Hammer and Anvil: The Threat of a Cross-Layer Jamming-aided Data Control Attack in Multihop Wireless Networks

Liyang Zhang, Tommaso Melodia
Department of Electrical and Computer Engineering
Northeastern University
Email: {liyangzh, melodia}@ece.neu.edu

***Abstract*—This paper considers potential risks to data security in multi-hop infrastructureless wireless networks where cross-layer routing protocols are used. We show that an adversary, as long as it controls a few of the nodes, and with the help of a few assisting jammers, can extend control over a significant portion of the data in the network even with very simple strategies and limited resources, by creating a so-called "wormhole" even without off-band links. We refer to this jamming-assisted data control threat as *hammer and anvil attack*.**

We model a prototype of the hammer and anvil attack in a wireless sensor network scenario with distributed cross-layer routing protocols. We show through extensive performance evaluation that the attack poses a serious threat to the resulting data security, and we provide observations that can be helpful in fine-tuning the attack, as well as in designing defense mechanisms against it.

I. Introduction

As the concept of *big data* becomes mainstream, wireless sensor networks (WSN) will become prevalent in data collection applications - it has been foreseen that WSNs will contribute amounts of data even larger than what generated by social networks [1].

However, while WSNs provide a solution for massive data collection that may possibly enable a variety of new applications, they also introduce significant risks. It is well known that wireless networks are vulnerable to various types of malicious attacks [2], and that data security is difficult to ensure. Security is even harder to guarantee in WSNs, which are typically composed of densely deployed and physically exposed devices. It is easy for an adversary to capture and compromise some of the nodes and gain control over the data flows traversing them. Clearly, in most scenarios, it is rather impractical for one to take control of a significant portion of the nodes without being noticed by the entity that owns or manages the WSN. However, even without controlling a significant percentage of nodes, the adversary may still be able to gain control over a significant portion of the network data. This can be done by exploiting and taking advantage of the cross-layer nature of many state-of-the-art protocols for WSNs.

For example, many routing protocols for wireless multi-hop networks are based on controlling the dynamics at multiple layers of the protocol stack (see, among others, [3]–[8]). This coupling of multiple layers in decision making implies that changes in the dynamics at layers other than the network layer also affect routing decisions. As a result, an adversary may be able to extend attacks to the network layer with proper assistance from other layers. Among such auxiliary means, jamming is a very simple and yet an effective one. By radiating interference to the spectrum in use, a jammer can in fact degrade the capacity of selected communication links. Then, because cross-layer routing protocols are often designed to avoid links with low capacity, jammed nodes are likely to redirect their traffic by choosing alternate paths. With proper collaboration from compromised nodes, data may be "driven" directly to compromised nodes, as shown in Fig. 1. We would like to illustrate this combined attack with an analogy to the way a blacksmith operates: assistant jammers act as a "hammer", striking on the traffic and driving the data to the captured or compromised nodes, the "anvil".

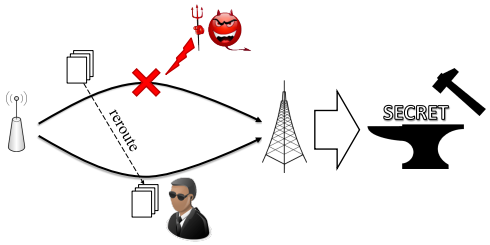


Fig. 1. Illustration of hammer and anvil attack.

To the best of our knowleadge, although the idea of a *cross-layer attack* has been mentioned in some occasions (for example, [9]), hammer and anvil attack is the first to explore the risks in cross-layer routing protocols. To better understand the vulnerability of WSNs (and of multi-hop wireless networks in general) to this attack, and to shed light on the design of possible countermeasures, we model a prototype of the attack. We consider a generic distributed routing protocol with limited local information, to model the uncertain environment that WSNs typically operate on. The adversary compromises a small portion of the nodes and gains some level of control on the traversing data (for example, traffic analysis or decryption of confidential data). Control over the data is extended with the help of assistant jammers.

We show through extensive simulations that the proposed attack can achieve control over the data in a network with proper tuning of the control knobs that characterize the attack. Furthermore, we reveal some underlying features of the attack by analyzing possible strategies of the adversary to achieve

its objective, and shed light on principles useful in designing effective countermeasures.

To summarize, this paper makes the following contributions:

1) We introduce the *hammer and anvil* attack. To the best of our knowledge, this work is the first to analyze the threat of attack combining physical and network layer means;
2) We model a prototype of the attack in a scenario with multi-hop sensor networks and cross-layer geographical routing protocols, and conduct an extensive performance evaluation of the attack;
3) We analyze various factors that affect the attack, and identify basic principles for tuning the attack and to design effective countermeasures;

The rest of the paper is organized as follows. In Section II, we briefly review the state of the art in both cross-layer design and related topics in wireless security. We describe the system model for both the attacker and the defender in Section III, and formally define the problem in Section IV. Simulation results are shown and discussed in Section V. Finally, we draw the main conclusions in Section VI.

II. Related Work

A. Cross-Layer Design in Wireless Networks

Cross-layer designs are now commonplace in state-of-the-art protocols stacks. Routing decisions, traditionally taken at the network layer, are therefore affected by decisions taken distributively at multiple layers. For example, in [3] the considered routing metric is a function of interference, packet success rate and raw data rate.

Numerous cross-layer protocols have been proposed where routing decisions are taken by modeling cross-layer interactions at multiple layers of the protocol stack. For example, in [4], routing is studied jointly with congestion control and scheduling through a multicommodity flow approach. Although the work mainly focuses on fixed link-capacity scenarios, the paper also addresses the multi-rate case and shows that variations in the channel state have significant impact on performance. In [5] [6], the authors consider variations in link capacity caused by dynamic channel state and mutual interference. In [7], link capacity affects the routing decision in a more direct way, for it serves explicitly as a factor in routing optimization. In [8], routing is jointly optimized with spectrum allocation and relay selection. The problem is eventually solved by a two-stage optimization problem, one of which aims at choosing the route with maximal capacity.

Among others, the papers discussed above have demonstrated that link capacity significantly affects routing decisions. This observation may however also provide the means for an adversary to extend control over the data flows in a network.

B. Wireless Security

Jamming attacks have drawn significant attention from the research community in recent years. Various anti-jamming strategies have been proposed [10]–[15]. In the existing literature, it is generally assumed that the objective of the adversary is to degrade the link throughput. There has instead been little focus on the interaction between jamming and attacks at other layers. Especially, for the interaction between jamming and network layer, researchers have mainly focused on how to mitigate jamming using multi-path routing [16] [17], or on how different routes affect physical layer security [18]. However, while routing diversity can potentially make the network more resilient against jamming, it can also be the source of other security issues, such as data control attacks.

