leq \kappa_{\mathrm{D}} + \rho_{\mathrm{D}}(t-\tau), \tag{15}$$

$$\mathcal{I}(\tau,t) \leq \kappa_{\mathrm{F}} + \rho_{\mathrm{F}}(t-\tau), \tag{16}$$

which are required to be satisfied for all $\tau \geq 0$ and $t \geq \tau$. Notice that Equations (15) and (16) imply Equations (13) and (14), but not vice versa.

In [48,50,51], average duration and frequency conditions in Equations (15) and (16) are utilized for modeling attacks in a networked control problem.

It is shown in [48] that asymptotic stabilization with an event-triggered controller can be achieved under any attack strategy that satisfies Assumptions 1 and 2 with sufficiently small scalars ρ_{D} and ρ_{F}. In particular, the sufficient condition given in [48] for asymptotic stability is

$$\Delta^* \rho_{\mathrm{F}} + \rho_{\mathrm{D}} < \omega,$$

where $\omega > 0$ is a scalar that depends on system dynamics, and $\Delta^* > 0$ is scalar that upper-bounds the intervals between network transmission instants. It is shown in [48] that this condition guarantees input-to-state stability for systems with disturbance on the condition that ρ_{D} and ρ_{F} satisfy Equations (15) and (16) (in addition to satisfying Equations (13) and (14)). The authors of [50,51] considered periodic sampled-data controllers and showed that stability condition in this case can be made less conservative by using predictor and buffer mechanisms (see also Section 5.1.2). As noted in [48,50,51], κ_{D} and κ_{F} used in the inequalities in Equations (13) and (14) (or Equations (15) and (16)) affect bounds on state trajectories and the performance, but they do not affect the stability properties of linear systems. In the case of nonlinear systems, κ_{D} and κ_{F} play a role also in stability properties. In particular, κ_{D} and κ_{F} are utilized in [55] for determining the initial capabilities of the attacker and for obtaining conditions of stabilization with a controller that is designed through a linearization approach.

For the multi-agent consensus problem discussed in Section 2.3, [71,73] utilized the attack characterization with the conditions in Equations (15) and (16). It is observed in [72] that, with randomized transmissions, consensus in multi-agent systems can be achieved if the average attack duration is restricted as in Equation (15) regardless of the attack frequency.

In the discrete-time setting, a similar modeling approach can be utilized. The attack intervals can be defined similarly through sequences $\{a_k \in \mathbb{N}_0\}_{k\in\mathbb{N}_0}$ and $\{\tau_k \in \mathbb{N}_0\}_{k\in\mathbb{N}_0}$. In particular, the kth attack interval is given by $\{a_k, a_k+1, \ldots, a_k+\tau_k-1\}$. Again, it is assumed that $a_{k+1} > a_k + \tau_k$. Furthermore, average duration and frequency restrictions in Equations (13) and (14) as well as Equations (15) and (16) can be imposed in a similar way. For discrete-time networked control problems, Cetinkaya et al. [25] and Wakaiki et al. [39] considered average duration and average frequency restrictions in obtaining sufficient conditions of stabilization over networks under DoS attacks.

We note that there are other deterministic modeling approaches such as periodic DoS attacks considered in [49]. In particular, Shisheh Foroush and Martínez [49] modeled DoS attacks in a general way as a pulse width modulated (PWM) signal. In this model, the attacker repeats cycles of jamming and sleeping. Furthermore, in the special case of periodic jamming, each cycle consists of T_{J} seconds of jamming that is followed by T_{S} seconds of sleeping. Shisheh Foroush and Martínez [49] considered the setup where both T_{J} and T_{S} are unknown in the networked control problem. In addition, constraints on attacks were considered previously in a finite horizon problem by Amin et al. [34]. There, attacks can happen at arbitrary time instants given that the total number of attacks does not exceed a threshold for a given finite time horizon. As we further discuss in Section 3.2, such constraints have also been used in game-theoretic approaches.

3.2. Game-Theoretic and Optimization-Based Approaches for Attack Modeling

Game theory provides a natural framework for studying cyber security of control systems under DoS attacks and has been explored in many works (see, e.g., Li et al. [62], Li et al. [66], Ding et al. [67], Alpcan and Başar [76], Gupta et al. [77], Bhattacharya et al. [78]). Through a *game-theoretic* approach, researchers have obtained optimal DoS attack and defense schemes in certain problem settings. In what follows, we discuss some of the approaches in those works.

3.2.1. Constraint-Based Models with Binary Actions

In several studies that deal with DoS attacks, the actions of the attacker and the defender are represented with binary variables corresponding to the choices between attacking and not attacking and similarly between defending and not defending.

For example, Li et al. [62] considered the finite-horizon state estimation problem discussed in Section 2.2, where binary variables $\lambda_{\mathrm{S}}(t) \in \{0,1\}$ and $\lambda_{\mathrm{A}}(t) \in \{0,1\}$ are used for indicating the decisions of the sensor and the DoS attacker, respectively. If, $\lambda_{\mathrm{S}}(t) = 1$, then the state estimate $\hat{x}_{\mathrm{S}}(t)$ is attempted to be transmitted over the communication channel at time t. Moreover, the presence of an attack that causes a transmission failure at time t is represented by $\lambda_{\mathrm{A}}(t) = 1$.

Notice that, if the attacker and the defender do not have any constraints, it may be ideal for both players to act at every time instant (i.e., $\lambda_{\mathrm{S}}(t) = \lambda_{\mathrm{A}}(t) = 1$ for all $t \in \mathbb{N}$). In [62], researchers considered scenarios where both the attacker and the sensor have constraints represented by

$$\sum_{t=1}^{T} \gamma_{\mathrm{S}}(t) \leq N_{\mathrm{S}}, \quad \sum_{t=1}^{T} \lambda_{\mathrm{A}}(t) \leq N_{\mathrm{A}}, \tag{17}$$

where $T \in \mathbb{N}$ is the time horizon of the estimation problem, and N_{S} and N_{A} are positive scalars that are strictly less than T. It is essential for the players to choose the best timing for their actions. To identify the worst-case attack scenarios as well as the best transmission strategies, Li et al. [62] proposed game-theoretic formulations, where a game is played by the sensor and the attacker. The goal of the defender is to minimize the cost in Equation (9) so as to minimize the estimation error, whereas the attacker wants to maximize Equation (9). For various constrained attack problems, closed-form optimal attack strategies $\lambda_{\mathrm{A}}(1), \lambda_{\mathrm{A}}(2), \ldots, \lambda_{\mathrm{A}}(T)$ that maximize $J_1(T)$ and $J_0(T)$ are obtained in [63,64].

A constraint on the total number of attacks in a given time horizon was considered also by Amin et al. [34] for a networked control problem under DoS attacks. Constraints similar to Equation (17) may characterize energy limitations of a jamming attacker. We note that, besides the formulation with constraints, there are also other formulations where the jamming energy is a part of the cost function of attacker (see, e.g., [76]). The effect of energy-related jamming costs was investigated by Zhu et al. [79], who considered a noncooperative game for analyzing the actions of a group of non-malicious nodes together with a malicious node that is capable of jamming and eavesdropping.

In addition to the energy constraints in Equation (17), the attacker may have additional constraints. In [63], some additional constraints are proposed to explore strategies of an attacker that does not want to get detected by an intruder detection system. It is discussed in [63] that a detection mechanism can check the number of transmission failures in the last $\tau_{\mathrm{D}} \in \mathbb{N}$ time steps and release an alarm if the failures go above a threshold $d_{\mathrm{D}} \in \mathbb{N}$. To avoid being detected by such a detection system, the attacker chooses a strategy that satisfies

$$\sum_{t=k+1}^{k+\tau_{\mathrm{D}}} \lambda_{\mathrm{A}}(t) \leq d_{\mathrm{D}}, \quad k \in \{0, 1, \ldots, T - \tau_{\mathrm{D}}\}. \tag{18}$$

Notice that under Equation (18), the number of attacks in every consecutive τ_{D} time steps does not exceed d_{D}. An extension of this constraint to infinite-horizon problems resembles the constraints discussed in Section 3.1.

3.2.2. SINR-Based Models

Recently, a few works considered Signal to Interference plus Noise Ratio (SINR) in modeling of the effect of jamming attacks to wireless communication channels (see, e.g., [66,80]). In those works, the probability of a packet transmission error depends on the Signal to Interference plus Noise Ratio (SINR), which is the ratio of the power of transmitted signal to the sum of the attacker's interference power and the power of the channel noise. If the power of transmitted signal is small or interference and noise have large powers, then an error becomes highly likely.

In [66], researchers investigated the estimation problem over a wireless channel with an SINR-based model. In this model the sensor chooses a power level $p_{\mathrm{S}}(t) \in [0, \infty)$ for transmitting the estimate $\hat{x}_{\mathrm{S}}(t)$. In addition, the jamming attacker chooses an interference power $p_{\mathrm{A}}(t) \in [0, \infty)$ at time t. The power values $p_{\mathrm{S}}(t)$ and $p_{\mathrm{A}}(t)$ affect the SINR given by $\frac{p_{\mathrm{S}}(t)}{p_{\mathrm{A}}(t)+\sigma^2}$, where σ^2 denotes the power of channel noise. The probability of a successful transmission at time t depends on SINR and is given by

$$1 - 2Q\left(\sqrt{\alpha \frac{p_{\mathrm{S}}(t)}{p_{\mathrm{A}}(t) + \sigma^2}}\right),$$

where $Q(x) \triangleq \frac{1}{\sqrt{2\pi}} \int_x^\infty e^{-s^2/2} \mathrm{d}s$, and $\alpha > 0$ is a parameter that depends on the wireless channel properties. Notice that successful transmission probability is affected by power levels $p_{\mathrm{S}}(t)$ and $p_{\mathrm{A}}(t)$ used by the sensor and the attacker.

