SecureMAC: Securing Wireless Medium Access Control Against Insider Denial-of-Service Attacks

Sang-Yoon Chang, *Member, IEEE* and Yih-Chun Hu, *Member, IEEE*

Abstract—Wireless network dynamically allocates channel resources to improve spectral efficiency and, to avoid collisions, has its users cooperate with each other using a medium access control (MAC) protocol. However, MAC assumes user compliance and can be detrimental when a user misbehaves. An attacker who compromised the network can launch more devastating denial-of-service (DoS) attacks than a network outsider by sending excessive reservation requests to waste bandwidth, by listening to the control messages and conducting power-efficient jamming, by falsifying information to manipulate the network control, and so on. We build SecureMAC to defend against such insider threats while retaining the benefits of coordination between the cooperative users. SecureMAC is comprised of four components: *channelization* to prevent excessive reservations, *randomization* to thwart reactive targeted jamming, *coordination* to counter control-message aware jamming and resolve over-reserved and under-reserved spectrum, and *power attribution* to determine each node's contribution to the received power. Our theoretical analyses and implementation evaluations demonstrate superior performance over previous approaches, which either ignore security issues or give up the benefit of cooperation when under attack by disabling user coordination (such as the Nash equilibrium of continuous wideband transmission). In realistic scenarios, our SecureMAC implementation outperforms such schemes by 76-159 percent.

Index Terms—Denial of service, network compromise, medium access control (MAC), wireless network

1 Introduction

From smartphones to wearable devices to Internet of Things (IoT)-based appliances, the demand for wireless communication keeps increasing. However, wireless communication consumes bandwidth, and the users inherently share a medium; therefore, one's signal becomes another's interference when they collide in channel access. To cope with the increased demand in wireless, the recent developments in radio technology (such as cognitive radio and software-defined radio) facilitate flexible and dynamic access and enable better adaptation to the ongoing traffic for greater spectral efficiency. These sophisticated technologies, however, increase the complexity of radio operations and network management, further necessitating a complementary protocol to coordinate the channel access when supporting multiple users.

To cope with the dynamism in channel access and avoid inter-user collision, *medium access control* (MAC) protocols have been designed to share a medium among multiple transmitters. Since wireless networks lack collision detection (in contrast to wired networks), they use MAC protocols that coordinate channel use through explicit messages. This process involves *control communication*, in which users *reserve* channels and notify the network of their transmission intentions before the data transmissions. The MAC protocol ensures collision avoidance among network users by ensuring that each user reserves channels separated in frequency, time, or processing/coding (we focus on frequency channel access although our approach generalizes to other access parameters).

MAC is designed for protocol-compliant users. However, we study the network behavior when some network users deviate from the protocol. There are three types of deviations that we may contemplate: accidental failures, selfish users, and malicious users. Previous work has shown that the Nash equilibrium when all users are selfish is to disable MAC exchanges and have each user access the entire bandwidth all the time [3]. The success of network protocols such as WiFi and TCP demonstrates that selfishness is not as prominent in real life as game theorists fear; instead, most users are protocol-compliant, and protocols based on user cooperations can yield overall network gain. Thus, to take advantage of the cooperative nature of most users, we focus on a group of compliant users sharing spectrum with malicious users (whose goal is to disrupt the network operations and have the option of behaving like a greedy user if other attacks fail).

In the presence of malicious users, much prior work in wireless MAC relies on the defense at the virtual network perimeter, e.g., filtering and blacklisting. Even when the network is compromised, prior work [4], [5], [6] focuses on detecting and isolating attackers based on their identities/credentials to make the attacker's insider capabilities obsolete, effectively reducing them into outsiders (whose identities grant no or limited capabilities and rights). Such perimeter-based approach works well when the network boundaries and the user behaviors (including the attackers's) are relatively static and is vulnerable against a sophisticated attacker who already knows the perimeter defense (by Kerckhoff's principle) and can thus bypass it. In addition,

- *S.-Y. Chang is with the Department of the Computer Science, University of Colorado Colorado Springs, Colorado Springs, CO 80918. E-mail: schang2@uccs.edu.*
- *Y.-C. Hu is with the Department of the Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, Champaign, IL 61801. E-mail: yihchun@illinois.edu.*

Manuscript received 12 May 2016; revised 29 Mar. 2017; accepted 9 Apr. 2017. Date of publication 12 Apr. 2017; date of current version 1 Nov. 2017. For information on obtaining reprints of this article, please send e-mail to: reprints@ieee.org, and reference the Digital Object Identifier below. Digital Object Identifier no. 10.1109/TMC.2017.2693990

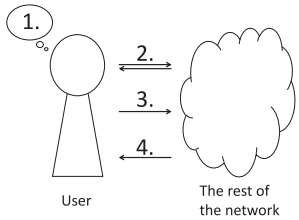


Fig. 1. Handshake-based MAC framework: 1. MAC control decision. 2. Control communication. 3. Data communication. 4. Feedback from receiver and network.

relying entirely on the perimeter defense for securing the network is becoming challenging as the wireless space becomes more complex in applications (e.g., IoT) and in operations (e.g., cognitive radio).

Thus, instead of depriving the attacker of its insider credentials, we adopt a defense in depth approach and implement a real-time strategy (updating the assigned network resources in every control communication) to build a layer of resiliency after the network perimeter. Therefore, we consider the more sophisticated threat model where attackers retain insider capabilities e.g., of reading and writing the network's control messages. Since we do not rely on identities or credentials but on real-time behaviors, our work supports dynamic network topology, e.g., a node entering or exiting a network.

In wireless MAC, an insider attacker can perform the following threats that are more devastating than those from an outsider: *false reservation injection* (initiating excessive MAC reservations and reserving the channel resources without using them), *false feedback distribution* (reporting false information to skew the decisions on MAC control to the attacker's favor), and *MAC-aware jamming* (adapting the jamming according to the received control messages). False reservation denies bandwidth to legitimate users and takes relatively little attacker resources (power to transmit control messages) and consumes network resources disproportionate to attacker effort; it is thus generally more efficient threat than jamming. In MAC-aware jamming, attackers use the information being exchanged in the MAC control communication for the jamming on data communication; this attack avoids wasting power on unoccupied channels and thus causes greater interference to the victim user than other jamming strategies, e.g., simple wideband jamming, with the same power. For our work, we consider an attacker that launches all three threats. However, the attacker is *power-limited* and wants to maximize its impact given a power constraint; such assumption is standard in wireless security because any jamming attacker without power limits can jam across all RF spectrum (from DC to light) at unlimited power, in which case none of the users can achieve any throughput.

We consider a *multi-channel environment* with power-limited users. The frequency spectrum is divided into multiple channels and each user competes for bandwidth on one channel at a time; our framework considers channels that have flexible bandwidth and varying center frequency. We also investigate both environments where a trusted entity exists and acts as an authority (centralized) and where such entity is absent (distributed); our analyses focus more on the distributed protocol that presents greater challenges.

