Queuing the Trust: Secure Backpressure Algorithm against Insider Threats in Wireless Networks

Zhuo Lu
Department of Computer Science
University of Memphis TN 38152
Email: zhuo.lu@memphis.edu

Yalin E. Sagduyu and Jason H. Li
Intelligent Automation Inc.
Rockville MD 20855
Emails: {ysagduyu, jli}@i-a-i.com

***Abstract*—The backpressure algorithm is known to provide throughput optimality in routing and scheduling decisions for multi-hop networks with dynamic traffic. The essential assumption in the backpressure algorithm is that all nodes are benign and obey the algorithm rules governing the information exchange and underlying optimization needs. Nonetheless, such an assumption does not always hold in realistic scenarios, especially in the presence of security attacks with intent to disrupt network operations. In this paper, we propose a novel mechanism, called *virtual trust queuing*, to protect backpressure algorithm based routing and scheduling protocols from various insider threats. Our objective is *not* to design yet another trust-based routing to heuristically bargain security and performance, *but* to develop a generic solution with strong guarantees of attack resilience and throughput performance in the backpressure algorithm. To this end, we quantify a node's algorithm-compliance behavior over time and construct a virtual trust queue that maintains deviations from expected algorithm outcomes. We show that by jointly stabilizing the virtual trust queue and the real packet queue, the backpressure algorithm not only achieves resilience, but also sustains the throughput performance under an extensive set of security attacks.**

I. Introduction

The backpressure algorithm [1]–[4], in theory, achieves the optimal network throughput by dynamically routing and scheduling network traffic. There have been significant efforts focused on translating and adapting the backpressure concept into a practical system for wireless networks [5]–[7].

In essence, the backpressure algorithm coordinates transmissions and maximizes the amount of total data delivery by adapting scheduling and routing decisions based on each node's per-flow queue backlogs and channel states in wireless networks. To this end, it presumes that all nodes obey the algorithm rules of information exchange, optimal link activation, and flow selection. However, in practice, a node may deliberately violate any rule to break the underlying premise assumed by the backpressure algorithm. Regardless of its selfish or malicious intent, there are two basic ways for an attacker to pursue: (i) it can falsify any information used in the backpressure algorithm; (ii) it can violate backpressure based protocols by offering no cooperation and not following decisions in routing and scheduling optimization. These potential attacks pose a major obstacle to practical deployment of the backpressure algorithm in real (especially wireless) systems.

This material is based upon work supported by the Air Force Office of Scientific Research (AFOSR) under grant FA9550-12-C-0037. Any opinions, findings and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the AFOSR.

As security emerges as a fundamental component of network design [5]–[16], it becomes vital to secure the backpressure algorithm against various security attacks. In the literature, integrating the backpressure algorithm into practical network applications [5]–[8], [11]–[13] and securing routing protocols against various attacks [15]–[19] have been investigated rather orthogonally. Recently, a trust-based routing approach was designed in [13] to help the backpressure algorithm defend against attacks in wireless sensor networks. The focus in [13] was on heuristically balancing trust and throughput components in implementation, but not on providing security guarantee of attack resilience.

In this paper, we aim at *providing a generic framework to secure the backpressure algorithm with guaranteed resilience against information falsification and protocol-violation attacks*. To this end, we propose a novel mechanism, called *virtual trust queuing*. There are three key components supporting our mechanism: (i) when an attacker deviates from legitimate behavior, nodes can collectively observe and quantify such a deviation; (ii) each node individually manages all the deviations in a virtual queue for every neighbor node in a distributed setting, and then the queue size can be limited (i.e., the deviation or damage of an attacker can be bounded) by using the queue-stabilizing technique jointly with a real packet queue; (iii) the service rate in a virtual queue can be adequately designed to mitigate imperfect observations (due to wireless effects) or false accusations (e.g., a benign node is mistakenly found to have abnormal behavior due to observation errors). Therefore, we show that the proposed virtual trust queue mechanism provides two performance guarantees: 1) Zero penalty: there is zero throughput performance penalty to use the virtual trust queue in the backpressure algorithm in the presence of no attack; 2) Impact bounding: the damage of attacks to the network can be bounded by a given tolerance level for the virtual trust queue.

We use a comprehensive simulation study to show the effectiveness of the proposed mechanism against an extensive set of security attacks, including blackhole, selective-forwarding, on-off, and opportunity-wasting attacks, as well as selfish behavior to prioritize transmission opportunities. Our contributions are as follows: (i) We develop a new mechanism, called virtual trust queuing, to secure the backpressure algorithm.

(ii) We show that the virtual trust queue mechanism, as a generic solution to secure the backpressure algorithm, offers guaranteed attack resilience as well as sustains the throughput performance for the backpressure algorithm. (iii) We demonstrate that the backpressure algorithm with virtual trust queuing is a viable secure solution for practical implementation of dynamic scheduling and routing in wireless networks. (iv) We conduct extensive simulations to show that the virtual trust queue mechanism can significantly improve the throughput performance by securing backpressure scheduling against a broad range of malicious attacks and selfish node behaviors.

The rest of this paper is organized as follows. In Section II, we describe preliminaries and models for the backpressure algorithm and its vulnerabilities. In Sections III and IV, we design and evaluate the virtual trust queue based backpressure algorithm, respectively. In Section V, we discuss related work. Finally, we conclude the paper in Section VI.

II. Preliminaries: Backpressure and Vulnerabilities

In this section, we use an example to introduce the backpressure algorithm and its vulnerabilities, then formulate the backpressure algorithm, and finally discuss attack models.

A. Example of Backpressure Algorithm and Vulnerabilities

The backpressure algorithm [1]–[4] is an optimal routing and scheduling policy that stabilizes packet queues with capability to achieve the maximum throughput. The backpressure algorithm dynamically selects the set of links to activate and flows to transmit on these links depending on queue backlogs and channel rates. In the following, we consider its application to a time-slotted wireless network.

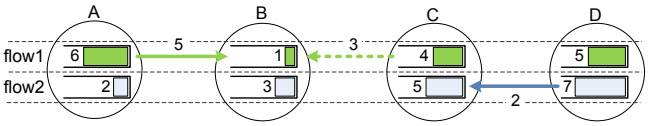

Fig. 1. Example of the backpressure algorithm.

Fig. 1 shows an example of how the backpressure algorithm works: nodes A, B, C, and D form a three-hop wireless network with two flows. Each node has the same transmission rate and cannot transmit and receive at the same time slot. At a time slot, the backlog of each node for each flow is illustrated in Fig. 1. The backpressure algorithm works as follows. First, compute the maximum differential queue backlog between each node pair as a link weight; i.e., A→B is 5 for flow 1, C→B is 3 for flow 1, and D→C is 2 for flow 2, and select these three links. Second, list all non-conflicting link sets, i.e., {A→B for flow 1, D→C for flow 2} and {C→B for flow 1}. Finally, choose the set that maximizes the sum of all link weights, i.e., {A→B for flow 1, D→C for flow 2}.