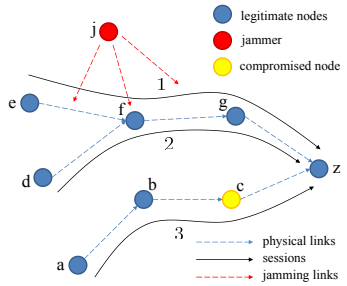


Fig. 2. An example network (c: compromised node, j: jammer).

If there are untrustful or compromised nodes, misbehavior in routing may lead to various data control attacks. In [19], the so-called "wormhole attack" was introduced. The attack utilizes "unusual" links, e.g., wired connections or directional antennas, to offer extra-ordinarily high throughput at some controlled nodes. The data flows are attracted to such nodes, where they fall under control of the attacker. Clearly, a crucial factor in wormhole attacks is the existence of the unusual links, which may not be available in all scenarios. In [20], Arsenal et al. consider a similar attack, where real links with unusually high throughput are not required. The adversary just claims to have such a good link. Apparently, if an end-to-end confirmation system is used, the attack will fail, since the senders will eventually learn the mismatch between claim and reality.

In this paper we will look at a different approach. Rather than "attracting" flows to compromised nodes, we consider strategies in which the attacker attempts to "force" the network to transfer information through compromised nodes by means of jamming. The interplay between two different attacks with a unified goal (jamming and data control) fundamentally separates the "hammer and anvil" attack from existing work.

III. System Model

In this section, we will introduce a model of the attack in a network with a typical cross-layer routing protocol, to illustrate the threat and the characteristics of it.

A. Basic Settings

We consider a wireless sensor network, in which multiple data sessions are generated at source nodes and forwarded to a data sink hop-by-hop. We assume that there are some compromised nodes controlled by the adversary, and some assistant jammers. Note that, in a wireless sensor network, nodes are typically deployed widely and exposed. Thus, it is fairly easy for an adversary to compromise some of them. An example is shown in Fig. 2.

The network is represented with a tuple $\{\mathcal{N}, \mathcal{E}\}$, where $\mathcal{N}$ denotes the set of nodes and $\mathcal{E} = \{e_{nm}\}_{n,m\in\mathcal{N}}$ is the set of physical links,

$$e_{nm} = \begin{cases} 1, & \text{if physical link (n,m) exists,} \\ 0, & \text{if physical link (n,m) does not exist.} \end{cases} \quad (1)$$

We assume that an orthogonal frequency division multiplexing (OFDM)-like transmission scheme is used at the physical layer. There is a set $\mathcal{F}$ of subchannels, each with bandwidth W. Each node allocates its power budget on the subchannels to maximize the physical-layer data rate. Without loss of generality, we assume that all nodes have the same power budget P^{max}, and we represent the power allocation profile for node n as $\mathbf{P}_n = \{P_n^1, P_n^2, \ldots, P_n^{|\mathcal{F}|}\}$. Then, the link capacity for receiver m can be expressed as

$$u_{nm}(\mathbf{P}_n) = W \sum_{f\in\mathcal{F}} \log\left(1 + \gamma_{nm}^f(P_n^f)\right), \quad (2)$$

where $\gamma_{nm}^f(P_n^f)$ is the SINR at the receiver on subchannel f. It is decided by

$$\gamma_{nm}^f(P_n^f) = \frac{P_n^f H_{nm}^f}{I_m^f + \eta_m^f}, \quad (3)$$

where H_{nm}^f, I_m^f, and η_m^f represent the channel gain of link $n \to m$, interference at m, and noise at m, repectively. We assume the noise i.i.d. Gaussian on all subchannels.

We consider a set of traffic sessions, denoted by $\mathcal{S}$. A session $s \in \mathcal{S}$ represents a data flow generated at a sensor node. The source node of s is denoted as $a(s)$. To ease the discussion, we assume that there is one sink node only, denoted as z, serving as the final destination node for all sessions. Our work can be easily extended to a multiple-sink scenario.

A packet may traverse multiple hops to reach the sink. To represent the path a packet traverses, we introduce the routing vector of a node n, $\mathbf{b}_n = \{b_n^m\}_{m\in\mathcal{N}}$

$$b_n^m = \begin{cases} 1, & m \text{ is selected as the next hop of } n, \\ 0, & \text{otherwise.} \end{cases} \quad (4)$$

Then, for the routing variables it needs to hold

$$b_n^m \le e_{nm}, \quad \forall n, m \in \mathcal{N}, \quad (5)$$

$$\sum_{m\in\mathcal{N}} b_n^m \le 1, \quad \forall n \in \mathcal{N}. \quad (6)$$

The path of a session s is denoted as $\mathcal{P}_s = \{n_i \in \mathcal{N} | n_1 = a(s), b_{n_i}^{n_{i+1}} = 1, \forall i \ge 1\}$.

B. Cross-Layer Routing

We consider cross-layer protocols with routing and link throughput coupled with each other. Depending on different applications, there are various of such protocols, with different objectives. It is infeasible to formalize a model capturing the characteristics of all these protocols. In this paper, we will limit the analysis of the attack to a typical cross-layer routing protocol, i.e, that with the per-packet end-to-end delay as the metric.

The packet delay at each hop consists of processing delay, propagation delay, queueing delay, and transmission delay. The former two are often negligible compared to the latter two, so we will only consider the queueing delay and transmission delay, which can be considered as the "service" delay of a packet at a node. We consider the following model:

1) The data generation process of any $s \in \mathcal{S}$, at the source node $A(s)$, is a Poisson process with rate r_s;
2) The service time of a packet at each given link $n \to m$ is exponentially distributed, with average service rate (inverse of the mean service time) of $\mu_{nm} = u_{nm}$, i.e., equal to the link capacity.

These assumptions are very commonly used in delay analysis of wireless networks, as in [21], among others.

