2015 American Control Conference
Palmer House Hilton
July 1-3, 2015. Chicago, IL, USA

Jamming-Based Adversarial Control of Network Flow Allocation: A Passivity Approach

Phillip Lee, Andrew Clark, Basel Alomair, Linda Bushnell, and Radha Poovendran

Abstract— **Wireless cyber-physical systems are vulnerable to jamming attacks, in which an adversary broadcasts an interfering signal in the vicinity of a receiver, causing packet decoding errors and reducing the throughput of the communication. Reduced throughput and increased delay could violate the real-time constraints of cyber-physical systems. In a flow redirection attack, an adversary jams a set of network links in order to cause network sources to divert traffic to links that are controlled by the adversary, enabling higher-layer attacks. In this paper, we introduce a passivity approach for modeling the flow redirection attack. Using our approach, we identify a class of dynamic jamming strategies for flow redirection, in which the adversary updates the probability of jamming based on the rate of flow traversing the link. We provide sufficient conditions for feasibility of the jamming strategies for energy-constrained adversaries, and develop an efficient algorithm for deriving an optimal jamming strategy for a given network and desired flow allocation. Our results are illustrated via a numerical study.**

I. Introduction

Cyber-physical systems (CPS), including wide-area monitoring in the smart grid, require real-time information exchange between distributed components [1]. This information exchange is increasingly provided by wireless networks. The use of a shared medium, however, leaves wireless networks vulnerable to medium-exploiting attacks. In a jamming attack [2], an adversary broadcasts an interfering signal in the vicinity of a receiver, thus preventing transmitted packets from being correctly decoded. All network flows traversing a jammed link will experience lower throughput and increased end-to-end latency.

Network sources respond to increases in latency by reallocating flows to lower-latency paths [3]. This approach mitigates the attack by leveraging the spatial diversity provided by multiple disjoint paths. Intelligent adversaries may exploit this behavior, however, by jamming specific links in order to redirect traffic to nodes that collude with, or have been compromised by, an adversary [4], [5]. Once a sufficient amount of network flow traverses these compromised or colluding nodes, an adversary can mount effective, stealthy attacks on higher-layer services, including man-in-the-middle attacks [5], [6] that can violate the real-time constraints of cyber-physical systems [7]. We denote this as the *flow-redirecting jamming attack*.

Current models for the impact of jamming focus on jamming individual links [2], [8], while network flow redirection affects the overall end-to-end performance of source-destination pairs. Existing work on flow jamming considers an adversary whose main goal is to reduce throughput and increase delay [9], as opposed to redirecting network flows towards compromised links.

In this paper, we develop a control-theoretic approach for modeling flow-redirecting jamming attacks on wireless networks. In our approach, from the adversary's perspective, the flow allocation by the network sources is modeled as a plant, while jamming at targeted network links acts as a control input. We formulate the adversary's goal of redirecting network flows to compromised links as introducing a control input to steer the system towards a desired equilibrium state, which represents a flow allocation where a desired rate of flow traverses compromised links. Modeling flow-redirection in a control-theoretic language enables integration of the attack into models of cyber-physical systems.

Developing a jamming strategy for flow redirection attacks poses two challenges. First, the network flow allocation by the sources in response to changes in network delays exhibits nonlinear dynamics [3]. Second, the feasible jamming strategies are limited by the power constraints of the adversary.

In order to resolve these challenges, we introduce passivity-based dynamic jamming strategies in which the adversary updates the jamming probability based on the rate of flow traversing each link. We show that our passivity-based jamming strategies guarantee convergence to the adversary's desired network flow under nonlinear flow allocation dynamics. We identify a class of physically relevant jamming strategies that can be represented as passive dynamical systems.

We formulate the optimal jamming strategy as the solution to a convex optimization problem. The power limitations of the adversary are mapped to constraints on the feasible jamming strategy. We prove that, if there exists a jamming strategy that satisfies a given power constraint and achieves a desired flow allocation, then a passivity-based jamming strategy can be constructed with the same power constraint, implying that the passivity-based approach is optimal in terms of power consumption. Our approach is illustrated through a numerical study.

The paper is organized as follows. Section III describes the network and adversary models, and gives needed background on passivity. Section IV presents a problem formulation for

P. Lee, A. Clark, L. Bushnell, and R. Poovendran are with the Department of Electrical Engineering, University of Washington, Seattle, WA 98195 USA. {leep3, awclark, lb2, rp3}@uw.edu

B. Alomair is with the National Center for Cybersecurity Technology, King Abdulaziz City for Science and Technology, Riyadh, Saudi Arabia. alomair@kacst.edu.sa

This work was supported by ONR grant N00014-14-1-0029, NSF grant CNS-1446866, and a grant from the King Abdulaziz City for Science and Technology (KACST).

the flow redirection attack. Section V contains our passivity-based approach to redirecting the flow to a desired operating point via jamming. Section VI includes our numerical results. Section VII concludes the paper.

II. Related Work

Jamming attacks and mitigation strategies have been studied in both security and control research communities [5], [10]. Impact of jamming at the physical layer in terms of bit error rate has been studied in [2], and analysis of jamming impact on higher layers including media access control (MAC) and network layers has been studied in [5], [9]. Existing jamming mitigation strategies are diversity-based mechanisms that utilize either the channel diversity in the frequency domain [2] or spatial diversity in the network [9].

In existing works, the goal of a jamming attack is to minimize the network throughput subject to power constraints, and efficient jamming mechanisms have been studied in the optimization framework in [9]. The feasibility of jamming attack to redirect the network flow into adversarial region, thus exposing the redirected traffic to higher-layer attacks, have been introduced in [4], [5], [6]. Currently, however, there exists no analytical framework to study the feasibility and efficient jamming strategies for the flow redirection attacks.

