A Passivity Framework for Modeling and Mitigating Wormhole Attacks on Networked Control Systems

Phillip Lee, Andrew Clark, Linda Bushnell, and Radha Poovendran
Network Security Lab, Dept. of Electrical Engineering
University of Washington, Seattle, WA, 98195, USA
{leep3, awclark, lb2, rp3}@uw.edu

***Abstract*—Networked control systems consist of distributed sensors and actuators that communicate via a wireless network. The use of an open wireless medium and unattended deployment leaves these systems vulnerable to intelligent adversaries whose goal is to disrupt the system performance. In this paper, we study the wormhole attack on a networked control system, in which an adversary establishes a link between two geographically distant regions of the network by using either high-gain antennas, as in the out-of-band wormhole, or colluding network nodes as in the in-band wormhole. Wormholes allow the adversary to violate the timing constraints of real-time control systems by first creating low-latency links, which attract network traffic, and then delaying or dropping packets. Since the wormhole attack reroutes and replays valid messages, it cannot be detected using cryptographic mechanisms alone. We study the impact of the wormhole attack on the network flows and delays and introduce a passivity-based control-theoretic framework for modeling and mitigating the wormhole attack. We develop this framework for both the in-band and out-of-band wormhole attacks as well as complex, hereto-unreported wormhole attacks consisting of arbitrary combinations of in-and out-of band wormholes. By integrating existing mitigation strategies into our framework, we analyze the throughput, delay, and stability properties of the overall system. Through simulation study, we show that, by selectively dropping control packets, the wormhole attack can cause disturbances in the physical plant of a networked control system, and demonstrate that appropriate selection of detection parameters mitigates the disturbances due to the wormhole while satisfying the delay constraints of the physical system.**

I. Introduction

Cyber-physical systems that are deployed over a wide geographic area often consist of distributed embedded devices, such as sensors and actuators, that exchange sensed data and control signals via a wireless network [1], thus forming a networked control system. When deployed in critical applications such as the smart grid, the real-time control system may be targeted by adversaries attempting to drive it to an undesirable or unsafe operating point. By introducing and modifying delays in the communication network, the adversary can cause violations of the timing constraints that are critical in maintaining safe operation of real-time cyber-physical systems [2].

The wormhole attack, first introduced in the context of wireless routing [3], is one such attack that exploits the time delays and violates the timing constraints of the targeted system. In the wormhole attack, an adversary records messages observed in one region of the network and replays them in a different region [4]. By doing so, the adversary creates a communication link (a wormhole tunnel) between two end points in otherwise disjoint geographic areas. This can be accomplished by either compromised or colluding network nodes, known as the in-band wormhole [5] or via a side channel such as high-gain directional antennas, known as the out-of-band wormhole [3]. Unsuspecting network nodes will route network traffic through the wormhole. Once significant traffic starts flowing through the wormhole, the adversary can selectively drop or delay time-critical packets in order to destabilize or degrade the system performance. As the attack replays or reroutes valid messages, it does not require compromising any cryptographic keys, and hence cannot be detected using cryptographic verification mechanisms alone [6].

While the wormhole attack does not violate cryptographic mechanisms, it does violate the physical constraints imposed by propagation delay and relative position of nodes. Current approaches that detect these violations include include graph-based methods [6], statistical methods [5], and timing analysis [3]. However, the current security analysis of the mitigation strategies do not incorporate the time-varying node behaviors or the adaptive strategy of the adversary. Hence, while the wormhole attack can significantly degrade the performance of cyber-physical systems, there is currently no analytical approach that represents the impact of wormholes and mitigation on the system dynamics. Furthermore, the composition of different types of wormhole attacks and the impact on system performance has not been studied.

In this paper, we introduce one such control-theoretic framework for modeling and mitigating the wormhole attack on networked control systems. The proposed framework models the impact of wormholes, as well as the integration of existing mitigation strategies, on the allocation of network flows and resulting delays. Our approach models three interdependent components, namely, flow allocation by network nodes, delay characteristics introduced by wormholes, and mitigation algorithms employed by the network. We develop this framework for both out-of-band and in-band wormholes. In addition, using our framework, we are able to model, represent and mitigate complex wormhole attacks that simultaneously make use of both in- and out-of-band wormholes. For each case, we prove that the flow allocation, wormhole delay, and mitigation components can be modeled as a passive dynamical system which allows the characterization of flow allocation and delay at the steady state. Since our framework is in control-theoretic language, it enables ease of composition with control models

of cyber-physical systems. We make the following specific contributions:

- We study the wormhole attack and mitigation by first identifying the network throughput and delay as time-varying system performance parameters that are impacted by the attack. We formulate dynamical system representations of the network flow allocation, delays and packet drops at the wormhole link, and the mitigation strategies of the system, for out-of-band, in-band, and joint in- and out-of-band wormhole attacks. We show that the overall flow allocation and delay are characterized by the interconnection of these dynamical systems.
- For the out-of-band wormhole, we develop dynamical models for the flow allocation by network nodes, the delays introduced by wormholes, and network mitigation. For the flow allocation by network nodes, we introduce a distributed algorithm for each node to adaptively divide its flow among a set of paths based on their delays. We model the delay characteristics of out-of-band wormhole links based on the rate at which the adversary drops packets traversing the wormhole link. We map the packet dropping strategy of the adversary to the optimization problem of selecting the optimal dropping rate which balances the goals of increasing delay and attracting flows to the wormhole. We then develop a dynamical model that integrates timing-based mitigation mechanisms, such as the packet leash, into our framework.
- We prove the dynamical systems describing the flow allocation, delays introduced by wormhole, and the mitigation schemes are passive. We leverage the passivity property to prove that the interconnection of these models is globally asymptotically stable with respect to a unique equilibrium point.
- For the in-band wormhole, we derive the delays introduced by wormhole as a function of number of colluding nodes and the network topology. We represent statistics based mitigation method against in-band wormhole as a penalty added to suspected wormhole links during the flow allocation. We then prove that the flow allocation algorithm introduced earlier together with the delay and mitigation models in the in-band case, can be represented as an interconnection of passive systems, which converges to a stable equilibrium point.
- We use our framework to model more complex wormhole attacks, which consists of both in- and out-of-band wormholes. Our approach composes the models of individual wormhole links via parallel interconnections of passive systems.
- We illustrate our approach via a numerical study, in which we compare the flow allocation and delay resulting from both out-of-band and in-band wormhole attacks and the detection mechanisms, and evaluate the impact of the wormhole attack and mitigation on a cyber-physical system. In the out-of-band case, simulation results show that detection mechanisms reduces the flow traversing through the wormhole link at the cost of increased delay. For the in-band case, simulation results suggest that detection mechanisms enable the source rates to converge to the same equilibrium regardless of the presence of a wormhole. We find that an adversary who creates an out-of-band wormhole can cause large disturbances on the physical plant by selectively dropping packets that are allocated to the wormhole link. We empirically determine parameters of the mitigation strategy that reduces the flow allocated to the wormhole link, while satisfying the system's delay constraints.

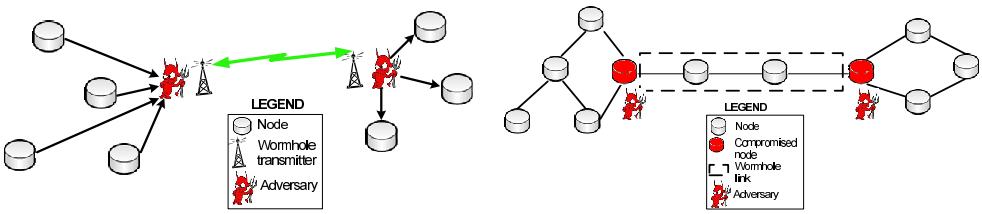
Our proposed framework enables quantitative analysis of the impact of the wormhole attack on system performance and the effectiveness of different mitigation mechanisms, as well as modeling of any arbitrary composition of in-band and out-of-band wormholes. Hence, this approach is complementary to recent efforts towards a science of cyber-security [7], where the goal is a scientific approach to characterizing, composing, and mitigating security threats. Moreover, our proposed framework explicitly captures the temporal dynamics of the attack and mitigation, including the adaptation and co-evolution of the adversary and defender strategies.

The paper is organized as follows. We present the related work in Section II. Section III presents our assumptions of the network and adversary capabilities, as well as a description of the wormhole attack. Section IV discusses our proposed modeling and mitigation framework for the out-of-band wormhole. Section V presents our approach to modeling and mitigating in-band wormholes. Section VI introduces passivity-based models and mitigation for joint out-of- and in-band wormholes. Numerical results are contained in Section VII. Section VIII concludes the paper. Appendix A presents background on passivity. Due to space constraints, some of the lengthier proofs of our results are contained in the technical report [8].

II. Related Work

The wormhole attack was originally identified as a form of routing misbehavior in ad hoc and sensor networks [4]. In [3], the packet leash defense was proposed, in which each packet is given a fixed expiration time and any packet received after its expiration time is discarded. Valid packets may also be discarded, however, due to propagation delays or clock skews between nodes, leading to a trade-off between detection effectiveness and network performance. Local broadcast keys, which are cryptographic keys that are distributed using specialized guard nodes and known only to nodes within a local neighborhood, were introduced in [6]. Anomalies in link delays, caused by propagation through the wormhole tunnel, are analyzed in [9], in which an FFT-based approach to identifying likely wormholes was presented. While these methods can be used to mitigate the impact of the wormhole attack, an analytical approach to dynamically tune each method in response to changes in the network state and adversary behavior, as well as estimate the stable operating point of the system, is currently lacking.

The in-band wormhole, in which the adversary creates the appearance of a link between two colluding nodes by tunneling packets through valid nodes, was identified as a security threat



(a) (b)

Fig. 1. Illustration of the two classes of wormhole. (a) In an out-of-band wormhole, the adversary creates a low-latency link between two network regions using a high-capacity channel, such as a directional antenna or wired link. (b) In an in-band wormhole, the adversary compromises network nodes in different regions and advertises a false one-hop link between two compromised nodes. The link actually consists of a path between unsuspecting valid nodes.

in [5]. The authors observed that the wormhole tunnel itself could contain routing loops, diminishing its effectiveness, a phenomenon they denoted as wormhole collapse. Necessary and sufficient conditions for the adversary to avoid wormhole collapse are derived in [10]. A statistical approach to detecting in-band wormholes, based on identifying increased delays or packet drops through wormhole links using sequential probability ratio testing, was studied in [11]. Our framework incorporates the probability of wormhole collapse, as well as the statistical detection algorithms, when modeling the temporal dynamics of the flow rates and resulting delays.