We carefully model our work to produce fundamental results. Thus, our work offers a modular design that supports generality in physical-layer design (e.g., in modulation and coding), and the implementation-specific work of optimizing energy and in-device computation are not the focuses of our work. Our goal is to increase the achievable communication rate in wireless capacity, which applies to *all* system implementations. Therefore, we use the channel capacity as our performance metric, which allows us to simultaneously assess the impact of bandwidth and channel condition while abstracting away physical-layer system decisions (which may introduce additional vulnerabilities apart from those inherent in our MAC framework).

To secure MAC, SecureMAC offers a cross-layer design between the physical and link layers and is comprised of four main components: *channelization* that allocates bandwidth to the users, *randomization* that varies the channel access, *coordination* that exchanges the access information across users and facilitates MAC adaptation for higher spectral efficiency, and *power attribution* that estimates each user's power. Integrating the four components, SecureMAC provides a countermeasure solution against intelligent and insider adversaries (we reduce the optimal attacker strategy to that of an outsider) while retaining the benefit of legitimate user collaborations and achieving significant performance gain over the strategy of disabling MAC (which is the typical MAC-layer solution when the network is compromised).

The rest of the paper is organized as follows. Section 2 outlines our contribution, and Section 3 discusses about the system model and establishes prior work (on which we build SecureMAC). SecureMAC protocol is elaborated in Section 4. We theoretically analyze SecureMAC in Section 5 and present the implementation and simulation evaluation results in Section 6. Lastly, Section 7 concludes our work.

2 SecureMAC Contribution

2.1 MAC Framework

In order to handle bursty traffic patterns characteristic of data transmissions, Medium Access Control (MAC) protocols are typically dynamic, rapidly adapting resource allocations based on user demand. One common approach is to have each node explicitly announce and share its channel usage intentions, which we call *handshaking*, before transmitting data; other users will avoid using that channel. Fig. 1 illustrates a general handshake-based MAC framework; to send a packet, the transmitter (1) makes a MAC-layer decision based on its observations and the history from previous transmission rounds, (2) reserves channels for data transmission and shares its channel usage intention with other users in a control packet, (3) transmits the data packet using the reserved channels, and (4) receives feedback from the receiver and the network.

Our wireless MAC framework is applicable to many standardized protocols in last-mile networking and single-hop ad hoc networking, such as IEEE 802.11 (WiFi), IEEE 802.16 (WiMAX), and Bluetooth. In WiFi, users handshake using *virtual carrier sense* in which they access the channel via backoff-based random access and reserve the channel by exchanging Request to Send (RTS) and Clear to Send (CTS) messages before the data transmission. In WiMAX, a base station uses centralized scheduling to assign time slots and bandwidth to each users using a control channel, common and published as a part of the standard. In Bluetooth, a master device initiates handshaking and sends control messages assigning frequency hopping channels to the slave nodes. These protocols rely on the trust in the participating nodes and yield security vulnerabilities discussed in Section 2.2.

TABLE 1
Threats (X) and Countermeasures (O) of Our MAC Framework (The Colored Cells Indicate Our Research Contributions)

Vulnerability in	2. Control
Confidentiality	(X) Enabling MAC-aware jamming (O) **SecureMAC coordination**
Integrity	(X) False reservation injection (O) **SecureMAC channelization**
Availability	(X) Control channel jamming (O) Spread spectrum [7], [8] and other secure broadcasting [4], [9], [10]
Vulnerability in	**3. Data**
Confidentiality	(X) Reactive eavesdropping (O) **SecureMAC** uses frequency hopping spread spectrum
Integrity	(X) Spoofing (O) Application-layer cryptography
Availability	(X) Data channel jamming (O) **SecureMAC randomization and coordination**
Vulnerability in	**4. Feedback**
Confidentiality	(X) Optimizing false information distribution (O) **SecureMAC** uses robust aggregation
Integrity	(X) False information distribution (O) **SecureMAC channelization and power attribution**
Availability	(X) Feedback channel jamming (O) Spread spectrum [7], [8] and other secure broadcasting [4], [9], [10]

2.2 SecureMAC Contribution

We focus solely on the threats that are inherent to our MAC framework described in Section 2.1. Table 1 lists the vulnerabilities of handshaking-based MAC protocols and how they can be exploited against the network. The table also lists the countermeasure of each threats. (Section 3 discusses in more detail about system assumptions, and Section 3.3 describes the prior work on which SecureMAC builds.)

In addition to incorporating prior work and building an integrative countermeasure, SecureMAC offers novel contributions (the shaded regions in Table 1 highlight our novel contributions). We make four major contributions and integrate them to build SecureMAC. First, we develop a resource-based *channelization* scheme where each user is allocated spectrum proportional to its demonstrated power, rather than the number of network identities demonstrated. The channelization eliminates the false reservation threat, since a falsely reserving node will demonstrate minimal power. Second, given the channel bandwidth allocations from the channelization scheme, SecureMAC *randomization* uses dynamic frequency hopping spread spectrum to thwart targetted narrowband jamming; we motivate the design principle of user-independent randomization by establishing the infeasibility of inter-user coordination for generating randomization patterns (that can avoid collisions and fully use the available bandwidth). Third, to subsequently mitigate the deficiencies of the randomization, we build SecureMAC *coordination* that takes two measures: it deprives misbehaving users of the insider information while still performing handshakes with protocol-compliant legitimate users; and it implements waterfilling (on the unreserved bandwidth) to ensure full bandwidth utilization. Finally, SecureMAC *power attribution* determines the amount of power that was sent by each node, using a randomized approach that accurately attributes the power contributions of multiple nodes in the same frequency band, while defending against false information distribution threat. Under the threats on our MAC framework described in Table 1, SecureMAC forces the optimal insider attacker strategy to be that of an outsider.

2.3 Related Work on Wireless Availability

In wireless MAC security, previous work considers a denial-of-service (DoS) attacker capable of either jamming [6], [11], [12], [13], [14], [15], sending bogus requests to reserve channels [16], [17], [18], [19], or falsifying information at the communication feedback [20]. However, these prior work focus on their respective threats and remain vulnerable when facing a more comprehensive threat model that introduces an attacker capable of performing all of the aforementioned threats.

3 System Model

Our model supports the MAC framework described in Section 2.1 and applies generally across the protocols that implement the framework. There are T non-idle transmitters, which form the set $\mathcal{T}$ (each user is indexed with i where $i \in \mathcal{T} = \{1, 2, \ldots, T\}$), that share a frequency band with a total bandwidth W via frequency division.[1] In $\mathcal{T}$, there are M malicious attackers, each identified by an index $k \in \mathcal{M} = \{1, 2, \ldots, M\}$, and the rest of them are protocol-compliant and collaborative. The network is a single-hop network, in which users communicate directly without any need for relaying, and each transmission is heard by all users. Thus, when two or more users operate on the same channel, they collide. The users do not favor any particular subset of spectrum, and every part experiences equal path loss in expectation. Furthermore, users operate in a repeated game with infinite-horizon; that is, the transmitters do not run out of queued packets. Also, all users are time-synchronized at the packet level, and they operate in the same phase in the protocol (e.g., control communication phase) at any give time.