Control and game theory have been used to study the impact of jamming on cyber-physical systems in [10], [11], [12] where the impact of jamming is modeled as unavailability of sensor measurements or control packets.

Passivity-based approaches for rate allocation [13] and control of networked CPS [14] have been proposed in the absence of security threats. In [15], a passivity framework was used to study the impact of wormhole attacks on network flows. The impact of jamming, however, was not considered.

III. Model and Preliminaries

In this section, we present the network and adversary models, as well as background on passivity.

A. Network Model

We consider a network with n source-destination pairs, indexed in the set $\{s_1, \ldots, s_n\}$. The set of network links is denoted $\mathcal{L}$, with $|\mathcal{L}| = L$. Each link $l \in \mathcal{L}$ has a capacity c_l. Each source s_i has a set of paths $\mathcal{P}_i$; we let $\mathcal{P} = \bigcup_{i=1}^{n} \mathcal{P}_i$, and $m_i = |\mathcal{P}_i|$, with $m = \sum_i m_i$. We define the $n \times m$ path matrix H by $H_{ip} = 1$ if path p is used by source i and $H_{ip} = 0$ otherwise. The $L \times m$ routing matrix A is defined by $A_{lp} = 1$ if link l belongs to path p and 0 otherwise. We let $x_p(t)$ denote the flow allocated to path p at time t, and $\mathbf{x}(t)$ denote the vector of flow allocations. Each source s_i chooses $x_p(t)$ for all $p \in \mathcal{P}_i$ at each time t. The vector $\mathbf{z} = A\mathbf{x}$ is the vector of flows allocated to each link, where z_l is the flow allocated to link l. The vector $\mathbf{y} = H\mathbf{x}$ is the total flow allocated to all sources. The link capacity constraints imply that $\mathbf{z} = A\mathbf{x} \leq \mathbf{c}$.

The limited capacities of the links leads to delays. For each link l, the function $\sigma_l : \mathbb{R} \to \mathbb{R}$ is defined such that $\sigma_l(z_l)$ is equal to the delay experienced on link l when the flow rate is equal to z_l. The delay function considered in this work is given as [3]

$$\sigma_l(z_l) = \left(\frac{z_l}{c_l}\right)^{\beta} \tag{1}$$

where $\beta > 1$.

B. Adversary Model

The network is assumed to be attacked by one or more distributed, coordinating jammers. Each jammer can eavesdrop on a link until a packet is observed and then broadcast an interfering signal in order to prevent the packet from being decoded (reactive jammer [2]). We assume that the interfering signal has sufficient power to cause the packet to be jammed with probability 1. The adversary is assumed to have knowledge of the network topology, link capacities, and flow rates allocated to each link. Furthermore, the flow allocation algorithms of the sources are assumed to be known by the adversary, so that the adversary can predict how the sources will react to a jamming attack.

The adversary is assumed to be power-constrained, with total power budget P_j and cost α_l to jam one bit of flow on link l. The cost α_l is determined by the adversary's distance to the receiver, the path-loss of the environment, and the anti-jamming mechanisms employed by the nodes comprising the link. Letting v_l denote the number of times that each packet is jammed on link l (due to retransmissions), the adversary's power constraint is modeled as the inequality $\sum_{l \in \mathcal{L}} \alpha_l v_l z_l \leq P_j$.

The adversary is assumed to control a subset of links $\mathcal{L}' \subseteq \mathcal{L}$. A link is controlled by the adversary if one or both of the nodes comprising the links has been compromised by or colludes with the adversary. The goal of the adversary is to redirect the network flows to links in $\mathcal{L}'$, in order to mount higher-layer attacks [6], [16].

C. Background on Passivity

In this section, we give relevant background on passive systems. The definitions and lemmas below can be found in [17]. We first define passivity for a state-space model of the form

$$(\Sigma) \begin{cases} \dot{x}(t) = f(x(t), u(t)) \\ y(t) = g(x(t), u(t)) \end{cases}$$

Definition 1: ([18]) The state space model (Σ) is passive if there exists a C^1 storage function V such that, for any state x, $\dot{V}(x) \leq -S(x) + u(t)^T y(t)$, where $S(x)$ is a positive semidefinite function.

A system is strictly passive if the function $S(x)$ in Definition 1 is positive definite. The following lemma gives composition rules for passive systems.

Lemma 1: ([18]) A parallel interconnection of two passive systems (H_1) and (H_2) is passive. In addition, a negative feedback interconnection of (H_1) and (H_2) is passive.

Stability analysis via passivity is enabled by the following.

Lemma 2: ([18]) A negative feedback interconnection of a strictly passive system and a passive system is globally asymptotically stable.

IV. Control-Theoretic Framework for Flow Redirection

We assume that each source s_i has an associated utility function $U_{s_i}(y_{s_i})$ which is concave and monotonically increasing in y_{s_i}, the total transmission rate of s_i. Each source s_i observes the end-to-end path delay of path $r_i \in \mathcal{P}_i$ and updates flow rate per each path via the following dynamics

$$\dot{x}_{r_i} = \left(U'_{s_i}(y_{s_i}) - \sum_{l \in r_i} \sigma_l(z_l, v_l) \right)^{x_{r_i}}_{+} \tag{2}$$

where

$$(f(x))^{x_{r_i}}_{+} = \begin{cases} 0, & x_{r_i} = 0 \text{ and } f(x) < 0 \\ f(x), & \text{else} \end{cases}$$

Eq. (2) can be interpreted as a gradient ascent, where each source aims to maximize the utility function U_{s_i} subject to the capacity constraint of each link l. It was shown in [3] that under the flow allocation dynamics (2), $\mathbf{x}(t)$ converges to the solution of an optimization problem

$$\max \sum_{i=1}^{n} U_{s_i}(y_{s_i}) - \sum_{l} \int_0^{z_l} \sigma_l(\tau) d\tau$$
$$\text{subject to } \mathbf{y} = \mathbf{A}\mathbf{x}, \mathbf{z} = \mathbf{H}\mathbf{x}$$

The impact of jamming on each link l is modeled as a reduction in capacity c_l, and the resulting increase of delay at link l. We assume that the delay at link l is written as

$$\sigma_l(z_l, v_l) = \left(\frac{z_l}{c_l} \right)^{\beta} (v_l + 1)$$

In the absence of any jamming at link l ($v_l = 0$), the delay function reduces to $\sigma_l(z_l)$.