Passivity-based techniques have been used to model network flow control and derive novel flow allocation algorithms in [12]. The work of [12] fits within the broader context of dual decomposition-based methods for designing network protocols as distributed algorithms for solving network optimization problems [13]. Passivity of networked control systems with packet drops was studied in [14]. In [14], the authors studied the passivity of networked control systems where the plant dynamics switches between open and closed loop due to control packet drops. Currently, however, such models do not incorporate security threats or network defenses.

In preliminary versions of this work [15], [16], we studied passive dynamical systems as a framework for modeling and mitigating network security threats. In [15], we presented passive dynamical models of the node capture, malware propagation, and control channel jamming attacks, and demonstrated that these attacks can be composed while preserving passivity. In [16], we studied a class of adaptive network defense mechanisms against control channel jamming that satisfy the passivity property, and demonstrated that the robustness of the system to delays and detection errors is affected by the parameters of the passive defense. Neither of these works, however, consider network flow-based attacks such as the wormhole attack.

III. Preliminaries

In this section, we state our assumptions regarding the capabilities of the network and adversary. We then give background on the wormhole attack.

A. Network Model

We consider a wireless network of n nodes. We assume that two nodes can communicate directly if their positions are within the maximum node communication range. We denote the set of links by $\mathcal{L}$, with $|\mathcal{L}| = L$. In order to facilitate sensing and control of the system, network flows must be maintained between a set of source nodes $\mathcal{S}$ and destination nodes $\mathcal{D}$. The ordered pair (S_i, D_i) denotes the source and destination of flow i. We assume that source S_i maintains a constant rate r_i, and that flows are originating from the set of sources. External flows that do not originate from $\mathcal{S}$ are not considered in this paper.

Any source and destination pair that is not in direct radio range relies on multi-hop communication. Since the topology changes due to node sleep/wake cycles and nodes joining and leaving the network, each source S_i uses a distributed routing protocol to identify a set of source-destination paths $\mathcal{P}_i = \{P_1, \ldots, P_{m_i}\}$, where m_i denotes the number of paths for source-destination pair (S_i, D_i).

B. Adversary Model

The network is deployed in a hostile environment where one or more mobile adversaries are present. We assume that each adversary is capable of eavesdropping as well as recording and replaying eavesdropped messages, including routing protocol messages. By eavesdropping on routing protocol messages, the adversary determines the network topology. The adversary is also capable of physically capturing the unattended nodes. Once the adversary has compromised a node, the adversary can extract its cryptographic secrets. This enables the adversary to replace the captured node with a malicious node assuming the identity of the captured node. Malicious nodes are under the control of the adversary and are capable of colluding with other malicious nodes. One such collusion attack is the wormhole, described as follows.

C. Wormhole Attack and Mitigation

In a wormhole attack, an adversary creates a covert path (referred to as *wormhole tunnel*) that connects two distant regions of the network. Since the wormhole creates the appearance of a short path between distant regions of the network, shortest-path routing protocols will route a large fraction of the network traffic through the wormhole tunnel. The adversary can then control this traffic and selectively drop packets, increase delays, or create routing instability. The wormhole link can also be used to record messages overheard in one network region, such as sensed data or control signals, and replay those messages in order to disrupt the performance of one or more system components. The wormhole can be further

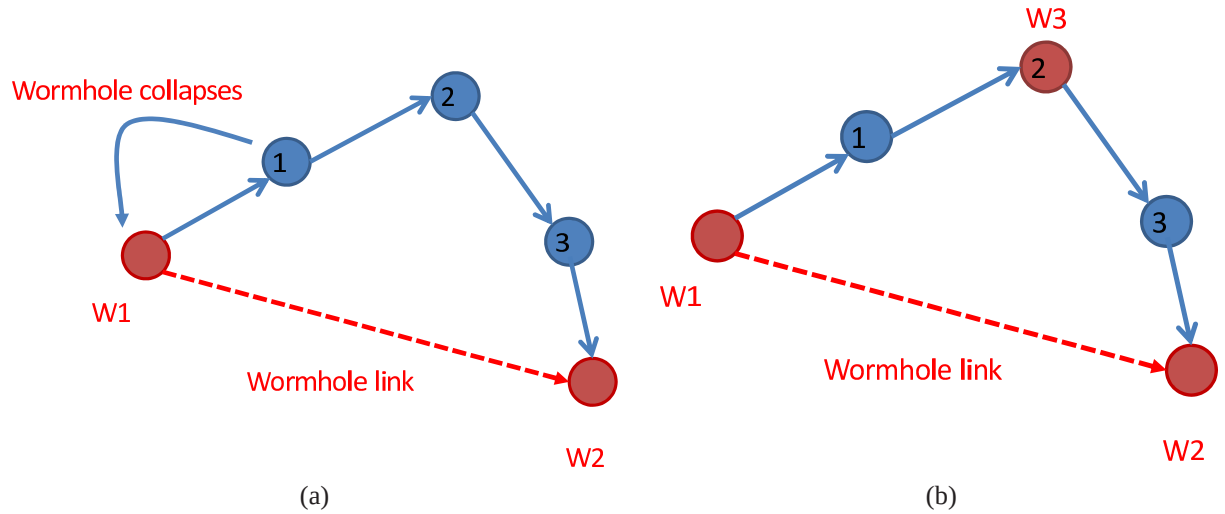


Fig. 2. Illustration of the collapse of in-band wormholes. (a) When the colluding nodes W_1 and W_2 advertise a one-hop link between them, the intermediate nodes on the path between W_1 and W_2 will attempt to forward packets through the advertised (W_1, W_2) link, creating a routing loop that causes the wormhole to collapse. (b) By tunneling packets to an intermediate node W_3 satisfying the conditions of Lemma 3.1, which then forwards the packets to W_2, the adversary avoids wormhole collapse.

classified as out-of-band or in-band, depending on the nature of the wormhole tunnel.

1) Out-of-band wormhole formation: In the out-of-band wormhole, an adversary establishes a low-latency link (wormhole link) between two distant regions of the network (Figure 1(a)). This may be done through wired links that are not available to network nodes, or through high-gain directional wireless antennas. Once the adversary has gained control over a large amount of packets flowing through the wormhole link, the adversary can disrupt the system performance by dropping or delaying packets. In order to create an out-of-band wormhole, the adversary does not need to compromise any node or cryptographic secrets.

2) Out-of-band wormhole mitigation: The out-of-band wormhole is based on replaying messages that are intended for a local geographic area in a different geographic region. As a result of physical constraints on propagation through the medium, the time for a message to propagate to a node's immediate neighbors will be less than the time required for the message to propagate to the eavesdropper, traverse the wormhole tunnel, and then propagate to any nodes on the other side of the wormhole tunnel. This discrepancy is the basis for the packet leash defense [3], in which the sender of each packet attaches an expiration time to the packet, equal to $t_s + \frac{R}{c} + \Delta$, where t_s is the transmission time, $\frac{R}{c}$ is the propagation time, and Δ is an estimate of the clock skew between the sending and receiving nodes. All packets received after their expiration time are discarded. Packets are signed using message authentication codes to prevent the adversary from modifying the expiration time.

3) In-band wormhole formation: In the in-band wormhole attack, an adversary compromises two nodes in different regions of the network and falsely advertises a one-hop link between those nodes via the routing protocol. As in the out-of-band case, the appearance of this short path will result in a large traffic flow into the two compromised nodes. The adversary then chooses a path, consisting of both valid and compromised nodes, between the two nodes comprising the wormhole tunnel. The in-band wormhole requires the adversary to compromise at least two nodes, but does not require any specialized hardware. The in-band wormhole is illustrated in Figure 1(b).

4) In-band wormhole collapse: In order to create an in-band wormhole, the adversary must avoid wormhole collapse, which occurs under the following conditions. The wormhole tunnel consists of a path between two colluding nodes, denoted W_1 and W_2. The intermediate nodes in the tunnel, however, will attempt to route packets from W_1 to W_2 using shortest-path routing. Since the wormhole tunnel is advertised as a one-hop link between W_1 and W_2, any packets sent from W_1 to W_2 are likely to be forwarded back to W_1, creating a routing loop (Figure 2(a)).

To avoid wormhole collapse, the adversary must capture a third node, denoted W_3. Instead of routing packets directly from W_1 to W_2 in the wormhole link, the adversary sends packets from W_1 to W_3, and then from W_3 to W_2, as shown in Figure 2(b). The conditions on W_3 to prevent wormhole collapse are given by the following lemma.

Lemma 3.1 ([10]): Let $d(i, j)$ denote the length of the shortest path between nodes i and j. Then the wormhole tunnel formed by colluding nodes W_1, W_2, and W_3 does not collapse if

$$d(W_1, W_3) < d(W_2, W_3) + 3.$$

5) In-band wormhole mitigation: Since the in-band wormhole is mounted using compromised nodes and their stored cryptographic keys, defenses against the out-of-band wormhole may be ineffective against in-bandwidth wormholes. The in-band wormhole, however, will incur longer delays than the out-of-band wormhole, since it relies on a multi-hop path of network nodes to forward packets. By performing statistical analysis, the network nodes can identify one-hop links with exceptionally long delays and/or packet-loss rates, which are

then suspected of being wormhole links and ignored for routing purposes [5].

IV. Proposed Passivity Framework for Out-of-Band Wormhole

In this section, we introduce our passivity-based framework for modeling and mitigating out-of-band wormholes in a networked control system. Our model considers the effect of the wormhole attack and mitigation on the delay and flow allocation of the network traffic. We first develop a dynamical model for the flow allocation by the network nodes. We then model the delays experienced due to the out-of-band wormhole, followed by the effect of mitigation mechanisms. Lastly, we consider the interconnection of these three dynamical models and characterize the flow allocation and delay at the unique equilibrium point via a passivity-based approach.

A. Dynamical Model of Network Flow Allocation

We assume that each source node S_i maintains a flow with total rate r_i to destination D_i. This flow is divided among the paths $\mathcal{P}_i$ used by source S_i in order to minimize the overall delay. Let $r_P(t)$ denote the flow allocated to path $P \in \mathcal{P}_i$ at time t, so that $\sum_{P\in\mathcal{P}_i} r_P = r_i$. The vector of flow rates is denoted $\mathbf{r}_i(t) \triangleq \{r_P(t) : P \in \mathcal{P}_i\}$. Furthermore, let $f_l(r_l)$ denote the delay experienced on link l when the rate of flow on link l is given by r_l. Let $q_P(r_P) \triangleq \sum_{l\in P} f_l(r_l)$ denote the total delay on path P, equal to the sum of the delays on each link comprising the path, where $\{l \in P\}$ denotes summing over the links l in path P. Finally, define the $L \times (\sum_{i=1}^{n} m_i)$ matrix A by

$$A_{lP} = \begin{cases} 1, & \text{link } l \text{ in path } P \\ 0, & \text{else} \end{cases}$$

so that $r_l = (A\mathbf{r})_l$.