Now suppose node C is malicious and declares its queue backlog for flow 1 is 100. Then, the maximum differential queue backlog between nodes B and C becomes 99, which makes backpressure scheduling choose only one link {C→B for flow 1}, thereby giving all the transmission opportunity to the malicious node C.

B. Backpressure Algorithm Formulation

More formally, we consider a network denoted by $(\mathcal{N}, \mathcal{F})$, where $\mathcal{N}$ and $\mathcal{F}$ are the sets of network nodes and flows, respectively. At time slot $t = 0, 1, 2, \cdots$, node $i \in \mathcal{N}$ has a queue backlog Q_i^f for flow $f \in \mathcal{F}$. The backpressure algorithm makes routing and scheduling decisions based on

$$\mathbf{u}^*(t) = \arg\max_{\mathbf{u}(t)\in\mathcal{R}(t)} \sum_{u_{i,j}(t)\in\mathbf{u}(t)} u_{i,j}(t) w_{i,j}(t), \tag{1}$$

where $u_{i,j}(t) \in \mathbf{u}(t)$ is the link rate from nodes i to j, $\mathbf{u}(t)$ is a feasible rate vector in the set of all feasible rate vectors $\mathcal{R}(t)$ in the network, and $w_{i,j}(t)$ is the maximum differential queue backlog

$$w_{i,j}(t) = \max_{f\in\mathcal{F}} (Q_i^f(t) - Q_j^f(t)), \tag{2}$$

where $Q_i^f(t)$ and $Q_j^f(t)$ are the backlogs for flow f at nodes i and j, respectively.

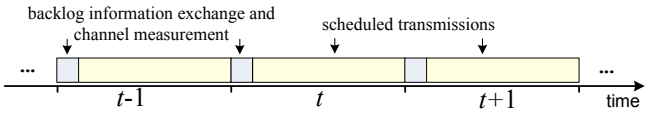

Fig. 2. Information exchange and transmission scheduling in the backpressure algorithm.

In this paper, our focus is not solving the particular optimization in (1), which has been extensively discussed in the literature regarding low-complexity, heuristic or distributed solutions and implementations [5]–[8], [11]. Rather, we aim to develop a generic framework to provide security guarantee integrated into any backpressure based routing protocols.

To this end, we adopt a generic implementation model for the backpressure algorithm shown in Fig. 2: at the beginning of each time slot, nodes broadcast information to their neighbors for distributed scheduling implementation (e.g., [3]) or to a controller for centralized coordination (e.g., [11]). The information includes queue backlogs for computing the differential queue backlog $w_{i,j}(t)$ in (2) and channel state information based on channel measurements for obtaining the best channel rate $u_{i,j}(t)$ for any node i to node j in (1). Then, scheduled transmissions happen at the rest of the time slot.

C. Insider Threats and Assumptions

We consider insider attackers that are nodes also involved in the routing and scheduling decisions in the network. In general, the behavior of an insider attacker can be classified to one or both of the following two categories.

1) *Information-falsification attack*: this happens during the information exchange phase at the beginning of each time slot shown in Fig. 2, where the attacker intentionally sends false information to others to affect backpressure routing. For example, the attacker broadcasts false backlog information or false channel state information

to result in wrong differential backlog computation in (2). As the backpressure algorithm is reactive to node queue backlogs and channel state information, its routing decisions can be significantly affected by information-falsification attacks.

2) *Protocol-violation attack*: this happens in the scheduled transmission phase shown in Fig. 2, where the attacker does not obey backpressure routing decisions. For example, an attacker does not transmit although it is scheduled to transmit at that time slot.

We assume that attackers can neither modify information (e.g., queue backlog) inside other nodes nor change the wireless channel characteristics (e.g., channel gain).

It is worth mentioning that the backpressure algorithm is resilient in terms of throughput performance to imperfect queue backlog estimation, as long as the error is bounded by a constant [20]. In this paper, we consider a different scenario, where attackers can arbitrarily manipulate queue backlogs and channel state information, and launch various attacks using falsified information to degrade the network performance.

III. Securing the Backpressure Algorithm

An attacker can launch either information-falsification or protocol-violation attacks, or both. To clearly present our solution, we first handle information-falsification attacks. In particular, we discuss how a node can observe information-falsification attacks, then we design our solution to secure the backpressure algorithm. Finally, we extend our solution to protocol-violation attacks.

A. Behavior of Attackers

We first address information-falsification attacks. Such attacks can have at least one of two intents: (i) *selfish behavior*: if the attacker is selfish, it is interested in performance gain for its own without care for others in the network; (ii) *malicious behavior*: if the attacker is malicious, it aims to degrade the throughput of others in the network as much as possible.

As the backpressure algorithm requires nodes broadcasting their queue backlogs and channel state information, one effective way for an attacker to fulfill its selfish or malicious intent is to falsify its queue backlogs or channel state information.

1) Manipulating backlogs. If the attacker wants to send its own packets immediately instead of receiving packets from others, it can broadcast falsified higher backlogs than actual ones. Then, it has a higher chance to be scheduled to transmit as a result of backpressure algorithm computation. If the attacker is malicious and tries to destroy packet delivery as much as possible, it can act like a blackhole and broadcast falsified lower or zero backlogs. Thus, it will attract more packets routed to itself under backpressure scheduling, then drop some or all of them. In summary, an attacker can manipulate its backlog information arbitrarily to affect the optimization solution in the backpressure algorithm.

2) Falsifying channel state information. If the attacker wants to gain the transmission opportunity, it can broadcast higher channel gains than the actual ones (so its link rate $u_{i,j}(t)$ is considered large in the backpressure optimization (1)). Then, it has a higher chance to be scheduled to transmit. Although broadcasting false channel information is one type of information falsification, we can categorize attacks that falsify channel state information into protocol-violation ones. This is because when an attacker cannot transmit with a claimed rate, it violates the scheduling decision. We will show in Section III-D that channel state information falsification can be solved jointly with other protocol-violation attacks.

B. Identification of Attack Behavior

Backlog manipulation is an essential way to launch various attacks against the backpressure algorithm. The question is how to identify or deduce possible backlog manipulation behavior of a node. To answer this, we first need to understand how the backlog dynamics evolve for benign nodes over time.

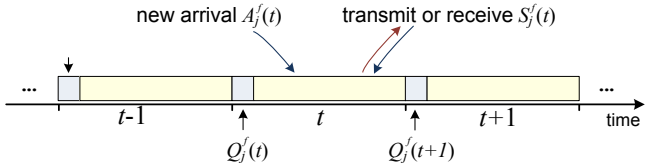

Fig. 3. Backlogs and activities of a node as time evolves.