We build our scheme on pre-established keys, such as Diffie-Hellman key exchange and those used in resource-constrained sensor networks [21], [22], [23], and each pair of nodes share a secret key; our main contributions lie after node registration and key establishment. We also timestamp and authenticate control packets either by using digital signatures or by authenticating them to an online trusted authority (the reservation messages need only be authenticated to that online authority); this authentication eliminates forged MAC control messages, thus ensuring that a user can be held responsible for the channels it has reserved. We further assume that each node knows which users are valid (e.g., based on a certificate signed by an offline trusted authority), which prevents the Sybil attack (one entity faking multiple identities).

1. Although many existing wireless MACs operate at a single frequency, the use of multiple frequencies is not only achievable with current technology (as discussed in Section 3.3) but is also common in wireless cellular networks. Furthermore, our techniques are as applicable in time-division systems as they are in frequency-division systems, though frequency-division systems are easier to describe and are tailored to a more realistic power-limited attacker (while a time-division system relies on attacker energy limitations).

3.1 Performance Metric

Our analysis holds when using *any* metric as long as it exhibits the following three properties: it is decreasing and convex with jamming power, monotonically increasing with transmitter's signal power, and linear in available bandwidth. As a representation, we use the Shannon channel capacity[2] to construct our performance metric. Channel capacity is strongly correlated with both bandwidth and signal-to-interference-and-noise ratio (SINR), while abstracting away physical-layer decisions such as modulation and coding.

Whenever user i transmits to its destination user j, it does so on a frequency channel, whose location is known to user i and user j and whose bandwidth is W_i. Under a flat fading Gaussian channel with Gaussian signals and interference being treated as noise, the channel capacity of the link $i \rightarrow j$ is

$$\mathcal{R}_i = W_i \log_2 \left[1 + \frac{P_{i,j}}{N_0 W_i + \sum_{\ell \neq i, \ell \in \mathcal{M}^c} P_{\ell,j} + \sum_{k \in \mathcal{M}} P_{k,j}} \right] . \quad (1)$$

In Equation (1), N_0 is the noise power spectral density; $\mathcal{M}$ is the indices of jammers; $\mathcal{M}^c$ is the indices of legitimate users; $P_{x,y}$ is the *effective* or *received* signal power of the link $x \rightarrow y$; and the fraction inside of the parenthesis is SINR.

We bound the power of all users including attackers such that user x has a bound of P_x: $E[P_{x,y}] \leq P_x < \infty, \ \forall x \in \mathcal{T}$, where $P_{x,y}$ is random due to the channel $x \rightarrow y$. As $\mathcal{R}_i$ monotonically increases with P_i, each transmitter emits at full power to maximize the signal power P_i at the receiver. Users with better channel gains can be modeled with larger power constraints. Jensen's inequality [26] yields the capacity of

$$E[\mathcal{R}_i] \leq W_i \log_2 \left[1 + \frac{P_i}{N_0 W_i + \sum_{\ell \neq i, \ell \in \mathcal{M}^c} I_\ell P_\ell + \sum_{k \in \mathcal{M}} J_k P_k} \right], \quad (2)$$

where I_ℓ is the amount of benign user ℓ's power that interferes with the transmitter's signal normalized with respect to the power constraint P_ℓ, and J_k is the attacker k's jamming power normalized to the power constraint P_k (that is, I_ℓ and J_k are control variables indicating the amount of power emitted on the channel). We use Equation (2) as our performance metric for the link $i \rightarrow j$. For our goal of maximizing the performance of the overall network, we introduce a network utility function U, which is the aggregate rate of the legitimate users

$$U = \sum_{i \in \mathcal{T}} E[\mathcal{R}_i] = \sum_{i \in \mathcal{M}^c} E[\mathcal{R}_i]. \quad (3)$$

3.2 Threat Model

An insider attacker launches a denial-of-service (DoS) attack on the network to reduce the network performance. We consider the worst-case attacker who minimizes the utility

$$\text{minimize } U \text{ subject to } J_k \leq 1, \ \forall k \in \mathcal{M}. \quad (4)$$

Under this model, the attackers will fully utilize their power budget. We also consider a strong threat of *an attacker network* where multiple entities compromised the network and they share all information through a secure, covert channel with unlimited bandwidth; such network of insider attackers is a stronger threat model than having one (entity) point of breach in the network and multiple outsiders colluding with that insider attacker, as such colluding outsiders' involvement in the MAC can only be passive (e.g., they can perform MAC-aware jamming from the information relayed by the insider but cannot falsely reserve channels).

We focus on threats that exploit vulnerabilities that are insufficiently addressed by prior work in wireless security. In specific, we are concerned with the following attacks: *false reservation injection*, which wastes network bandwidth, and *jamming* on the remaining bandwidth. If successful, false reservation is the more power-efficient attack of the two, since it allows an attacker to reduce bandwidth available to legitimate nodes at nearly no power cost. Each attacker can send a short reservation request message and reserve a channel for an extended period of time (supposedly for data transmission) without the intention of using the channel, preventing legitimate users from using the bandwidth resource. After successful false reservation, attackers can use the majority of their power to jam and disrupt the communication of legitimate users. In this case, attackers are successful in both wasting resource by falsely reserving portions of spectrum and degrading the channel conditions of the rest of the spectrum by jamming. To realize this, attackers are capable of accessing non-contiguous frequency band, e.g., [27].

Attackers can also target the feedback communication and perform *false feedback distribution* to manipulate MAC parameters and influence the user's decisions on MAC control. Attackers can do so in two ways: they can attack the aggregation of the power estimations (for bandwidth allocation in distributed settings) or affect the users' power sensing by over-claiming transmissions (especially for those band that are occupied by more than one user). We discuss each of these threats in greater details and present our corresponding countermeasures in Sections 4.2 and 4.5, respectively.

3.3 Prior Work and Bases for Our Work

SecureMAC builds on prior work, and we review them in this section. Our approach diverges from the conventional slotted channelization (where the spectrum is divided into channels with fixed bandwidth and static location), the typical approach when studying security in wireless MAC. Instead, we allocate channels with varying bandwidth and center frequency to more effectively match the power of each user, increasing our system's spectral efficiency. Researchers have used flexible channelization in non-security contexts [27], [28], [29].

The resource consumption of control communication can be made much smaller than that of data communication (this actually helps the attacker and makes the false reservation threat more efficient, as described in Section 3.2) because the overhead of a control message can be amortized over data frame and we can choose arbitrarily large data frames. Thus, we focus on the performance of data communication when evaluating SecureMAC. Furthermore, control communication being relatively small helps in building link reliability by making it more affordable to use measures that are generally costly; wireless researchers widely use the gain from time and processing redundancy to increase resistance to noise and interference [4], [7], [14], [15]; thus, we rely on such techniques to ensure the availability of control channel.