Achieving the minimum possible delay is equivalent to finding $\{r_P : P \in \mathcal{P}_i\}$ satisfying

$$\min\left\{\sum_{P\in\mathcal{P}_i} r_P q_P(r_P) : \sum_{P\in\mathcal{P}_i} r_P = r_i\right\},$$

since $r_P q_P(r_P)$ is the total delay on path P, $\sum_{P\in\mathcal{P}_i} r_P$ is the overall delay experienced on all paths, and $\sum_{P\in\mathcal{P}_i} r_P = r_i$ is a constraint on the total throughput. Determining whether this condition is satisfied requires the source S_i to determine the incremental change in delay from shifting flow from path P to path P' for all $P, P' \in \mathcal{P}_i$. The incremental change, however, depends on parameters that the source cannot observe, such as the rates of the other sources and the excess capacity of each link, and hence cannot be computed directly by the source. Instead, we assume that each source attempts to minimize the total delay based on the currently observed delay characteristics of each link. This condition is formalized by the concept of a *Wardrop equilibrium* [17], defined as follows.

Definition 4.1: The flow allocation $\{r_P : P \in \mathcal{P}_i\}$ is a *Wardrop equilibrium* for source S_i if for any path P, $r_P > 0$ implies that $q_P \le q_{P'}$ for all $P' \in \mathcal{P}_i$.

Definition 4.1 implies that a positive flow rate is allocated to path $P \in \mathcal{P}_i$ if and only if there is no path P' currently experiencing lower delays than path P. We now introduce flow rate dynamics that, when used by each source S_i to choose $\mathbf{r}_i(t)$, cause the network to converge to a Wardrop equilibrium. We prove convergence to the Wardrop equilibrium by first proving that $\mathbf{r}_i$ is a steady state for the dynamics if and only if it is a Wardrop equilibrium, and that the Wardrop equilibrium is unique. We then use a passivity-based approach to prove the system converges to a unique steady state and hence converges to the Wardrop equilibrium.

Let $P_i^{min}(q)$ denote a time-varying index satisfying

$$P_i^{min}(q) \in \arg\min\{q_P : P \in \mathcal{P}_i\}.$$

We define the dynamics of the flow rate $r_P(t)$ allocated to path $P \in \mathcal{P}_i$ by

$$\dot{r}_P(t) = \begin{cases} -\{q_P(r_P(t)) - q_{P^{min}}(r_{P_i^{min}}(t))\}_+^{r_P}, \\ \qquad\qquad P \neq P_i^{min}(q) \\ -\sum_{P\neq P_i^{min}(q)} \dot{r}_P(t), \\ \qquad\qquad P = P_i^{min}(q) \end{cases} \tag{1}$$

where

$$\{x\}_+^{r_P} = \begin{cases} 0, & x > 0 \text{ and } r_P = 0 \\ x, & \text{else} \end{cases}$$

Equation (1) has the following interpretation. When the observed delay on path P is greater than the delay observed on path P^{min}, which has the minimum delay of any path in $\mathcal{P}_i$, the flow allocated to path P is reduced if it is positive. When the path P has the minimum delay of any path in $\mathcal{P}_i$ ($P = P_i^{min}(q)$), additional flow is allocated to path P (note that, since $\dot{r}_P(t) \le 0$ if $P \neq P_i^{min}(q)$, $-\sum_{P\neq P_i^{min}(q)} \dot{r}_P(t) \ge 0$). Since the total flow from source S_i is constant, the dynamics are chosen such that $\sum_{P\in\mathcal{P}_i} \dot{r}_P(t) = 0$. The following proposition verifies that the dynamics (1) define a feasible flow allocation for all time t.

Proposition 4.2: Suppose that $\sum_{P\in\mathcal{P}_i} r_P(0) = r_i$ and $r_P(0) \ge 0$ for all $P \in \mathcal{P}_i$. Then for all $t > 0$, $\sum_{P\in\mathcal{P}_i} r_P(t) = r_i$ and $r_P(t) \ge 0$ for all $P \in \mathcal{P}_i$.

A proof is given in [8]. We next show that the equilibria of (1) are equivalent to the Wardrop equilibria of the system.

Proposition 4.3: The dynamics (1) have an equilibrium at $\mathbf{r}_i^*$ if and only if $\mathbf{r}_i^*$ is a Wardrop equilibrium.

Proof: First, suppose that $\dot{r}_P(t) = 0$ for all $P \in \mathcal{P}_i$, and assume that $\mathbf{r}_i(t)$ is not a Wardrop equilibrium. By Definition 4.1, there exists P such that $q_P(r_P) > q_{P_i^{min}(t)}(r_{P_i^{min}})$ and $r_P(t) > 0$. The condition $\dot{r}_P(t) = 0$ implies that

$$\{q_P(r_P) - q_{P_i^{min}}(r_P^*)\}_+^{r_P} = 0. \tag{2}$$

Since $q_P(r_P) > q_{P_i^{min}}(r_{P_i^{min}})$, condition (2) holds if and only if $r_P = 0$, contradicting the assumption that $r_P > 0$.

Now, suppose that $\mathbf{r}_i$ is a Wardrop equilibrium. The goal is to show that $\mathbf{r}_i$ is an equilibrium of (1). Consider $P \in \mathcal{P}_i$, and suppose that $P \neq P_i^{min}$. We show that $\dot{r}_P(t) = 0$ by separately considering the cases where $q_P(r_P) = q_{P_i^{min}}(r_{P_i^{min}})$ and $q_P(r_P) > q_{P_i^{min}}(r_{P_i^{min}})$ ($q_P(r_P) < q_{P_i^{min}}(r_{P_i^{min}})$ contradicts the definition of P_i^{min}).

If $q_P(r_P) = q_{P_i^{min}}(r_P^*)$, then $\dot{r}_P(t) = 0$. On the other hand, if $q_P(r_P) > q_{P_i^{min}}(r_{P_i^{min}})$, then the delay experienced on path P exceeds the minimum delay, and therefore

$r_P(t) = 0$ by Definition 4.1. Hence $\dot{r}_P(t) = \{q_P(r_P) - q_{P_i^{min}}(r_{P_i^{min}})\}_+^{r_P} = 0$.

Finally, we have

$$\dot{r}_{P_i^{min}} = -\sum_{P \neq P_i^{min}} \dot{r}_P = 0,$$

which proves that $\mathbf{r}_i$ is an equilibrium point of (1). ■

Proposition 4.3 implies that the equilibria of (1) are equal to the Wardrop equilibria of the system. The following Lemma proves the equilibria of (1) are unique.

Lemma 4.4: If the functions $f_l : \mathbb{R} \to \mathbb{R}$ are strictly increasing for all links l, then there exists a unique equilibrium for the dynamics (1).

A proof of Lemma 4.4 is given in [8]. Finally, we show that the dynamics (1) converge to the unique Wardrop equilibrium. As a first step, we present an equivalent representation of (1). We define the system $\tilde{H}_1$, which takes input $u^1 \in \mathbb{R}^{m_i}$, by

$$(\tilde{H}_1) \begin{cases} \dot{\tilde{r}}_P(t) = -\{q_P^* - u_P - q^*_{P^{min}(q^*-u)} + u_{P^{min}(q^*-u)}\}_+^{r_P} & P \neq P_i^{min}(q^*-u) \\ \dot{\tilde{r}}_P(t) = -\sum_{P \neq P^{min}(q^*-u)} \dot{\tilde{r}}_P(t), & P = P_i^{min}(q^*-u) \\ \tilde{y}_P(t) = \dot{\tilde{r}}_P(t), & \forall P \in \mathcal{P}_i \end{cases}$$

We define a system $(\tilde{H}_2)$, which takes input $u^{(2)}(t) \in \mathbb{R}^L$, as

$$(\tilde{H}_2) \begin{cases} \dot{z}_l(t) = u_l^{(2)}(t) \\ y_l(t) = f_l(z_l(t)) - f_l(z_l^*) \end{cases}$$

where z_l^* is the rate through link l in the unique equilibrium guaranteed by Lemma 4.4. We let $(\tilde{H})$ denote the system formed by a negative feedback interconnection between $(\tilde{H}_1)$ and $(\tilde{H}_2)$ (Figure 3). The following proposition establishes the equivalence between the state dynamics defined by (1) and system $(\tilde{H})$.

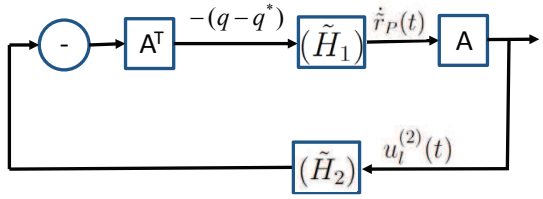


Fig. 3. Illustration of the flow allocation and link delay dynamics $(\tilde{H}_1)$ and $(\tilde{H}_2)$. The passive system $(\tilde{H}_1)$ represents the flow allocation by each source based on the observed delays at each path. The passive system $(\tilde{H}_2)$ represents the delays experienced at each link as a function of the flows allocated to the link. Since $(\tilde{H}_1)$ is strictly passive and $(\tilde{H}_2)$ is passive, the overall system is asymptotically stable (Theorem 4.6).

Proposition 4.5: For all t, $\tilde{\mathbf{r}}(t) = \mathbf{r}(t)$.

The proof can be found in [8]. The following theorem establishes that the flow rate allocation converges to the unique Wardrop equilibrium.

Theorem 4.6: Suppose that $\sum_{P \in \mathcal{P}_i} r_P(0) = r_i$. If the link delay $f_l(r_l)$ is strictly increasing as a function of r_l for all links l, then

$$\lim_{t \to \infty} \mathbf{r}_i(t) = \mathbf{r}_i^*,$$

where $\mathbf{r}_i^*$ is the unique Wardrop equilibrium.

Proof: It suffices to show that the system $(\tilde{H}_1)$ is strictly passive from input $u_P^{(1)}(t)$ to output $\tilde{y}_P^{(1)}(t)$ and the system $(\tilde{H}_2)$ is passive from input $u_l^{(2)}(t)$ to output $\tilde{y}_l^{(2)}(t)$.