Consider now an arbitrary session. Burke's theorem guarantees that the departure process of an M/M/1 queue is still a Poisson process with the same rate as the arrival process, and Kleinrock independence approximation justifies the Poisson arrival assumption of other nodes regardless of the interaction between traffic of different sessions [22]. Therefore, it is appropriate, under the considered scenario, to model each hop in the network as an individual M/M/1 queue. Denote the set of input sessions of n as $\mathcal{S}_n = \{s \in \mathcal{S} | n \in \mathcal{P}_s\}$. Then, the data arrival rate and service rate are, respectively,

$$\lambda_n = \sum_{s\in\mathcal{S}_n} r_s, \quad (7)$$

and

$$\mu_n(\mathbf{b}_n, \mathbf{P}_n) = \sum_{m\in\mathcal{N}} b_n^m u_{nm}(\mathbf{P}_n), \quad (8)$$

while the delay of the hop beginning with node n is

$$\tau_n(\mathbf{b}_n, \mathbf{P}_n) = \frac{1}{\mu_n(\mathbf{b}_n, \mathbf{P}_n) - \lambda_n}. \quad (9)$$

Finally, the end-to-end delay of a session s can be expressed as

$$T_s = \sum_{n\in\mathcal{P}_s} \sum_{m\in\mathcal{N}} b_n^m \tau_n. \quad (10)$$

Although (10) gives the theoretical end-to-end delay from n to the sink, it is usually impractical for a node to compute this value in an instantatneuos fashion. This is because, it is almost impossible for the nodes far away from n to report the instantaneous delay back to n. In most practical distributed algorithms, small-time-scale information exchange is usually limited between 1-hop neighbors. So, node n has to estimate the delay from the chosen next hop to the sink based on this limited information.

To achieve this goal, a simple yet reasonable way is to take advantage of geographic information, which is widely used in distributed routing protocols for wireless sensor networks [23]–[25]. To be specific, node n estimates the delay of the downstream hops by projecting the local delay of the next hop over the geographic distance to the sink, i.e., the estimated delay is given by

$$\tilde{T}_n(\mathbf{b}_n, \mathbf{P}_n) = \tau_n(\mathbf{b}_n, \mathbf{P}_n) + \kappa \sum_{m\in\mathcal{N}} b_n^m \tau_m d_{mz}. \quad (11)$$

In (11) τ_n is the delay from n to the next hop, given the routing decision $\mathbf{b}_n$. It is estimated based on the instantaneous channel

gain. Similarly, τ_m is the instantaneous delay from m to its next hop. Since m is 1 hop away from n, this information can be sent to n during information exchange. However, for the nodes with more hops away from n, the instantaneous local delay is not available. Therefore, n estimates the delay from m to the sink by computing the product of the local delay at m and the distance from m to the sink, represented by the second term in (11). It is a rough guess, but with the limited information, it it the best can be done. Besides, we introduce an adjustable factor κ to tune the weight between the 2 terms. If the estimated value is not reliable, small κ can be used to lower its influence.

C. Adversary Model

The primary objective of the adversary is to gain control over as much of the data in the network as possible. There are two core components in the adversary mode, i.e., compromised nodes and jammers.

We assume that the adversary controls some compromised nodes, which might conduct attacks such as traffic analysis, packet dropping, or even decryption. However, we will not focus on the specific type of attack that the adversary launches at the compromised nodes. Without loss of generality, we consider any data traversing the compromised nodes as insecure. In terms of observable behavior, compromised nodes are indistinguishable from legitimate nodes. In this paper we only consider a scenario with one compromised node, denoted as c, but the work can be easily extended to the case of multiple compromised nodes. The natural metric to evaluate the attack is the input data rate of the compromised node, i.e., λ_c.

The set of jammers is denoted as $\mathcal{J}$. Their objective is to drive traffic to the compromised node to expand the adversary's control on data. Like the legitimate users, the strategy space of a jammer $j \in \mathcal{J}$ is given by the power allocation on different channels, i.e., $\mathbf{P}_j = \{P_f\}_{f\in\mathcal{F}}$. The jammer j is also constrained by its power budget P_j^{max}.

Different jamming strategies can be adopted. In our model, we consider 2 types of jammers. The *type 1* jammer first evaluates the traffic load on every channel by measuring the interference plus noise level. If we denote the value as $D_j^f = I_j^f + \eta_j^f$, then j allocates the power budget as

$$P_j^f = \frac{D_j^f}{\sum_{f\in\mathcal{F}} D_j^f} \cdot P_j^{max}, \forall f \in \mathcal{F}. \tag{12}$$

Here, we are using the observed traffic at j to estimate the traffic load on different channels in the neighborhood of j. Without any additional information, this is a reasonable assumption.

Type 2 jammers are assumed to have knowledge of nodes within a certain range, which we refer to as the *influence set* of a jammer. We denote it as $\mathcal{R}_j$, as illustrated in Fig. 3. For every link $n \to m, m \in \mathcal{R}_j$, the service rate μ_n is a function of the jamming power $\mathbf{P}_j$. We assume j is aware of all the information required for the calculation of $\mu_n(\mathbf{P}_j)$, such as the power allocation of n, the channel gain from n to m etc. Then, j can optimally allocate its power budget to minimize $\sum_{n\in\{n|\exists m\in\mathcal{R}_j, b_n^m=1\}} \mu_n(\mathbf{P}_j)$.

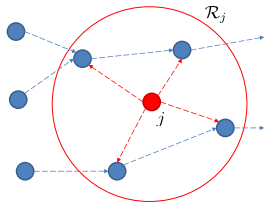


Fig. 3. Influence range of a jammer.

There are 2 remarks on the type 2 jammer. First, it requires perfect knowledge on the strategy and channel usage of other nodes, which is generally not practical. However, we intend to rely on this "omniscient" jammer to evaluate, under extreme conditions, how the attack will harm the network. Second, although a type 2 jammer has more knowledge on legitimate nodes, it does not necessarily lead to larger λ_c. In fact, the increase of λ_c relies on the reaction of legitimate users to jamming in the *next* strategy update period, and, for the strategy of omniscient jammer, it is almost impossible to include the reaction analytically (remind, even the legitimate nodes themselves have to solve a complex optimization problem to find the strategy for reaction). In other words, the optimality in decreasing traffic in $\mathcal{R}_j$ does not always agree with the optimality in increasing the traffic at c. Nevertheless, we will refer to type 1 and type 2 jammers as "blind jammers" and "omniscient jammers", respectively.

It must be pointed out that, the above model has not considered how to coordinate the jammer and compromised node. It still remains uncertain whether the jamming strategy will bring improvement in λ_c. We will find out rules on how to coordinate them through simulations.