Suppose node j is benign and obeys the backpressure scheduling. Fig. 3 shows the behavior of node j over time. Node j's backlogs for flow f are denoted by $Q_j^f(t)$ and $Q_j^f(t+1)$ at times t and $t+1$, respectively. The number of new arrivals at node j for flow f is $A_j^f(t)$ during time slot t, whose value is only known to node j and is never broadcasted to others. In addition, node j may transmit or receive at time t. Let $S_j^f(t)$ be the amount of data that node j sends or receives during time t for flow f ($S_j^f(t) > 0$ or $S_j^f(t) < 0$ when node j transmits or receives for flow f, respectively). Then, it must hold that node j's next-slot backlog $Q_j^f(t+1)$ equals to its current-slot backlog $Q_j^f(t)$ with its new arrivals $A_j^f(t)$ added and its transmitted data $S_j^f(t)$ removed; i.e.,

$$Q_j^f(t+1) = Q_j^f(t) + A_j^f(t) - S_j^f(t) \tag{3}$$

for each flow $f \in \mathcal{F}$.

From (3), we can get the arrival rate $A_j^f(t)$ as

$$A_j^f(t) = Q_j^f(t+1) - Q_j^f(t) + S_j^f(t) \in [0, A_{\max}], \tag{4}$$

where $A_{\max}$ is the upper limit of the packet arrival rate in the network, depending on a particular application. The purpose of obtaining the arrival rate is that we will show potential backlog manipulation at node j can be identified by a neighbor node i that examines whether node i's estimate of node j's arrival rate estimate is within $[0, A_{\max}]$.

In particular, node j may not be benign and can broadcast its true backlogs $Q_j^f(t+1)$ and $Q_j^f(t)$ as false backlogs $\hat{Q}_j^f(t+1)$ and $\hat{Q}_j^f(t)$, respectively. The transmitted/received data $S_j^f(t)$ can be observed as $\hat{S}_{i,j}^f(t)$ by node i.

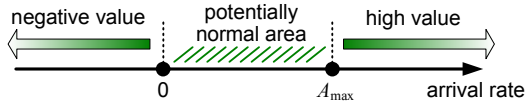

Fig. 4. Negative and high arrival rates indicate attacking behavior.

Due to the coordinated nature of the backpressure algorithm, if node j is scheduled to transmit, a neighbor of node j will know the amount of data $S_j^f(t)$ that node j transmits. Thus, node i's perfect observation is $\hat{S}_{i,j}^f(t) = S_j^f(t)$ if the attacker obeys the scheduling decision to transmit. However, due to wireless channel fading and collision, node i's observation $\hat{S}_{i,j}^f(t)$ may not be exactly equal to $S_j^f(t)$ or may be even completely wrong. Moreover, protocol-violation attacks do not need to obey scheduling decisions, which can also lead to $\hat{S}_{i,j}^f(t) \neq S_j^f(t)$. We will handle the imperfect observation case in Section III-C2 and protocol-violation attacks in Section III-D.

For better presentation of our idea, we assume that $\hat{S}_{i,j}^f(t) = S_j^f(t)$ in the following. Thus, given $\hat{Q}_j^f(t+1)$, $\hat{Q}_j^f(t)$ and $\hat{S}_{i,j}^f(t)$, node i (observing node j's transmit/receive behavior) can estimate node j's arrival rate as

$$\hat{A}_{i,j}^f(t) = \hat{Q}_j^f(t+1) - \hat{Q}_j^f(t) + \hat{S}_{i,j}^f(t). \tag{5}$$

Then, we will show via examples how node j's selfish or malicious behavior results in node i's arrival rate estimate $\hat{A}_{i,j}^f(t)$ going outside of the normal region $[0, A_{\max}]$.

- *Negative arrival rate*: consider that node j is a blackhole attacker who intends to attract packets to be routed to itself and drop all packets. To achieve this goal efficiently, node j keeps broadcasting zero backlogs (i.e., $\hat{Q}_j^f(t) = 0$ for all t). Obviously, because of its zero backlog, it should always receive data from other node, and this effect is observed by its neighbor node i as $\hat{S}_{i,j}^f(t) < 0$. It follows that the arrival rate estimate at node i satisfies

  $$\hat{A}_{i,j}^f(t) = \hat{Q}_j^f(t+1) - \hat{Q}_j^f(t) + \hat{S}_{i,j}^f(t) = 0 - 0 + \hat{S}_{i,j}^f(t) < 0.$$

  Accordingly, we see that if a node is deliberately attracting packets, it can exhibit a negative arrival rate.
- *High arrival rate*: consider that node j does not get the chance to transmit at time t (i.e., $\hat{S}_{i,j}^f(t) = 0$ observed by node i), but wants to capture the transmission opportunity at time $t+1$. Thus, it broadcasts a much higher backlog at the start of time $t+1$ (i.e., $\hat{Q}_j^f(t+1) > \hat{Q}_j^f(t) + A_{\max}$). Consequently, its arrival rate estimate can be written as

  $$\hat{A}_{i,j}^f(t) = \hat{Q}_j^f(t+1) - \hat{Q}_j^f(t) + \hat{S}_{i,j}^f(t) > A_{\max} + 0 > A_{\max},$$

  indicating the arrival rate estimate exhibits a very large value that exceeds its limit $A_{\max}$.

It is easy to verify that either negative or high arrival rate indicates attacking behavior as shown in Fig. 4. We say that node i's arrival rate estimate $\hat{A}_{i,j}^f(t)$ of node j for flow f is within the normal area if $0 \leq \hat{A}_{i,j}^f(t) \leq A_{\max}$.

C. Virtual Trust Queue to Defend Backpressure Algorithm

We have already identified that estimating packet arrival rate of a node can help us find out whether the node exhibits backlog manipulation behavior or not. Our next goal is to design a strategy based on estimating packet arrival rates to defend the backpressure algorithm. We first introduce an augmented optimization approach to protect the backpressure algorithm, then present how to build a comprehensive virtual trust queue solution to provide security guarantee.

1) Augmented Optimization Approach: As we have already mentioned, the arrival rate estimate $\hat{A}_{i,j}^f(t)$ is critical to determine whether a node is an attacker or not at time t. Either $\hat{A}_{i,j}^f(t) < 0$ or $\hat{A}_{i,j}^f(t) > A_{\max}$ indicates attacking behavior. As shown in Fig. 4, the farther the estimate of node j's arrival rate is from the actual one, the more aggressive the attack behavior becomes, and accordingly there is less trust that another node should put in node j.