In [66], optimal strategies of the sensor and the attacker are explored. In particular, first, a finite-horizon problem similar to the one in [62] is considered. The goal of the attacker is to find an optimal strategy $p_{\mathrm{A}}(1), p_{\mathrm{A}}(2), \ldots, p_{\mathrm{A}}(T)$ that maximizes a utility function while satisfying an energy constraint

$$\sum_{t=1}^{T} p_{\mathrm{A}}(t) = P_{\mathrm{A}},$$

where $P_{\mathrm{A}} > 0$. In particular, the attacker's utility is chosen as $TJ_1(T)$ with $J_\alpha(\cdot)$ given by Equation (9). The sensor's utility function is considered to be the additive inverse of the utility of the attacker. Moreover, the energy constraint for the sensor is given by

$$\sum_{t=1}^{T} p_{\mathrm{S}}(t) = P_{\mathrm{S}},$$

where $P_{\mathrm{S}} > 0$. A game-theoretic approach is taken in [66] to investigate optimal sensor and attack strategies. In [64], researchers considered a similar problem and provides an analysis on the optimal attack strategies $p_{\mathrm{A}}(1), p_{\mathrm{A}}(2), \ldots, p_{\mathrm{A}}(T)$ that yield the worst-case scenario in terms of the estimation performance. Optimal interference power levels and their effects were explored by Zhang et al. [80], who considered several settings of attack capabilities. In particular, Zhang et al. [80] considered both the case where the attacker can eavesdrop the acknowledgement messages and the case where the attacker has no knowledge of whether the attack is successful. In the case of infinite-horizon problems with an SINR-based formulation, Li et al. [66] showed that a *Q-learning* algorithm can be used by the sensor to obtain optimal strategies for selecting transmission powers.

A game with SINR-based formulation for wireless networked control systems was also considered by Yang et al. [81]. The players in the game are: (1) the user who decides the power of transmissions from the controller to the plant; and (2) the jamming attacker who decides the jamming interference power. In particular, Yang et al. [81] explored a *Stackelberg game*, where the user is the leader and acts first; the action of the user is then followed by that of the jamming attacker. In the problem setting in [81], the utilities of the user and the attacker depend directly on the SINR. They are expressed as $\frac{L\eta P}{\beta J+\sigma^2}$, where L, η, and β are fixed positive constants representing channel properties, $\sigma^2 > 0$ is the background channel noise, and $P \in [0, \infty)$ and $J \in [0, \infty)$, respectively, denote the transmission power of the user and interference power of the attacker. The cost of transmission and the cost of jamming for one unit of power are given respectively by the positive scalars E and C. Moreover, the utilities of the user and the jammer are, respectively, given by

$$V_{\text{User}}(P,J) \triangleq \frac{L\eta P}{\beta J + \sigma^2} - EP, \quad V_{\text{Jammer}}(P,J) \triangleq -\frac{L\eta P}{\beta J + \sigma^2} - CJ.$$

In this formulation, the optimal strategy of the jamming attacker for a given transmission power P is denoted by $J^*(P)$ and is obtained by finding $J \in [0,\infty)$ that maximizes $V_{\text{Jammer}}(P,J)$. Then, based on the jamming attacker's optimal strategy, the user's best strategy is obtained in [81] through solving the problem

$$\underset{P\in[0,\infty)}{\text{maximize}} \quad V_{\text{User}}(P,J^*(P)).$$

A Stackelberg game was also utilized by Liu [82] to investigate optimal attack and defense strategies in a multi-channel estimation problem. In this problem, a number of sensors acquire measurements of a plant and attempt to transmit these measurements to a remote receiver over insecure wireless channels. Each channel may be subject to a jamming attack and the transmission failure probabilities are characterized through an SINR formulation. In [82], two cases with incomplete information are considered: (i) the defender knows the probability of a possible attack and the total jamming power used on the wireless channels when there is an attack; and (ii) the defender knows the probabilities of possible attacks on each channel with the corresponding power levels.

In the context of multi-agent systems, Nugraha et al. [75] explored a game-theoretical formulation, where a game between a jamming attacker and a defender is considered by extending the infrastructure network modeling approach in [83]. In this game, the jamming attacker's goal is to optimally choose communication links to attack, whereas the defender wants to recover those links. To this end, a new quantitative network connectivity notion is introduced in [75] to find optimal attack and defense strategies for scenarios where the attacker wants to decrease the connectivity by attacking certain communication links, whereas the defender wants to increase it by reestablishing the connection on the attacked links. In the problem, both players are assumed to have energy constraints that vary in time based on the previous actions of the players.

4. Probabilistic Approaches to Models of DoS Attacks and Non-Malicious Transmission Failures

In Section 3, we looked at deterministic and game-theoretic DoS attack models and analysis techniques. Our goal in this section is to discuss *probabilistic* approaches for modeling and analyzing the effects of DoS attacks. In particular, we focus on networks with wireless channels and multi-hop transmissions. For such networks, DoS attacks may not be the only source of failures, as transmissions may also fail due to non-malicious reasons [17,18]. For instance, wireless channels face unintentional interference, channel noise, and fading issues. Moreover, non-malicious issues such as link errors and congestion cause failures in multi-hop networks. In networked control systems, the transmission failures due to non-malicious issues are typically modeled through the use of stochastic processes such as Bernoulli processes [30,84] and Markov processes [31,32]. In [25], we observed that both non-malicious transmission failures and malicious DoS attacks as well as their combinations can be modeled through a *probabilistic* approach.

The probabilistic approach in [25] is developed upon tail-probability bounds for the binary-valued processes that describe the occurrences of transmission failures on a network. In what follows, we first explain this probabilistic approach and illustrate its generality by considering non-malicious failures and DoS attacks on a network. Then, in Sections 4.1 and 4.2, we consider its utility in wireless channel and multi-hop network modeling.

Consider the binary-valued process $\{l(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ discussed in Section 2.1.1. This process is used for indicating the status of packet transmissions, where $l(i)=1$ represents a failure and $l(i)=0$ represents a successful transmission at time t_i. To describe the effects of certain non-malicious and malicious failure models in a unified manner, in [25,27], we investigated classes of binary-valued transmission failure indicator processes that describe networks where the number of failures in the long run is bounded in a probabilistic sense. First, for a given scalar $\rho \in [0,1]$, consider the class Λ_ρ of binary-valued processes given by

$$\Lambda_\rho \triangleq \left\{ l\colon l(i) \in \{0,1\}, i \in \mathbb{N}_0; \sum_{t=1}^{\infty} \mathbb{P}\left[\sum_{i=0}^{t-1} l(i) > \rho t\right] < \infty \right\}. \tag{19}$$

Notice that the inequality $\sum_{t=1}^{\infty} \mathbb{P}\left[\sum_{i=0}^{t-1} l(i) > \rho t\right] < \infty$ describes a condition on the tail probability $\mathbb{P}[\frac{1}{t}\sum_{i=0}^{t-1} l(i) > \rho]$ (i.e., the probability of the tail event where the ratio $\frac{1}{t}\sum_{i=0}^{t-1} l(i)$ of transmission failures exceeds ρ). Under this condition, the average number of failures is guaranteed to be bounded in the long run. In particular, a consequence of the Borel–Cantelli lemma [85] is that $\limsup_{t\to\infty} \frac{1}{t}\sum_{i=0}^{t-1} l(i) \leq \rho$, almost surely, for every $l \in \Lambda_\rho$. For the network control system discussed in Section 2.1.1, it is shown in [25] that the closed-loop system becomes stable if $l \in \Lambda_\rho$ for a sufficiently small ρ.

It was further noted by the authors of [25] that classes Λ_ρ with different ρ values can be used to characterize binary-valued transmission failure indicators that are associated with networks that face: (1) non-malicious transmission failures; (2) malicious DoS attacks; and (3) combination of non-malicious and malicious issues.

In particular, to model non-malicious transmission failures, a time-inhomogeneous Markov chain $\{l_\mathrm{R}(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ can be considered with initial distributions $\vartheta_q \in [0,1]$, $q \in \{0,1\}$, and time-varying transition probabilities $p_{q,r}\colon \mathbb{N}_0 \to [0,1]$, $q,r \in \{0,1\}$, satisfying

$$\begin{aligned} \mathbb{P}[l_\mathrm{R}(0) = q] &= \vartheta_q, \\ \mathbb{P}[l_\mathrm{R}(i+1) = r | l_\mathrm{R}(i) = q] &= p_{q,r}(i), \quad i \in \mathbb{N}_0. \end{aligned} \tag{20}$$

The following result shows that, if the probabilities $p_{0,1}(i)$ and $p_{1,1}(i)$ of transition towards the failure state 1 are bounded by a scalar $p_1 \in (0,1)$, then l_R belongs to the failure class Λ_ρ for ρ values larger than p_1.

Proposition 3 ([25])**.** *Suppose $p_{0,1}(i) \leq p_1$ and $p_{1,1}(i) \leq p_1$, for $i \in \mathbb{N}_0$, where $p_1 \in (0,1)$. Then, $l_\mathrm{R} \in \Lambda_\rho$ for any $\rho \in (p_1, 1]$.*

To model DoS attacks through the class Λ_ρ, consider a network with a single DoS attacker and let $l_\mathrm{A}(i) \in \{0,1\}$ denote the possible actions of the attacker, where $l_\mathrm{A}(i) = 1$ represents an attack and $l_\mathrm{A}(i) = 0$ represents the absence of an attack. In certain scenarios, the DoS attacker has complete control of the network, and thus the values of $l(i)$ can be solely decided by the actions of the attacker. In such scenarios, $l(i) = l_\mathrm{A}(i)$. If $l_\mathrm{A}(i) = 1$ for all $i \in \mathbb{N}_0$, then it means that all packets on the network fail to be transmitted. In the networked control problem, to achieve stabilization, some constraints on $l_\mathrm{A}(\cdot)$ were considered by Cetinkaya et al. [25] through the following assumption.

Assumption 4. *There exist scalars $\kappa_\mathrm{A} \geq 0$ and $\rho_\mathrm{A} \in [0,1)$ such that for every $t \in \mathbb{N}$,*

$$\sum_{i=0}^{t-1} l_\mathrm{A}(i) \leq \kappa_\mathrm{A} + \rho_\mathrm{A} t, \tag{21}$$

holds almost surely.