IV. Problem Formulation

We now give the formal problem statement for the two sides of the attack. For a benign node $n \in \mathcal{N}/c$, there is a set of input sessions $\mathcal{S}_n$ and a set of neighboring nodes $\mathcal{V}_n = \{m \in \mathcal{N} | e_{mn} = 1\}$. The objective is to find the optimal power allocation $\mathbf{P}_n$ and routing decision $\mathbf{b}_n = \{b_n^m\}_{m\in\mathcal{N}}$ that minimize the estimated delay to the sink, as defined in (11). The problem is formulated as

$$\begin{aligned}
\text{given} \quad & \lambda_n, \mathcal{V}_n, \mathcal{E}, P^{max} && (13)\\
\underset{\mathbf{P}_n,\mathbf{b}_n}{\text{minimize}} \quad & \tilde{T}_n(\mathbf{P}_n, \mathbf{b}_n) && (14)\\
\text{subject to} \quad & b_n^m \in \{0,1\}, \forall m \in \mathcal{N} && (15)\\
& b_n^m \le e_{nm}, \forall m \in \mathcal{N} && (16)\\
& \textstyle\sum_{m\in\mathcal{V}_n} b_n^m \le 1 && (17)\\
& \mu_n(\mathbf{b}_n, \mathbf{P}_n) \ge \lambda_n + \epsilon && (18)\\
& \textstyle\sum_{f\in\mathcal{F}} P_n^f = P^{max}. && (19)
\end{aligned}$$

Constraint (18) implies that the service rate must be greater than the arrival rate, so that the delay is finite. We introduce a parameter ϵ to avoid the arbitrary greater relation (">") which results in an unbounded domain. Since it is possible that none of the links to the neighbors are good enough to meet the requirement, we allow n to refrain from forwarding data. This case corresponds to the strict inequality in (17).

The problem defined in (13)-(19) is a binary problem. However, if the next hop is given, i.e., $\mathbf{b}_n$ is fixed, then the problem

degrades to a throughput maximization problem with the power profile as the optimization variable. The degraded problem can be solved using classical waterfilling algorithm. Therefore, an enumerate-and-compare algorithm can be designed to solve the problem, as shown in Algorithm 1. As discussed in Section III, the compromised node acts identically to legitimate nodes, so we do not have to formulate a specific strategy for it.

Algorithm 1 Enumerate-and-Compare Algorithm for Cross-Layer Routing Problem

set $\mathbf{b}_n^* = \mathbf{0}_{1\times|\mathcal{N}|}, \mathbf{P}_n^* = \mathbf{0}_{1\times|\mathcal{F}|}, \tilde{T}_n^* = \infty$
for $m \in \mathcal{V}_n$ **do**
  if $d_{mz} \geq d_{nz}$ **then**
    continue
  end if
  set $b_n^m = 1, b_n^{m'} = 0, \forall m' \neq m$
  find optimal $\mathbf{P}_n$ using classical waterfilling algorithm
  if $\tilde{T}_n(\mathbf{b}_n, \mathbf{P}_n) < \tilde{T}_n^*$ **then**
    set $\mathbf{b}_n^* = \mathbf{b}_n, \mathbf{P}_n^* = \mathbf{P}_n, \tilde{T}_n^* = \tilde{T}_n(\mathbf{b}_n, \mathbf{P}_n)$
  end if
end for

The strategy of a blind jammer has been described in (12). The behavior of the omniscient jammer $j \in \mathcal{J}$ is defined by the following optimization problem

$$\text{given} \quad \mathcal{R}_j, P_j^{max} \tag{20}$$

$$\underset{\mathbf{P}_n}{\text{minimize}} \quad \sum_{n\in\{n|\exists m, b_n^m=1, m\in\mathcal{R}_j\}} \mu_n(\mathbf{P}_j) \tag{21}$$

$$\text{subject to} \quad P_j^f \geq 0, \forall f \in \mathcal{F} \tag{22}$$

$$\mathbf{1}^T\mathbf{P}_j = P_j^{max}. \tag{23}$$

In (20), influence range $\mathcal{R}_j$ defines the set of nodes that j intends to affect. By (21) the jammer tries to minimize the total service rate of all the influenced links. (22) and (23) give constraints on power allocation for the jammer.

The problem defined in (20)-(23) can be viewed as a "reverse waterfilling problem" and can be solved in polynomial time. We will not give the formal proof due to limited space.

V. Performance Analysis of the Attack

We evaluate the attack by conducting simulations. First, we show how the traffic map of a network is affected by jamming, and analyze how the jammer and compromised node should coordinate to achieve the attacking gain. Several factors affecting the routing map are investigated, and basic rules to tune the attack are derived based on the observations. Then, we analyze the performance of the attack quantitatively following these tuning rules.

A. Simulation Settings

We set the size of the simulation terrain to $500\,\mathrm{m} \times 500\,\mathrm{m}$. The area is divided into lattices with size of $100\mathrm{m}\times100\mathrm{m}$, and one node is located at a random location within each of them. Therefore, there is a total of 25 nodes. The sink is located at the center of the right side. A link exists between two nodes if the distance between them is no more than $150\,\mathrm{m}$. For simplicity, we only consider one jammer located sufficiently far away from the sink. The radius of the influence range is set to $50\,\mathrm{m}$.

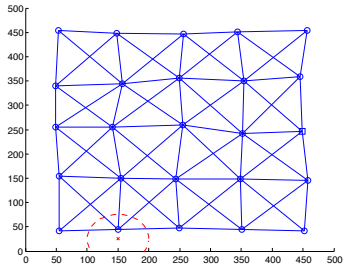


Fig. 4. A typical topology.

We ensure that the jammer is within $50\,\mathrm{m}$ of a legitimate node. An example of the resulting topology is shown in Fig. 4. Circles, squares, and bold lines represent legitimate nodes, sinks, and links, respectively.

Traffic sessions are generated at the leftmost 5 nodes. We do not fix the data generation rates. Instead, they are randomly generated in each topology, with the mean of the sum set to $200\,\mathrm{kbit/s}$. There are 10 mutually orthogonal channels, each with a bandwidth of $100\,\mathrm{kHz}$. Channels are associated with path loss and fading. The path loss factor is set to be 3, and the channel fading is set to be Rayleigh distributed with parameter 0.5. We set the power budget of the nodes to be $1\,\mathrm{W}$, and the noise power is $1\times10^{-9}\,\mathrm{W}$ on each channel. The parameter κ is set to 0.1×10^{-2}, unless otherwise specified. The value is selected to the order of 10^{-2} because the distances between neighboring nodes have a scale of $10^2\,\mathrm{m}$.