The impact of jamming on flow allocation dynamics can be written as the following. For each route r_i,

$$\dot{x}_{r_i} = \left(U'_{s_i}(y_{s_i}) - \sum_{l \in r_i} \sigma_l(z_l) + \sum_{l \in r_i} \sigma_l(z_l) - \sum_{l \in r_i} \sigma_l(z_l, v_l) \right)^{x_{r_i}}_{+}$$

The flow allocation dynamics can be simplified to

$$\dot{x}_{r_i} = \left(U'_{s_i}(y_{s_i}) - \sum_{l \in r_i} \sigma_l(z_l) + \sum_{l \in r_i} \sigma_l(z_l)(v_l) \right)^{x_{r_i}}_{+}$$

The v_l can be interpreted as the adversarial control exerted by jammers at link l, and we define the parameter $u_l = v_l$. From the adversary's perspective, the flow allocation can be viewed as a state-space system defined by

$$(\Sigma) \begin{cases} \dot{\mathbf{x}}(t) = f(\mathbf{x}(t)) + g(\mathbf{x}(t))\mathbf{u}(t) \\ \mathbf{y}(t) = \mathbf{x}(t) \end{cases} \tag{3}$$

The goal of the jammer is to choose the signal $\mathbf{u}(t)$ in order to stabilize the system at the flow allocation $\mathbf{x}^*$.

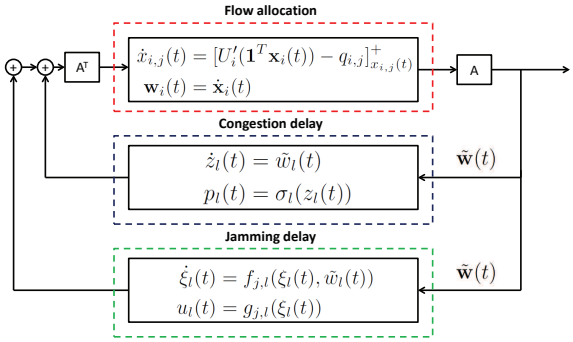


Fig. 1. Decomposition of network flow dynamics under jamming attack into flow allocation, congestion delay, and jamming delay components. The decomposition enables passivity-based design of the optimal jamming strategy.

V. Passivity Approach to Optimal Jamming Strategy

In this section, we present a passivity-based approach for optimal jamming by the adversary. The goal of the adversary is to introduce a control input $\mathbf{u}(t)$ that drives the network flow rates to the adversary's desired allocation $\mathbf{x}^*$, while satisfying the adversary's power constraints at each time t. In Section V-A, we present a decomposition of the network flow allocation and link delay dynamics, and prove the passivity properties of each component of the decomposed model. In Section V-B, we formulate a passivity-based jamming strategy of the adversary and prove that this jamming strategy drives the flow allocation to the desired equilibrium point. Section V-C incorporates the adversary's power constraint into our framework by presenting an efficient approach to designing a jamming strategy that guarantees the desired equilibrium point while satisfying the adversary's power constraints.

A. Decomposition of Flow Allocation and Jamming

We decompose the dynamical system of (3) into three components, the *flow allocation*, *congestion delay*, and *jamming delay* (Figure 1). The flow allocation component contains the flow allocation by the network sources, with state variables $x_{i,j}(t)$ representing the rate of flow allocated by sources s_i to path $p_j \in \mathcal{P}_i$. It takes as input the total delay $q_{i,j}$ on each path, and has state dynamics $\dot{x}_{i,j}(t) = [U'(\mathbf{1}^T\mathbf{x}_i) - q_{i,j}]^+_{x_{i,j}}$ as in Section IV. The output of the flow allocation is the rate of change of the flow allocation, $\dot{x}_{i,j}(t)$. This output is multiplied by the routing matrix A to yield the rate of change of the flow allocation on each link, $\tilde{w}_l(t) \triangleq \dot{z}_l(t)$. The signal $\tilde{w}_l(t)$ acts as input to the remaining components.

The second component consists of the delays due to congestion, and takes as input the rate of change in the flow allocation at each link, $\tilde{w}_l(t)$. The state is equal to the flow allocated to the link, $z_l(t)$, and hence the state is equal to the integral of the input. Since the delay is an increasing function σ_l of the incoming flow rate, the delay dynamics are given by $p_l(t) = \sigma_l(z_l(t))$.

The final component consists of the delays due to jamming by the adversary. In its most general form, the adversary's jamming strategy has an internal state $\xi_l(t)$ for each link, with dynamics $\dot{\xi}_l(t) = f_{j,l}(\xi_l(t), \tilde{w}_l(t))$. The output is the additional delay in link l due to jamming, denoted $u_l(t)$, which is a function of the current state $\xi_l(t)$ and the input $\tilde{w}_l(t)$.

B. Passivity-Based Jamming Strategy

We now describe the passivity-based approach to designing the jamming strategy. Since the goal of the adversary's strategy is to drive the flow allocation to a desired point $\mathbf{x}^*$, we first introduce a sufficient condition for $\mathbf{x}^*$ to be a fixed point of the dynamics (Σ) in Figure 1.