2. The channel capacity given by Shannon-Hartley Theorem provides an asymptotic upper bound for the communication rate of an independent AWGN channel [24], [25]. This bound is commonly used for evaluating performance and is generally considered tight (information theorists continue to pursue even tighter bounds in more complex and realistic channel models).

To build resistance against outsider jammers targeting specific users, we incorporate randomization and build on the traditional anti-jamming technique of spread spectrum, where the spreading code is known to only the sender and the receiver [7]. Using frequency hopping spread spectrum (FHSS), each user transmits data using frequency hopping on randomly generated hopping patterns chosen independently for each packet. To avoid reactive jamming, where an attacker senses the channel use and jams as soon as it detects the victim's transmission, we use fast hopping where the hopping duration is less than the attacker's reaction time. Even though incorporating FHSS-based hopping complicates our scheme, it is crucial to add robustness against outsider jammers who dynamically adapt its strategy; otherwise, their relatively inefficient strategy is already effective in disrupting transmission.

SecureMAC coordination builds on our prior work, SimpleMAC [14], [30]; compared to SimpleMAC, SecureMAC incorporates greater complexity and is comprised of multiple components. Unlike insecure MACs, which blindly trust and handshake with everybody in the network, SimpleMAC uses a feedback-based trial-and-error mechanism to select a subset of the network users with which to perform handshaking (in order to avoid sharing the critical MAC information to the compromised network users); we call this set the *handshaking list* and denote it with S in this paper (our prior work in SimpleMAC calls this set the *recipient list* of control messages). Unlike other prior work that detects and isolates attackers [4], [6], [31], SimpleMAC [14], [30] chooses the handshaking list based on the performance history of handshaking lists rather than the behavior of the individual entities. This approach makes SimpleMAC inherently robust to colluding attackers such as those who do not jam themselves but relay the jamming-relevant information to the jammers, since the end-user observes the same performance regardless of whether the insider attacker jams itself or provides the information to colluding attacker. The scheme dynamically explores among possible handshaking lists and quickly outperforms the Nash equilibrium in expectation and converges to the ideal handshaking list. To facilitate the coordination component, SecureMAC relies on SimpleMAC's exploration mechanism, which details we do not further discuss in this paper. Even though our prior work in SimpleMAC facilitates to counter MAC-aware jamming, its use is within the coordination component (Section 4.1) and does not contribute to the rest of the SecureMAC components; in fact, SimpleMAC design does not aim to be effective against MAC-proactive threats such as false reservation injection and false information distribution.

4 SecureMAC Scheme

4.1 SecureMAC Overview

SecureMAC node executes channelization, randomization, coordination, data communication, and power attribution in sequenece; unlike the other components, power attribution occurs after data communication. *Channelization* determines the amount of bandwidth to allocate to each user based on prior power measurements. The goal of channelization is to allocate spectrum bandwidth to each user proportional to its power capability, ensuring a constant power spectral density, known to be optimal in channel capacity [32]. Channelization decisions are made once per round. Within a round, channel access based on allocations cannot be based on fixed center frequencies because a static allocation of channels is vulnerable to outsider jammers who can monitor the channel use and dynamically adapt their strategies. We thus have a *randomization* component, which implements frequency hopping spread spectrum (FHSS) that varies the center frequency, while maintaining the bandwidth allocation. (Unlike the other components, we do not further describe FHSS randomization in this section since it is well-studied in prior literature and we provide an overview in Section 3.3.) Randomization in channel access results in collisions in some parts of frequency band and vacancy in others. The *coordination* addresses these problems by sharing the bandwidth allocation and the randomization results, resolving known conflicting reservations arising from randomization-induced collisions, and allocating transmission to regions that would otherwise be underutilized. Data communication for goodput delivery follows. Finally, after a round of data transmission is complete, each node performs *power attribution* to determine the amount of power contributed for data communication by each node while leveraging commit-and-reveal to build resilience against the manipulation of power attribution. These transmission power estimates are then used for MAC control in the next round.

Fig. 2 illustrates the spectral occupancy of Nash equilibrium and each of the SecureMAC components when two users, one of which has twice as much bandwidth as the other, share the band. In the Nash equilibrium of wideband access, all users fully utilize the bandwidth while interfering with each other (Fig. 2a); the users can filter the interference and noise via signal processing, e.g., direct sequence spread spectrum (DSSS), but such processing performance is bounded by the channel capacity; wideband access does not require MAC, corresponds to when the network users give up on collaboration, and thus serves as a baseline to our scheme. In SecureMAC channelization, users allocate bandwidth proportionally to their power capabilities, which has greater channel capacity than the wideband access in the ideal case of fully orthogonal channel access (Fig. 2b) except for when the channel noise dominates the signal. SecureMAC randomization causes partial collision and underutilization (Fig. 2c) while SecureMAC coordination resolves the collision and waterfills the underutilized spectrum (Fig. 2d).

4.2 SecureMAC Channelization

SecureMAC channelization counters the false reservation attack with three properties: first, it provides power-fairness across users (from the receivers' perspectives); second, it achieves the optimal performance in terms of spectral efficiency; and third, it prevents the attacker from simultaneously making effective reservations and using all of its power for jamming. In fact, as we will see in Section 6.1, the optimal power-limited strategy for attackers is to forgo false reservation and exclusively focus on jamming. Our protocol thus performs substantially better than previous protocols that do not counter false reservations since, in those protocols, an optimal attacker can simultaneously perform false reservation and jamming, as described in Section 3.2. Table 2 presents our scheme when only considering false reservation threats.

SecureMAC channelization assigns bandwidth to a user proportional to the received power from the user; only the current bandwidth allocation (which is necessary to perform power attribution on each users) and the update (proportional to the users' power attribution results) affect

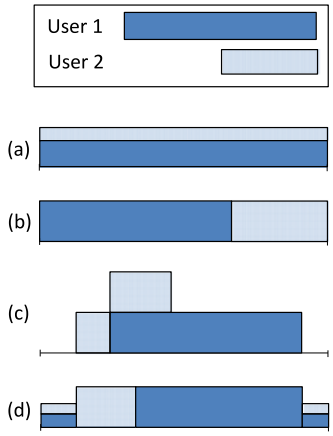


Fig. 2. We illustrate the spectrum of: (a) Nash equilibrium (wideband access). (b) Our scheme after channelization. (c) After randomization. (d) After bandwidth coordination. Frequency in horizontal axis and power spectral density (PSD) in vertical axis.

the upcoming allocation. To determine and disseminate the bandwidth allocation results of the channelization, the scheme has two stages: first, each node performs *individual channelization* and then, for environments that lack an online central authority, the nodes perform *distributed channelization* to decide and agree on the bandwidth allocation while minimizing the effect of colluding adversaries. In contrast, in the presence of a trusted authority, the authority broadcasts its own individual channelization results to assign bandwidths, and we can bypass the distributed channelization.