Assumption 4 is similar to Assumption 1 in the sense that the inequality in Equation (21) places a restriction on the total number attacks by a certain ratio of the total number of transmission attempts. The scalar ρ_A in this inequality is an upper-bound on the long-run average number of times the attacker attacks the network. As pointed out in [25], in the case of jamming, this scalar can be used for characterizing the energy use of the attacker and it is also related to the *jamming rate* mentioned in [86].

Notice that, in the context of jamming attacks, the formulation here corresponds to *reactive jamming*, where the attacker knows about the transmission times and directly attacks the network at those times.

It is mentioned in [14] that, in *reactive jamming*, the attacker monitors the channel and attacks it when a transmission is detected. This approach differs from *active jamming* attacks where the attacker's goal is to simply prevent the use of a communication channel even if the channel is not currently used. Furthermore, as mentioned in [87], there are also situations where the attacker can decide to attack based on the content of packets. Specifically, in selective jamming attacks discussed in [87], a part of the content of the packet being transmitted can become available to the attacker who can then use this information to decide whether to send jamming signals to cause failure in the delivery of this packet. A similar malicious behavior is also seen in multi-hop networks where malicious nodes can drop certain packets based on their content [88].

Notice that the characterization in Assumption 4 provides a model based on a constraint on the total number of failures due to DoS attacks and it does not describe particular attack strategies. In this sense, it differs from the probabilistic attack models (Bernoulli- and Markov-modulated cases) considered in [34,42], where the attack strategies are described through probability distributions.

The following result from [25] shows that DoS attack indicator processes $\{l_{\mathrm{A}}(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ satisfying Equation (21) belong to the class Λ_ρ for $\rho \in (\rho_{\mathrm{A}}, 1]$.

Proposition 5 ([25])**.** *Suppose* $\{l_{\mathrm{A}}(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ *satisfies Assumption 4 with* $\rho_{\mathrm{A}} \in [0,1)$*. Then,* $l_{\mathrm{A}} \in \Lambda_\rho$ *for any* $\rho \in (\rho_{\mathrm{A}}, 1]$*.*

Interestingly, the combination of non-malicious transmission failures and malicious DoS attacks can also be modeled with processes that belong to the class Λ_ρ for certain values of ρ. To see this, first let the failure indicator process $\{l(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ be given by

$$l(i) = \begin{cases} 1, & l_{\mathrm{R}}(i) = 1 \text{ or } l_{\mathrm{A}}(i) = 1, \\ 0, & \text{otherwise}, \end{cases} \qquad i \in \mathbb{N}_0. \tag{22}$$

The following result covers two cases: (1) non-malicious failures and DoS attacks occur independently, i.e., $l_{\mathrm{R}}(\cdot)$ and $l_{\mathrm{A}}(\cdot)$ are independent processesl and (2) the DoS attack strategy of the attacker may depend on non-malicious failures in the network, i.e., $l_{\mathrm{R}}(\cdot)$ and $l_{\mathrm{A}}(\cdot)$ are *not* independent.

Proposition 6 ([25])**.** *Consider a time-inhomogeneous Markov chain* $\{l_{\mathrm{R}}(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ *with transition probabilities that satisfy* $p_{q,0}(i) \leq p_0$ *and* $p_{q,1}(i) \leq p_1$*, for* $i \in \mathbb{N}_0$*, where* $p_0, p_1 \in (0,1)$*. Moreover, consider the process* $\{l_{\mathrm{A}}(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ *satisfying Assumption 4 with* $\rho_{\mathrm{A}} \in [0,1)$*. If* $l_{\mathrm{R}}(\cdot)$ *and* $l_{\mathrm{A}}(\cdot)$ *are independent processes and* $p_1 + p_0\rho_{\mathrm{A}} < 1$*, then* $l(\cdot)$ *given by Equation (22) satisfies* $l \in \Lambda_\rho$ *for* $\rho \in (p_1 + p_0\rho_{\mathrm{A}}, 1]$*. If, on the other hand,* $l_{\mathrm{R}}(\cdot)$ *and* $l_{\mathrm{A}}(\cdot)$ *are not independent processes and* $p_1 + \rho_{\mathrm{A}} < 1$*, then* $l(\cdot)$ *given by Equation (22) satisfies* $l \in \Lambda_\rho$ *for* $\rho \in (p_1 + \rho_{\mathrm{A}}, 1]$*.*

The proof of this result utilizes a key lemma (see Lemma A.1 in [25]), where Markov's inequality is used for obtaining Chernoff-type tail probability bounds for the term $\mathbb{P}\left[\sum_{i=0}^{t-1} l(i) > \rho t\right]$. In the literature, Chernoff-type bounds are essential in obtaining concentration inequalities for sums of random variables (see Section 1.9 in [89], Chapter 27 in [90], and [91]).

Notice that in the case where the DoS attack strategy of the attacker may depend on non-malicious failures in the network, $l \in \Lambda_\rho$ holds for larger values of ρ indicating that the average number of failures in the long run can be larger in that case. Ranges of ρ values associated with different transmission issues are illustrated in Figure 5.

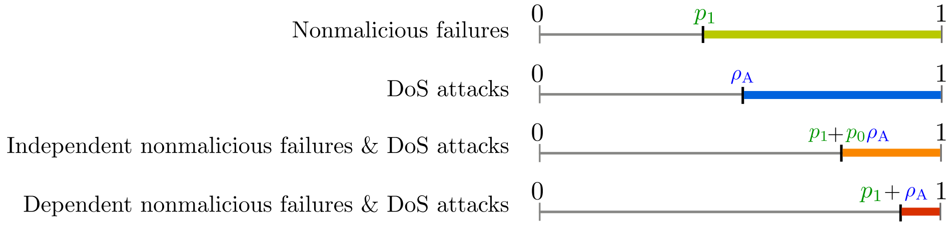

Figure 5. Ranges of ρ values for the class Λ_ρ. The ranges are different, when different transmission issues are considered in the network.

4.1. SINR-Based Probabilistic Jamming Models

The authors showed in [26] that the probabilistic approach to characterization of DoS attacks proposed in [25] is also useful for modeling jamming attacks in wireless channels. In particular, transmission failures caused by an energy-constrained jamming attacker can be described by utilizing an SINR-based model similar to those in [66,80,82]. Specifically, Cetinkaya et al. [26] explored a networked control problem where the transmission power of the control input packets and the power of the channel noise are fixed constants. On the other hand, the interference power of the jamming attacker is allowed to depend on time and represented by the process $\{v(i) \in [0,\infty)\}_{i\in\mathbb{N}_0}$. The likelihood of a transmission failure at a given time t_i depends on the interference power $v(i)$ of the attacker. If $v(i)$ is large, then a transmission failure becomes more likely.

Our work [26] utilizes a Borel-measurable, nondecreasing function $p\colon [0,\infty) \to [0,1]$ to describe the probability of failures. This function is used in the characterization of the transmission failure indicator $l(i)$ as

$$l(i) \triangleq \mathbb{1}[r(i) \le p(v(i))], \tag{23}$$

where $r(i)$ is a random variable that is uniformly distributed in $[0,1]$ for each $i \in \mathbb{N}_0$. It is important to observe that Equation (23) implies

$$\mathbb{P}[l(i) = 1 | v(i) = \vartheta] = p(\vartheta), \tag{24}$$

that is, the conditional failure probability given that the jamming attacker sets the interference power to $\vartheta \in [0,\infty)$ is represented by $p(\vartheta)$. It is assumed that $r(0), r(1), \ldots$ in Equation (23) are mutually independent so that failures occurring at different times are *conditionally independent* given the jamming interference powers at those times. In other words, for every $t_1 < t_2 < \cdots < t_k$, $k \in \mathbb{N}$,

$$\mathbb{P}[l(t_1) = 1, \cdots, l(t_k) = 1 | v(t_1) = \vartheta_1, \cdots, v(t_k) = \vartheta_k] = \prod_{i=1}^{k} \mathbb{P}[l(t_i) = 1 | v(t_i) = \vartheta_i].$$

In this setup, $l(\cdot)$ becomes a Bernoulli process with transmission failure probability $\mathbb{P}[l(t) = 1] = p(\vartheta)$, if $v(\cdot)$ is constant with $v(i) = \vartheta$, $i \in \mathbb{N}_0$.

Note that the function $p(\cdot)$ depends on SINR. For instance, if we consider the wireless channel setup in [66] (see Section 3.2.2), we set $p(v) = 2Q\Big(\sqrt{\alpha\frac{\zeta}{v+\sigma^2}}\Big)$ where $Q(x) \triangleq \frac{1}{\sqrt{2\pi}}\int_x^\infty e^{-\frac{s^2}{2}}\mathrm{d}s$, $\alpha > 0$, and $\zeta \in (0,\infty)$ and $\sigma^2 \in (0,1)$ are, respectively, the transmission power and the power of the channel noise in the SINR $\frac{\zeta}{v+\sigma^2}$.

The energy constraints of the attacker are captured in [26] by means of introducing the following assumption, which places a bound on the average jamming interference power.

Assumption 7. *There exist scalars $\kappa_{\mathrm{J}} \geq 0$ and $\overline{v}_{\mathrm{J}} \geq 0$ such that*

$$\mathbb{P}\Big[\sum_{i=0}^{t-1} v(i) \leq \kappa_{\mathrm{J}} + \overline{v}_{\mathrm{J}} t\Big] = 1, \quad t \in \mathbb{N}. \tag{25}$$

In this assumption, $\overline{v}_{\mathrm{J}} \geq 0$ characterizes the long-run upper-bound on the average interference power that can be utilized by the attacker. Moreover, $\kappa_{\mathrm{J}} \geq 0$ determines the attacker's initial capabilities. More specifically, $\limsup_{t\to\infty} \frac{1}{t}\sum_{i=0}^{t-1} v(i) \leq \overline{v}_{\mathrm{J}}$, almost surely. Furthermore, $\frac{1}{t}\sum_{i=0}^{t-1} v(i) \leq \frac{\kappa_{\mathrm{J}}}{t} + \overline{v}_{\mathrm{J}}$ for the first t transmission attempts. In [37], we considered a more restricted version of Assumption 7 to study the joint effects of jamming interference and disturbance in networked control systems. The following result shows that, under Assumption 7, the failure indicator process $l(\cdot)$ defined in Equation (23) belongs to the class Λ_ρ for certain values of ρ.