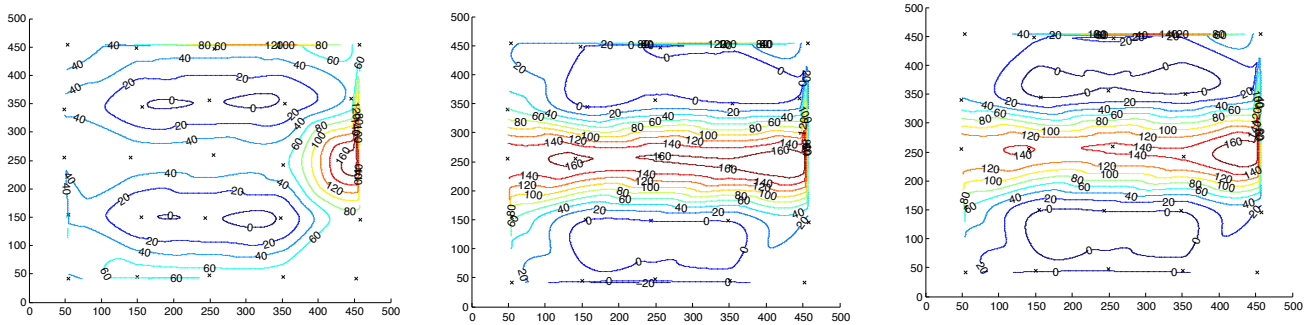
The simulation is event driven. In each strategy update period, a new set of channel fading and noise is randomly generated. Then, the legitimate nodes and the jammer update their strategies as defined in Section IV. Each experiment runs for 1000 strategy update periods.

B. The Impact of Jamming on Traffic Map

To gain insights in how to coordinate the jammer and compromised node, we must find out how the jamming strategy affects the traffic map. To this end, we first run simulations over 200 randomly generated topologies. For each one, three different settings are used, namely, without a jammer, with blind jammer, and with omniscient jammer. In these simulations, we set the power budget of jammers to the same value as the legitimate nodes, i.e., $P_j^{max} = 1\,\mathrm{W}$. We do not include any compromised nodes in this initial set of simulations.

Driving Effect. As an introduction, we first show in Fig. 5 the traffic map corresponding to the topology in Fig. 4. The traffic is depicted in the form of contour. The values at the nodes are the average data input rate over all the simulation periods. Note that the values at locations without nodes are interpolated. They are introduced to provide an intuitive visualization of the traffic "flows" in the entire network.

We observe obvious traffic changes with both the blind jammer and omniscient jammer. In fact, when there is no jammer, the network ends up setting up three major routes, as shown in Fig. 5(a). These traverse the upmost nodes, the central line of nodes, and the bottom nodes, respectively. It is consistent with the logic of the distributed routing protocol, i.e., nodes will generally try to avoid mutual interference to reduce delay.



(a) (b) (c)

Fig. 5. Traffic map: (a) no jammer; (b) blind jammer; (c) omniscient jammer.

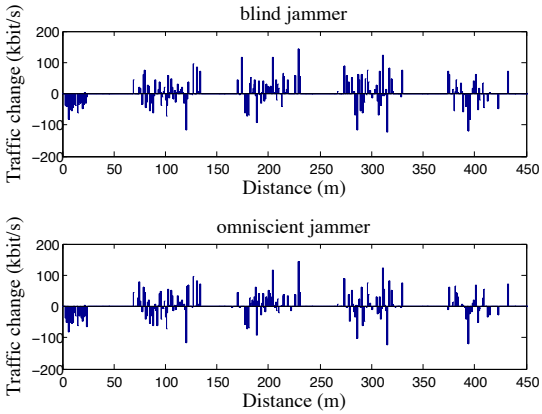


Fig. 6. Traffic change vs distance to the jammer.

With the jammer activated, however, we can see that, the lower route is completely disrupted. As a consequence, the traffic shifts to the center significantly. This is the major effect of jamming on the traffic map, as we observe it in almost all the simulations. We refer to this effect as the *driving effect* of the jammer.

For a certain node, the most important factor affecting the traffic change is apparently the distance to the jammer. We calculate the statistics over all the simulated topologies and plot the average traffic change vs distance to the jammer in Fig. 6. By traffic change we refer to the increase in average input data rate. Note that it is unfair to compare nodes with significantly different distances to the sink, since generally the traffic will be more concentrated at nodes closer to the sink. Therefore, for each simulated topology, we only consider the node closest to the jammer, and those with similar distance to the sink (compared with the node closest to the jammer). Taking Fig. 4 as an example, only the second column of nodes (those with x-axis values around 150) are compared. Because of the settings considered, the nodes are naturally divided in groups of 5, with distances of approximately (0 50], (50 150], (150 250], (250, 350], (350 450] m away from the jammer. We will refer to them as the group within 1,2,3,4,5 hops away from jammer in the following contexts, respectively.

Unsurprisingly, we observe that, within 1 hop distance to the jammer, almost every node experiences considerable decrease in input data rate. Conversely, we observe traffic increase for nodes located far away from the jammer. We can conclude that traffic close enough to the jammer is expected to be "driven" away. We refer to the distance within which most nodes experience traffic decrease as the *driven area*.

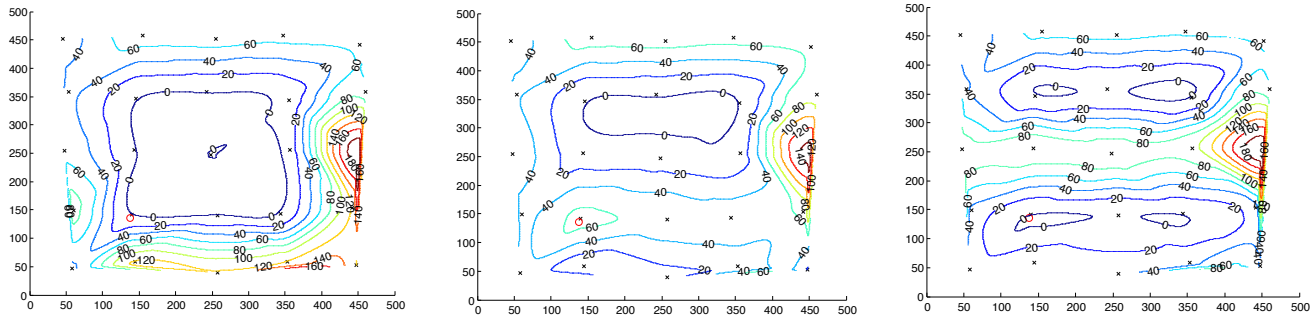
Rebalancing Effect. Intuitively, the nodes close to the jammer should always experience traffic decrease. However, we do observe some unusual cases where, at the node closest to the jammer, the traffic increases. We show a typical example in Fig. 7, where the 1-hop node experiences higher traffic with blind jammer than that without jammer.

A key observation for this phenomenon is that, without jamming, there is barely any traffic traversing the 1-hop node. Therefore, there is nothing that the jammer can drive away. Instead, the 2-hop node, i.e., the one at the bottom, has a considerable amount of traffic. After the jammer is activated, this node is also affected, so the traversing traffic is rerouted. Note that, even if a node is very near the jammer, it may still be able to support some level of traffic. Thus a certain amount of the rerouted traffic is rebalanced to the 1-hop node. In fact, by comparing Fig. 7 (b) and (c), we can verify this point. In (b), the blind jammer strategy is affected by the strategies of all other nodes, thus it is not focusing on the closest node, and there is still some room for the traffic; however in (c), the omniscient jammer aims at minimizing the service rate of the closest node and it is more likely that it cannot support much traffic, thus the traffic is driven to even farther nodes.