The *individual channelization* assigns bandwidth proportional to the observed received power; all users have unique observations because they are in different spatial locations (which affects the wireless propagation attenuation) and wireless channels naturally fluctuate and experience fading.

The *distributed channelization* aggregates the individual channelization decisions in a distributed manner, so that users agree on the channelization results of which user gets how much bandwidth. Each user disseminates its channelization result using the Byzantine General's algorithm with signed messages [33]. All users then compute the median bandwidth allocation for each node (median is known to be an attack-resistent aggregation mechanism [34]), and use these values as the network-wide consensus. Because each node computes the median over the same set of data, each node arrives at the same channelization. Thus, the SecureMAC channelization is resilient to Byzantine failure and requires only one round of message delivery.

However, because the attackers compromise a fraction of the network and have legitimate rights to vote, the distributed channelization is vulnerable to an attack where attackers attempt to distort the consensus to their advantage. In this false feedback distribution attack, attackers report false channelizations to distort the outcome of the distributed channelization. Because SecureMAC's distributed channelization uses the median, it is somewhat resilient to such attacks [34]. Nevertheless, since attackers know each other, they can still distort the median by reporting favorable values for fellow attackers and discredit legitimate nodes by claiming low power observations. As a result, the consensus median value will be shifted towards the value that the attackers report. Furthermore, if the number of attackers exceeds half the network population, the attackers gain total control over the distributed scheme.

SecureMAC does not attempt to detect and isolate false reporting attackers because the variable channel conditions caused by wireless fading adds randomness to each user's received power observations and makes detection difficult. A threshold-based scheme can be defeated by attackers who infer other legitimate users' observations based on the past reports. Attackers can then decide how much to distort the median by reporting moderately biased values while avoiding detection. Because such detection approaches may be ineffective, yet add complexity and a new attack vector (e.g., false positive creation), we do not use them in SecureMAC.

4.3 SecureMAC Randomization

After SecureMAC channelization determines the bandwidth allocation for each user, SecureMAC randomizes the users' channel access locations to thwart power-efficient targeted jamming. SecureMAC builds on frequency hopping spread spectrum (FHSS), described in Section 3, and each user chooses its center frequency at each point in time from a uniform distribution. Though incorporating FHSS in SecureMAC complicates the scheme, it is crucial when attackers can learn about the channel parameters and perform targeted jamming. SecureMAC aims to defend against such targeted attacks.

This section presents a fundamental result about channel randomization (Section 5 presents more theoretical results). In particular, although inter-user coordination in generating hopping patterns can help in achieving perfect orthogonality between channels and may potentially offer full bandwidth utilization (for example, a centralized authority can use random permutation to generate hopping patterns so that the hopping access does not overlap between users), we show that control communication overhead for any such approach is prohibitive (in the presence of an insider attacker monitoring and recording the hopping patterns to learn about the hopping pattern), motivating SecureMAC to generate random and inter-user-independent hopping patterns.

Definition 1. *A system* resists jamming against an insider attacker*if the insider attacker, from its available information, gains no additional advantage on the channels used by any other node, except that already available through any assurances of orthogonality.*

Theorem 1. *In a system where T transmitters first coordinate amongst themselves and then transmit for a fixed period of time representing h hops, no system can resist jamming against an insider attacker with overhead less than $\Omega(Th \log_2 c)$ per period where c is the number of distinct channels.*

Proof. We show that per-user overhead is $\Omega(h \log_2 c)$. At time t (in hops), the user chooses the channel c_t from a uniform distribution, i.e., $\Pr[c_t = a] = \frac{1}{c}, \forall a$ where a is some channel. Thus, the entropy of each hop is $H(c_t) = \log_2 c$ for attackers. We consider an attacker who knows and records the transcripts of the user's past hops before t (the knowledge of other users' past transcripts do not help as the channel access is independent across t, although the users' accesses are dependent to each other at the same t).

We use contradiction. Suppose there exists a coordination protocol with some per-node overhead of $x < \Omega(h \log_2 c)$. Since the entropy of each hop is $\log_2 c$, the entropy is $x - \log_2 c$ after one hop, $x - 2 \log_2 c$ after two hops (because the hops are independent across t), and

TABLE 2
Channelization, Data Communication, and Feedback

	Channelization
1. *Allocation*	Assign bandwidth according to the received power
2. *Data communication*	Transmit goodput data
3. *Feedback*	Report the receiver's observations in performance and power

so on. At the last hop of h, the remaining entropy is $x - h \log_2 c$, which is negative and thus impossible. Thus, by contradiction the per-node overhead is no less than $\Omega(h \log_2 c)$. □

Remark 1. The proof assumes that the channel access is in uniform distribution. However, the attackers can introduce bias, for example, by false reservation attack, effectively reducing the $H(c_t) = f(c) < \log_2 c$. Then, the overhead is $\Omega(Thf(c))$.

In Theorem 1, we learn that any system that attempts to coordinate the dynamic frequency hopping pattern does not scale well with the number of users T and the number of hops h, latter of which can grow significantly in the presence of processing-powerful reactive jammers (by causality, the hopping duration is, however, lower-bounded by the signal travel time coming from the triangular distance between the attacker and the transmitter-receiver pair). Therefore, due to the overhead cost in control communication, we build SecureMAC randomization on FHSS where all users choose their frequency hopping patterns independently to each other.

4.4 SecureMAC Coordination

As discussed in Section 4.3, SecureMAC randomization selects hopping patterns individually without regarding potential collisions. Therefore, much like the traditional FHSS, SecureMAC randomization causes *collisions* (channels in which multiple users make a reservation) and *under-utilization* (channels in which no users make a reservation). To avoid spectral inefficiency caused by collision and underutilization, legitimate nodes perform SecureMAC coordination. SecureMAC coordination offers secure *handshaking* where users exchange the center frequencies of their reserved channels and adjust the channel access to minimize mutual interference; furthermore, the users utilize the under-utilized bandwidth by waterfilling such bandwidth with their transmissions. The handshaking process involves a single one-way multicast delivery, i.e., everybody delivers one handshaking package that contains the reservation information (however, to realize secure delivery, this entitles redundant transmission and user interaction, as we will discuss in Section 4.5). Table 3 presents an overview of the SecureMAC; the coordination (Section 4.4) and the power attribution (Section 4.5) are shaded in the table to contrast with Table 2; these are the additional complexities required to incorporate randomization to thwart outsider jamming and build resilience against false feedback distribution.