Theorem 8 ([26,36])**.** *Let $\hat{p}\colon [0,\infty) \to [0,1]$ be a continuous, nondecreasing, and concave function such that $\hat{p}(v) \geq p(v)$ for $v \in [0,\infty)$. Suppose that the transmission failure indicator $l(\cdot)$ is given by Equation (23), where the jamming interference power process $\{v(i) \in [0,\infty)\}_{i\in\mathbb{N}_0}$ satisfies Assumption (7) with $\overline{v}_{\mathrm{J}} \geq 0$. Then, $l \in \Lambda_\rho$ for $\rho \in (\hat{p}(\overline{v}_{\mathrm{J}}), 1]$.*

Theorem 8 indicates that the probabilistic characterization through the class Λ_ρ can also be utilized for wireless channels with SINR-based jamming models. Notice that the term $\hat{p}(\overline{v}_{\mathrm{J}})$ provides the lower bound of the range of ρ for which $l \in \Lambda_\rho$ holds. Here, $\hat{p}$ is a concave function that upper-bounds the transmission failure probability function p (see Figure 6 for an example), and $\overline{v}_{\mathrm{J}}$ is the upper bound of average jamming interference power. Theorem 8 is proved in [26] for the setup where the processes $\{r(i) \in [0,1]\}_{i\in\mathbb{N}_0}$ and $\{v(i) \in [0,\infty)\}_{i\in\mathbb{N}_0}$ are mutually independent. In the networked control problem discussed in Section 2.1.1, this assumption restricts the strategies of the attacker so that they are independent of the state and the control input information. Our recent work [36] shows that Theorem 8 also holds when $\{r(i) \in [0,1]\}_{i\in\mathbb{N}_0}$ and $\{v(i) \in [0,\infty)\}_{i\in\mathbb{N}_0}$ may depend on each other. The dependent case allows state-dependent attack strategies. In [36], a state-dependent attack strategy that maximizes the expected state norm in a rolling-horizon fashion is considered.

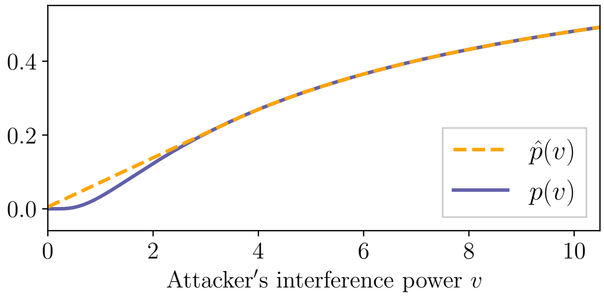

Figure 6. The transmission failure probability function p and a concave upper-bounding function $\hat{p}$ for an example wireless channel under jamming attacks.

4.2. Multi-Hop Network Models

In addition to SINR-based jamming models, the probabilistic characterization through the class Λ_ρ can be employed for modeling transmission failures in multi-hop networks. A multi-hop network (similar to those considered on the right diagram in Figure 1) can be represented by a directed acyclic graph $\mathcal{G} \triangleq (\mathcal{V}, \mathcal{E})$, where $\mathcal{V}$ is the set of nodes, and $\mathcal{E} \subset \mathcal{V} \times \mathcal{V}$ is the set of edges. Note that $\mathcal{V}$ and $\mathcal{E}$, respectively, represent the set of communication devices and the set of communication links. On a multi-hop network, data packets are transmitted over paths, which are sequences of non-repeating edges. Specifically, a *path* $\mathcal{P}$ from a node $v_1 \in \mathcal{V}$ to another node $v_h \in \mathcal{V}$ is given as

$\mathcal{P} = \big((v_1, v_2), (v_2, v_3), \ldots, (v_{h-1}, v_h)\big)$. Notice that there may be multiple paths between two nodes, and, moreover, those paths may be utilized in transmission of the same data.

It is shown in our previous work [27] that the class Λ_ρ can be utilized in modeling failures on individual links as well as paths and entire graphs. Specifically, in [27], a network $\mathcal{G}$ with source v_{P} (corresponding to the plant) and sink v_{C} (corresponding to the controller) ia considered (see Figure 7). The paths between nodes v_{P} and v_{C} are identified as $\mathcal{P}_1, \mathcal{P}_2, \ldots, \mathcal{P}_{|\mathcal{G}|}$, where $|\mathcal{G}|$ denotes the total number of paths. Moreover, the individual links on the ith path are denoted as $\mathcal{P}_{i,1}, \mathcal{P}_{i,2}, \ldots, \mathcal{P}_{i,|\mathcal{P}_i|}$, where $|\mathcal{P}_i|$ is the number of links on path $\mathcal{P}_i$. Transmission failures on those links can be represented by binary-valued failure indicator processes $l_{\mathcal{P}_i}^{\mathcal{P}_{i,j}}(\cdot)$. Similarly, overall failures on each path $\mathcal{P}_i$ can be represented with an indicator process $l_{\mathcal{P}_i}(\cdot)$, and, moreover, the failures of transmission between nodes v_{P} and v_{C} on network $\mathcal{G}$ can be represented with a binary-values indicator process $l_{\mathcal{G}}$. Notice that $l_{\mathcal{G}}(t) = l_{\mathcal{P}_1}(t) \wedge l_{\mathcal{P}_2}(t) \wedge \cdots \wedge l_{\mathcal{P}_{|\mathcal{G}|}}(t)$ and $l_{\mathcal{P}_i}(t) = l_{\mathcal{P}_i}^{\mathcal{P}_{i,1}}(t) \vee l_{\mathcal{P}_i}^{\mathcal{P}_{i,2}}(t) \vee \cdots \vee l_{\mathcal{P}_i}^{\mathcal{P}_{i,|\mathcal{P}_i|}}(t)$.

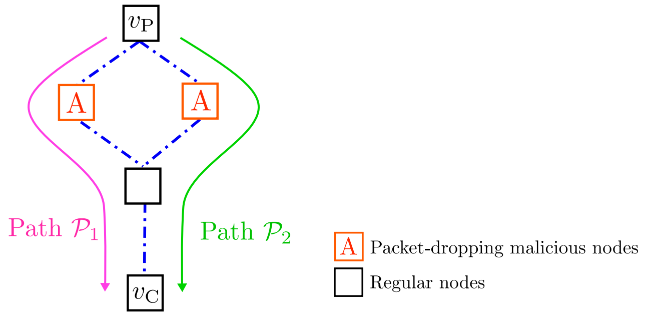

Figure 7. A multi-hop network between the plant (v_{P}) and the controller (v_{C}). State measurement packets on this network are transmitted over two paths $\mathcal{P}_1$ and $\mathcal{P}_2$, which are both subject to malicious packet-dropping attacks.

The following result is obtained in [27] to show that the class Λ_ρ can be used for characterizing the failure indicators for each individual link as well as the paths that include those links.

Proposition 9 ([27]). *Suppose* $l_{\mathcal{P}_i}^{\mathcal{P}_{i,j}} \in \Lambda_{\rho_{\mathcal{P}_i}^{\mathcal{P}_{i,j}}}$, $j \in \{1, \ldots, |\mathcal{P}_i|\}$, *where* $\rho_{\mathcal{P}_i}^{\mathcal{P}_{i,j}} \in [0, 1]$ *and* $j \in \{1, \ldots, |\mathcal{P}_i|\}$ *satisfy* $\sum_{j=1}^{|\mathcal{P}_i|} \rho_{\mathcal{P}_i}^{\mathcal{P}_{i,j}} \leq 1$. *Then,* $l_{\mathcal{P}_i} \in \Lambda_{\rho_{\mathcal{P}_i}}$ *with* $\rho_{\mathcal{P}_i} \triangleq \sum_{j=1}^{|\mathcal{P}_i|} \rho_{\mathcal{P}_i}^{\mathcal{P}_{i,j}}$.

The next result shows that the overall failures on a network $\mathcal{G}$ can be characterized with the class Λ_ρ where the ρ value is identified as the minimum of $\rho_{\mathcal{P}_i}$ obtained for each path $\mathcal{P}_i$ on the network $\mathcal{G}$.

Proposition 10 ([27]). *Suppose* $l_{\mathcal{P}_i} \in \Lambda_{\rho_{\mathcal{P}_i}}$ *for each path* $\mathcal{P}_i$ *where* $\rho_{\mathcal{P}_i} \in [0, 1]$. *Then,* $l_{\mathcal{G}} \in \Lambda_{\rho_{\mathcal{G}}}$ *with* $\rho_{\mathcal{G}} \triangleq \min_{i \in \{1, \ldots, |\mathcal{G}|\}} \rho_{\mathcal{P}_i}$.

In [27], we present additional results, where more specific models for non-malicious failures and DoS attacks can be utilized in characterization of the network. It is important to note that in [27], we provide different methods to handle transmission failures due to data corruption and those due to packet dropping. In wireless multi-hop networks, data-corruption can be due to jamming attacks on the communication links, whereas packet-dropping issues are typically due to malicious nodes conducting blackhole or grayhole attacks (see [9]) and non-malicious routing protocols to avoid congestion.

5. An Overview of Attack-Resilient Control and Communication Techniques

In this section, we provide an overview on some of the recently developed control and communication techniques that aim to achieve resiliency against DoS attacks. These techniques rely on the modeling and analysis approaches discussed in previous sections.

5.1. Resilient Control Approaches

In what follows, we discuss event-triggered control schemes as well as predictor and buffer-based control frameworks.

5.1.1. Event-Triggered Control

In the literature, one of the most common control strategies used against denial-of-service attacks is the *event-triggered* control. In the design and the analysis of event-triggered control schemes, the attack models presented in Sections 3 and 4.1 are utilized.

In particular, for the continuous-time networked control problem discussed in Section 2.1.2, De Persis and Tesi [48] provided an event-triggered control mechanism that achieves asymptotic stabilization under any attack strategy that satisfies Assumptions 1 and 2. In their approach, a transmission of the state information is triggered when the error between the current state $x(t)$ and the previously transmitted state exceeds a certain threshold.