This observation suggests that, a jammer should refrain form acting, if the close nodes experience very low traffic. In fact, if we neglect the results for the cases in which the 1-hop node experiences traffic less than $20\,\mathrm{kbits/s}$, we have the traffic change vs distance as in Fig. 8. We can observe more consistent traffic change for the 2-hop nodes. To be specific, almost all of them experience traffic increase now. We will refer to this area as the *concentration area*, as the traffic driven away from the 1-hop nodes mainly concentrates here.

Yet, for even farther nodes, the trend remains chaotic. There are both considerable increases and decreases observed. This is due to the unpredictable influence of the jammer on faraway nodes. Theoretically, because of the path loss, the influence of the jammer decreases with power law. While the jammer's influence on the closest node is quite significant, its influence on farway nodes is less considerable. Therefore, the mutual interference between different nodes becomes more important. As a result of multiple, comparable affecting factors, the traffic change pattern becomes more unpredictable. In fact, Fig. 7 can give us some ideas on it.

Since there is very little traffic for the closest node to



(a) (b) (c)

Fig. 7. Rebalancing effect: (a) no jammer; (b) blind jammer; (c) omniscient jammer.

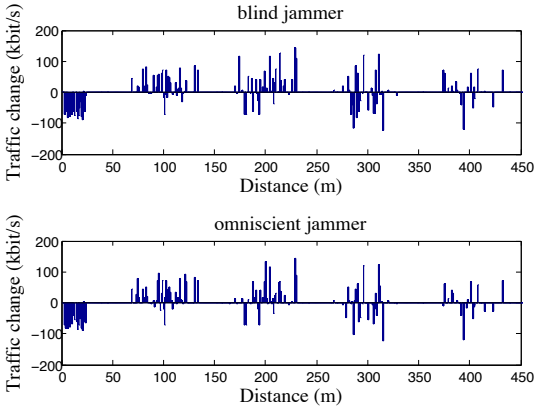


Fig. 8. Traffic change vs distance, jammer remains silent when closest node experience little traffic.

the jammer without jamming, this traffic change in Fig. 7 actually reveals how the jammer affects the traffic at the nodes farther than 1 hop. We observe that the traffic is "rebalanced" among other nodes, but there is not obvious driven-concentrate pattern, as the traffic of the 1-hop traffic experiences. In fact, the traffic that originally traverses the bottom node spreads among several nodes, without an obvious trend. We will refer to the effect on faraway traffic as the *rebalancing effect*.

General rules. To sum up, the affect of the jammer is different for nodes with different distance from it. For nodes within 1 hop distance, jammer has signicant influence and the traffic experiences "driving effect". Clear driven and concentration areas can be expected. For farther nodes, the influence of the jammer decreases, and the mutual interference between nodes becomes comparably important. With multiple affecting factors coupled together, the traffic traversing these nodes experiences "rebalancing effect". In this case, it is very difficult to predict the traffic change pattern.

As a result, the attacker should focus on the traffic at the closest node, and coordinate the locations of jammer and compromised node accordingly, so that the compromised node is in the concentration area. Besides, the jammer should not jam if the close nodes experience very low traffic load.

For example, if $P_j^{max} = 1$ W and $\kappa = 0.1 \times 10^{-2}$, we can locate the jammer within 1-hop distance of a node. Then, the nodes within 2 hops away from the jammer form the concentration area. Therefore, if the compromised node is within this area, the attack is very likely to achieve gain and therefore succeed.

C. Other Affecting Factors

Besides distance to the jammer, the change of traffic map may be affected by some other factors as well, such as the power budget of the jammer P_j^{max}, and the factor κ in the routing protocol. We will analyze the influence of these factors.

If the jammer is able to create distinct "driven area" and "concentration area", it will be easy for the attacker to coordinate the locations of the jammer and compromised node. For the areas to be distinct, it is required that the nodes in the same area experience decrease (or increase) with very high probability. In order to measure this, we introduce the "consistence index" α as a metric.

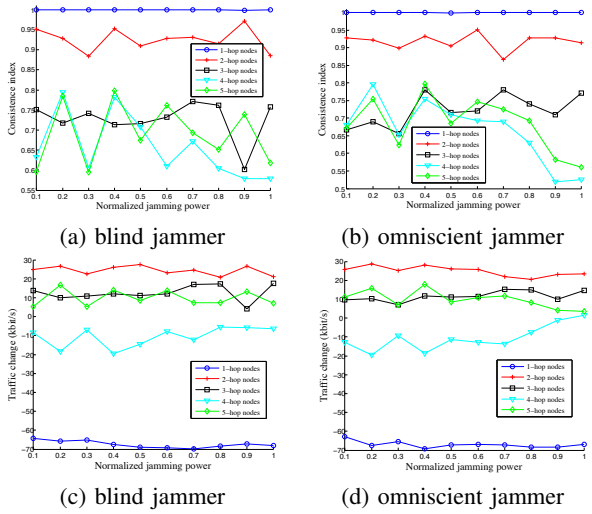
To be specific, for each node n in a certain group, we record the traffic change $\Delta\lambda_n$. It can be positive or negative. We sum the positive traffic change and negative traffic change for the whole group, take the greater one, and divided it by the sum of absolute traffic change. Then, we have

$$\alpha = \frac{\max\left(\sum_n \min(\Delta\lambda_n, 0), -\sum_n \max(\Delta\lambda_n, 0)\right)}{\sum_n |\Delta\lambda_n|}. \quad (24)$$

Generally, the higher α is, the more consistent the traffic change that the nodes experience. We also compare another important metric, i.e., the average value of traffic change in $\mathrm{kbit/s}$ of each group, too. The results are shown in Fig. 9. The jamming power is normalized to the legitimate node power.

We observe that, there is no obvious trend in the consistence index, with the increasing of jamming power, although small fluctuation exists. For 1-hop and 2-hop nodes, the indices are very high (almost constantly 1 for 1-hop and around 0.9 for 2-hop). Similarly, the traffic change is quite steady with varying jamming power for these two areas. This suggests that the driving effect is not sensitive to the normalized jamming power budget in the range $[0.1, 1]$. For all possible P_j^{max} in this range, we can use the same rules to locate jammer and compromised node, and achieve the same traffic change with respect to the nodes within 1 and 2 hops away from the jammer.