4.4.1 Handshaking List Selection

A user that handshakes with a misbehaving user may experience decreased performance, since the attacker can now use randomization information to perform targeted jamming against that user. Therefore, SecureMAC builds trust and shares MAC-sensitive information only with those that are beneficial. A user's *handshaking list* S is the the subset of the network users with which it handshakes. As described in Section 3, we use SimpleMAC to determine and update the handshaking list [14], [30]. SecureMAC handshaking involves sharing its handshaking list S and its randomized center frequency sequence with every node in S for channel access coordination.

TABLE 3
SecureMAC Protocol

	SecureMAC protocol
1. *Channelization*	Assign bandwidth according to the received power
2. *Commit*	Commit to handshaking list and waveform (for attribution)
3. *Handshake*	Handshake and disclose hopping pattern to handshaking list Handshaking users adjust bandwidth and waterfill
4. *Data communication*	Transmit goodput data on predetermined bandwidth
5. *Reveal*	Reveal the handshaking list and waveform
6. *Power attribution*	Observe the spectrum and determine users' power levels
7. *Feedback*	Report performance and power levels observed this round

4.4.2 Bandwidth and Power Control

In this section, we describe how SecureMAC resolves channels that have conflicting reservations or that lack reservations. For each time slot, SecureMAC performs three steps. First, when two nodes i and j have mutual knowledge of their impending collision, the nodes divide the collided bandwidth, so that each node obtains an amount of bandwidth proportional to their respective bandwidth allocations. Second, when node i knows of an impending collision with j, but j does not know of i's intentions, i defers to j. (We do not claim that this is an optimal choice; rather, we make it for simplicity.) Finally, SecureMAC determines the set of channels that are not reserved by any user and plans to waterfill that spectrum. The user divides its power between its solely-operating reserved channel and the channel that apparently nobody has reserved based on its estimate of interference power on both the reserved channel and the under-utilized channel.

4.5 SecureMAC Power Attribution & Commit-and-Reveal

As SecureMAC channelization is based on the power observed from each transmitter, we provide a physical-layer supplement to our MAC protocol that attributes power to users given a received signal. Separating out the power from each user requires two parts: first, we need to know where each user is transmitting at any time, and second, for bandwidth regions where multiple users transmit at the same frequency and the same time, we need to be able to determine the power of each user. After the coordination in Section 4.4, for regions where one user has sole access, we can trivially determine that user's power level by filtering

and observing the amount of power in the user's reserved channel. However, for bands where multiple users transmit, such passband-based attribution schemes are ineffective. Thus, users *commit* to the waveform signature that they will transmit prior to data transmission.

In every round, our protocol involves five steps: two before the data is sent, and three afterwards. First, the user chooses a randomization pattern for hopping and commits to the data, a random nonce, and the waveform signature. Second, the user sends a control message to each node and includes the randomization pattern in that message for coordination. Then the user sends the data using its randomization pattern. Third, each user reveals their waveform signature and the nonce from initial commitment. Fourth, each user combines the random numbers (e.g., using XOR) to determine a network-wide random number, and uses that random number to determine a short portion of its data transmission to reveal (e.g., using a PRF keyed with the random number); this interval could be identical system-wide, or it could be determined on a per-transmitter basis. Finally, each user A reconstructs the perspective of each other user B during B's revealed time t_B, and determines the amount of power transmitted by B. To do so, A considers the reservations that B has sent and received, determines the output of B's coordination, determines the data that B will send, and obtains the waveform that B sent at time t_B. User A then takes the cross-correlation between the signal received by A at time t_B and the waveform that B sent at time t_B to determine B's contribution on the A's received signal. This correlator-based approach for attribution is widely used in communications such as in signal detection (e.g., preamble synchronization), matched filter, and direct sequence spread spectrum (DSSS).

We now describe the commit-and-reveal protocol in greater detail. In step one, each node commits to its data, nonce, randomization pattern, and handshaking list. For efficiency and attack-resilience reasons, we commit to these as follows. First, the data is subdivided into small blocks and committed using a Merkle hash tree [35]. Second, a commitment is made to the nonce. Next, the randomization pattern and handshaking list can be combined in a third commitment. Finally, the three commitments (the root of the Merkle Hash Tree for the data, the commitment to the nonce, and the commitment to the randomization pattern and handshaking list) are reliably disseminated to all nodes with authentication, for example, through Byzantine agreement with digital signatures [33]. When a node receives a handshaking message in step two, the node checks to make sure that it is on the handshaking list declared in the message, and that the handshaking message is consistent with the sender's commitment from step one. If either of these checks fails, the node disregards the message.

After data transmission, each node provides enough information so that every other node can determine the state at that node. In particular, it composes a message with the nonce, randomization pattern, handshaking list, and the set of nodes from which it received a valid coordination message. This message is also distributed reliably and authentically, for example, through Byzantine agreement with digital signatures. In the event that any node F does not send such a message, the network detects the lack of such a message, and any node that received a coordination message from F can reveal F's randomization pattern and handshaking list.

Once all nodes have the same subset of nonces (ensured through the use of Byzantine agreement and previous commitment), they combine those nonces (e.g., by computing exclusive-or across them) to compute a network-wide random value. Each node A then determines the time slot t_A in which it is to be audited by using a function on this random value, such as a pseudorandom function, keyed with the random value, computed on the node's node identifier. This time slot can, but need not, be the same for all users. Each node A then reveals the data it transmitted during slot t_A, together with sufficient nodes in the Merkle Tree, to allow each receiver to verify that the data is the same as the data that has been committed. Each user can also determine that A sent the correct part of the data, because A's transmission rate does not depend on the data, but only on the presence of conflicts in A's reserved bandwidth and on the unused space detected by A.

At this point, each user can verify:

- The randomization pattern and handshaking list claimed by each node that either sent a coordination message to a legitimate host or participated in the protocol
- The information from which node A claimed to perform coordination at each point in time, for each participating node A, and
- The data that node A transmitted at time t_A, for each participating node A.

The user then computes the cross-correlation described above to attribute a portion of the power received at time t_A to A.

5 Theoretical Analysis

In this section, we present our theoretical analyses results and establish the bases for the testbed evaluation in Section 6.

5.1 Two-Party Game for Channelization

Our protocol reduces the problem of false reservations to a two-party game between the *legitimate user network* and the *attacker network*, because we assume cooperative behavior among benign users and collusion among attackers, and because the channelization outcome depends only on the received power. Specifically, the users' behavior and the attacker's optimal strategy depend on the relative power capabilities of the legitimate and attacker networks, rather than on the number of users. In our theoretical analysis, we consider nodes with equal power constraints; all individual users, including attackers, have the same power constraint $\bar{P}$, i.e., $P_i = \bar{P},\ \forall i \in \mathcal{T}$. Then, the power capability ratio of the legitimate user network to that of the attacker network is $\frac{T-M}{M}$, so we control the power capabilities of the two groups by varying the number of users (T) and attackers (M). Because all users have equal power, they have the same expected performance $\mathcal{R}$, i.e., $\mathcal{R} = E[\mathcal{R}_i],\ \forall i \in \mathcal{T}$. We introduce α to represent the fraction of attacker power expended on channels reserved by the attacker, so that $1-\alpha$ represents the fraction of attacker power used for jamming other channels. Since the attacker network uses $(\alpha \cdot \bar{P} \cdot M)$ power for false reservation, Equation (2) yields

$$\mathcal{R} = \frac{W}{T - M + M\alpha} \log_2 \left[1 + \frac{\mathrm{SNR}}{\frac{T}{T-M+M\alpha} + \frac{M(1-\alpha)}{(T-M)}\mathrm{SNR}} \right], \quad (5)$$

where the SNR is the ratio between the network power capability (including that of the insider attackers) and the natural noise on the entire frequency band ($\text{SNR} = \frac{T \cdot \bar{P}}{W \cdot N_0}$).