Define the function $V_1(\mathbf{r}) = q^{*T}(\mathbf{r} - \mathbf{r}^*)$, and let $q = q^* - u$. Then

$$\dot{V}_1(\mathbf{r}) = q^{*T}\dot{\mathbf{r}} = q^T\dot{\mathbf{r}} + \tilde{u}^{(1)}(t)^T\dot{\mathbf{r}}.$$

To prove strict passivity, it therefore suffices to show that $q^T\dot{\mathbf{r}} < 0$. Without loss of generality, suppose that $|\mathcal{P}_i| = m_i + 1$ and $P_i^{\min}(q^* - u) = P_i^{\min}(q) = m_i + 1$. Then

$$\begin{aligned} q^T\dot{\mathbf{r}} &= \sum_{j=1}^{m_i+1} q_j\dot{r}_j(t) = \sum_{j=1}^{m_i} q_j\dot{r}_j(t) - \sum_{j=1}^{m_i} q_{m_i+1}\dot{r}_j(t) \\ &= -\sum_{j=1}^{m_i} q_j(q_j - q_{m_i+1})_+^{r_j} + \sum_{j=1}^{m} q_{m_i+1}(q_j - q_{m_i+1})_+^{r_j}. \end{aligned}$$

By definition, $(q_j - q_{m_i+1})_+^{r_j} \geq 0$. Furthermore, $q_j \geq q_{m_i+1}$ for all j, and so

$$q^T\dot{\mathbf{r}} \leq -\sum_{j=1}^{m_i} q_{m_i+1}(q_j - q_{m_i+1})_+^{r_j} + \sum_{j=1}^{m_i} q_{m_i+1}(q_j - q_{m_i+1})_+^{r_j},$$

thus establishing the passivity of $(\tilde{H}_1)$. To prove passivity of $(\tilde{H}_2)$, define the storage function

$$V_2(z_l) = \int_0^{z_l - z_l^*} f_l(s + z_l^*) - f_l(z_l^*)\, ds.$$

We have $\dot{V}_2(z_l(t)) = (f_l(z_l(t) - f_l(z_l^*))\dot{z}_l(t) = u_l^{(2)}(t)\tilde{y}_l^{(2)}(t)$, implying passivity of $(\tilde{H}_2)$. ■

Theorem 4.6 implies that the flow allocation converges to a unique equilibrium when the delays experienced at each link is a strictly increasing function in flows allocated to each link. The next step in modeling the wormhole attack is to characterize the delays experienced by the wormhole links, which is the topic of the following section.

B. Delay Characteristics of the Out-of-Band Wormhole

For the out-of-band wormhole, we assume that the wormhole tunnel uses a high-throughput channel, so that the delay for packets traversing the wormhole tunnel l is equal to the propagation delay α_l. Let $\Phi_l(r_l)$ denote the fraction of packets dropped by the wormhole, which we assume to be increasing in r_l. The delay for packets traversing the wormhole tunnel, equal to the time per packet transmission multiplied by the average number of retransmissions, is therefore given by $p_l = \alpha_l/(1 - \Phi_l(r_l))$.

Since the packet-loss rate Φ_l is increasing in r_l, p_l is increasing as a function of r_l as well, thus preserving the passivity property required by the proof of Theorem 4.6. In what follows, we provide a method for modeling the packet-loss rate $\Phi_l(r_l)$ based on the goals of the adversary.

In mounting the wormhole attack, the goal of the adversary is to attract flow to the wormhole tunnel, in order to either selectively drop packets or mount secondary attacks. The rate at which packets are dropped by the adversary is equal to $\Phi_l(r_l)r_l$, while we model the utility of the adversary from mounting secondary attacks as $U_A(r_l)$. The adversary's overall

utility is therefore given by $\Phi_l(r_l)r_l + U_A(r_l)$. By decreasing Φ_l, the adversary increases r_l and hence $U_A(r_l)$, at the cost of dropping fewer packets.

The optimal dropping rate depends on the flow rate through the wormhole link in steady-state, which in turn depends on the delays experienced by the other links in the network, since higher delays at other links will increase the flow allocated to the wormhole link. Based on the network topology, the adversary estimates the delay between source S_i and destination D_i as $\zeta d(S_i, D_i)$, where $\zeta \geq 0$ is the per-hop delay and $d(\cdot,\cdot)$ is the length of the shortest path between two nodes. Similarly, the delay experienced by the wormhole path will be equal to $\zeta d(S_i, W_1) + \frac{\alpha_l}{1-\Phi_l(r_l)} + \zeta d(W_2, D_i)$, where W_1 and W_2 are the entrance and exit to the wormhole tunnel, respectively. Define $\Delta_{i,l}$ by

$$\Delta_{i,l} = \zeta(d(S_i, D_i) - (d(S_i, W_1) + d(W_2, D_i))).$$

By Proposition 4.3, the flow from source S_i to destination D_i will traverse the wormhole tunnel if and only if the delay experienced by the wormhole path is less than the delay experienced by the next-shortest path. Hence, the flow from source S_i to destination D_i that traverses the wormhole tunnel in steady-state will be equal to

$$r^*_{i,l} \triangleq \begin{cases} r_i, & p_l < \Delta_{i,l} \\ 0, & \text{else} \end{cases}$$

Without loss of generality, assume that the indices i are rank-ordered such that $\Delta_{1,l} > \Delta_{2,l} > \cdots > \Delta_{n,l}$, and define $i^* = \max\{i : p_l < \Delta_{i,l}\}$. The flow rate r^*_l traversing the wormhole in steady-state is equal to

$$r^*_l = \sum_{i=1}^{i^*} r_i. \tag{3}$$

The following proposition describes the set of possible optimal packet-dropping rates Φ^*_l at equilibrium.

Proposition 4.7: The possible solutions Φ^*_l to the optimization problem

$$\begin{array}{ll} \text{maximize} & r^*_l(\Phi_l)\Phi_l + U_A(r^*_l(\Phi_l)) \\ \Phi_l & \\ \text{s.t.} & \Phi_l \in [0,1] \end{array} \tag{4}$$

are given by $\{\gamma_1, \ldots, \gamma_n\}$, where

$$\gamma_i = 1 - \frac{\alpha_l}{\Delta_{i,l}} - \epsilon$$

for some $\epsilon << 1$.

Proof: Suppose that the optimal solution Φ^*_l to (4) lies within the interval (γ_i, γ_{i+1}) for some i. Then by definition of γ_i, $p^*_l > \Delta_{l,i+1}$ and $p^*_l < \Delta_{l,i}$, so that $i^* = i$. Consider $\Phi^*_l + \delta$ for some $\delta > 0$ satisfying $\Phi^*_l + \delta < \gamma_{i+1}$. Then by (3),

$$r^*_l(\Phi^*_l) = \sum_{k=1}^{i} r_k = r^*_l(\Phi^*_l + \delta).$$

We therefore have that

$$\begin{aligned} r^*_l(\Phi^*_l)\Phi^*_l + U_A(r^*_l(\Phi^*_l)) &< r^*_l(\Phi^*_l)(\Phi^*_l + \delta) + U_A(r^*_l(\Phi^*_l)) \\ &= r^*_l(\Phi^*_l + \delta)(\Phi^*_l + \delta) \\ &\quad + U_A(r^*_l(\Phi^*_l + \delta)), \end{aligned}$$

contradicting the assumption that Φ^*_l is optimal. ■

The adversary can therefore determine the optimal packet-dropping rate at equilibrium, Φ^*_l, by evaluating $r^*_l\Phi^*_l + U_A(r^*_l)$ at the set of points $\Phi^*_l = \gamma_1, \ldots, \gamma_n$ and choosing Φ^*_l that gives the maximum value of $r^*_l(\Phi_l)\Phi_l + U_A(r^*_l(\Phi_l))$.

C. Model of Mitigation for Out-of-Band Wormhole

The mitigation model is as follows. Each packet is assigned a packet leash chosen by the source, so that the packet is valid for time $\frac{R}{c} + \Delta_{max}$, where R is the propagation distance, c is the speed of light, and Δ_{max} is the maximum permissible value of the clock skew. When the packet traverses a wormhole, the packet violates the packet leash requirement and is dropped when

$$\frac{R_1}{c} + \frac{R_2}{c} + \alpha_l + \Delta > \frac{R}{c} + \Delta_{max},$$

where R_1 and R_2 are the distances of the sender and receiver from the wormhole start and end points, respectively, and α_l is the wormhole tunnel propagation time as in the previous section. The random variable Δ represents the clock skew between the nodes comprising the link. Hence the probability of a packet drop is equal to

$$P_d = \begin{cases} Pr\left(\Delta > \Delta_{max}\right), & l \text{ valid} \\ Pr\left(\Delta > \frac{1}{c}(R - R_1 - R_2) - \alpha_l + \Delta_{max}\right), & l \text{ wormhole} \end{cases} \tag{5}$$

We assume that the network maintains a lower threshold Δ_{max}, representing a more stringent mitigation strategy, when the rate of flow through a link increases. From (5), the packet drop rate is therefore an increasing function of Δ_{max}.

The effect of the packet leash can be modeled by the increase in delay for each packet due to retransmissions. This additive delay is equal to $\left(\frac{1}{1-P_d} - 1\right) f_l(r_l)$, which represents the additional delay due to packet leash. The dynamics of the additive delay introduced by the mitigation mechanism are given as

$$(H_3) \quad \begin{cases} \dot{r}_l(t) = u^{(3)}_l(t) \\ y^{(3)}_l(t) = \left(\frac{1}{1-P_d} - 1\right)(f_l(r_l(t))) \end{cases}$$

D. Steady-state and Stability Analysis for the Out-of-Band Wormhole

In this section, we analyze the steady-state characteristics of the overall system. As a first step, we define the system $(\tilde{H}_3)$ as

$$(\tilde{H}_3) \quad \begin{cases} \dot{r}_l(t) = u^{(3)}_l(t) \\ \tilde{y}^{(3)}_l(t) = \left(\frac{1}{1-P_d} - 1\right)(f_l(r_l(t))) \\ \qquad - \left(\frac{1}{1-P^*_d} - 1\right) f_l(r^*_l) \end{cases}$$

where P^*_d is the probability of packet drops when the flow allocated to link l is r^*_l. The joint dynamics of the flow allocation, wormhole delay, delays on valid links, and delay introduced by mitigation mechanisms can be represented as a negative feedback interconnection between dynamical systems

$(\tilde{H}_1)$, $(\tilde{H}_2)$, and $(\tilde{H}_3)$ (Figure 4). The following lemma guarantees global asymptotic stability of the overall system.