Lemma 3: Let $\boldsymbol{\xi}^*$ satisfy $f_{j,l}(\xi_l, 0) = 0$ for all $l \in \mathcal{L}$, and define $\mathbf{u}^* = g_j(\boldsymbol{\xi}^*)$, $p_l^* = \sigma_l(z_l^*)$, $\mathbf{p}^* = \{p_l^* : l \in \mathcal{L}\}$, and $\mathbf{q}^* = A^T(\mathbf{p}^* + \mathbf{u}^*)$. If $U_i'(\mathbf{1}^T\mathbf{x}_i^*) = q_{ij}^*$ for all $i = 1, \ldots, n$ and $j = 1, \ldots, m_i$, then $(\mathbf{x}^*, \boldsymbol{\xi}^*)$ is an equilibrium point of the dynamics in Figure 1.

Proof: It suffices to show that all of the state variables of Figure 1 achieve equilibrium at the point $(\mathbf{x}^*, \boldsymbol{\xi}^*)$. By assumption, $U_i'(\mathbf{1}^T\mathbf{x}_i^*) = q_{ij}^*$ for all $i = 1, \ldots, n$ and $j = 1, \ldots, m_i$, and hence $\dot{x}_{i,j} = 0$ for all $i = 1, \ldots, n$ and $j = 1, \ldots, m_i$. Since $\tilde{\omega}_l(t) = A\dot{\mathbf{x}}(t) = 0$, $\dot{z}_l(t) = 0$ for all $l \in \mathcal{L}$, and hence z_l reaches a fixed point. Finally, since $f_{j,l}(\xi_l^*, 0) = 0$ for all $l \in \mathcal{L}$, the state $\boldsymbol{\xi}(t)$ is in equilibrium as well. ■

Let $\mathbf{q}^*$ be the vector of path costs satisfying $q_{ij}^* = U_i'(\mathbf{1}^T\mathbf{x}_i^*)$ for all $i = 1, \ldots, n$, $j = 1, \ldots, m_i$. The following theorem defines a class of jamming strategies that are guaranteed to converge to the desired state $\mathbf{x}^*$.

Theorem 1: Define a jamming strategy by $f_{j,l}(\xi_l, \tilde{w}_l) = \tilde{w}_l$. Choose $g_{j,l}(\xi_l) = \tilde{\sigma}_l(\xi_l) - \sigma_l(\xi_l)$, where $\tilde{\sigma}_l$ is an increasing function satisfying $\tilde{\sigma}_l(z_l^*) = u_l^*$ and $\mathbf{u}^*$ satisfies $A^T(\mathbf{u}^* + \mathbf{p}^*) = q^*$. Then $\lim_{t\to\infty} \mathbf{x}(t) = \mathbf{x}^*$.

Proof: By Lemma 3, $\mathbf{x}^*$ is an equilibrium point. The remainder of the proof is in two parts. We first show that, for appropriate choice of input and output, each of the three blocks in Figure 1 is a passive dynamical system. We then leverage the fact that a negative feedback interconnection of passive systems is globally asymptotically stable to prove that the system converges to the equilibrium $\mathbf{x}^*$.

Consider the component (H_1). We show that (H_1) is passive from input $-(\mathbf{q} - \mathbf{q}^*)$ to output $\mathbf{w}$. Defining

$$V_1(\mathbf{x}) = \sum_{i=1}^{n} \left(U_i(\mathbf{1}^T\mathbf{x}_i^*) - U_i(\mathbf{1}^T\mathbf{x}_i)\right) + (\mathbf{q}^*)^T(\mathbf{x} - \mathbf{x}^*),$$

we have

$$\begin{aligned}
\dot{V}_1 &= -\left(\sum_{i=1}^{n} U_i'(\mathbf{1}^T\mathbf{x}_i)\right)^T \dot{\mathbf{x}}_i + (\mathbf{q}^*)^T\mathbf{x} \\
&= -\left(\sum_{i=1}^{n} U_i'(\mathbf{1}^T\mathbf{x}_i)\dot{\mathbf{x}}_i\right) + \mathbf{q}^T\dot{\mathbf{x}} + (\mathbf{q}^* - \mathbf{q})^T\dot{\mathbf{x}} \\
&= -||\dot{\mathbf{x}}||_2^2 + (\mathbf{q} - \mathbf{q}^*)^T\dot{\mathbf{x}} \leq -(\mathbf{q} - \mathbf{q}^*)^T\dot{\mathbf{x}}
\end{aligned}$$

implying passivity of (H_1).

We now show that the bottom two blocks can be viewed jointly as a passive system with input $\tilde{\mathbf{w}}$ and output $(\mathbf{p} + \mathbf{u} - \mathbf{p}^* - \mathbf{u}^*)$. Define a storage function equal to

$$V_2(\mathbf{z}, \boldsymbol{\xi}) = \sum_{l\in\mathcal{L}} \int_0^{z_l - z_l^*} \tilde{\sigma}_l(\tau_l + z_l^*) - \tilde{\sigma}_l(z_l^*)\, d\tau_l.$$

We then have

$$\begin{aligned}
\dot{V}_2(\mathbf{z}, \boldsymbol{\xi}) &= \sum_{l\in\mathcal{L}} (\tilde{\sigma}_l(z_l) - \tilde{\sigma}_l(z_l^*))\tilde{w}_l \\
&= \sum_{l\in\mathcal{L}} (\sigma_l(z_l) + g_{j,l}(\xi_l) - \sigma_l(z_l^*) - g_{j,l}(\xi_l^*))\tilde{w}_l \\
&= \tilde{\mathbf{w}}^T(\mathbf{p} + \mathbf{u} - \mathbf{p}^* - \mathbf{u}^*)
\end{aligned}$$

establishing passivity of the joint dynamics of (H_2) and (H_3).