5.2 Attacker's Advantage on Distributed Protocol

Our distributed channelization scheme takes the median of each user's bandwidth allocations to reach a consensus channelization. In this section, we study the impact of wireless channel fluctuations when our protocol is under attack by false-feedback-distribution attackers. We use β to denote the attacker's *bandwidth advantage* over a legitimate user. As discussed in Section 4.2, attackers can reserve more bandwidth than legitimate users with the same power ($\beta \geq 1$) because attackers collude while legitimate users report truthfully. Due to channel diversity and fading, legitimate nodes report different power levels for the same transmission. An attacker can shift the median by reporting an extreme value. Without any attackers, the median returns the 50th percentile measurement for each transmitter. When assessing the data transmission power of a colluding attacker, attackers report large power observations, shifting the observed median upward to the $100 \cdot \frac{0.5 \cdot T}{T-M} > 50$th percentile of legitimate observations. Also, for a legitimate user, the attackers report low power to shift the median downward to the $100 \cdot \frac{0.5 \cdot T - M}{T-M} < 50$th percentile of observations. In contrast, legitimate users report their true observations that include random wireless channel fluctuation. Assuming an iid channel for all users with each channel characterized by a cumulative distribution function CDF, the attacker's advantage is: $\beta = \frac{\text{CDF}^{-1}(\frac{0.5 \cdot T}{T-M})}{\text{CDF}^{-1}(\frac{0.5 \cdot T - M}{T-M})}$.

Fig. 3 plots the attacker bandwidth advantage β under varying channel fading where channel characteristics vary in Rician fading with ν and σ, where ν^2 is the power of the line-of-sight path[3] and $2\sigma^2$ is the power of the other scattered paths. In particular, we study three choices of channel fading characteristics: *strong line-of-sight* ($\frac{\nu}{\sigma} = 10$), *weak line-of-sight* ($\frac{\nu}{\sigma} = 2$), *no line-of-sight* ($\frac{\nu}{\sigma} = 0$). The *no line-of-sight* case is equivalent to the Rayleigh fading model, suitable for a highly dynamic environments, e.g., a mobile application in the cities [36], [37]. Increasing the number of attackers results in greater error in the computed median and greater attacker bandwidth advantage. Because channel fluctuation affects the randomness within the power reports, the attacker's bandwidth advantage β depends on $\frac{\nu}{\sigma}$. The advantage increases as the line-of-sight path becomes less dominant.

Under the false feedback distribution attack, one legitimate node's bandwidth is one part in $T - M + \alpha\beta M$, since $T - M$ is the number of legitimate users and $\alpha\beta M$ is the effective requests made by attackers, resulting in per-user performance of: $\mathcal{R} = \frac{W}{T - M + M\alpha\beta} \log_2[1 + \frac{\text{SNR}}{\frac{T}{T-M+M\alpha\beta} + \frac{M(1-\alpha)}{(T-M)}\text{SNR}}]$. Thus, compared to the performance of a centralized scheme (Equation (5)), our distributed scheme gives attackers an additional factor of β more bandwidth.

5.3 Static α Strategy for Attackers

We study the optimal attacker strategy and show that the optimal α is static in time. Let $\mathcal{U}$ be the aggregate utility over time, i.e., $\mathcal{U} = \sum_t U_t$, where U_t is the network performance (Equation (3)) at time t; let $\hat{\alpha}$ be the static-game α strategy minimizing U; and let α_t be the amount of power used to reserve channels at time t.

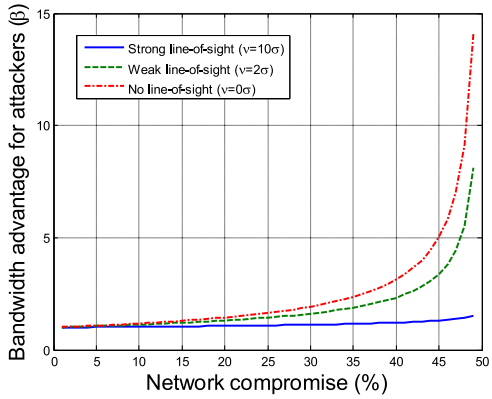


Fig. 3. Ratio of attacker's and legitimate user's bandwidth under false feedback distribution attack on SecureMAC channelization.

Theorem 2 *Given* $\hat{\alpha}$, $\alpha_t = \hat{\alpha}, \ \forall t$, *minimizes* $\mathcal{U}$.

Proof. We provide a sketch of the proof and overlook the impact of fading (and β) here. From Equation (5), both $\frac{(T-M) \cdot W}{T - M + M\alpha}$ and $\log_2[1 + \frac{\text{SNR}}{\frac{T}{T-M+M\alpha} + \frac{M(1-\alpha)}{(T-M)}\text{SNR}}]$ are convex, monotonic, and positive for all possible α. Therefore, the product, U_c is also convex with respect to α. By using Jensen's inequality, $\alpha_t = E[\hat{\alpha}] = \hat{\alpha}, \ \forall t$ minimizes $\mathcal{U}$.

SecureMAC Randomiztion introduces colored fading, in which the accessed frequency band experiences different levels of interference/noise and thus SNR varies with frequency. In such environment, this proof using Jensen's inequality is extended to per subcarrier basis where the transmission capacity is the aggregate capacity of the subcarriers accessed. □

6 Testbed Evaluations

We take a modular approach in analyzing each of the components and then implement the protocol as a whole. Our implementation uses four WARP software-defined radio (SDR) platforms [38], each of which has two antenna chains. Using the multiple input multiple output (MIMO) capability of the platform, we build a network with four transmitters and four receivers. Each transmitter has equal power budget unless otherwise noted (e.g., Section 6.1 introduces an identity-only attacker with zero power transmission). We manually calibrate the antenna locations and the antenna gains so that each receiver observes approximately the same power from each transmitter (the relative power between the nodes affects the performances, as we discuss in Section 5.1, as long as the absolute power is within the receivers' dynamic ranges). In the absence of interference, the channel experiences a SNR of approximately 16 dB for any transmitter-receiver pair. For power attribution, we assume that each transmitter can learn its power level relative to other transmitters, either through full-duplex radio techniques or by, for each transmitter node, designating a single receiver node trusted by that transmitter.