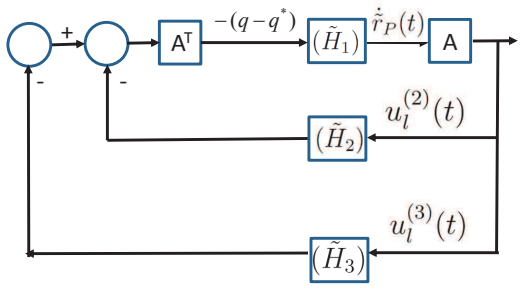


Fig. 4. Block diagram illustrating the out-of-band wormhole link and mitigation. As in Figure 3, systems $(\tilde{H}_1)$ and $(\tilde{H}_2)$ are passive dynamical systems representing flow allocation and link delays respectively. Passive dynamical system $(\tilde{H}_3)$ represents the network mitigation mechanisms. By Corollary 4.9, the interconnection of these passive systems is asymptotically stable.

Lemma 4.8: The system $(\tilde{H}_3)$ is passive from input $u_l^{(3)}(t)$ to output $\tilde{y}_l^{(3)}(t)$.

Proof: Define

$$V_l(r_l) = \int_{r_l^*}^{r_l} \left(\left(\frac{1}{1-P_d(s)} - 1 \right) f_l(s) - \left(\frac{1}{1-P_d^*} - 1 \right) f_l(r_l^*) \right) ds.$$

Since $\left(\frac{1}{1-P_d(s)} - 1 \right) f_l(s)$ is nondecreasing as a function of s, $V_l \geq 0$. Furthermore, $V_l(r_l^*) = 0$ and

$$\begin{aligned} \dot{V}_l(t) &= \left(\left(\frac{1}{1-P_d(r_l)} - 1 \right) f_l(r_l) - \left(\frac{1}{1-P_d^*} - 1 \right) f_l(r_l^*) \right) \dot{r}_l \\ &= \dot{r}_l \tilde{y}_l^{(3)}(t), \end{aligned}$$

thus establishing passivity of $(\tilde{H}_3)$. ■

Corollary 4.9: The system of Figure 4 is globally asymptotically stable.

Proof: By Theorem 4.6, the blocks $(\tilde{H}_1)$ and $(\tilde{H}_2)$ in Figure 4 form a negative feedback interconnection of passive systems, and hence are passive. Since $(\tilde{H}_3)$ is passive by Lemma 4.8, the system consists of a negative feedback interconnection of passive systems, which is globally asymptotically stable. ■

Corollary 4.9 implies that the overall system consisting of the flow allocation, out-of-band wormhole, and mitigation converges to a unique stable equilibrium point. This enables the characterization of delay experienced by the networked control system in steady state.

Our passivity based approach for modeling and mitigating in-band wormhole attacks is described in the following section.

V. Proposed Passivity Framework for In-band Wormhole

In this section, we present a passivity framework for modeling and detecting in-band wormhole attacks mounted by colluding malicious nodes. As in the out-of-band case, the goal of each source is to select the flow rate on each path in order to minimize the average delay experienced while avoiding the wormhole tunnel. In designing network dynamics, including the source rates and detection mechanism, that achieve this goal, we first model the delay experienced on the wormhole link as a function of the number of compromised nodes. Since the delay depends on the number of compromised nodes, we then model the temporal dynamics of the number of compromised nodes. Lastly, we incorporate the impact of the detection mechanism described in Section III on both the valid and wormhole links, and show stability of the overall system.

A. Delay Characteristics of the In-Band Wormhole

Delays experienced by packets traversing an in-band wormhole are proportional to the number of nodes comprising the wormhole tunnel. Let W_1 and W_2 denote the compromised nodes that create the in-band wormhole tunnel. Recall from Section III that, in order to avoid wormhole tunnel collapse, packets entering the wormhole tunnel must be routed through a third colluding node, denoted W_3. The number of hops in the wormhole tunnel is therefore equal to $d(W_1, W_3) + d(W_3, W_2)$. Furthermore, from Lemma 3.1, the node W_3 must satisfy

$$d(W_1, W_3) < d(W_2, W_3) + 3. \tag{6}$$

While the locations of W_1 and W_2 are fixed for a given wormhole tunnel, the location of W_3 depends on the set of nodes compromised by the adversary, denoted $\mathcal{C}$.

In order to minimize delays, and therefore attract more network flow to the wormhole tunnel, the adversary selects the node $W_3 \in \mathcal{C}$ that minimizes $d(W_1, W_3) + d(W_3, W_2)$ to collude in establishing the wormhole, subject to the constraint (6). Letting x denote the fraction of nodes that are misbehaving, and letting $\tilde{\mathcal{C}} = \{W_3 \in \mathcal{C} : d(W_1, W_3) < d(W_2, W_3)+3\}$, we define

$$\beta(x) \triangleq \mathbf{E}\left[\min_{W_3 \in \tilde{\mathcal{C}}} \{d(W_1, W_3) + d(W_3, W_2)\} \mid |\mathcal{C}| = nx \right],$$

where $\mathbf{E}(\cdot)$ denotes expectation and n is the total number of nodes.

Since the delay experienced by the in-band wormhole is a function of the fraction of compromised nodes, a dynamical model of the fraction of compromised nodes is required.

B. Dynamics of Fraction of Compromised Nodes

The goal of the adversary is to minimize the delay of the wormhole link by compromising nodes. We let $c_A x$, where $c_A > 0$, denote the cost of compromising a fraction x of the nodes, and define the adversary's utility function by $U_A(x) \triangleq (n - \beta(x)) - c_A x$, where the first term is the reduction in the path length caused by compromising the fraction of nodes x, and $c_A x$ is the cost. In order to obtain the maximum value, we assume that the adversary chooses the rate at which nodes are compromised via a gradient ascent algorithm, so that

$$\dot{x}(t) = (-\beta'(x) - c_A)_+, \tag{7}$$

where $(z)_+ = z$ if $z \geq 0$ and $(z)_+ = 0$ otherwise. The following proposition proves that $U_A(x)$ has a unique global maximum.

Proposition 5.1: Suppose that, for a given value of x, the set of compromised nodes is chosen uniformly at random from $\mathcal{C}_x = \{\mathcal{C} : |\mathcal{C}| = nx\}$. Then the function $\beta(x)$ is decreasing and convex in x.

A proof can be found in [8]. Intuitively, $\beta(x)$ is a non-increasing function in x since as the number of colluding malicious nodes increases, the number of paths that can potentially be used as in-band wormhole tunnels also increases.

Proposition 5.1 implies that the dynamics (7) converge to a unique equilibrium which is the global maximum of the utility function. To complete the model of the in-band wormhole, the next step is modeling the mitigation by the network.

C. Model of Mitigation for In-Band Wormhole

The detection of the in-band wormhole is based on the probability that a communication link is a wormhole tunnel, given observation of the flow rate through the link and the associated delay characteristics. A link experiencing anomalously long delays is judged to have a high probability of being a wormhole. We define B_1 as the event that link l is a wormhole and B_0 as the event that link l is valid. Furthermore, we let $w_l(t)$ denote the system's belief at time t that the link l is a wormhole, with $w_l(t) = Pr(B_1|r_l(t), p_l(t))$, where

$$p_l(t) = \begin{cases} f_l(r_l(t)), & l \text{ valid} \\ \beta_l(x)f(r_l), & l \text{ wormhole} \end{cases}$$

The effect of the detection process on the flow allocation is modeled as an increase in the link price, so that the price is increased by $K\mathbf{1}(w_l(t) > \overline{w})$, where K represents a penalty for routing packets through suspected wormhole links, $\mathbf{1}$ denotes the indicator function, and $\overline{w}$ is a predefined threshold.

A model of the wormhole delay dynamics, taking the derivative of the source rate $\dot{r}$ as input and giving the delay $p - p^*$ as output, is given by

$$(H_l) \begin{cases} \dot{r}_l(t) &= u(t) \\ \dot{x}(t) &= (-\beta'(x) - c_A)_+ \\ y_l(t) &= \beta_l(x)f(r_l) + K(\mathbf{1}(w_l(t) > \overline{w})) \end{cases}$$

The source rate dynamics are unchanged from Section IV, since detection is performed at the link instead of the source level. The steady-state behavior of the system is described as follows.

D. Steady-state and Stability Analysis for the In-Band Wormhole

In this section, we prove the stability of the in-band wormhole, enabling us to characterize the average delay due to the wormhole in steady state. Stability of the network in the presence of the in-band wormhole is a result of the following proposition, which establishes the passivity of the wormhole link price.

Proposition 5.2: The wormhole link dynamics (H_l) are passive with input $\dot{r}_l$ and output y_l.

Proof: To prove passivity when l is a wormhole link, we use the Lyapunov function $V_l(\cdot)$ defined by

$$\begin{aligned} V_l(r_l, x) = \int_{r_l^*}^{r_l} & \beta_l(x)f(s) - \beta_l(x^*)f(r_l^*) \\ & + K(\mathbf{1}(w_l(t) > \overline{w}) - \mathbf{1}(w_l^* > \overline{w}))\ ds \\ & + \int_{x^*}^{x} \left(\int_0^{r_l^*} f(v)\ dv \right) \beta_l'(s)\ ds. \end{aligned}$$

We have

$$\begin{aligned} \dot{V}_l(r_l, x) &= (\beta_l(x)f(r_l) - \beta_l(x^*)f(r_l^*) \\ &\quad + K(\mathbf{1}(w_l(t) > \overline{w}) - \mathbf{1}(w_l^* > \overline{w})))u_l \\ &\quad + \beta_l'(x) \left(\int_{r_l^*}^{r_l} f(s)\ ds + \int_0^{r_l^*} f(s)\ ds \right) \dot{x} \\ &= y_l u_l + \beta_l'(x) \left(\int_0^{r_l} f(s)\ ds \right) (-\beta_l'(x) - c_A)_+ \\ &\leq y_l u_l, \end{aligned}$$

where the final inequality follows from the the fact that $\beta_l(x)$ is nonincreasing (Proposition 5.1) and $f(s) \geq 0$. The fact that $V_l(r_l^*, x^*) = 0$ holds by inspection. It remains to show that $V_l(r_l, x) \geq 0$ for all r_l and x. This holds because f_l and $\mathbf{1}(w_l(t) > \overline{w})$ are assumed to be nondecreasing functions of r_l, while β_l' is an increasing funtion of x by Proposition 5.1. ■

The stability of the system under the in-band wormhole attack is established by the following theorem.

Theorem 5.3: The source rate $\mathbf{r}_i$ satisfies $\lim_{t\to\infty} \mathbf{r}_i(t) = \mathbf{r}_i^*$.

Proof: The proof follows from the passivity of the source rate (Theorem 4.6) and wormhole delay (Proposition 5.2), and the fact that they form a negative feedback interconnection. ■

Theorem 5.3 implies that the average delay converges to a stable point in the presence of in-band wormhole.

In what follows, using our framework, we show how complex wormhole attacks consisting of both in- and out-of band wormholes can be jointly modeled and mitigated.