Thus, we define the *deviation in arrival* of node j for flow f observed at node i as the distance of arrival rate estimate $\hat{A}_{i,j}^f(t)$ to the normal arrival rate region $[0, A_{\max}]$; namely,

$$d_{i,j}^f(t) = \begin{cases} |\hat{A}_{i,j}^f(t)| & \text{for } \hat{A}_{i,j}^f(t) < 0, \\ 0 & \text{for } 0 \leq \hat{A}_{i,j}^f(t) \leq A_{\max}, \\ \hat{A}_{i,j}^f(t) - A_{\max} & \text{for } \hat{A}_{i,j}^f(t) > A_{\max}. \end{cases} \tag{6}$$

It is easy to see that $d_{i,j}^f(t)$ is always non-negative. Larger $d_{i,j}^f(t)$ means more deviation from a node's normal behavior. Then, we define the deviation in arrival (for all flows) as

$$D_{i,j}(t) = \sum_{f \in \mathcal{F}} d_{i,j}^f(t) + \epsilon, \tag{7}$$

where $\epsilon > 0$ is a small number serving only as a uniform offset such that all behaviors exhibit positive deviations, i.e., $D_{i,j}(t) \geq \epsilon$ for all $t > 0$.

Accordingly, increasing $D_{i,j}(t)$ decreases node i's trust in node j. If node j is associated with a high value of $D_{i,j}(t)$, it should be attacking other nodes or misbehaving in the network, and should be punished during the backpressure scheduling. Thus, the augmented optimization approach is to add a penalty term to the backpressure algorithm in (1) as

$$\mathbf{u}^*(t) = \arg\max_{\mathbf{u}(t) \in \mathcal{R}(t)} \sum_{u_{i,j}(t) \in \mathbf{u}(t)} \left(u_{i,j}(t) w_{i,j}(t) - v D_{i,j}(t) \right), \tag{8}$$

where $-vD_{i,j}(t)$ ($v > 0$) is the penalty term. If a node is an attacker with a large value of $D_{i,j}$, the penalty term $-vD_{i,j}(t)$ is then a large negative value, indicating that the link (i,j) is less likely to be scheduled by the maximization in (8). Here, $v > 0$ is a weighted factor for the deviation in arrival, meaning the optimization allows for a flexible tradeoff between throughput performance and the trust level by adjusting the value of v.

2) Virtual Trust Queue: There are three major drawbacks of the approach in (8): (i) If an attacker causes a very large value of $D_{i,j}(t)$ at time t (e.g., deliberately dropping all packets) and then returns to legitimate behavior after time t, the penalty in (8) only happens and lasts during time t (i.e., there is no

memory in tracking the trust); (ii) there is no systematic way to determine the value of v; and (iii) there is no systematic way to know, control, or limit the damage that an attacker can cause to the network performance.

To address the first issue, we can define a sliding window to record the history and keep applying the penalty. However, the sliding window method requires careful adjustment of window size and still cannot solve the second and third issues. Another way to remember and use history is to represent it in a queue structure. Mathematical tools in the queuing theory can then provide a theoretical understanding of how we can use a queue to limit an attack's behavior.

As a consequence, we use a queue to manage the deviations of arrival. Motivated by [12] that uses a virtual energy queue to limit the power consumption while at the same time sustaining the throughput performance, our objective is to construct a virtual queue, called *virtual trust queue*, to limit the damage of an attacker while at the same time sustain the throughput performance. We call it virtual because the queue only stores a single trust value. In particular, node i maintains a virtual trust queue for node j and enqueues the deviation in arrival $D_{i,j}(t)$ with constant service rate $\delta > \epsilon > 0$. In other words, the queue size (or the value stored in the queue) $X_{i,j}(t)$ can be written as

$$X_{i,j}(t+1) = \max\left(X_{i,j}(t) - \delta, 0\right) + D_{i,j}(t). \tag{9}$$

It is easy to see that if $X_{i,j}(t)$ becomes larger, node j is less trustable. We then integrate the virtual trust queue into (1) in the backpressure algorithm as

$$\mathbf{u}^*(t) = \underset{\mathbf{u}(t)\in\mathcal{R}(t)}{\arg\max} \sum_{u_{i,j}(t)\in\mathbf{u}(t)} \left(u_{i,j}(t)w_{i,j}(t) - X_{i,j}(t)D_{i,j}(t)\right). \tag{10}$$

We next show that (10) provides two essential guarantees, called zero penalty and attack bounding.

- *Zero penalty*: if there is no attack, there is no throughput performance penalty to use the virtual trust queue.
- *Impact bounding*: if there are attacks, the virtual trust queue based optimization (10) guarantees the attack's damage to the network is always bounded from above.

In what follows, the two guarantees of the virtual trust queue are presented in Theorems 1 and 2, respectively.

Theorem 1 (Zero Penalty of the Virtual Trust Queue): In a network without presence of attacks, the virtual trust queue based optimization (10) is equivalent to the original backpressure optimization in (1).

Proof: If there is no attack, $D_{i,j}(t) = \epsilon$ for all $t > 0$. Thus, the virtual trust queue size in (9) satisfies $X_{i,j}(1) = \max(0-\delta, 0) + \epsilon = \epsilon$, $X_{i,j}(2) = \max(\epsilon - \delta, 0) + \epsilon = \epsilon$, $X_{i,j}(3) = \max(\epsilon - \delta, 0) + \epsilon = \epsilon$, and so on. Then, $X_{i,j}(t) = \epsilon$ for all $t > 0$.

Inserting $D_{i,j}(t) = X_{i,j}(t) = \epsilon$ into (10) yields

$$\begin{aligned}\mathbf{u}^*(t) &= \underset{\mathbf{u}(t)\in\mathcal{R}(t)}{\arg\max} \sum_{u_{i,j}(t)\in\mathbf{u}(t)} \left(u_{i,j}(t)w_{i,j}(t) - \epsilon^2\right) \\ &= \underset{\mathbf{u}(t)\in\mathcal{R}(t)}{\arg\max} \sum_{u_{i,j}(t)\in\mathbf{u}(t)} \left(u_{i,j}(t)w_{i,j}(t)\right), \end{aligned} \tag{11}$$

which completes the proof. □

Remark 1: Theorem 1 ensures that we can always use this virtual trust queue mechanism under any circumstance with and without attacks. It incurs no cost in terms of performance loss when there is no attack in the network.

Theorem 2 (Impact Bounding of the Virtual Trust Queue): If a virtual trust queue established in (9) is stable, it is guaranteed that the deviation in arrival $D_{i,j}(t)$ satisfies

$$\limsup_{t\to\infty} \frac{1}{t} \sum_{\tau=1}^{t} \mathbb{E}(D_{i,j}(\tau)) \le \delta. \tag{12}$$

Otherwise, (10) degenerates to an optimization over a subset that excludes from $\mathcal{R}(t)$ all links with nodes showing unstable queues as $t \to \infty$.