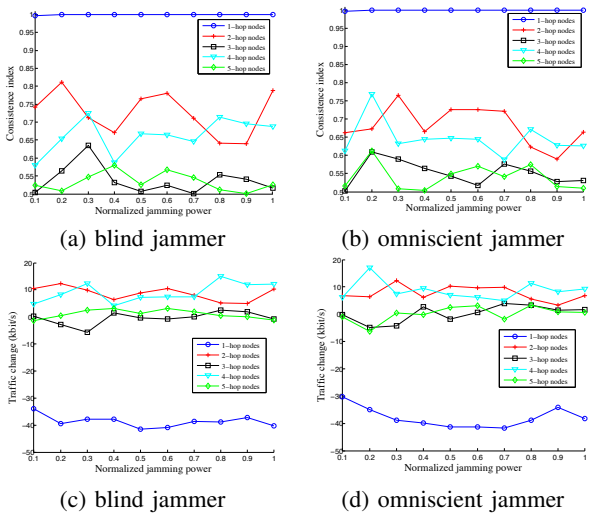
Another important factor is the myopic factor κ in the routing protocol. In Fig. 10, we show the consistence index and traffic change with $\kappa = 1 \times 10^{-2}$. We find that the driven traffic is significantly decreased compared to Fig. 9. This is because, with $\kappa = 1 \times 10^{-2}$, the delay of future hops becomes more important in routing decisions. Since the future delay is closely related to the distance from next hop to the sink (recall (11)),



(a) blind jammer (b) omniscient jammer

(c) blind jammer (d) omniscient jammer

Fig. 9. (a)(b) Consistence index vs jamming power; (c)(d) Traffic change vs jamming power. $\kappa = 0.1 \times 10^{-2}$.



(a) blind jammer (b) omniscient jammer

(c) blind jammer (d) omniscient jammer

Fig. 10. (a)(b) Consistence index vs jamming power; (c)(d) Traffic change vs jamming power. $\kappa = 1 \times 10^{-2}$.

the nodes will tend to focus more on the "shortest" physical distance rather than the smallest current hop delay.

The consistence indices for all the areas, except for the nodes very close to the jammer, are considerably lower than their counterparts with $\kappa = 0.1 \times 10^{-2}$. This observation seems quite anti-intuitive, since it is expected that the routing decision is less sensitive to jamming, with larger κ. However, it is not appropriate to evaluate the impact of jamming on routing only by the consistence index. This index only reveals how the traffic change, but does not provides information on how large the change is. In fact, we have already observed that, the absolute traffic change is decreased. In other words, the nodes are indeed more unwilling to change their routes. Only, the less occasional traffic changes tend to be more random in increase/decreas. The reason for this observation is, with the impact of jammer on traffic becoming weak, there is no longer a dominating factor affecting the traffic change. So the traffic change is expected to become more unpredictable.

In summary, with larger κ, the traffic change becomes smaller and more unpredictable. This observation suggests a way to design countermeasures for this attack, i.e., to design routing protocols that are less sensitive to current hop delay, and relies more on geographical distance and delay of future hops.

For all the above results, we observe no obvious difference between blind jammer and omniscient jammer. This finding confirms the divergence between the optimality of the problem defined in (20)-(23) and the objective of the attack. It also implies that, for the attacker, it is likely that the simpler jamming strategy, i.e., blind jamming strategy is used, since it requires much less information and gives comparable results.

D. Performance Evaluation

We have analyzed how to coordinate the jammer and compromised nodes to achieve best attack results, i.e.,

1) Given the location of the compromised node, the jammer should be located in such a way that the compromised node is within the "concentration area";
2) For certain jamming power (in our case, $1/10 - 1$ times that of the legitimate users), nodes approximately 1 - 2 hops away from the jammer form the concentration area;
3) The jammer can use a very simple strategy, i.e., measuring the interference-plus-noise level at different channels and allocate power budget on each of them proportional to the values;
4) The jammer should refrain from jamming if no significant traffic is traversing nearby nodes.

To evaluate the performance of the attack, in terms of the input data rate, we further run simulations with one compromised node. In these simulations, the location of the compromised node is chosen randomly, but with the distance to the sink within $[350\ 450]$ m. The location of the jammer is chosen following the aforementioned rules. The results are shown in Fig. 11.

For $\kappa = 0.1 \times 10^{-2}$, up to 116% increase in input data rate for the compromised node is observed. For all considered cases, the gain of the compromised node is quite steady, i.e., around 100%. For $\kappa = 1 \times 10^{-2}$, the gain is up to 77.8%. However, it varies significantly. Both blind and omniscient jammer achieve similar results. All the observations are consistent with our previous findings.

VI. Conclusions

We discussed a potential threat to data security in wireless networks. Unlike traditional attacks, the considered "hammer and anvil" attack exploits vulnerabilities introduced by cross-layer routing protocols, and amplifies weaknesses at the network layer with the assistance of physical layer jamming.

We formulate a general model of the attack, and analyze through extensive simulations how to coordinate the "hammer" and "anvil" to achieve the best attacking result. Some basic rules were found. Following these rules, we showed that considerable gain, with respect to the amount of controlled

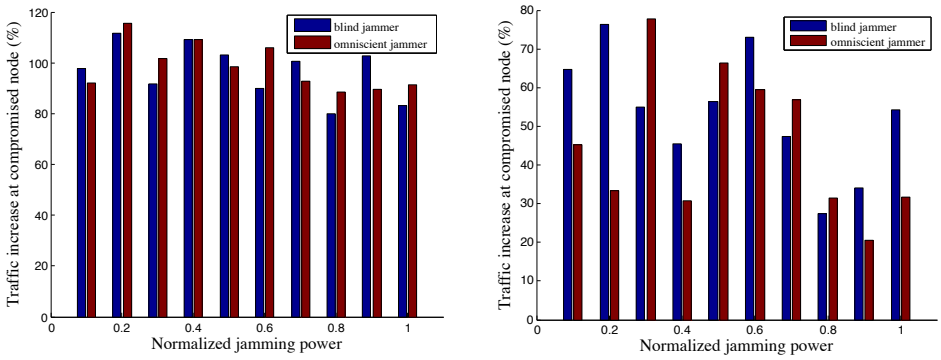


Fig. 11. The performance of the attack: (a) $\kappa = 0.1 \times 10^{-2}$; (b) $\kappa = 1 \times 10^{-2}$.

data in the network, can be achieved. While our findings reveal a new and serious threat to wireless networks, the observations also provide some insights on how to design countermeasures.

REFERENCES

[1] S. Higginbotham, "Sensor Networks Top Social Networks for Big Data," http://gigaom.com/2010/09/13/sensor-networks-top-social-networks-for-big-data-2/.