It is mentioned in [48] that the event-triggering approach requires continuous monitoring of the state. Specifically, there is a need to continuously monitor the state $x(t)$ to check if the triggering condition is satisfied or not. To avoid continuous monitoring, self-triggering approach is helpful. In the self-triggering approach proposed in [48], the predicted value of the state is used for calculating the next transmission time t_{k+1}. Notice that under DoS attacks, some of the transmissions may fail. The triggering approach in [48] takes into account the status of transmissions. If, for instance, the transmission attempt at time t_k fails, then the next transmission is attempted shortly afterwards. If, on the other hand, the transmission at time t_k is successful, the next transmission can be made after a longer duration. The parameters of the triggering schemes in [48] are designed to ensure that the overall control system is stable. Specifically, Lyapunov-function techniques are utilized for obtaining sufficient conditions concerning the event-triggering parameters that ensure global asymptotic stability under DoS attacks.

An interesting resilient event-triggered control strategy is proposed in [49]. In one of the scenarios considered in that work, jamming attacks on a communication channel happen periodically where the attacker repeats cycles of jamming and sleeping. For such attacks, control and transmission strategy in [49] can identify the transition times between jamming and sleeping states of the attack; thus, it allows selection of times where the communication is guaranteed to be successful. As a result, number of transmission attempts is further reduced.

In addition, event-triggered control of a discrete-time networked control system (see Section 2.1.1) is explored in our previous works [25,38]. There, a Lyapunov-like function is utilized for determining the triggering time instants. Specifically, consider $V\colon \mathbb{R}^n \to [0,\infty)$ given by $V(x) \triangleq x^{\mathrm{T}}Px$, where $P > 0$. The network transmissions are attempted at times $t_0 = 0$, and t_i, $i \in \mathbb{N}$, given by

$$t_{i+1} \triangleq \min\Big\{t \in \{\tau_i + 1, \tau_i + 2, \ldots\} \colon t \geq t_i + \theta \;\text{ or }\; V(Ax(t) + Bu(t_i)) > \beta V(x(t_i))\Big\}, \tag{26}$$

where $\theta \in \mathbb{N}$ and $\beta \in [0,1)$ are parameters of the event-triggered controller. The triggering condition $V(Ax(t) + Bu(t_i)) > \beta V(x(t_i))$ guarantees that $V(x(t))$ stays within certain limits after a successful transmission at time t_i. As indicated in Theorem 11, the scalar β can be chosen so that when the transmission attempt at time t_i is successful, then the closed-loop system shows stable behavior and the state goes inside a level set $\{x \in \mathbb{R}^n \colon V(x) = \beta V(x(t_i))\}$ at the next time instant. This is illustrated in Figure 8 (left). Furthermore, the next transmission event is triggered only when the state is predicted to leave this level set. For the example case shown Figure 8 (right), a transmission event is triggered at time $t_i + 3$. If, on the other hand, the transmission at time t_i is unsuccessful (see Figure 8, right), another transmission may be triggered in the next time instant if $V(Ax(t_i + 1) + Bu(t_i)) > \beta V(x(t_i))$. Notice that in this case the state trajectory indicates unstable behavior due to lack of control input in the system.

For the probabilistic network characterizations discussed in Section 4, sufficient stability conditions under the event-triggered control framework in [25] are provided in the following result.

Theorem 11 ([25])**.** *Consider the linear dynamical system in Equation (1). Suppose that the transmission failure indicator $\{l(i) \in \{0,1\}\}_{i\in\mathbb{N}_0}$ satisfies $l \in \Lambda_\rho$ with scalar $\rho \in [0,1]$. If there exist a matrix $K \in \mathbb{R}^{m\times n}$, a positive-definite matrix $P \in \mathbb{R}^{n\times n}$, and scalars $\beta \in (0,1)$, $\varphi \in [1,\infty)$ such that*

$$(A+BK)^{\mathrm{T}}P(A+BK) - \beta P \le 0, \tag{27}$$

$$A^{\mathrm{T}}PA - \varphi P \le 0, \tag{28}$$

$$(1-\rho)\ln\beta + \rho\ln\varphi < 0, \tag{29}$$

then the event-triggered control law in Equations (3) and (26) guarantees almost sure asymptotic stability of the zero solution $x(t) \equiv 0$ of the closed-loop system dynamics.

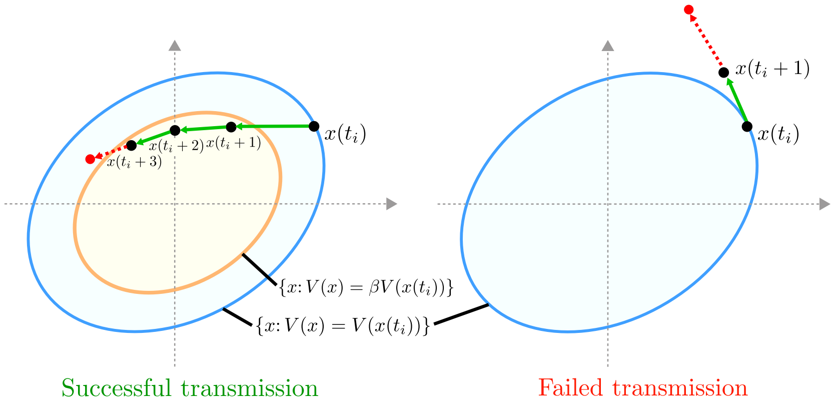

Figure 8. Illustration of the event-triggering approach in [25] for the cases of successful and failed transmissions at time t_i. A transmission is triggered at time t_{i+1} when the state is predicted to make the move indicated with red dotted lines. In the case of successful transmissions (**Left**), the state is guaranteed to stay inside the level set $\{x \in \mathbb{R}^n\colon V(x) = \beta V(x(t_i))\}$ in between two event-triggering instants.

The scalars $\beta \in (0,1)$ and $\varphi \in [1,\infty)$ in the conditions in Equations (27) and (28) of Theorem 11 characterize upper bounds on the growth of the Lyapunov-like function $V(x) = x^{\mathrm{T}}Px$, when the system evolves with the closed-loop dynamics (corresponding to a successful transmission) and open-loop dynamics (corresponding to a transmission failure). Notice that since $\beta < 1$ and $\ln\beta < 0$, if ρ is sufficiently small, then Equation (29) holds indicating stability. Based on the conditions of Theorem 11, our work [25] also provides a method for designing the scalar β and the positive-definite matrix P that are utilized in the event-triggering condition in Equation (26). The proof of Theorem 11 is based on a technique similar to that used for obtaining upper bounds of *top Lyapunov exponents* (see [92,93]) of stochastic dynamical systems. In [28], we provided a less conservative analysis approach based on a lifting technique. There, the stability of the system is checked by solving a linear programming problem.

5.1.2. Control Frameworks with Predictors and Buffers

To mitigate the effects of DoS attacks in an output-feedback networked control problem, Feng and Tesi [51] introduced a controller with a predictor and an impulsive observer. In that work, the output $y(t)$ of the system in Equations (4) and (5) is measured periodically and transmitted over a network that faces DoS attacks. Moreover, the control input packets are assumed to be transmitted over a secure network.

In [51], the system dynamics involve disturbance, and the transmitted output measurements can be noisy. The observer and the predictor at the controller side are designed in a way to ensure that accurate state estimates are obtained at the controller side after a certain number of successful transmissions. In particular, in the case without disturbance and noise, the state estimate at the controller matches the actual state if μ number of consecutive output measurements can be received at the controller side, where $\mu \in \{1, \ldots, n\}$ is the observability index of the pair $(e^{A\Delta}, C)$ with Δ denoting the output measurement/transmission period. When μ consecutive measurements are not available, the knowledge of the system dynamics is utilized in the predictor to predict future state values.

For this framework, it is shown in [51] that the closed-loop system stability can be preserved under any attack strategy satisfying the constraints in Equations (15) and (16), if the scalars $\rho_{\mathrm{D}}, \rho_{\mathrm{F}}$ in those constraints also satisfy $\rho_{\mathrm{D}} + \Delta\rho_{\mathrm{F}} < 1 - (\mu - 1)\Delta\rho_{\mathrm{F}}$. It is important to note that this condition is independent of the choice of control gain. Note also that if instead of the output measurements, the state measurements are sent to the controller (i.e., $\mu = 1$), then the condition takes the form

$$\rho_{\mathrm{D}} + \Delta\rho_{\mathrm{F}} < 1. \tag{30}$$

This inequality shows that the predictor based approach guarantees stability regardless of the dynamics of the open-loop and the closed-loop systems.

When the control input packets are transmitted over channels that also face DoS, the right-hand side of the condition in Equation (30) is replaced by a term that depends on system dynamics. The work in [50] considers such scenarios, where DoS attacks affect the delivery of both control and measurement packets. There, a buffer is utilized at the plant side. The controller at each time sends the current control input together with future control inputs. When there is no DoS attack, the transmitted control input packets are placed in the buffer so that they can be utilized later when the attacker becomes active and blocks transmissions. It is shown in [50] that for sufficiently large buffer sizes, the closed-loop stability can be guaranteed for attacks that satisfy the condition in Equation (30).

5.2. Resilient Communication Techniques

Besides the event-based communication approaches discussed in Section 5.1.1, there are a few other communication techniques specifically developed for achieving resiliency in multi-agent consensus as well as in networked state estimation problems. In what follows, we provide an overview of those protocols.

5.2.1. Self-Triggered and Randomized Communication Techniques in Multi-Agent Consensus

In [71,73], the authors explored the multi-agent consensus problem in Section 2.3, where the network is subject to jamming attacks. In those works, one of the deterministic attack models discussed in Section 3.1 is utilized, and a self-triggered communication rule is developed. The utility of the self-triggered approach is that with self-triggering, inter-agent communications are asynchronous and agents are not required to possess synchronized clocks. Furthermore, the self-triggered communication technique provides resiliency against a large class of attack strategies.

In the self-triggered communication technique, the $(k+1)$th communication attempt time t_{k+1}^{i} for the agent i is determined based on the information available to agent i at time t_{k}^{i}. If the i agent knows its neighbors' values at time t_{k}^{i}, then it uses this information in designing the next communication attempt time t_{k+1}^{i}. If, on the other hand, no information is available at t_{k}^{i} (due to jamming attacks), the ith agent sets the waiting time until t_{k+1}^{i} to be a fixed duration.