VI. Joint Modeling of Out-of-Band and In-Band Wormholes

At present, in the security literature, out-of-band wormholes and in-band-wormholes are treated using different methods. A more general wormhole that consists of in-band and out-of-band wormholes has not been identified or discussed, though such wormholes can be conceived. Our framework can naturally model complex wormholes formed by composing in-band and out-of-band wormholes.

We consider a system with a set of out-of-band wormhole links $\mathcal{L}' = \{l_1', \ldots, l_w'\}$ and in-band wormhole links $\mathcal{L}'' = \{l_1'', \ldots, l_w''\}$. The delay experienced by a valid link is an increasing function of r_l, the flow through the link. The delay experienced by an out-of-band wormhole link is defined by the propagation time and the packet dropping rate, as described in Section IV. For an in-band wormhole link, the delay experienced by the wormhole link is function of the expected number of hops in the wormhole tunnel, as described

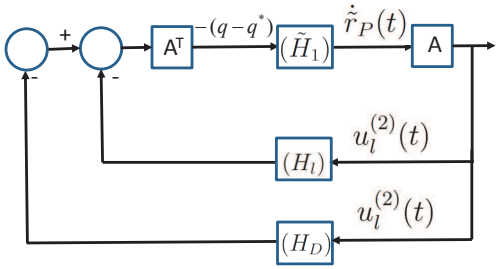


Fig. 5. Illustration of the interconnection between flow allocation, link delay characteristics, and mitigation when multiple out-of-band and in-band wormholes are present. The system $(\tilde{H}_1)$ defines the flow allocation dynamics as a function of observed delays. The system (H_l) defines the delays experienced by valid, out-of-band, and in-band wormhole links as a function of the flow rates. The system (H_D) models the impact of mitigation mechanisms on the flow allocation dynamics.

in Section V. These delay characteristics are described by the following dynamics, where the input $u(t)$ is equal to the change in the source rate $\dot{r}(t)$:

$$(H_l)\begin{cases} \dot{r}_l(t) = u_l(t) \\ y_l(t) = \frac{\alpha_l}{1-\Phi_l(r_l)} - \frac{\alpha_l}{1-\Phi_l(r_l^*)}, & l \in \mathcal{L}' \\ y_l(t) = \beta_l(x) f(r_l) - \beta_l(x^*) f(r_l^*), & l \in \mathcal{L}'' \\ y_l(t) = f_l(r_l) - f_l(r_l^*), & \text{else} \end{cases}$$

We assume that the network employs mitigation schemes for both the in- and out-of-band wormholes. The out-of-band wormhole mitigation mechanism increases the delay on valid and out-of-band wormhole links as discussed in Section IV. However, since the in-band wormhole contains colluding nodes that can modify the time stamps using valid cryptographic keys, the out-of-band wormhole mitigation is ineffective and hence adds no delay to in-band wormhole links. The in-band wormhole mitigation mechanism described in Section V is employed on the valid and in-band wormhole links. Since the out-of-band wormhole link is created using a high capacity, low-latency channel, the adversary can manipulate the delays in order to thwart the statistical mitigation mechanism. Hence our model of the impact of mitigation on the link delays is given by the following dynamics:

$$(H_D)\begin{cases} \dot{r}_l(t) = u_l(t) \\ y_l(t) = \left(\frac{1}{1-P_d} - 1\right) f_l(r_l) - \left(\frac{1}{1-P_d^*} - 1\right) f_l(r_l^*), \\ \qquad\qquad l \in \mathcal{L}' \\ y_l(t) = K(\mathbf{1}(w_l(t) > \overline{w}) - \mathbf{1}(w_l^* > \overline{w})), \\ \qquad\qquad l \in \mathcal{L}'' \\ y_l(t) = \left(\frac{1}{1-P_d} - 1\right) f_l(r_l) - \left(\frac{1}{1-P_d^*} - 1\right) f_l(r_l^*) \\ \qquad +K(\mathbf{1}(w_l(t) > \overline{w}) - \mathbf{1}(w_l^* > \overline{w})), \\ \qquad\qquad \text{else} \end{cases}$$

The flow allocation, delay, and mitigation models are illustrated in Figure 5. The following theorem characterizes the stability properties of the system when both in-band and out-of-band wormholes are present.

Theorem 6.1: The interconnected system of Figure 5 is globally asymptotically stable.

Proof: By Theorem 4.6, the top block of Figure 5 is strictly passive. The blocks (H_l) and (H_D) are passive by Theorem 4.6 (if l is an out-of-band wormhole) and Proposition 5.2 (if l is an in-band wormhole). Hence the negative feedback interconnection of Figure 5 is globally asymptotically stable. ■

Theorem 6.1 implies the passivity based framework enables us to compose in-band and out-of-band wormholes and characterize the overall delay and flow allocation.

VII. Numerical Study

In this section, we conduct a numerical study using MATLAB. We use our passivity-based framework to answer the following questions for the out-of-band and in-band wormhole attacks: 1) What is the overall flow allocated and delays experienced by sources for a given adversary's strategy? and 2) How do the proposed mitigation methods affect the flow allocation and delays experienced by sources? 3) What is the impact of wormhole attack on a networked control system?

We consider a network which consists of two source nodes S_1, S_2 and a single destination node D shown in Figure 7. The source rates for sources 1 and 2 are given as 10 and 5, respectively. Each source allocates flows to three different paths. We denote the path which traverses links 4 and 5 as path 1, the path which traverses links 6 and 7 as path 2, and the path which traverses link 9 as path 3. We assume the propagation

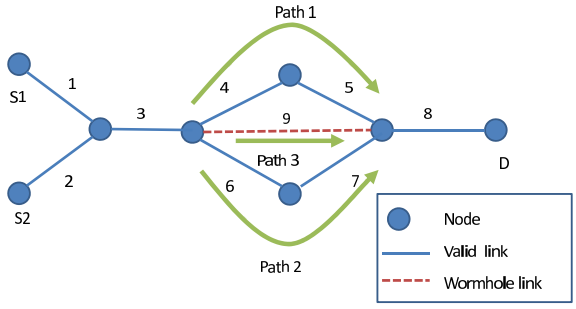


Fig. 7. Network topology used in numerical study. Two sources send flows with total rate of 10 and 5 to destination D. Each source maintains a path through links 4 and 5 (path 1), a path through links 6 and 7 (path 2), and a path through the wormhole link 9 (path 3).

delays for valid links are equal and normalized to 1 time unit. The average delay is given as the propagation delay times the expected number of transmissions. The expected number of transmissions for a link is given as $\frac{1}{1-P_d}$ where P_d is the probability of a packet drop. For valid links, we assume the probability of packet drop is due to buffer overflow in an M/M/1/K queue [18]. We denote $\rho_l = \frac{r_l}{c_l}$, where r_l is the amount of traffic flowing into link l, and c_l is the capacity of link l. The probability of a packet drop is given as

$$P_d = \frac{\rho^K - \rho^{K+1}}{1 - \rho^{K+1}} \tag{8}$$

In this simulation, we assume the buffer size $K = 5$ for all links.

The propagation delay for the wormhole tunnel, α_l, is assumed to be 2. The clock skew Δ is an exponential random variable with mean 1. $\Delta_{\max}$ is given as

$$\Delta_{\max} = \alpha_l - 1 + \frac{1}{r}, \tag{9}$$

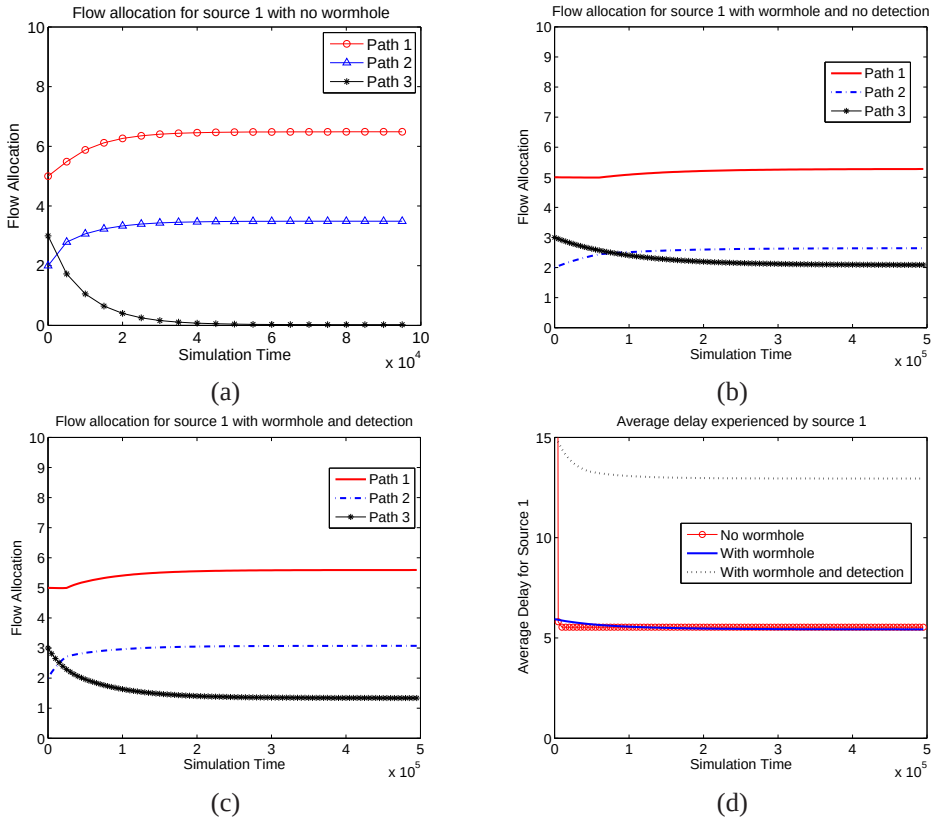


Fig. 6. Simulation of our passivity framework for modeling the out-of-band wormhole. The time scales represent the number of iterations of the simulation. Each iteration represents a single update step of the wormhole dynamics. The source rates for sources 1 and 2 are given as 10 and 5. Initial flow allocation for source 1 is [5,2,3], and flow allocation for source 2 is [2,2,1] for paths 1, 2, and 3 respectively. (a) The convergence of flow allocation without the wormhole when link 9 has capacity 0.01. (b) The impact of the wormhole on flow allocation with no mitigation mechanisms. (c) The flow allocation when packet leashes method are used.

which is a monotonic decreasing function in r.

A. Simulation of the Out-of-band Wormhole

In the out-of-band wormhole simulation, we assume that link 9 in Figure 7 is the wormhole link. The propagation delay for the wormhole link is denoted as α_l, where $\alpha_l > 1$ due to longer physical distance the packet traverses through the wormhole link. The delay for the wormhole link is given as $\frac{\alpha_l}{1-\Phi(r)}$ where $\Phi(r)$ is the dropping rate of packets that flow into the wormhole link. The function $\Phi(r)$ is given as $\Phi(r) = (1-\frac{1}{r})\mathbf{1}_{(r>1)}$.