Hence, under these jamming dynamics, the overall system (3) illustrated in Figure 1 can be viewed as a negative feedback interconnection of passive systems, and hence is globally asymptotically stable, with equilibrium point $\mathbf{x}^*$. ■

Theorem 1 provides a simple jamming strategy in which the adversary's control input at each link is an increasing function of the flow traversing the link. The jammer dynamics are sufficient to guarantee that the network flow reaches the desired allocation $\mathbf{x}^*$. The theorem, however, does not incorporate the power constraints of the adversary, and hence may provide an infeasible jamming strategy. In the following section, we present an approach to selecting the function $\tilde{\sigma}(\cdot)$ in order to satisfy the resource constraints of the adversary.

C. Incorporating Power Constraint of Adversary

When constructing the adversary's jamming strategy $\tilde{\sigma}_l$, we first observe that the function must be increasing in z_l. The next requirement is that the point $\mathbf{x}^*$ is an equilibrium. Define $\tilde{\boldsymbol{\sigma}}^* = \{\tilde{\sigma}_l^{(m_l)} : l \in \mathcal{L}\}$. The equilibrium requirement can then be stated as $\mathbf{q}^* = A^T\tilde{\boldsymbol{\sigma}}^*$, where $\mathbf{q}^*$ is defined as in Theorem 1.

The final requirement is the power constraint. As described in Section III-B, the adversary's power constraint is given by

$$\sum_{l\in\mathcal{L}} \alpha_l v_l(z_l) z_l \leq P_j, \tag{4}$$

where α_l is the cost to jam each packet, v_l is the expected number of times to jam each packet, and z_l is the rate of flow traversing link l. In order to ensure feasibility of the jamming strategy, we require that this constraint is satisfied for each feasible flow allocation, i.e., each $\mathbf{z}$ satisfying $\mathbf{z} = A\mathbf{x}$ and $\mathbf{z} \leq \mathbf{c}$. The following theorem defines a construction for the functions $\tilde{\sigma}_l$ that guarantees that all of the constraints are satisfied.

Theorem 2: Suppose that there exists $\tilde{\boldsymbol{\sigma}}^*$ such that $A^T\tilde{\boldsymbol{\sigma}}^* = \mathbf{q}^*$, $\tilde{\sigma}_l^* \geq \sigma_l(z_l^*)$, and

$$\sum_{l\in\mathcal{L}} \left(\left(\frac{c_l}{z_l^*}\right)^{\beta} \tilde{\sigma}_l^* - 1\right) \alpha_l z_l < P_j. \tag{5}$$

Then there exists a set of functions $\{\sigma_l : l \in \mathcal{L}\}$ that satisfies the conditions of Theorem 1 and the power constraint (4).

Proof: We prove that a function exists of the form

$$\tilde{\sigma}_l(z_l) = \begin{cases} \sigma_l(z_l), & z_l \in [0, z_l^* - \epsilon) \\ \frac{\tilde{\sigma}_l^* - \sigma_l(z_l^* - \epsilon)}{\epsilon}(\sigma_l - \sigma_l^*) + \tilde{\sigma}_l^*, & z_l \in [z_l^* - \epsilon, z_l^*] \\ \max\left\{\sigma_l(z_l), \tilde{\sigma}_l^* + \epsilon(z_l - z_l^*)\right\}, & z_l \in (z_l^*, \infty) \end{cases} \tag{6}$$

for some $\epsilon > 0$. We observe that the function $\tilde{\sigma}_l$ is increasing as a function of z_l for all $l \in \mathcal{L}$. By construction, $\tilde{\sigma}_l(z_l^*) = \tilde{\sigma}_l^*$ for all $l \in \mathcal{L}$ and $A^T\tilde{\boldsymbol{\sigma}}^* = \mathbf{q}^*$. Hence, the conditions of Theorem 1 are satisfied and convergence to the desired flow allocation $\mathbf{x}^*$ is guaranteed. It suffices to prove that the power constraints are satisfied.

Our approach is to bound $\alpha_l v_l(z_l) z_l$ on each link for all $z_l \in [0, c_l]$. First, suppose that $z_l \in [0, z_l^* - \epsilon)$. We have $\tilde{\sigma}_l(z_l) = \sigma_l(z_l)$, and hence $v_l(z_l) = 0$.

Now, suppose that $z_l \in [z_l^* - \epsilon, z_l^*]$. Define

$$R_l(\epsilon) = \sup\left\{\alpha_l v_l(z_l) z_l : z_l \in [z_l^* - \epsilon, z_l^*]\right\}.$$

The function $R_l(\epsilon)$ is continuous as a function of ϵ and satisfies

$$\lim_{\epsilon \to 0} R_l(\epsilon) = \left(\left(\frac{c_l}{z_l^*}\right)^\beta \tilde{\sigma}_l^* - 1\right)\alpha_l z_l^*.$$

Defining δ as

$$\delta \triangleq \frac{P_j - \sum_{l \in \mathcal{L}}\left(\left(\frac{c_l}{z_l^*}\right)^\beta \tilde{\sigma}_l^* - 1\right)\alpha_l z_l^*}{L} > 0,$$

we can choose ϵ sufficiently small such that

$$R_l(\epsilon) < \sum_{l \in \mathcal{L}}\left(\left(\frac{c_l}{z_l^*}\right)^\beta \tilde{\sigma}_l^* - 1\right)\alpha_l z_l^* + \delta$$

for all $l \in \mathcal{L}$.