The minimum interval between consecutive communication attempts of all agents is given in [71] by $\Delta^{*} > 0$. It is noted in [71] that consensus can be achieved under any attack strategy subject to the constraints in Equations (15) and (16) with scalars ρ_{D} and ρ_{F} that satisfy

$$\rho_{\mathrm{D}} + \Delta^{*}\rho_{\mathrm{F}} < 1. \tag{31}$$

The inequality in Equation (31) guarantees that the average duration and the average frequency of attacks are sufficiently small. Note that, if the attacker can attack at a frequency that is larger than the frequency of communication attempts (i.e., $\rho_{\mathrm{F}} > \frac{1}{\Delta^*}$), then the attacker may be able to block all attempts of communication by the agents. The reason is that the attacker may actually be knowledgeable on the self-triggered mechanism used by the agents for deciding the times t_k^i. This would allow the attacker to attack the network directly at those instants for very short durations. In such cases, the attacker can preserve energy and satisfy Equation (15) for arbitrarily small ρ_{D}.

To achieve resilient consensus against attacks with high frequency, [72] proposed a randomized communication strategy. The key idea in the randomized setting is that the agents pick their communication times randomly (see Figure 9). In particular, each agent i, first picks a deterministic interval length $\Delta^i > 0$. Then, for each $k \in \mathbb{N}_0$, the communication attempt time t_k^i is selected as a random variable that is uniformly distributed in the interval $[k\Delta^i, (k+1)\Delta^i)$.

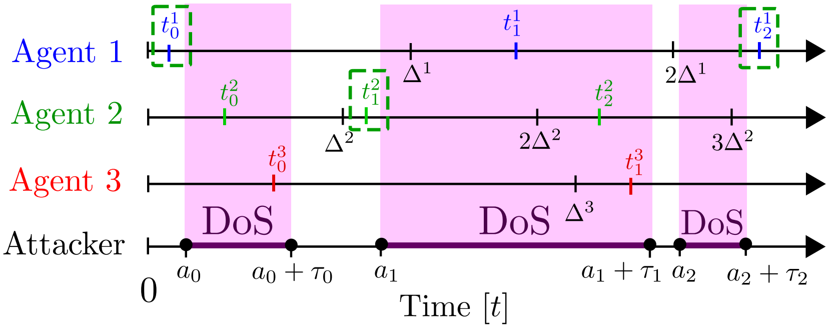

Figure 9. Illustration of the randomized communication protocol, where each agent attempts communicating with its neighbors at random time instants. At time instants denoted inside rectangles with green dashed borders, the communication attempts can avoid DoS attacks.

Randomized transmissions prevent the attacker to know about future communication attempt times of agents. It is shown in [72] that consensus in the randomized communication setting is achieved if the attack constraint in Equation (15) holds with ρ_{D} that satisfy

$$\rho_{\mathrm{D}} < 1. \tag{32}$$

In other words, the randomized communication approach guarantees consensus under any attack strategy that is only constrained in its average duration as in Equation (15) regardless of its frequency.

5.2.2. Fake Acknowledgement Messages in State Estimation

In a networked state estimation problem, an interesting communication technique was considered by Ding et al. [65]. In the problem formulation, Ding et al. [65] considered an estimator that attempts to transmit state estimates to a remote receiver over an insecure wireless channel. The decision to attempt transmission or not is made by the estimator in a stochastic fashion by setting a probability value $\theta_{\mathrm{S}}(t) \in [0,1]$ such that a transmission attempt at time t is made with probability $\theta_{\mathrm{S}}(t)$.

When a transmission attempt is made at time t, it is not guaranteed that it will be successful due to the jamming attacks on the channel. The likelihood of a transmission failure is determined based on the power level of the jamming interference signal emitted to the wireless channel by the attacker at that time instant.

The goal in [65] is to minimize the time-averaged variance of the estimation error. To this end, Ding et al. [65] proposed the idea of generating a *fake acknowledgement message sequence* $\{\phi(t) \in \{0,1\}\}_{t\in\mathbb{N}}$. Instead of sending real acknowledgements, the receiving node follows the fake acknowledgement sequence and sends back to the sensor acknowledgement messages that are possibly misleading for the attacker. For instance, if $\phi(t) = 1$, the receiving node sends a positive acknowledgement indicating that a packet is successfully received, even if no packet is received at time t. Under certain assumptions on the jamming interference powers, the work [65] derives the optimal transmission attempt probabilities $\{\theta_{\mathrm{S}}(t)\}_{t\in\mathbb{N}}$ as well as the optimal fake acknowledgement message sequence $\{\phi(t)\}_{t\in\mathbb{N}}$ that minimizes the time-averaged variance of the estimation error. It is shown that fake acknowledgements improve the estimation performance.

5.2.3. Design of Routing Protocols to Ensure Security Against DoS

As discussed in [94,95], denial-of-service can be a big problem in the delivery of packets in multi-hop networks. To increase the resilience of multi-hop networks against attacks, several works proposed routing protocols. In particular, for the case of mobile ad hoc networks (MANET), where the network topology is time-varying, the authors of [12,96,97] developed routing protocols that can avoid certain attacks. In the protocol developed in [12], each node keeps a list of weights for its communication links, and these weights are utilized for detecting faulty/attacked links and discovering reliable communication paths. Sanzgiri et al. [96] showed that authentication based techniques with cryptographic certificates can be utilized for detection of malicious and faulty nodes. Moreover, Bianchi et al. [97] proposed a routing mechanism that is based on identifying potentially cooperating malicious nodes that launch blackhole attacks in a multi-hop network. In the context of multi-hop networked control, the detection of malicious nodes and their isolation is explored in [45,46].

We note that, in addition to the attack-resilient control and communication techniques discussed above, there are also a few works that focus on denial-of-service attack detection in control systems. In particular, the authors of [63,98] discussed threshold-based attack detection mechanisms, and the analysis of transmission failure patterns to distinguish strategic attacks and non-malicious failures was explored by Cetinkaya et al. [26]. In addition, Ali et al. [99] recently considered methods from information technologies for detecting and mitigating distributed DoS attacks against networked control systems.

6. Conclusions

In this paper, we present an overview of the literature on denial-of-service attacks in control systems. In particular, we present a list of problems considered by researchers in the fields of networked control, networked state estimation, and multi-agent consensus. We provide a discussion on deterministic and game-theoretic approaches to modeling attacks on networks. We then focus on a probabilistic approach for characterizing the attacks in wireless channels as well as multi-hop networks. The notion of constraints can be considered as a common theme that connects the different modeling approaches. In particular, the cost of attacks and the energy available to the attacker play a role in most of the derived models. We discuss the utility of these models for analyzing the security of existing systems as well as for developing new attack-resilient control and communication techniques.

It appears that the detection problem for DoS attacks can be an interesting future research topic in control-system studies. Thus far, this problem has been explored in only a few works, and we think that some of the techniques from information technologies can be useful in investigation of DoS attack detection and mitigation problems in control systems if the dynamical properties of the system can also be taken into account.

As more and more control systems are expected to incorporate wireless technologies, it seems that the risk of DoS will also increase, making cyber-security of control systems against DoS an even more important research field.

Funding: This work was supported in part by JSPS under Grant-in-Aid for Scientific Research Grant No. 18H01460 and by the JST CREST Grant No. JPMJCR15K3.

Conflicts of Interest: The authors declare no conflicts of interest.

References

1. Cárdenas, A.A.; Amin, S.; Sastry, S. Research challenges for the security of control systems. In Proceedings of the 3rd Conference on Hot Topics in Security, San Jose, CA, USA, 28 July–1 August 2008.
2. Sandberg, H.; Amin, S.; Johansson, K.H. Special issue on cyberphysical security in networked control systems. *IEEE Control Syst. Mag.* **2015**, *35*.
3. Teixeira, A.; Shames, I.; Sandberg, H.; Johannson, K.H. A secure control framework for resource-limited adversaries. *Automatica* **2015**, *51*, 135–148. [CrossRef]
4. Zhang, L.; Zhang, H. A survey on security and privacy in emerging sensor networks: From viewpoint of close-loop. *Sensors* **2016**, *16*, 443. [CrossRef]
5. Lun, Y.Z.; D'Innocenzo, A.; Smarra, F.; Malavolta, I.; Di Benedetto, M.D. State of the art of cyber-physical systems security: An automatic control perspective. *J. Syst. Softw.* **2019**, *149*, 174–216.
6. Mo, Y.; Garone, W.; Casavola, A.; Sinopoli, B. False data injection attacks against state estimation in wireless sensor networks. In Proceedings of the 49th IEEE Conference on Decision and Control (CDC), Atlanta, GA, USA, 15–17 December 2010; pp. 5967–5972.
7. Teixeira, A.; Pérez, D.; Sandberg, H.; Johansson, K.H. Attack models and scenarios for networked control systems. In Proceedings of the 1st International Conference on High Confidence Networked Systems, Beijing, China, 17–18 April 2012; pp. 55–64.
8. Fawzi, H.; Tabuada, P.; Diggavi, S. Secure estimation and control for cyber-physical systems under adversarial attacks. *IEEE Trans. Autom. Control* **2014**, *59*, 1454–1467. [CrossRef]
9. Jhaveri, R.H.; Patel, S.J.; Jinwala, D.C. DoS attacks in mobile ad hoc networks: A survey. In Proceedings of the 2012 Second International Conference on Advanced Computing & Communication Technologies, Rohta, India, 7–8 January 2012; pp. 535–541.
10. Mahmoud, M.M.E.A.; Shen, X.S. *Security for Multi-hop Wireless Networks*; Springer: New York, NY, USA, 2014.
11. Marti, S.; Giuli, T.J.; Lai, K.; Baker, M. Mitigating routing misbehavior in mobile ad hoc networks. In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking, Boston, MA, USA, 6–11 August 2000; pp. 255–265.
12. Awerbuch, B.; Holmer, D.; Nita-Rotaru, C.; Rubens, H. An on-demand secure routing protocol resilient to Byzantine failures. In Proceedings of the 1st ACM Workshop on Wireless Security, Atlanta, GA, USA, 28 September 2002; pp. 21–30.
13. Just, M.; Kranakis, E.; Wan, T. Resisting malicious packet dropping in wireless ad hoc networks. In Proceedings of the International Conference on Ad-Hoc Networks and Wireless, Montreal, QC, Canada, 8–10 October 2003; pp. 151–163.
14. Xu, W.; Ma, K.; Trappe, W.; Zhang, Y. Jamming sensor networks: Attack and defense strategies. *IEEE Netw.* **2006**, *20*, 41–47.
15. Pelechrinis, K.; Iliofotou, M.; Krishnamurty, S.V. Denial of Service attacks in wireless networks: The case of jammers. *IEEE Commun. Surv. Tut.* **2011**, *13*, 245–257. [CrossRef]
16. Fragkiadakis, A.; Askoxylakis, I.; Chatziadam, P. Denial-of-Service attacks in wireless networks using off-the-shelf hardware. In Proceedings of the nternational Conference on Distributed, Ambient, and Pervasive Interactions, Heraklion, Greece, 22–27 June 2014; pp. 427–438.
17. Mizrak, A.T.; Savage, S.; Marzullo, K. Detecting malicious packet losses. *IEEE Trans. Parallel Distrib. Syst.* **2009**, *20*, 191–206. [CrossRef]
18. Shu, T.; Krunz, M. Privacy-preserving and truthful detection of packet dropping attacks in wireless ad hoc networks. *IEEE Trans. Mob. Comput.* **2015**, *14*, 813–828. [CrossRef]
19. Wood, A.D.; Stankovic, J.A. Denial of service in sensor networks. *Computer* **2002**, *35*, 54–62. [CrossRef]
20. Loukas, G.; Öke, G. Protection against denial of service attacks: A survey. *Comput. J.* **2010**, *53*, 1020–1037. [CrossRef]
21. Mahjabin, T.; Xiao, Y.; Sun, G.; Jiang, W. A survey of distributed denial-of-service attack, prevention, and mitigation techniques. *Int. J. Distrib. Sens. Netw.* **2017**, *13*, 1–32. [CrossRef]
22. Zargar, S.T.; Joshi, J.; Tipper, D. A survey of defense mechanisms against distributed Denial of Service (DDoS) flooding attacks. *IEEE Commun. Surv. Tut.* **2013**, *15*, 2046–2069. [CrossRef]