[2] L. Buttyan and J.-P. Hubaux, *Security and Cooperation in Wireless Networks: Thwarting Malicious and Selfish Behavior in the Age of Ubiquitous Computing*. New York, NY, USA: Cambridge University Press, 2007.

[3] L. Iannone, R. Khalili, K. Salamatian, and S. Fdida, "Cross-Layer Routing in Wireless Mesh Networks," in *Proc. of International Symposium on Wireless Communication Systems*, Barcelona, Spain, Sep. 2004, pp. 319–323.

[4] L. Chen, S. Low, M. Chiang, and J. Doyle, "Cross-Layer Congestion Control, Routing and Scheduling Design in Ad Hoc Wireless Networks," in *Proc. of IEEE Conference on Computer Communications (INFOCOM)*, Barcelona, Spain, Apr. 2006, pp. 1–13.

[5] R. Cruz and A. Santhanam, "Optimal routing, Link Scheduling and Power Control in Multihop Wireless Networks," in *Proc. of IEEE Conference on Computer Communications (INFOCOM)*, vol. 1, San Francisco, CA, Mar. 2003, pp. 702–711.

[6] S. Cui, R. Madan, A. Goldsmith, and S. Lall, "Joint Routing, MAC, and Link Layer Optimization in Sensor Networks with Energy Constraints," in *Proc. of IEEE International Conference on Communications (ICC)*, vol. 2, Seoul, Korea, May. 2005, pp. 725–729 Vol. 2.

[7] A. Eryilmaz and R. Srikant, "Joint Congestion Control, Routing, and MAC for Stability and Fairness in Wireless Networks," *IEEE Journal on Selected Areas in Communications*, vol. 24, no. 8, pp. 1514–1524, Aug. 2006.

[8] L. Ding, T. Melodia, S. Batalama, and J. Matyjas, "Distributed Routing, Relay Selection, and Spectrum Allocation in Cognitive and Cooperative Ad Hoc Networks," in *Proc. of IEEE Conf. on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, Boston, MA, USA, Jun. 2010.

[9] J. Hernandez-Serrano, O. León, and M. Soriano, "Modeling the Lion Attack in Cognitive Radio Networks," *EURASIP Journal on Wireless Communication Network*, vol. 2011, pp. 2:1–2:10, Jan. 2011.

[10] Y. Sagduyu, R. Berry, and A. Ephremides, "MAC Games for Distributed Wireless Network Security with Incomplete Information of Selfish and Malicious User Types," in *Proc. of International Conference on Game Theory for Networks (GameNets)*, Istanbul, Turkey, May 2009.

[11] B. Wang, Y. Wu, K. J. R. Liu, and T. Clancy, "An Anti-Jamming Stochastic Game for Cognitive Radio Networks," *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 29, no. 4, pp. 877–889, Apr. 2011.

[12] R. Gohary, Y. Huang, Z.-Q. Luo, and J.-S. Pang, "A Generalized Iterative Water-filling Algorithm for Distributed Power Control in The Presence of a Jammer," in *Proc. of IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP)*, Taipei, Taiwan, Apr. 2009.

[13] D. Yang, G. Xue, J. Zhang, A. Richa, and X. Fang, "Coping with a Smart Jammer in Wireless Networks: A Stackelberg Game Approach," *IEEE Transactions on Wireless Communications*, vol. 12, no. 8, pp. 4038–4047, Aug. 2013.

[14] Q. Yan, H. Zeng, T. Jiang, M. Li, W. Lou, and Y. Hou, "MIMO-based Jamming Resilient Communication in Wireless Networks," in *Proc. of IEEE Conference on Computer Communications (INFOCOM)*, Toronto, Canada, Apr. 2014, pp. 2697–2706.

[15] L. Zhang, Z. Guan, and T. Melodia, "Cooperative Anti-jamming for Infrastructure-less Wireless Networks with Stochastic Relaying," in *Proc. of IEEE Conference on Computer Communications (INFOCOM)*, Toronto, Canada, Apr. 2014.

[16] U. Patel, T. Biswas, and R. Dutta, "A Routing Approach to Jamming Mitigation in Wireless Multihop Networks," in *Proc. of IEEE Workshop on Local Metropolitan Area Networks (LANMAN)*, Chapel Hill, NC, USA, Oct. 2011, pp. 1–6.

[17] P. Tague, S. Nabar, J. Ritcey, and R. Poovendran, "Jamming-Aware Traffic Allocation for Multiple-Path Routing Using Portfolio Selection," *IEEE/ACM Transactions on Networking*, vol. 19, no. 1, pp. 184–194, Feb. 2011.

[18] M. Ghaderi, D. Goeckel, A. Orda, and M. Dehghan, "Efficient Wireless Security through Jamming, Coding and Routing," in *Proc. of IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks (SECON)*, New Orleans, LA, USA, Jun. 2013, pp. 505–513.

[19] Y.-C. Hu, A. Perrig, and D. Johnson, "Wormhole Attacks in Wireless Networks," *IEEE Journal on Selected Areas in Communications (JSAC)*, vol. 24, no. 2, pp. 370–380, 2006.

[20] M. Arslan, K. Pelechrinis, I. Broustis, S. Krishnamurthy, P. Krishnamurthy, and P. Mohapatra, "Detecting Route Attraction Attacks in Wireless Networks," in *International Conference on Mobile Adhoc and Sensor Systems (MASS)*, Valencia, Spain, Oct. 2011, pp. 371–380.

[21] S. Kompella, S. Mao, Y. Hou, and H. Sherali, "On Path Selection and Rate Allocation for Video in Wireless Mesh Networks," *IEEE/ACM Transactions on Networking*, vol. 17, no. 1, pp. 212–224, Feb. 2009.

[22] D. Bertsekas and R. Gallager, *Data Networks (2nd Ed.)*. Upper Saddle River, NJ, USA: Prentice-Hall, Inc., 1992.

[23] B. Karp and H. T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," in *Proc. of ACM International Conference on Mobile Computing and Networking (MobiCom)*, Boston, MA, USA, Aug. 2000, pp. 243–254.

[24] I. Stojmenovic and X. Lin, "Loop-Free Hybrid Single-Path/Flooding Routing Algorithms with Guaranteed Delivery for Wireless Networks," *IEEE Transactions on Parallel and Distributed Systems*, vol. 12, no. 10, pp. 1023–1032, Oct. 2001.

[25] T. Melodia, D. Pompili, and I. F. Akyildiz, "On the interdependence of Distributed Topology Control and Geographical Routing in Ad Hoc and Sensor Networks," *Journal of Selected Areas in Communications (JSAC)*, vol. 23, no. 3, pp. 520–532, Mar. 2005.