Finally, if $z_l > z_l^*$, we have two cases. If $\sigma_l(z_l) > \tilde{\sigma}_l^* + \epsilon(z_l - z_l^*)$, then $v_l = 0$. Otherwise,

$$v_l = \left(\frac{c_l}{z_l}\right)^\beta (\tilde{\sigma}_l^* + \epsilon(z_l - z_l^*)) - 1$$

and

$$\alpha_l v_l z_l = \left(c_l^\beta z_l^{(1-\beta)}(\tilde{\sigma}_l^* + \epsilon(z_l - z_l^*)) - z_l\right)\alpha_l.$$

Dividing by α_l and differentiating with respect to z_l yields

$$c_l(1-\beta)z_l^{-\beta}(\tilde{\sigma}_l^* + \epsilon(z_l - z_l^*)) + c_l^\beta z_l^{(1-\beta)}\epsilon - 1. \tag{7}$$

When $\epsilon = 0$, Eq. (7) is equal to $c_l(1-\beta)z^{-\beta}\tilde{\sigma}_l^* - 1$, which is negative since $\beta > 1$. Hence ϵ can be chosen sufficiently small such that Eq. (7) is negative for all $z_l \leq c_l$. This analysis implies that $\alpha_l v_l(z_l) z_l$ is a decreasing function of z_l when $z_l > z_l^*$ and ϵ is chosen appropriately.

Taking these conditions together, we have that (4) holds for all $\mathbf{z} \leq \mathbf{c}$, and hence for all feasible flow allocations, completing the proof. ∎

Theorem 2 provides a jamming strategy (6) that can be interpreted as not jamming until the flow rate z_l exceeds the desired flow rate z_l^*, and then jamming at the equilibrium rate determined by $\tilde{\sigma}_l^*$. Since there may be multiple feasible jamming strategies $\tilde{\boldsymbol{\sigma}}^*$, we formulate the problem of selecting the minimum-energy jamming strategy as

$$\begin{array}{ll} \text{minimize} & \sum_{l \in \mathcal{L}}\left(\left(\frac{c_l}{z_l^*}\right)^\beta \tilde{\sigma}_l^* - 1\right)\alpha_l z_l^* \\ \tilde{\boldsymbol{\sigma}}^* & \\ \text{s.t.} & A^T\tilde{\boldsymbol{\sigma}}^* = \mathbf{q}^* \\ & \tilde{\sigma}_l^* \geq \sigma_l(z_l^*)\ \forall l \in \mathcal{L} \end{array} \tag{8}$$

Eq. (8) defines a linear program in $\tilde{\boldsymbol{\sigma}}^*$, and hence can be solved in polynomial time. If the solution of (8) satisfies (5), then redirecting the network flow to allocation $\mathbf{x}^*$ is feasible.

In fact, a converse result can also be shown, implying that any feasible flow allocation can be achieved using the passivity-based approach.

Proposition 1: Suppose that

$$\sum_{l \in \mathcal{L}}\left(\left(\frac{c_l}{z_l^*}\right)^\beta \tilde{\sigma}_l^* - 1\right)\alpha_l z_l^* \tag{9}$$

for any $\tilde{\boldsymbol{\sigma}}^*$ satisfying the constraints of (8). Then there is no energy-feasible jamming strategy that guarantees global asymptotic stability of $\mathbf{x}^*$.

Proof: Let $\dot{\xi}_{j,l}(t) = f_{j,l}(\xi_{j,l}(t), \tilde{w}_l(t))$ and $u_{j,l}(t) = g_{j,l}(\xi_{j,l}(t))$ define a jamming strategy that guarantees global asymptotic stability of $\mathbf{x}^*$. Since $\mathbf{x}^*$ is globally asymptotically stable, $\lim_{t\to\infty}||\dot{\mathbf{x}}(t)|| = 0$ and

$$\lim_{t \to \infty}||U'(\mathbf{x}(t)) - \mathbf{q}(t)|| = 0.$$

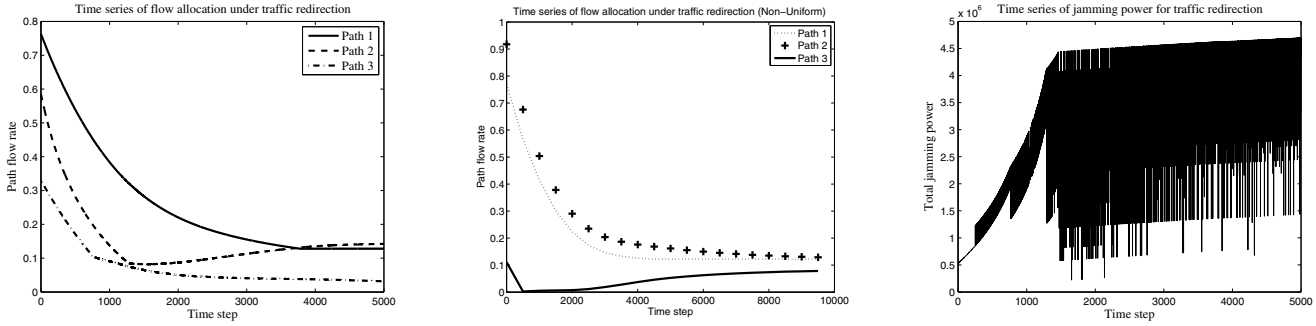
Furthermore, since $\lim_{t\to\infty}\mathbf{x}(t) = \mathbf{x}^*$ and $U'(\mathbf{1}^T\mathbf{x}^*) = \mathbf{q}^*$, we have that $\lim_{t\to\infty}||\mathbf{q}^* - \mathbf{q}(t)|| = 0$.