23. Dong, Y.; Zhou, P. Jamming attacks against control systems: A survey. In *Intelligent Computing, Networked Control, and Their Engineering Applications, Proceedings of the International Conference on Life System Modeling and Simulation (LSMS 2017) and International Conference on Intelligent Computing for Sustainable Energy and Environment (ICSEE 2017), Nanjing, China, 22–24 September 2017*; Springer: Singapore, 2017; pp. 566–574.
24. Peng, C.; Sun, H.; Yang, M.; Wang, Y.L. A survey on security communication and control for smart grids under malicious cyber attacks. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**. [CrossRef]
25. Cetinkaya, A.; Ishii, H.; Hayakawa, T. Networked control under candom and malicious packet losses. *IEEE Trans. Autom. Control* **2017**, *62*, 2434–2449. [CrossRef]
26. Cetinkaya, A.; Ishii, H.; Hayakawa, T. The effect of time-varying jamming interference on networked stabilization. *SIAM J. Control Optim.* **2018**, *56*, 2398–2435. [CrossRef]
27. Cetinkaya, A.; Ishii, H.; Hayakawa, T. A probabilistic characterization of random and malicious failures communication failures in multi-Hop networked control. *SIAM J. Control Optim.* **2018**, *56*, 2398–2435. [CrossRef]
28. Cetinkaya, A.; Ishii, H.; Hayakawa, T. Analysis of stochastic switched systems with application to networked control under jamming attacks. *IEEE Trans. Autom. Control* **2019**. [CrossRef]
29. Kellett, C.M.; Mareels, I.M.Y.; Nešic, D. Stability results for networked control systems subject to packet dropouts. *IFAC Proc. Vol.* **2005**, *38*, 73–78. [CrossRef]
30. Hespanha, J.P.; Naghshtabrizi, P.; Xu, Y. A survey of recent results in networked control systems. *Proc. IEEE* **2007**, *95*, 138–172. [CrossRef]
31. Gupta, V.; Martins, N.C.; Baras, J.S. Optimal output feedback control using two remote sensors over erasure channels. *IEEE Trans. Autom. Control* **2009**, *54*, 1463–1476. [CrossRef]
32. Okano, K.; Ishii, H. Stabilization of uncertain systems with finite data rates and Markovian packet losses. *IEEE Trans. Control Netw. Syst.* **2014**, *1*, 298–307. [CrossRef]
33. Schenato, L.; Sinopoli, B.; Franceschetti, M.; Poolla, K.; Sastry, S.S. Foundations of control and estimation over lossy networks. *Proc. IEEE* **2007**, *95*, 163–187. [CrossRef]
34. Amin, S.; Cárdenas, A.A.; Sastry, S.S. Safe and secure networked control systems under denial-of-service attacks. In Proceedings of the 12th International Conference on Hybrid Systems: Computation and Control (HSCC), San Francisco, CA, USA, 13–15 April 2009; pp. 31–45.
35. Lai, S.; Chen, B.; Li, T.; Yu, L. Packet-based state feedback control under DoS attacks in cyber-physical systems. *IEEE Trans. Circuits Syst. II* **2019**. doi:10.1109/TCSII.2018.2881984. [CrossRef]
36. Cetinkaya, A.; Ishii, H.; Hayakawa, T. State-dependent jamming interference in networked stabilization. In Proceedings of the 2018 IEEE Conference on Decision and Control (CDC), Miami Beach, FL, USA, 17–19 December 2018, pp. 7249–7254.
37. Cetinkaya, A.; Ishii, H.; Hayakawa, T. Wireless networked control facing combined effects of disturbance and jamming interference. In Proceedings of the 23rd International Symposium on Mathematical Theory of Networks and SystemsHong Kong University of Science and Technology, Hong Kong, China, 16–20 July 2018; pp. 387–392.
38. Cetinkaya, A.; Ishii, H.; Hayakawa, T. Event-Triggered output feedback control resilient against jamming attacks and random packet losses. *IFAC-PapersOnLine* **2015**, *22*, 270–275. [CrossRef]
39. Wakaiki, M.; Cetinkaya, A.; Ishii, H. Quantized output feedback stabilization under DoS attacks. In Proceedings of the 2018 Annual American Control Conference (ACC), Milwaukee, WI, USA, 27–29 June 2018; pp. 6487–6492.
40. Liu, S.; Li, S.; Xu, B. Event-triggered resilient control for cyber-physical system under denial-of-service attacks. *Int. J. Control* **2018**, 1–13. [CrossRef]
41. Zhang, H.; Cheng, P.; Shi, L.; Chen, J. Optimal denial-of-service attack scheduling against linear quadratic Gaussian control. In Proceedings of the 2014 American Control Conference, Portland, OR, USA, 4–6 June 2014; pp. 3996–4001.
42. Befekadu, G.K.; Gupta, V.; Antsaklis, P.J. Risk-sensitive control under Markov modulated Denial-of-Service (DoS) attack strategies. *IEEE Trans. Autom. Control* **2015**, *60*, 3299–3304. [CrossRef]
43. Li, H.; Lai, L.; Qiu, R.C. A denial-of-service jamming game for remote state monitoring in smart grid. In Proceedings of the 45th Annual Conference on Information Sciences and Systems, Baltimore, MD, USA, 23–25 March 2011; pp. 1–6.