Proof: The proof consists of two parts: (i) virtual queue is stable, and (ii) virtual queue is not stable. The first part follows the similar strategy to stabilize two queues in [12]. The second part is straightforward: suppose a virtual trust queue $X_{i,j}(t)$ is unstable, i.e., $\liminf_{t\to\infty} X_{i,j}(t) = \infty$. Then, the term $-X_{i,j}(t)D_{i,j}(t)$ becomes negative infinity as $D_{i,j}(t) > \epsilon > 0$, which offers no effect on the $\arg\max$ in (10). □

Remark 2: The virtual trust queue $X_{i,j}(t)$ saved at node i is not a real queue, but a single value whose operation in (9) works similar to a queue. Therefore, maintaining a virtual trust queue only incurs negligible amount of memory at each node. Similarly, broadcasting the trust queue information also incurs negligible amount of additional transmission overhead.

3) Choosing the Service Rate in Trust Queue: Theorem 2 states that the designed virtual trust queue produces two outcomes for an attacker: 1) if the attacker exhibits mild behavior (e.g., alternating legitimate and selfish behaviors over time) such that the virtual trust queue is still stable (i.e., queue size is small and bounded), we guarantee that the attacker's average deviation in arrival is below the service rate δ. That is, δ serves as a tolerance level to the attacker. 2) if the attacker's behavior is too aggressive (e.g., keeps attacking all the time) such that the virtual trust queue becomes unstable (i.e., queue size is very large and keeps increasing), we guarantee that the attacker is eliminated from any routing decision.

It is emphasized that our goal is not to detect any possible attack against the backpressure algorithm, but to sustain performance for all legitimate nodes under attacks that can significantly degrade the performance. Given our virtual trust queue mechanism with a tolerance level, there will be some greedy attackers that achieve slight gains without being detected. However, they will be immediately penalized once they go beyond the tolerance level.

We can specify any positive value of the service rate δ in the virtual trust queue, which reflects our tolerance level or bound for attackers as indicated in (12). The virtual trust queue mechanism guarantees that it involves any potential attackers in scheduling under the given tolerance level δ, and at the same time eliminates any potential attackers that go beyond δ.

As we have mentioned, the virtual trust queue mechanism is based on the observations on other nodes, which may have

errors in the real world. Such errors may also lead to false accusation to some benign nodes. Therefore, the value of δ can be set proportional to the expected level of observation errors in a practical network scenario to mitigate observation errors. For example, due to possible channel collision, a node may not be able to observe a transmission. Therefore, δ can be set to be the data amount value for a single transmission such that the observation error due to channel collision is mitigated by the virtual queue service.

D. Handling Protocol-Violation Attacks

To defend against backlog information falsification attacks, we have so far built a virtual trust queue mechanism, in which we assume that an attacker only falsifies backlog information to affect scheduling decisions, but it obeys any scheduling decision. In practice, an attacker has the freedom to both falsify information and violate any scheduling decision. We next show our solution can be directly integrated to combat protocol-violation attacks at the same time.

A protocol-violation attacker is the one that does not obey the backpressure scheduling decision, such as (i) a selective-forwarding attacker that does not transmit packets for a particular flow even when it is scheduled to transmit, (ii) an attacker that claims to have a very good channel rate but uses a much lower rate to transmit, or (iii) an attacker that transmits data to another node that is not scheduled to receive.

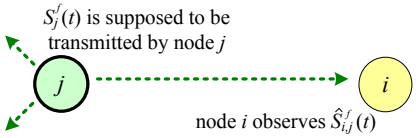

Fig. 5. Node j's scheduled transmission vs. node i's observation.

To defend against protocol-violation attacks, we adopt a similar neighborhood watch strategy that we used previously for queue backlogs. As shown in Fig. 5, node j is scheduled to transmit data with amount $S_j^f(t)$, which is known to its neighbor node i during information exchange in backpressure scheduling. If node j obeys the scheduling decision, then node i's observation on the transmission is $\hat{S}_{i,j}^f(t) = S_j^f(t)$. Otherwise, $\hat{S}_{i,j}^f(t) \neq S_j^f(t)$. For example, if node j does not transmit or transmits to a wrong destination, $\hat{S}_{i,j}^f(t) = 0$. If node j uses a lower rate to transmit, $\hat{S}_{i,j}^f(t) < S_j^f(t)$. Note that in this case, imperfect observation or false accusation may also happen, which can also be mitigated by choosing the value of service rate equal to the data amount value for a signal transmission.

As a result, we define the *deviation in scheduling* as the absolute difference between node i's observation $\hat{S}_{i,j}^f(t)$ and node j's scheduling $S_j^f(t)$, i.e.,

$$E_{i,j}(t) = \sum_{f\in\mathcal{F}} |\hat{S}_{i,j}^f(t) - S_j^f(t)| + \eta, \tag{13}$$

where $\eta > 0$ is a small offset similar to previously defined ϵ in (7). It is obvious that if a node exhibits large deviations of scheduling in (13), the node may misbehave and should be penalized in the backpressure algorithm.

In a similar way, we construct another virtual trust queue: node i maintains a second virtual trust queue for node j with size $Y_{i,j}(t)$ that enqueues the deviation in scheduling $E_{i,j}(t)$ with constant service rate $\sigma > \eta > 0$; i.e.,

$$Y_{i,j}(t+1) = \max\left(Y_{i,j}(t) - \sigma, 0\right) + E_{i,j}(t). \tag{14}$$

Finally, in order to handle both information-falsification and protocol-violation attacks, we integrate the two virtual trust queues together into the backpressure optimization as

$$\mathbf{u}^*(t) = \arg\max_{\mathbf{u}(t)\in\mathcal{R}(t)} \sum_{u_{i,j}(t)\in\mathbf{u}(t)} (u_{i,j}(t)w_{i,j}(t) - X_{i,j}(t)D_{i,j}(t) - Y_{i,j}(t)E_{i,j}(t)), \tag{15}$$

where $X_{i,j}(t)$ are $Y_{i,j}(t)$ are the virtual trust queues for deviation in arrival $D_{i,j}(t)$ and deviation in scheduling $E_{i,j}(t)$, respectively.

Remark 3: It is easy to verify that Theorems 1 and 2 still hold when we integrate two virtual trust queues in (15). Therefore, the designed virtual trust queue mechanism provides a guaranteed (rather than heuristic) solution to defend the backpressure algorithm against both information-falsification and protocol-violation attacks. Moreover, the proposed virtual trust queue mechanism is generic and flexible to accommodate more queues for the quantification of any other attack behavior, and at the same time provides guarantee of attack resilience.