Since $\mathbf{q}(t) = A^T(\mathbf{p}(t) + \mathbf{u}(t))$, there exists $\tilde{\boldsymbol{\sigma}}^*$ such that $A^T\tilde{\boldsymbol{\sigma}}^* = \mathbf{q}^*$, $\tilde{\sigma}_l^* \geq \sigma_l(z_l^*)$, and $||\mathbf{p}(t) + \mathbf{u}(t) - \tilde{\boldsymbol{\sigma}}^*|| < \epsilon$ for any $\epsilon > 0$ and t sufficiently large. Eq. (9) then implies that, for t sufficiently large, $\sum_{l\in\mathcal{L}} v_l(t) z_l(t) \alpha_l > P_j$, and hence the jamming strategy violates the power constraint and is infeasible. ∎

Proposition 1 implies that, if there exists a feasible jamming strategy of any type that guarantee convergence to a desired equilibrium point $\mathbf{x}^*$, then there exists a passivity-based jamming strategy of the form described in Theorems 1 and 2 that guarantees convergence to the desired equilibrium point. Equivalently, Proposition 1 implies that the passivity-based jamming strategies are optimal from a power consumption perspective.

VI. Numerical Study

We evaluated our approach through a Matlab numerical study. We considered two networks of 200 nodes, one deployed uniformly at random over a square area of width 1200 meters, and the other network deployed non-uniformly such that the average position of each node is at $(500, 500)$ instead of $(600, 600)$. A link was created between two nodes if and only if they were within 300 meters of each other. Three source-destination pairs were selected. Three disjoint paths were chosen for each source-destination pair. Each link was assumed to have unit capacity. Nodes were assumed to have logarithmic utility function, so that $U_{s_i}(\mathbf{y}_i) = \log y_i$



(a) (b) (c)

Fig. 2. A numerical study of flow redirection attacks via jamming on network with 200 nodes deployed uniformly at random over a square area of width 1200 meters. Links were created between nodes within 300 meters of each other. Three source-destination pairs with three disjoint paths each were considered. The goal of the jammer was to cause a fraction $\gamma = 0.2$ of flow to traverse compromised links. (a) Rate of flow allocated to each of the three disjoint paths by source 1 over time. Due to jamming, the rate of flow allocated to paths 1 and 3 decreases, causing more flow to be allocated to path 2, which contains compromised links.(b) Rate of flow allocated to each of the three disjoint paths by source 1 over time in the non-uniform deployment case. In this case, path 3 contained compromised links, and flow increases to path 3 due to jamming on paths 1 and 2. This again resulted in $\gamma = 0.2$ fraction of total flow rate being allocated to path 3. (c) Power consumption of the jammer over time. In order to conserve power, the passivity-based jamming strategy only jams packets when the rate over a link exceeds a certain threshold, resulting in oscillations in the jamming power.

for each node i. The cost function for each link $l \in \mathcal{L}$ was chosen as $\sigma_l(z_l) = \left(\frac{z_l}{c_l}\right)^{\beta}$.

The number of jammers was equal to 3 and locations of jammers were placed uniformly at random. The power required to jam a link was given by the path-loss model $||p_j - p_r||^{\alpha}$, where p_j is the position of the jammer and p_r is the position of the receiver. Each link was assumed to be compromised by the adversary with probability 0.15. In our study, the goal of the jammer was to ensure that at least fraction $\gamma = 0.2$ of flow traversed the compromised links. A candidate flow allocation of this type was chosen by solving the convex program

$$\begin{aligned} \underset{\mathbf{q},\mathbf{x},\mathbf{y},\mathbf{z}}{\text{minimize}} \quad & \mathbf{1}^T\mathbf{q} \\ & q_p = q_{p'} \ \forall p, p' \in \mathcal{P}_i \\ & \mathbf{z} = A\mathbf{x}, \mathbf{z} \leq \mathbf{c} \\ & \mathbf{y} = H\mathbf{x} \\ & U_i'(y_i) \leq q_p \ \forall p \in \mathcal{P}_i \\ & q_p \geq \textstyle\sum_{l \in p} \sigma_l(z_l) \end{aligned} \tag{10}$$

In this formulation, the constraints $q_p = q_{p'}$ for all paths p assigned to a given node were chosen so that $\mathbf{q}$ could define an equilibrium point of the source rate allocation dynamics. The constraint $\mathbf{z} \leq \mathbf{c}$ ensured that the chosen rate satisfied the capacity constraint, while the constraint $U_i'(y_i) \leq q_p$ was chosen as a relaxation of the equilibrium equation $U_i'(y_i) = q_p$. The constraint $q_p \geq \sum_{l \in p} \sigma_l(z_l)$ ensured that the price due to jamming at the equilibrium was greater than the price without jamming. Finally, minimizing over $\mathbf{1}^T\mathbf{q}$ ensured that the program chose $\mathbf{q}$ as small as possible, making the constraint $q_p \geq U_{s_i}'(y_i)$ tight. Since this program was used as a heuristic, we manually verified that the points $\mathbf{x}$ were valid equilibria of the flow allocation dynamics.

The goal of our simulation was to observe the impact of the jamming attack on the network flow allocation, and in particular observe the time required for the passivity-based jamming strategy to cause convergence to the adversary's desired allocation. We also investigated the temporal dynamics of the jamming power.

Figure 2(a) shows the temporal progression of the flow rate on each path for source 1. In this case, source 1 maintained three disjoint paths to the destination. Paths 1 and 3 contained only non-compromised links, while path 2 contained one compromised link. Over time, the fraction of flow allocated to paths 1 and 3 is reduced, as the adversary jams those paths in order to ensure that additional packets traverse the compromised path 2.

Figure 2(b) shows the temporal progression of the flow rate in the non-uniform network case. In this case, path 3 contained compromised links, and jammers were able to redirect the flow to the compromised path by jamming paths 1 and 2. However, because the network was clustered around upper-left corner of the deployed area, the average distances between jammers links increased compared to the uniform deployment case. It was numerically verified that the total power budget P_j required to redirect the flow increases compared to uniform deployment case on average.