We illustrate the impact of the out-of-band wormhole by comparing the flow allocation without the wormhole (Figure 6(a)) with the flow allocation resulting from the wormhole (Figure 6(b)). In both cases, simulation result shows that our choice of dynamics results in the convergence to the stable equilibrium. Figure 6(a) shows that when path 3 contains a poor quality link with low capacity of 0.01 (link 9), both sources allocate negligible amount of flows to path 3 in equilibrium. Figure 6(b) shows that packet drops by the wormhole path result in increased delay on path 3, thus reducing the flow allocated to path 3. At the equilibrium, the wormhole drops half of the packets on average. As a result, the wormhole is able to attract only 2 units of flow from both source 1 and 2 combined.

Figure 6(d) shows that in order to attract flow, the wormhole has to provide a low-latency link whose performance is comparable to other links. Therefore, the average delay experienced by the sources is approximately the same regardless of the presence of the wormhole link. Figure 6(c) shows that when packet leash mitigation methods are employed, the amount of flow allocated to the wormhole link is reduced from 2 to 1.3 units. The overall delay, however, increases due to packet drops caused by the packet leash mitigation method.

B. Simulation of the In-band Wormhole

In the in-band wormhole simulation, we assume that link 9 is an in-band wormhole. Upon receiving packets allocated to path 3, the malicious node allocates λ fraction of traffic to path 1 and $1-\lambda$ fraction of traffic to path 2. This results in increased traffic to paths 1 and 2 and hence increased overall delay experienced by sources. The perceived delay for path 3 is given as $q(P_3) = \lambda q(r_{P_1} + \lambda r_{P_3}) + (1-\lambda) q(r_{P_2} + (1-\lambda) r_{P_3})$. The mitigation mechanism is based on the anomalous delay experienced at the wormhole link. The link will be avoided if the ratio of actual delay experienced at link l, denoted D_l, to the expected delay exceeds a predefined threshold. The penalty of $K = 10$ was added to the link price when $\log \frac{D_l}{f_l(r_l)} > 0$. The delay experienced at link l is modeled as an exponential random variable with mean $f_l(r_l)$.

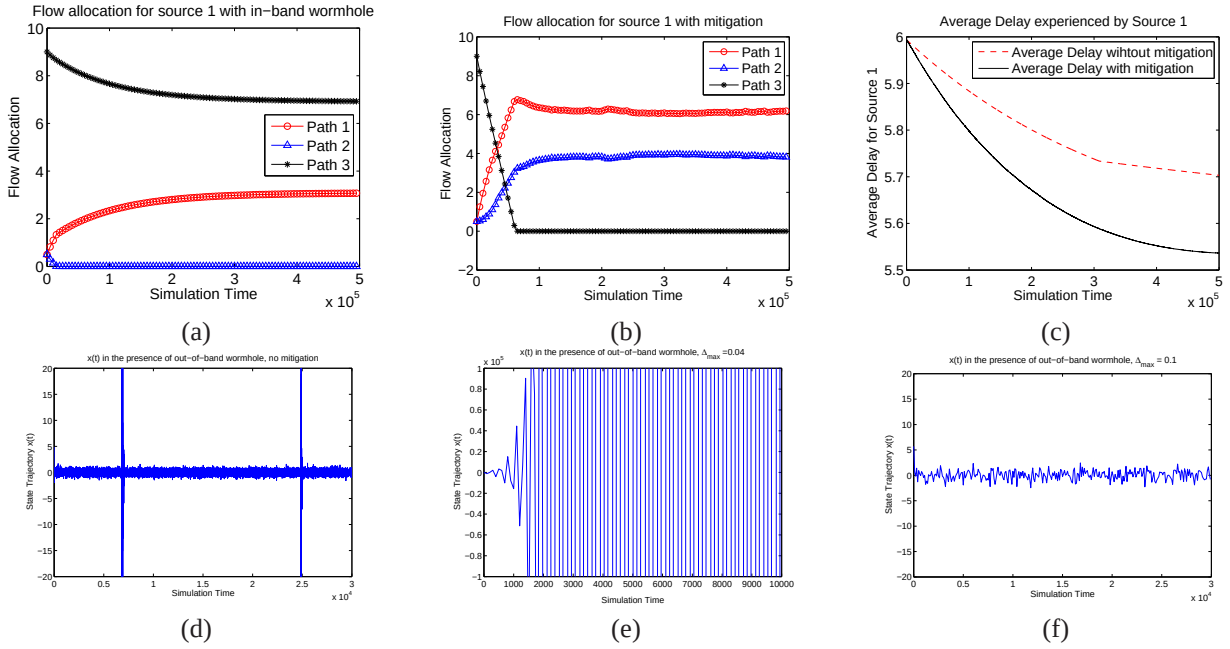


Fig. 8. Simulation of our passivity framework for modeling the in-band wormhole and the effect of wormhole attacks on the networked control system. The time scales represent the number of iterations of the simulation. Each iteration represents a single update step of the in-band wormhole dynamics. The source rates for sources 1 and 2 are given as 10 and 5. Initial flow allocation for source 1 is [0.5,0.5,9], and flow allocation for source 2 is [0.5,0.5,4] for paths 1, 2, and 3 respectively. Link 9 is an wormhole link with falsely advertised capacity of 15. Packets allocated to path 3 will be rerouted to path 1 with probability 0.3 and to path 2 with probability 0.7. (a) The impact of an in-band wormhole on flow allocation with no mitigation mechanisms. (b) The flow allocation when mitigation method is used. (c) The impact of mitigation method on average delay. (d) No mitigation strategy employed (e) Packet-leash is employed with $\Delta_{\max} = 0.04$ (f) Packet-leash is employed with $\Delta_{\max} = 0.1$.

We evaluate the impact of the in-band wormhole on flow allocation (Figure 8(a)). Packets allocated to path 3, which contains the wormhole link, are rerouted by the adversary to path 2 with probability 0.7. This results in longer delay experienced over path 2. Without mitigation, source 1 is unaware of packets flowing through wormhole tunnels, and allocates all its traffic through paths 1 and 3. Figure 8(b) shows the flow allocation when statistical mitigation method is used. Since the packets allocated to path 3 do not traverse a one-hop link with capacity 15 as advertised, but instead traverse a two-hop path with lower capacity, the delay will deviate significantly from its expected value. Hence the statistical mitigation mechanism will identify the wormhole link (link 9) with high probability. This results in an equilibrium point similar to the case without wormhole. Figure 8(c) shows the impact of mitigation on average delay. The average delay experienced by source 1 is reduced when mitigation is used. These results suggest that the sources become aware of the true topology of the network, which does not contain path 3, and achieve a Wardrop equilibrium consisting only of paths 1 and 2.

C. Simulation of Impact of Out-of-band Wormhole on a Physical System

We now study the impact of the out-of-band wormhole on a physical system. We consider a networked control system where the control loop is closed through the network shown in Figure 7. The physical plant considered is a single-input, single-output integrator with dynamics given in equation (10). We assume the state value $x(t)$ is measured, and sampled every $h = 0.3$ time units by node S_1 and relayed to the controller node D. Disturbance $w(t)$ is assumed to be white Gaussian noise with zero mean and variance 1. Control gain $G = 2$ is considered in the simulation.

$$\begin{aligned} \dot{x}(t) &= u(t) + w(t), \quad t \in [kh + \tau_k, (k+1)h + \tau_{k+1}] \\ u(t) &= -Gx(t - \tau_k), \quad t \in [kh + \tau_k, (k+1)h + \tau_{k+1}] \end{aligned} \tag{10}$$

We consider the same M/M/1/K queue model for valid links except the propagation delay α_l for valid links is now assumed to be 0.05 time units, and propagation delay for the out-of-band wormhole link (link 9) is assumed to be 0.1 time units. Adversary controlling the wormhole link provides a low-latency link with delay 0.1 when the flow rate traversing through the wormhole is less than 5 units of flow, and once the flow rate through the wormhole link exceeds 5 units of flow, the adversary drops packets with probability 0.9.

We evaluate the impact of out-of-band wormhole on the physical system in three different cases. In the first case, we assume no mitigation strategy is employed by the network. In the second and third cases, we assume packet leash defense is employed with $\Delta_{\max} = 0.04$ and $\Delta_{\max} = 0.1$ respectively. The clock skew Δ is assumed to be an exponential random variable with mean 0.05.

The impact of wormhole on the physical plant when no mitigation strategy is employed is illustrated in Figure 8(d). Adversary first starts providing a low-latency link, attracting a large amount of packets traversing through the wormhole. Once the flow rate through the wormhole exceeds the threshold, the adversary drops packets with high probability, resulting in large disturbance of the plant state $x(t)$. Source

node S_1 reallocates flows to paths 1 and 2 once high delay is observed on path 3, and adversary starts attracting flows again by providing low-latency link.

Figures 8(e) and (f) illustrate the effect of mitigation strategies on the physical plant. In both cases, flows allocated to path 3 quickly converges to 0 due to packet leash. However, as shown in Figure 8(e), a stringent packet leash with $\Delta_{\max} = 0.04$ results in growing oscillation of $x(t)$ due to overall increased delay. On the other hand, Figure 8(f) illustrates that when $\Delta_{\max}$ is chosen appropriately as $\Delta_{\max} = 0.1$, the plant stabilizes around the equilibrium point while successfully mitigating the wormhole attack. This case study shows that parameters of the defense mechanism need to be chosen and adjusted over time to mitigate the attack while maintaining the performance of the physical plant.

VIII. Conclusion

In this paper, we studied the wormhole attack on networked control systems, in which an adversary creates a link between two geographically distant network regions, either using a side channel, as in the out-of-band wormhole, or by colluding network nodes, as in the in-band wormhole. Using the wormhole attack, the adversary can cause violations of timing constraints in real-time systems, including dropping or delaying packets flowing into wormholes. We presented a passivity-based control-theoretic framework for modeling and mitigating the wormhole attack. Under our framework, the flow allocation of the valid nodes, the delays experienced on the wormholes, and the wormhole mitigation algorithms were modeled as distinct, interconnected passive dynamical systems. The passivity approach enabled us to prove stability and convergence of the system to a unique equilibrium, which satisfies the criteria for the well-known Wardrop equilibrium, under general assumptions on the adversary behavior and network mitigation mechanism. This allowed us to characterize the delays experienced by source nodes at the steady-state.