44. Smarra, F.; Benedetto, M.D.D.; D'Innocenzo, A. A sub-optimal method for routing redundancy design over lossy networks. *IFAC-PapersOnLine* **2017**, *50*, 2604–2609. [CrossRef]
45. D'Innocenzo, A.; Di Benedetto, M.D.; Serra, E. Fault tolerant control of multi-hop control networks. *IEEE Trans. Autom. Control* **2013**, *58*, 1377–1389. [CrossRef]
46. D'Innocenzo, A.; Smarra, F.; Di Benedetto, M.D. Resilient stabilization of multi-hop control networks subject to malicious attacks. *Automatica* **2016**, *71*, 1–9. [CrossRef]
47. De Persis, C.; Tesi, P. Resilient control under Denial-of-Service. *IFAC Proc. Vol.* **2014**, *47*, 134–139. [CrossRef]
48. De Persis, C.; Tesi, P. Input-to-state stabilizing control under denial-of-service. *IEEE Trans. Autom. Control* **2015**, *60*, 2930–2944. [CrossRef]
49. Shisheh Foroush, H.; Martínez, S. On triggering control of single-input linear systems under pulse-width modulated DoS signals. *SIAM J. Control Optim.* **2016**, *54*, 3084–3105. [CrossRef]
50. Feng, S.; Tesi, P. Networked control systems under denial-of-service: Co-located vs. remote architectures. *Syst. Control Lett.* **2017**, *108*, 40–47. [CrossRef]
51. Feng, S.; Tesi, P. Resilient control under denial-of-service: Robust design. *Automatica* **2017**, *79*, 42–51. [CrossRef]
52. Lu, A.Y.; Yang, G.H. Input-to-state stabilizing control for cyber-physical systems with multiple transmission channels under denial of service. *IEEE Trans. Autom. Control* **2018**, *63*, 1813–1820. [CrossRef]
53. De Persis, C.; Tesi, P. Networked control of nonlinear systems under denial-of-service. *Syst. Control Lett.* **2016**, *96*, 124–131. [CrossRef]
54. Dolk, V.S.; Tesi, P.; De Persis, C.; Heemels, W.P.M.H. Event-triggered control systems under denial-of-service attacks. *IEEE Trans. Control Netw. Syst.* **2017**, *4*, 93–105. [CrossRef]
55. Kato, R.; Cetinkaya, A.; Ishii, H. Stabilization of nonlinear networked control systems under denial-of-service attacks: A linearization approach. *Proc. Amer. Control Conf.* **2019**, (to appear).
56. An, L.; Yang, G.H. Decentralized adaptive fuzzy secure control for nonlinear uncertain interconnected systems against intermittent DoS attacks. *IEEE Trans. Cybern.* **2018**, *49*, 827–838. [CrossRef]
57. Feng, S.; Tesi, P.; De Persis, C. Towards stabilization of distributed systems under denial-of-service. In Proceedings of the IEEE 56th Annual Conference on Decision and Control (CDC), Melbourne, VIC, Australia, 12–15 December 2017; pp. 5360–5365.
58. Tomic, I.; Breza, M.J.; Jackson, G.; Bhatia, L.; McCann, J.A. Design and evaluation of jamming resilient cyber-physical systems. In Proceedings of the IEEE International Conference on Cyber, Physical and Social Computing (CPSCom), Halifax, NS, Canada, 30 July–3 August 2018.
59. Weitenberg, E.; De Persis, C.; Monshizadeh, N. Exponential convergence under distributed averaging integral frequency control. *Automatica* **2018**, *98*, 103–113. [CrossRef]
60. Peng, C.; Li, J.; Fei, M. Resilient event-triggering H_∞ load frequency control for multi-area power systems with energy-limited DoS attacks. *IEEE Trans. Power Syst.* **2017**, *32*, 4110–4118. [CrossRef]
61. Feng, S.; Cetinkaya, A.; Ishii, H.; Tesi, P.; De Persis, C. Data rates for stabilizing control under denial-of-service attacks. *Proc. Amer. Control Conf.* **2019**, (to appear), arXiv:1809.04892.
62. Li, Y.; Shi, L.; Cheng, P.; Chen, J.; Quevedo, D.E. Jamming attacks on remote state estimation in cyber-physical systems: A game-theoretic approach. *IEEE Trans. Autom. Control* **2015**, *60*, 2831–2836. [CrossRef]
63. Zhang, H.; Cheng, P.; Shi, L.; Chen, J. Optimal denial-of-service attack scheduling with energy constraint. *IEEE Trans. Autom. Control* **2015**, *60*, 3023–3028. [CrossRef]
64. Qin, J.; Li, M.; Shi, L.; Yu, X. Optimal denial-of-service attack scheduling with energy constraint over packet-dropping networks. *IEEE Trans. Autom. Control* **2018**, *63*, 1648–1663. [CrossRef]
65. Ding, K.; Ren, X.; Shi, L. Deception-based sensor scheduling for remote estimation under DoS attacks. *IFAC-PapersOnLine* **2016**, *49*, 169–174. [CrossRef]
66. Li, Y.; Quevedo, D.E.; Dey, S.; Shi, L. SINR-based DoS attack on remote state estimation: A game-theoretic approach. *IEEE Trans. Control Netw. Syst.* **2017**, *4*, 632–642. [CrossRef]
67. Ding, K.; Li, Y.; Quevedo, D.E.; Dey, S.; Shi, L. A multi-channel transmission schedule for remote state estimation under DoS attacks. *Automatica* **2017**, *78*, 194–201. [CrossRef]
68. Yang, C.; Yang, W.; Shi, H. DoS attack in centralised sensor network against state estimation. *IET Control Theory Appl.* **2018**, *12*, 1244–1253. [CrossRef]
69. Guo, Z.; Shi, D.; Johansson, K.H.; Shi, L. Optimal linear cyber-attack on remote state estimation. *IEEE Trans. Control Netw. Syst.* **2017**, *4*, 4–13. [CrossRef]

70. Guan, Y.; Ge, X. Distributed attack detection and secure estimation of networked cyber-physical systems against false data injection attacks and jamming attacks. *IEEE Trans. Signal Inf. Process Netw.* **2018**, *4*, 48–59. [CrossRef]
71. Senejohnny, D.; Tesi, P.; De Persis, C. Self-triggered coordination over a shared network under denial-of-service. In Proceedings of the 54th IEEE Conference on Decision and Control (CDC), Osaka, Japan, 15–18 December 2015; pp. 3469–3474.
72. Kikuchi, K.; Cetinkaya, A.; Hayakawa, T.; Ishii, H. Stochastic communication protocols for multi-agent consensus under jamming attacks. In Proceedings of the IEEE 56th Annual Conference on Decision and Control (CDC), Melbourne, VIC, Australia, 12–15 December 2017; pp. 1657–1662.
73. Senejohnny, D.; Tesi, P.; De Persis, C. A jamming-resilient algorithm for self-triggered network coordination. *IEEE Trans. Control Netw. Syst.* **2017**, *5*, 981–990. [CrossRef]
74. Feng, Z.; Hu, G. Distributed secure average consensus for linear multi-agent systems under DoS attacks. In Proceedings of the American Control Conference (ACC), Seattle, WA, USA, 24–26 March 2017; pp. 2261–2266.
75. Nugraha, Y.; Cetinkaya, A.; Hayakawa, T.; Ishii, H.; Zhu, Q. Subgame perfect equilibrium analysis for jamming attacks on resilient graphs. *Proc. Amer. Control Conf.* **2019**, (to appear).
76. Alpcan, T.; Başar, T. *Network Security: A Decision and Game-Theoretic Approach*; Cambridge University Press: Cambrifge, UK, 2010.
77. Gupta, A.; Nayyar, A.; Langbort, C.; Başar, T. A dynamic transmitter-jammer game with asymmetric information. In Proceedings of the IEEE 51st IEEE Conference on Decision and Control (CDC), Maui, HI, USA, 10–13 December 2012; pp. 6477–6482.
78. Bhattacharya, S.; Gupta, A.; Başar, T. Jamming in mobile networks: A game-theoretic approach. *J. Num. Algeb. Control Optim.* **2013**, *3*, 1–30.
79. Zhu, Q.; Saad, W.; Han, Z.; Poor, H.V.; Başar, T. Eavesdropping and jamming in next-generation wireless networks: A game-theoretic approach. In Proceedings of the IEEE MILCOM 2011 Military Communications Conference, Baltimore, MD, USA, 7–10 November 2011; pp. 119–124.
80. Zhang, H.; Qi, Y.; Wu, J.; Fu, L.; He, L. DoS attack energy management against remote state estimation. *IEEE Trans. Control Netw. Syst.* **2018**, *5*, 383–394. [CrossRef]
81. Yang, H.; Shi, M.; Xia, Y.; Zhang, P. Security research on wireless networked control systems subject to jamming attacks. *IEEE Trans. Cybern.* **2018**, 1–10. [CrossRef] [PubMed]
82. Liu, H. SINR-based multi-channel power schedule under DoS attacks: A Stackelberg game approach with incomplete information. *Automatica* **2019**, *100*, 274–280. [CrossRef]
83. Chen, J.; Touati, C.; Zhu, Q. A dynamic game analysis and design of infrastructure network protection and recovery. *ACM SIGMETRICS Perf. Eval. Rev.* **2017**, *45*, 125–128. [CrossRef]
84. Ishii, H. Limitations in remote stabilization over unreliable channels without acknowledgements. *Automatica* **2009**, *45*, 2278–2285. [CrossRef]
85. Klenke, A. *Probability Theory: A Comprehensive Course*; Springer: Berlin/Heidelberg, Germany, 2008.
86. Anantharamu, L.; Chlebus, B.S.; Kowalski, D.R.; Rokicki, M.A. Medium access control for adversarial channels with jamming. In Proceedings of the 18th International Colloquium SIROCCO, Gdańsk, Poland, 26–29 June 2011; pp. 89–100.
87. Proano, A.; Lazos, L. Packet-hiding methods for preventing selective jamming attacks. *IEEE Trans. Depend. Secure Comput.* **2012**, *9*, 101–114. [CrossRef]
88. Xiao, B.; Yu, B.; Gao, C. CHEMAS: Identify suspect nodes in selective forwarding attacks. *J. Parallel Distr. Com.* **2007**, *67*, 1218–1230. [CrossRef]
89. Billingsley, P. *Probability and Measure*; Wiley: Hoboken, NJ, USA, 2012.
90. Kallenberg, O. *Foundations of Modern Probability*; Springer: New York, NY, USA; Berlin/Heidelberg, Germany, 2001.
91. McDiarmid, C. Concentration. In *Probabilistic Methods for Algorithmic Discrete Mathematics*; Springer: Berlin/Heidelberg, Germany, 1998; pp. 195–248.
92. Fang, Y.; Loparo, K.; Feng, X. Stability of discrete time jump linear systems. *J. Math. Syst. Estim. Control* **1995**, *5*, 275–321.

93. Bolzern, P.; Colaneri, P.; De Nicolao, G. On almost sure stability of discrete-time Markov jump linear systems. In Proceedings of the IEEE 43rd IEEE Conference on Decision and Control (CDC) (IEEE Cat. No.04CH37601), Nassau, Bahamas, 14–17 December 2004; pp. 3204–3208.
94. Karlof, C.; Wagner, D. Secure routing in wireless sensor networks: Attacks and countermeasures. In Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications, Anchorage, AK, USA, 11 May 2003; pp. 113–127.
95. Singh, A.; Kalita, K.P.; Medhi, S.P. Blackhole attack on MANET and its effects. In Proceedings of the 5th International Conference on Computing for Sustainable Global Development, New Delhi, India, 14–16 March 2018; pp. 1–5.
96. Sanzgiri, K.; Dahill, B.; Levine, B.N.; Shields, C.; Belding-Royer, E.M. A secure routing protocol for ad hoc networks. In Proceedings of the 10th IEEE International Conference on Network Protocols, Paris, France, 12–15 November 2002; pp. 78–87.
97. Bianchi, A.; Pizzutilo, S.; Vessio, G. Intercepting blackhole attacks in MANETs: An ASM-based model. In Proceedings of the International Conference on Software Engineering and Formal Methods, Trento, Italy, 4–5 September 2017; pp. 137–152.
98. Zhang, H.; Qi, Y.; Zhou, H.; Zhang, J.; Sun, J. Testing and defending methods against DoS attack in state estimation. *Asian J. Control* **2017**, *19*, 1295–1305. [CrossRef]
99. Ali, Y.; Xia, Y.; Ma, L.; Hammad, A. Secure design for cloud control system against distributed denial of service attack. *Control Theory Tech.* **2018**, *16*, 14–24. [CrossRef]