The jamming power required to achieve this outcome is illustrated in Figure 2(c). The adversary expends jamming power on links that have not been compromised. When the flow traversing a non-compromised link l exceeds the adversary's desired flow rate z_l^*, the adversary increases the probability of jamming, and hence the average jamming power. These increases in power are represented by the peaks in Figure 2(b). When the flow is reduced below the level z_l^*, the adversary reduces the jamming probability, causing the local minima in Figure 2(b).

VII. Conclusions

We considered flow redirection attacks on wireless networks, in which an adversary jams a set of communication links in order to redirect network flow towards compromised links. The redirected flows are then exposed to higher-layer

man-in-the-middle attacks. We studied the problem from the adversary's perspective, and formulated the flow redirection within a control-theoretic framework. In this framework, the network flow allocation by source nodes is viewed as a plant, while the changes in link delays introduced by jamming are modeled as a control input.

We developed a passivity-based approach for selecting a jamming strategy. Based on the passivity framework, we derived a class of dynamic jamming strategies that guarantee convergence to a desired flow allocation. Intuitively, these are threshold-based strategies in which the adversary begins jamming the network flow on a given link after the flow exceeds the desired rate. We proved that, in addition to guaranteeing convergence, these strategies are energy optimal, i.e., if there exists a jamming strategy with a given power constraint that results in a desired flow allocation, then a passivity-based jamming strategy can be derived that satisfies the same power constraint. We characterized the set of feasible flow allocations as the solution to a convex optimization problem.

While our approach assumed that the network protocols, and hence the flow rate dynamics, are known to the adversary, in practice the parameters of higher-layer protocols may be unknown or uncertain. We will investigate robust techniques that incorporate these uncertainties while guaranteeing convergence to a desired flow allocation. Robustness of the attack against external disturbances including changes in network topology will also be analyzed and incorporated. In future work, we will also investigate efficient mitigation strategies against flow redirection attack including detection and identification of colluding nodes and jammers in the network. We will extend our approach to other denial-of-service attacks in wired networks including the Coremelt attack [19].

REFERENCES

[1] M. Hadley, J. McBride, T. Edgar, L. ONeil, and J. Johnson, "Securing wide area measurement systems," *US Department of Energy*, 2007.

[2] R. Poisel, *Modern Communications Jamming: Principles and Techniques*. Artech House, 2011.

[3] F. Kelly and T. Voice, "Stability of end-to-end algorithms for joint routing and rate control," *ACM SIGCOMM Computer Communication Review*, vol. 35, no. 2, pp. 5–12, 2005.

[4] L. Lazos, S. Liu, and M. Krunz, "Mitigating control-channel jamming attacks in multi-channel ad hoc networks," *Second ACM Conference on Wireless Network Security*, pp. 169–180, 2009.

[5] E. Bayraktaroglu, C. King, X. Liu, G. Noubir, R. Rajaraman, and B. Thapa, "Performance of IEEE 802.11 under jamming," *Mobile Networks and Applications*, vol. 18, no. 5, pp. 678–696, 2013.

[6] C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," *Ad Hoc Networks*, vol. 1, no. 2, pp. 293–315, 2003.

[7] K.-D. Kang and S. H. Son, "Real-time data services for cyber physical systems," *IEEE Distributed Computing Systems Workshops*, pp. 483–488, 2008.

[8] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," *International Symposium on Mobile ad hoc Networking and Computing*, pp. 46–57, 2005.

[9] P. Tague, D. Slater, R. Poovendran, and G. Noubir, "Linear programming models for jamming attacks on network traffic flows," *International Symposium on Modeling and Optimization in Mobile, Ad Hoc, and Wireless Networks and Workshops*, pp. 207–216, 2008.

[10] S. Bhattacharya and T. Başar, "Game-theoretic analysis of an aerial jamming attack on a UAV communication network," *American Control Conference (ACC)*, pp. 818–823, 2010.

[11] F. Pasqualetti, F. Dorfler, and F. Bullo, "Attack detection and identification in cyber-physical systems," *IEEE Transactions on Automatic Control*, vol. 58, no. 11, pp. 2715–2729, 2013.

[12] C. Langbort and V. Ugrinovskii, "One-shot control over an avc-like adversarial channel," pp. 3528–3533, 2012.

[13] J. T. Wen and M. Arcak, "A unifying passivity framework for network flow control," *IEEE Transactions on Automatic Control*, vol. 49, no. 2, pp. 162–174, 2004.

[14] J. Sztipanovits, X. Koutsoukos, G. Karsai, N. Kottenstette, P. Antsaklis, V. Gupta, B. Goodwine, J. Baras, and S. Wang, "Toward a science of cyber–physical system integration," *Proceedings of the IEEE*, vol. 100, no. 1, pp. 29–44, 2012.

[15] P. Lee, A. Clark, L. Bushnell, and R. Poovendran, "A passivity framework for modeling and mitigating wormhole attacks on networked control systems," *IEEE Transactions on Automatic Control*, vol. 59, no. 12, pp. 3224 – 3237, 2014.

[16] E.-H. Ngai, J. Liu, and M. R. Lyu, "On the intruder detection for sinkhole attack in wireless sensor networks," *IEEE International Conference on Communications*, vol. 8, pp. 3383–3389, 2006.

[17] B. Brogliato, O. Egeland, R. Lozano, and B. Maschke, *Dissipative Systems Analysis and Control: Theory and Applications*. Springer, 2007.

[18] H. K. Khalil, *Nonlinear Systems*. Prentice Hall Upper Saddle River, 2002.

[19] A. Studer and A. Perrig, "The Coremelt Attack," in *Computer Security - Esorics*. Springer, 2009, pp. 37–52.