For the out-of-band wormhole attack, we quantified the increase in delay caused by the wormhole link and mapped the adversary's strategy to the optimization problem of selecting the packet-dropping rate. We also introduced an approach for dynamically adapting the parameters of packet leash-based defenses in response to the observed network delays. For the in-band wormhole, we used spatial statistics to estimate the delays experienced by the wormhole tunnel as a function of the number of misbehaving network nodes. In addition, we identified a new class of complex wormhole attacks consisting of both in- and out-of band wormholes, which we modeled and analyzed using our framework.

Our simulation results illustrate the trade-off between the effectiveness of the network defense and the increase in delay for the out-of-band case. In particular, we found that out-of-band wormhole causes large disturbances in the physical system by selectively dropping packets, and the parameters of packet leash defense can be chosen to reduce flow allocation to the wormhole while satisfying the delay constraint of the physical system. For the in-band case, our simulation suggests that the network defense allows the system to reach the same flow allocation equilibrium regardless of the presence of wormhole.

In our future work, we will investigate whether the steady-state values of our passivity framework arise as equilibria of an equivalent dynamic game between the network and adversary.

Appendix A
Background on Passivity

We consider a state-space model (Σ), with state $x(t)$, input $u(t)$, and output $y(t)$, defined by

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

The definitions and results in this subsection can be found in [19]. A passive system is defined as follows.

Definition A.1: The system (Σ) is passive if there exists a nonnegative C^1 function $V : \mathbb{R} \to \mathbb{R}_{\geq 0}$ satisfying $V(0) = 0$ and

$$\dot{V}(t) \leq -S(x(t)) + u(t)^T y(t) \tag{11}$$

where $S(\cdot)$ is a nonnegative continuous function. If $S(x) > 0$ for all $x \neq 0$, then the system is *strictly passive*. A function V satisfying (11) for a system (Σ) is a *storage function* for (Σ).

The following two lemmas are used to construct passive systems as interconnections of passive components.

Lemma A.2: Suppose that the system (Σ) is passive with $u(t) \in \mathbb{R}^m$ and $y(t) \in \mathbb{R}^n$. Then for any $m \times n$ matrix A, the system Σ', defined by

$$(\Sigma')\begin{cases} \dot{x}(t) &= f(x(t), A^T u'(t)) \\ y'(t) &= Ag(x(t), A^T u'(t)) \end{cases}$$

is passive from input $u' \in \mathbb{R}^n$ to output $y' \in \mathbb{R}^m$.

Lemma A.3: The negative feedback interconnection of two passive systems is passive. If at least one of the systems is strictly passive, then the negative feedback interconnection is strictly passive.

Passivity leads to a variety of techniques for guaranteeing stability of dynamical systems, such as the following proposition.

Proposition A.4: A negative feedback interconnection between two passive systems is globally asymptotically stable if at least one of the systems is strictly passive.

For a negative feedback interaction between two strictly passive systems with storage functions V_1 and V_2, the function $V = V_1 + V_2$ is a Lyapunov function for the combined system.

References

[1] M. Pajic, S. Sundaram, G. Pappas, and R. Mangharam, "The wireless control network: A new approach for control over networks," *IEEE Transactions on Automatic Control*, vol. 56, no. 10, pp. 2305–2318, 2011.

[2] F. Jahanian and A. K.-L. Mok, "Safety analysis of timing properties in real-time systems," *IEEE Transactions on Software Engineering*, no. 9, pp. 890–904, 1986.

[3] Y.-C. Hu, A. Perrig, and D. B. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," *Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies (INFOCOM)*, pp. 1976–1986, 2003.

[4] 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.

[5] P. Kruus, D. Sterne, R. Gopaul, M. Heyman, B. Rivera, P. Budulas, B. Luu, T. Johnson, N. Ivanic, and G. Lawler, "In-band wormholes and countermeasures in OLSR networks," *Securecomm and Workshops, 2006*, pp. 1–11, 2006.

[6] R. Poovendran and L. Lazos, "A graph theoretic framework for preventing the wormhole attack in wireless ad hoc networks," *Wireless Networks*, vol. 13, no. 1, pp. 27–59, 2007.

[7] F. Schneider, "Blueprint for a science of cyber security," *The Next Wave*, vol. 19, no. 2, pp. 47–57, 2012.

[8] P. Lee, A. Clark, L. Bushnell, and R. Poovendran, "A passivity framework for modeling and mitigating wormhole attacks on networked control systems," *arXiv preprint*, 2013.

[9] R. Song, P. C. Mason, and M. Li, "Enhancement of frequency-based wormhole attack detection," *IEEE Military Communications Conference (MILCOM)*, pp. 1139–1145, 2011.

[10] V. Mahajan, M. Natu, and A. Sethi, "Analysis of wormhole intrusion attacks in MANETs," *IEEE Military Communications Conference (MILCOM)*, pp. 1–7, 2008.

[11] J. S. Baras, S. Radosavac, G. Theodorakopoulos, D. Sterne, P. Budulas, and R. Gopaul, "Intrusion detection system resiliency to byzantine attacks: The case study of wormholes in OLSR," *IEEE Military Communications Conference (MILCOM)*, pp. 1–7, 2007.

[12] 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.

[13] M. Chiang, S. H. Low, A. R. Calderbank, and J. C. Doyle, "Layering as optimization decomposition: A mathematical theory of network architectures," *Proceedings of the IEEE*, vol. 95, no. 1, pp. 255–312, 2007.

[14] Y. Wang, V. Gupta, and P. J. Antsaklis, "On passivity of networked nonlinear systems with packet drops," *ISIS Technical Report*, 2012.

[15] A. Clark, L. Bushnell, and R. Poovendran, "A passivity-based framework for composing attacks on networked control systems," *50th Allerton Conference on Communication, Control, and Computing*, 2012.

[16] P. Lee, A. Clark, L. Bushnell, and R. Poovendran, "Modeling and designing network defense against control channel jamming attacks: A passivity-based approach," *to appear in IEEE Annual Conference on Information Sciences and Systems, Workshop on Control of Cyber-Physical Systems*, March 2013.

[17] E. Altman and L. Wynter, "Equilibrium, games, and pricing in transportation and telecommunication networks," *Networks and Spatial Economics*, vol. 4, no. 1, pp. 7–21, 2004.

[18] S. M. Ross, *Introduction to Probability Models*. Academic Press, 2009.

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

Phillip Lee (S'14) is currently a Ph.D. candidate in the Department of Electrical Engineering at the University of Washington. He received the B.S. (*magna cum laude*) degree in Electrical Engineering and the M.S. degree in Electrical and Computer Engineering from the University of Washington - Seattle and University of California - San Diego in 2006 and 2009, respectively. He is a recipient of the Powell fellowship award in 2006. His research interests include control-theoretic modeling of cyber threats, modeling and design of cyber-physical systems and smart-grid security.

Andrew Clark (S'09) is currently a Ph.D. candidate in the Department of Electrical Engineering at the University of Washington. He received the B.S. degree in Electrical Engineering and the M.S. degree in Mathematics from the University of Michigan - Ann Arbor in 2007 and 2008, respectively. He was co-author of the IEEE/IFIP William C. Carter award-winning paper (2010) and the WiOpt Best Paper (2012), and was a finalist for the IEEE CDC 2012 Best Student Paper Award. His research interests include leader selection for control and security of complex networks, control-theoretic modeling of network security threats, and deception-based network defense mechanisms.

Linda Bushnell (SM'99) received the B.S. and M.S. degrees in electrical engineering from the University of Connecticut, Storrs, CT, USA, in 1985 and 1987, the M.A. degree in mathematics and the Ph.D. degree in electrical engineering from the University of California, Berkeley, CA, USA, in 1989 and 1994, and the MBA from the University of Washington, Seattle, WA, USA, in 2010. She is currently a Research Associate Professor in the Department of Electrical Engineering, University of Washington. Her research interests include networked control systems and control of complex networks. Dr. Bushnell is a recipient of the US Government Superior Civilian Service Award, National Science Foundation ADVANCE Fellowship, and IEEE Control Systems Society (CSS) Recognition Award. For IEEE CSS, she is a Distinguished Lecturer, a member of the Women in Control Committee, a member of the TC Control Education, Liaison to IEEE Women in Engineering, and 2014 Appointed Member to the Board of Governors. Previously, she was the Secretary-Administrator, Member of the Executive Committee, Member of the Board of Governors, Associate Editor of the IEEE Control Systems Magazine, Chair of the History Standing Committee, Vice-Chair for Invited Sessions for 2001 CCA, and Vice-Chair for Invited Sessions for 2000 CDC. For AACC, she is currently the Treasurer of the AACC and a member of the TC on Control Education. She was the Workshop Chair for 2013 ACC, Technical Program Chair for 2007 ACC, Publicity Chair for 2005 ACC, Vice-Chair for Publications for 1999 ACC, and Vice-Chair for Invited Sessions for 1998 ACC. For ACM, she is the General Co-Chair for the Conference on High Confidence Networked Systems (HiCoNS) at CPSWeek 2014, and was the Technical Program Chair for HiCoNS at CPSWeek 2013.

Radha Poovendran (SM'06) is a Professor and founding director of the Network Security Lab (NSL) in the Electrical Engineering (EE) Dept. at the University of Washington (UW). He is a founding member and the associate director of research of the University of Washington Center for Excellence in Information Assurance Research and Education. His research interests are in the areas of wireless and sensor network security, adversarial modeling, privacy and anonymity in public wireless networks, control-security, games-security and Information Theoretic-Security in the context of wireless mobile networks. Professor Poovendran is a recipient of the NSA LUCITE Rising Star Award (1999), National Science Foundation CAREER (2001), ARO YIP (2002), ONR YIP (2004), and PECASE (2005) for his research contributions to multi-user wireless security. He is also a recipient of the Outstanding Teaching Award and Outstanding Research Advisor Award from UW EE (2002) and Graduate Mentor Award from Office of the Chancellor at University of California San Diego (2006). He was co-author of award-winning papers including IEEE&IFIP William C. Carter Award Paper (2010) and WiOpt Best Paper Award (2012). He has co-chaired multiple conferences and workshops including the first ACM Conference on Wireless Network Security (WiSec) in 2008 and NITRD-NSF National workshop on high-confidence transportation cyber-physical systems in 2009, trustworthy aviation information systems at the 2010 and 2011 AIAA Infotech@Aerospace and 2011 IEEE Aerospace. He was chief editor for the Proceedings of the IEEE special issue on cyber-physical systems (2012), an editor of IEEE TMC and ACM TOSN, co-guest editor for two special issues on security and privacy (IEEE Networks 2013; IEEE TPDS 2013). He co-chairs of the IEEE CNS 2014. He is a co-inventor of four recently issued patents in the area of wireless security.