E. Falsifying Virtual Trust Queue

The virtual trust queue mechanism uses (15) to coordinate node transmissions. On one hand, virtual trust queues provide attack resilience; on the other hand, it may introduce another line of vulnerability in the backpressure algorithm. In particular, nodes need to broadcast additional virtual trust queue information $X_{i,j}(t)$, $D_{i,j}(t)$, $Y_{i,j}(t)$, and $E_{i,j}(t)$ for either distributed or centralized coordination at time t. It is quite possible that an attacker can also falsify virtual trust queue information to circumvent the virtual trust queue mechanism.

There is an effective way to identify and correct such falsified information. Let us focus on deviation in arrival $D_{i,j}(t)$ and its virtual trust queue $Y_{i,j}$. First, notice that $D_{i,j}(t)$ reflects node i's observation on node j. This indicates that if node i is an attacker, it can only falsify its own $D_{i,j}(t)$ on node j. However, node i is not the only one providing such information. There are other neighbors that provide their observations on node j at the same time. Denote by $\mathcal{N}_j$ the set of node j's neighbors. Then, there are $|\mathcal{N}_j|$ observations on node j. For any pair of benign nodes $k, l \in \mathcal{N}_j$, they receive the same backlog information from node j and can observe the transmission behavior of node j. Thus, their quantified deviations in arrival $D_{k,j}(t)$ and $D_{l,j}(t)$ should be in close value (due to some observation errors in practice). Accordingly, $X_{k,j}(t)$ and $X_{l,j}(t)$ should also be in close value (since the queue size is solely based on the deviation in arrival as shown in (9)). Therefore, we can correct any isolated values

in all reported virtual trust queue information using

$$D_{k,j}(t) = \arg\min_{d \in \mathcal{D}_j(t)} |d - D_j(t)| \tag{16}$$

for all $k \in \mathcal{N}_j$, where $\mathcal{D}_j(t)$ is the set of all deviations of arrival reported by node j's neighbors, and $D_j(t)$ is the average of all these deviations. Similar corrections will also be applied to $X_{i,j}$, $E_{i,j}$, and $Y_{i,j}$.

Fig. 6 shows an example how the correction to falsified virtual trust queue information works. Suppose that node i sends false information $(D_{i,j}(t) = 9, X_{i,j}(t) = 2)$. At the same time, node i's other benign neighbors, nodes a, b, c and d, also send $(D_{a,j}(t), X_{a,j}(t))$, $(D_{b,j}(t), X_{b,j}(t))$, $(D_{c,j}(t), X_{c,j}(t))$, and $(D_{d,j}(t), X_{d,j}(t))$, respectively, which satisfy $D_{i,j}(t) \neq D_{a,j}(t) = D_{a,j}(t) = D_{b,j}(t) = D_{c,j}(t) = D_{d,j}(t) = 5$ and $X_{i,j}(t) \neq D_{a,j}(t) = X_{a,j}(t) = X_{b,j}(t) = X_{c,j}(t) = X_{d,j}(t) = 20$. Using (16), the corrections are $D_{i,j}(t) = 5$ and $X_{i,j}(t) = 20$.

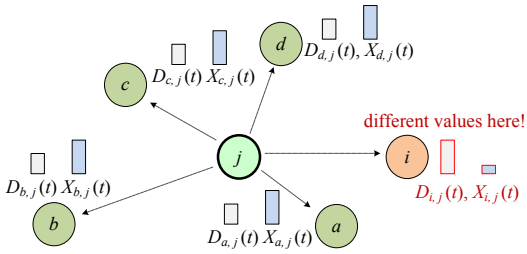

Fig. 6. Node j has neighbor nodes i, a, b, c, and d. Node i is falsifying virtual trust queue information. Nodes a, b, c, and d are benign and send correct information.

It is also worth noting that the proposed trust mechanism is fully *distributed* and maintained at individual nodes. For a centralized implementation (e.g., [11]), a virtual trust queue does not need to be maintained at each node. The centralized controller can establish the queue for each node. At each time slot, node k reports its computed deviation $D_{k,j}(t)$ to the controller. Then, the controller chooses the most uniformly agreed value using (16) into its trust queue for node j. Therefore, the virtual trust queue mechanism can be further integrated with a control center for more efficient attack mitigation strategies.

IV. Performance Evaluation

In this section, we conduct an extensive simulation study to evaluate the performance of the designed secure backpressure algorithm with virtual trust queues.

We set up a wireless network with 50 nodes with transmission range 100m uniformly distributed over a 200m-by-200m area. Each node is half-duplex thus cannot transmit and receive at the same time. We adopt the protocol interference model; i.e., if two nodes are within each other's transmission range, their link rate is set to be 100 packets/s; otherwise, the rate is 0. In addition, if a node is receiving from a neighbor at a time slot, none of its other neighbors will be scheduled to transmit.

There are in total 10 end-to-end flows with randomly selected source-destination pairs in the network. Per-flow packet arrival in each node at each time slot follows the uniform distribution over time $[0, A_{\max}]$, where $A_{\max} = 5$ packets/s. The simulation starts at time 0 with all node's queue backlogs equal to zero. Each benign node uses two virtual trust queues with $\epsilon = \eta = 0.5$ for each of its neighbors along with the data packet queues.

We consider a comprehensive set of attack scenarios in the simulations: 1) *Blackhole attacks*, which always broadcast zero queue backlogs and high channel rates to attract packets to be routed to them, then drop all received packets. 2) *Selective-forwarding attacks*, which keep relatively low profile compared with blackhole attacks. They do not falsify any information and obey the backpressure scheduling, but only drop packets routed to them for particular flows. 3) *On-off attacks*, which act as blackholes or legitimate nodes during on and off periods. 4) *Transmission-opportunity-wasting attacks*, which never falsify information, but simply abandon its scheduled transmission opportunity to degrade the network throughput. 5) *Selfish nodes*, which always attempt to empty its queues by broadcasting high queue backlogs to capture the transmission opportunity. 6) *Heterogeneous attacks*, which include all above attackers on different nodes in the same network.

In our performance evaluation, we define the metric of (normalized) throughput as the average amount of delivered data per time slot normalized by the link rate.

A. Blackhole Attacks

We randomly select one node in the network acting as a blackhole. Fig. 7 shows the throughput in the network under the blackhole attack. It is noted from Fig. 7 that initially, the network throughput increases as run time goes. This is because the network is lightly loaded in the initial state. As more packets arrive at each node, the network throughput increases gradually and becomes stable. When there is no attack, the throughput approaches near 1 over time. However, when there is an attacker, we can see over 80% degradation for the throughput in the network due to the blackhole that keeps dropping packets.

We deploy the two virtual trust queues with two service rates: (i) $\delta = \sigma = 1$ and (ii) $\delta = \sigma = 50$. As we have discussed, a smaller value of service rate δ or σ mean a smaller tolerance level for attack behavior. If an attacker operates beyond the given tolerance level, which results in an unstable queue, the attacker will be excluded from the routing decision as indicated in Theorem 2. Consequently, it is observed from Fig. 7 that the throughput is substantially improved under the virtual trust queue strategy, in particular for the low tolerance case with $\delta = \sigma = 1$.

Fig. 7 also demonstrates that a low tolerance virtual trust queue (i.e., small values of δ and σ) exhibits better performance than a high tolerance queue. As the virtual trust queue mechanism is based on the observations on other nodes, which may have errors in the real world, it is desirable to choose reasonably small values of δ and σ to account for observation errors in practical applications.

We also measure the throughput performance under different numbers of blackholes in Table I, which shows that

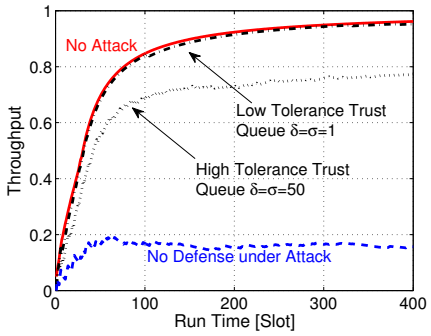

Fig. 7. Throughput over run time for different scenarios.

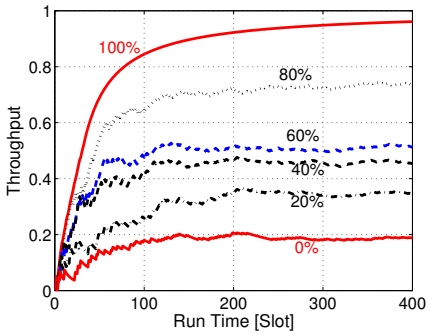

Fig. 8. Throughput under selective-forwarding attacks for forwarding ratio ρ from 0% to 100%.

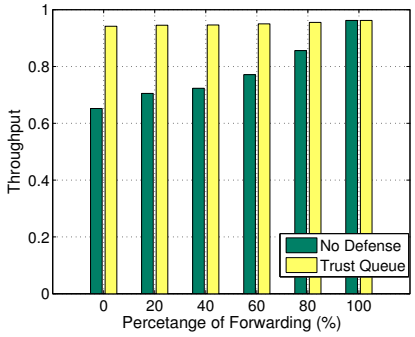

Fig. 9. Throughput under selective-forwarding attacks with and without virtual trust queue.

when the number of blackholes increases to three, the network exhibits zero throughput. However, when two virtual trust queues are deployed, the throughput is almost not affected by the number of blackholes.

TABLE I
THROUGHPUT AT TIME SLOT $t = 400$.

Number of Blackholes:	0	1	2	3	4
w/o. virtual queues	0.96	0.17	0.0	0.0	0.0
w. virtual queues	0.96	0.96	0.95	0.95	0.95

B. Selective-Forwarding Attacks

Next, we consider selective-forwarding attacks. We randomly select two nodes in the network acting as selective-forwarding attacks with forwarding ratio $\rho \in [0\%, 100\%]$, which means that an attacker only forwards packets for a percentage ρ of all flows in the network.

Fig. 8 depicts the throughput performance under selective-forwarding attacks for forwarding ratio ρ = 0%, 20%, 40%, 60%, 80%, and 100%, where $\rho = 100\%$ means no attack. The performance is measured without any defense in Fig. 8. We can see that as the performance is substantially degraded as ρ decreases. For example, as run time goes, we find that the throughput is stabilized at around 0.9622 and 0.1821 for the $\rho = 100\%$ and $\rho = 0\%$ cases, respectively.

Then, we show in Fig. 9 the throughput at time slot $t = 400$ with and without our virtual trust queue mechanism that is set with $\delta = \sigma = 2$. If there is no defense, the throughput increases gradually as the forwarding ratio of attackers ρ increases, and finally reaches the no-attack throughput. If the virtual trust queues are used, we can see that regardless of the value of ρ, the throughput is always close to the non-attack throughput. For example, when $\rho = 0\%$, the virtual trust queue strategy achieves throughput of 0.9417 compared with the non-attack throughput of 0.9622.

C. On-Off Attacks

We also consider the on-off attacks, which act as blackholes and legitimate nodes during on and off periods. We randomly choose one node in the network as an on-off attacker, whose on and off periods are both equal to 50 time slots.

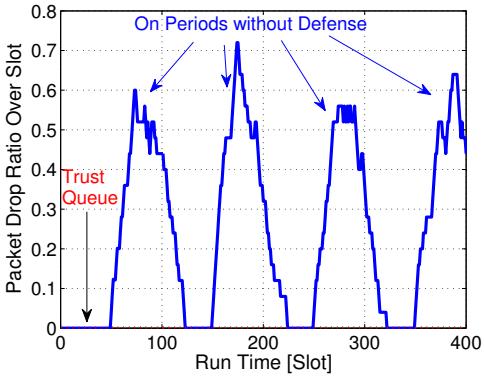

Fig. 10. Packet drop ratio in the network under on-off attacks: virtual trust queue vs. no defense.

To capture how the network reacts in transient states under the on-off attacker, we use packet drop ratio as the performance metric, which is defined as the ratio between the number of dropped packets (by the attacker) and the number of transmitted packets. Fig. 10 illustrates the packet drop ratio in the network under the on-off attack. It is noted from Fig. 10 that if there is no defense in the network, the packet drop ratio increases and decreases sharply, and these trends alternate. This is due to the fact that attackers only attack during the on-periods. In contrast, if the virtual trust queue mechanism with $\delta = \sigma = 1$ is used in the network, we observe in Fig. 10 that the packet drop ratio is always 0, indicating that our mechanisms can immediately find and exclude the attackers when they are on.

D. Multiple Heterogonous Attacks

We have shown that the virtual trust queue mechanism is effective to combat (1) blackhole, (2) selective-forwarding, and (3) on-off attacks. We next evaluate its effectiveness against (4) transmission-opportunity-wasting attacks and (5) selfish nodes as part of heterogeneous attacks. We do not evaluate (4) and (5) individually due to the page limit. Instead, we combine the (4) and (5) attacks with the (1), (2), and (3) attacks to form the attack scenario. In the experiments, the forwarding ratio

of the selective-forwarding attack is set to be $\rho = 60\%$, and the on and off periods of the on-off attacker are equally set to be 50 time slots.

TABLE II
THROUGHPUT AT TIME SLOT $t = 400$ UNDER DIFFERENT ATTACKS.

Combination:	4	5	4,5	3,4,5	2,3,4,5	all
w/o. virtual queues	0.23	0.85	0.21	0.15	0.09	0.0
w. virtual queues	0.96	0.96	0.96	0.96	0.95	0.95

We measure the throughput under different attacks shown in Table II. We can conclude that the virtual trust queue mechanism always achieves near-optimal performance regardless of different combinations of attacks present in the network.

V. RELATED WORK

The backpressure algorithm was originally introduced by Tassiulas and Ephremides in [1]. Since then, significant efforts have been devoted to adapting the backpressure algorithm with realistic network constraints (e.g., [2]–[4], [8], [20]), and developing backpressure based system prototypes for wireless networks (e.g., [5]–[7], [11]) and emerging network systems such as smart grids [21]–[23]. The state-of-the-art greatly enhanced our understanding of the backpressure algorithm, and supported the feasibility of real-system implementation of backpressure-based routing and scheduling solutions in multi-hop wireless networks. However, the backpressure algorithm and its variants remain vulnerable to insider threats with a variety of attacking behaviors. This appears as one major obstacle to practical deployment of the backpressure algorithm.

Another line of work related to this paper has investigated the design of trust-based routing to combat selfish or malicious nodes in the network (e.g., [15]–[19]). However, they are designed for different other routing mechanisms and cannot be readily adapted to the backpressure algorithm due to its specific information exchange and optimization characteristics.

It is worth noting that a recent paper [13] proposed a trust-based backpressure algorithm for wireless senor networks. But there is no means to track trust over time. In addition, it is still not clear to what extent the approach can limit or control various attack behaviors. The proposed virtual trust queue based mechanism can be regarded as a generic solution to secure any backpressure based routing and scheduling protocols against a variety of attacks with a guarantee of sustaining resilience and throughput.

VI. CONCLUSIONS

In this paper, we provided a systematic study on securing the backpressure algorithm. We proposed a novel virtual trust queuing mechanism to defend against both information-falsification and protocol-violation attacks. We showed that by jointly stabilizing the virtual trust queue and the real packet queue, the backpressure algorithm achieves guarantees of attack resilience as well as throughput performance. Finally, we conducted extensive simulations to validate the effectiveness of the virtual trust queue mechanism. Our results showed that the virtual trust queue mechanism secures the backpressure algorithm against a variety of attacks. Our proposed solution clears a major barrier for practical deployment of backpressure algorithm for secure wireless applications.

REFERENCES

[1] L. Tassiulas and A. Ephremides, "Stability properties of constrained queueing systems and scheduling policies for maximum throughput in multihop radio networks," *IEEE Trans. Automatic Control*, vol. 37, pp. 1936–1948, Dec. 1992.

[2] M. Alresaini, M. Sathiamoorthy, B. Krishnamachari, and M. J. Neely, "Backpressure with adaptive redundancy (BWAR)," in *Proc. of IEEE INFOCOM*, 2012.

[3] A. Warrier, S. Janakiraman, S. Ha, and I. Rhee, "DiffQ: Practical differential backlog congestion control for wireless networks," in *Proc. of IEEE INFOCOM*, 2009.

[4] H. Seferoglu and E. Modiano, "Diff-Max: Separation of routing and scheduling in backpressure-based wireless networks," in *Proc. of IEEE INFOCOM*, 2013.

[5] L. Huang, S. Moeller, M. J. Neely, and B. Krishnamachari, "LIFO-backpressure achieves near optimal utility-delay tradeoff," *ACM/IEEE Trans. Networking*, pp. 831–844, June 2013.

[6] J. Nunez-Martinez, J. Mangues-Bafalluy, and M. Portoles-Comeras, "Studying practical any-to-any backpressure routing in Wi-Fi mesh networks from a Lyapunov optimization perspective," in *Proc. of IEEE MASS*, 2011.

[7] J.-Y. Yoo, C. Sengul, R. Merz, and J. Kim, "Experimental analysis of backpressure scheduling in IEEE 802.11 wireless mesh networks," in *Proc. of IEEE ICC*, 2011.

[8] L. Ding, T. Melodia, S. Batalama, J. Matyjas, and M. Medley, "Cross-layer routing and dynamic spectrum allocation in cognitive radio ad hoc networks," *IEEE Trans. Vehicular Technology*, vol. 59, 2010.

[9] Z. Lu, W. Wang, and C. Wang, "From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic," in *Proc. of IEEE INFOCOM*, 2011.

[10] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential DSSS: Jamming-resistant wireless broadcast communication," in *Proc. of IEEE INFOCOM*, 2010.

[11] R. Laufer, T. Salonidis, H. Lundgren, and P. L. Guyadec, "XPRESS: A cross-layer backpressure architecture for wireless multi-hop networks," in *Proc. of ACM MobiCom*, 2011.

[12] M. J. Neely, "Energy optimal control for time varying wireless networks," *IEEE Trans. Information Theory*, vol. 52, pp. 2915–2934, Jul. 2006.

[13] R. Venkataraman, S. Moeller, B. Krishnamachari, and T. R. Rao, "Trust-based backpressure routing in wireless sensor networks," *Int. J. Sensor Networks*, 2014.

[14] Z. Lu, W. Wang, and C. Wang, "On order gain of backoff misbehaving nodes in CSMA/CA-based wireless networks," in *Proc. of IEEE INFOCOM*, 2010.

[15] A. A. Pirzada, C. McDonald, and A. Datta, "Performance comparison of trust-based reactive routing protocols," *IEEE Trans. Mobile Computing*, vol. 5, pp. 695–710, June 2006.

[16] I. Chen, F. Bao, M. Chang, and J. Cho, "Dynamic trust management for delay tolerant networks and its application to secure routing," *IEEE Trans. Parallel and Distributed Systems*, Apr. 2013.

[17] C. Zhang, X. Zhu, Y. Song, and Y. Fang, "A formal study of trust-based routing in wireless ad hoc networks," in *Proc. of IEEE INFOCOM*, 2010.

[18] S. Jain and J. Baras, "Distributed trust based routing in mobile ad-hoc networks," in *Proc. of IEEE MILCOM*, 2013.

[19] F. Bao, I.-R. Chen, M. Chang, and J.-H. Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," *IEEE Trans. Network and Service Management*, vol. 9, pp. 169–183, Mar. 2012.

[20] L. Georgiadis, M. J. Neely, and L. Tassiulas, "Resource allocation and cross-layer control in wireless networks," *Foundations and Trends in Networking*, vol. 1, pp. 1–144, 2006.

[21] M. Wei and W. Wang, "Greenbench: A benchmark for observing power grid vlunerability under data-centric threats," in *Proc. of IEEE INFOCOM*, 2014.

[22] B. Hu and H. Gharavi, "Greedy backpressure routing for smart grid sensor networks," in *Proc. of IEEE CCNC*, 2014.

[23] M. Wei and W. Wang, "Toward distributed intelligent: A case study of peer to peer communication in smart grid," in *Proc. of IEEE GlobeCom*, 2013, pp. 2210–2216.