Each node continuously transmits to maximize network utility U. At the physical layer, we use DQPSK modulation with a BPSK-modulated Barker sequence preamble. We use

3. As is common in wireless communications, the term *line-of-sight* path refers to the most dominant channel path, and not necessarily the straight-line path between the two nodes.

12 MHz of network bandwidth divided into 300 subcarriers using OFDM. For example, if the bandwidth is allocated equally among n registered users (the baseline channelization strategy, as defined in Section 6.1), each user will use $\frac{300}{n}$ subcarriers. The experiment results are averaged over 1,000 runs. Each run is for a single round, and each round lasts for 6 hops. Each transmitter sends random bits to its receiver, and its receiver demodulates the received signal and uses the BER to estimate the SINR at the receiver, using the equation from [39], [40]: $\overline{\text{BER}} = \frac{1}{2}(1 - \frac{\sqrt{2 \cdot \overline{\text{SINR}}}}{\sqrt{1+4 \cdot \overline{\text{SINR}}+2 \cdot \overline{\text{SINR}}^2}})$. Equation (1) then yields the capacity based on the observed SINR.

6.1 Channelization

6.1.1 Individual Channelization

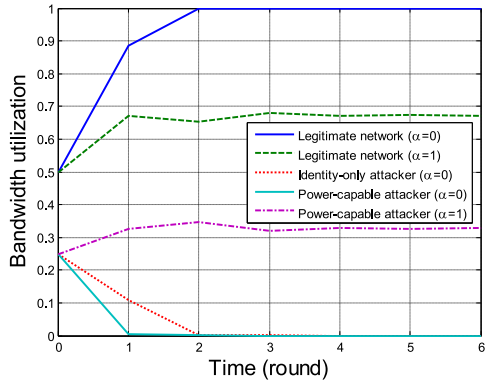
We compare the performance of SecureMAC channelization to a baseline protocol. In the *baseline protocol*, the frequency band is divided equally into multiple channels and each user gets one channel, regardless of whether they use the allocated channel or not. Optimal attacker strategy against this baseline protocol is to use no power in the spectrum allocated to them ($\alpha = 0$), wasting $\frac{M}{T}$ of the entire network bandwidth for free, and focus all its power on jamming ($1 - \alpha = 1$). In our evaluation, we consider two legitimate transmitters, one attacker, and one *identity-only attacker* (which has zero power budget).

We study individual channelization under the two attacker strategies of $\alpha = 0$ (using all power for jamming) and $\alpha = 1$ (using all power for effective reservation). Fig. 4a shows the outcome of the channelization and, in specific, the expected normalized bandwidth allocation to the four transmitters. Beginning from the baseline strategy of equal-bandwidth channelization (i.e., each of the four entities occupy 0.25 of the network bandwidth), our scheme quickly converges to the steady-state channelization in two rounds, where the delay is caused by noise in the spectrum reserved by attackers. We plot the *legitimate network bandwidth*, the fraction of bandwidth allocated to legitimate network users, which converges to 1 for $\alpha = 0$ and to $\frac{2}{3}$ for $\alpha = 1$, validating our steady-state theoretical results. The $\alpha = 0$ attacker is quickly found to be emitting no power in reserved spectrum. Furthermore, the identity-only attacker also quickly converges to zero bandwidth as it emits no power and thus has no impact on network performance under our scheme.

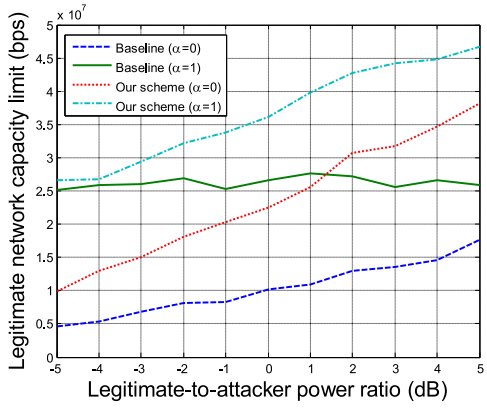
We also vary the attacker's power budget relative to the legitimate user's power (the identity-only attacker retains zero power budget) in Fig. 4b. As expected, larger legitimate-to-attacker power ratios result in better performance, where the performance increase comes from reduced interference for $\alpha = 0$ (jamming) and from increased bandwidth for $\alpha = 1$ (reserving). For each MAC, $\alpha = 0$ represents a stronger attack than $\alpha = 1$. Power increments are best spent on jamming; spending power to make effective reservations shows less impact with increasing power. Thus, the attacker chooses to jam rather than to spend power to make effective channel reservations under our scheme; we also verify these results in detailed MATLAB simulations in a technical report [2] where $0 < \alpha < 1$ cases are also analyzed.

6.1.2 Distributed Channelization

Here we summarize our findings of SecureMAC's distributed channelization scheme in order to preserve space and



(a) Normalized BW utilization



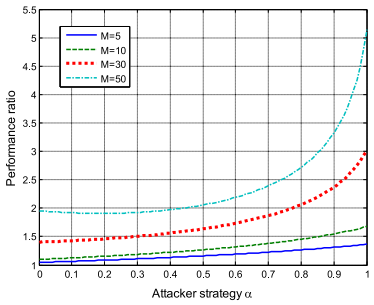
(b) Varying power budget

Fig. 4. Individual channelization performance.

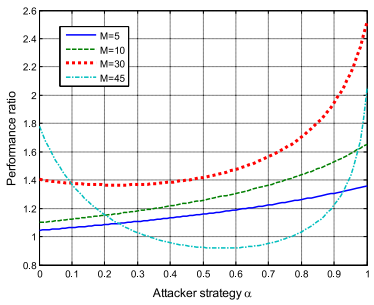
because they are consistent with our MATLAB simulation of larger networks with more dynamic channels in Section 6.1.3. First, the distributed channelization performs worse than the individual channelization due to the impact of the false information injection attack; for instance, at steady-state, distributed channelization achieves 92.4 percent of the individual channelization performance and 88.7 percent when $\alpha = 0$ and $\alpha = 1$, respectively. Second, despite the persistent effect of false information injection, distributed channelization performs better than the baseline strategy of entity-fair channelization. Third, the influence of false feedback makes it more beneficial for attackers to reserve some spectrum, so $\alpha > 0$. Section 6.1.3 investigates these phenomena in more detail.

6.1.3 Computer Simulation Evaluations

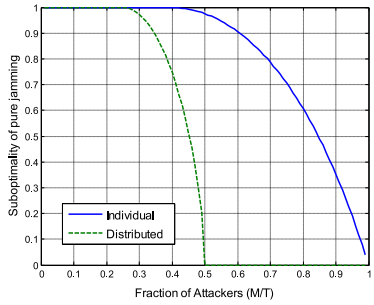
In Sections 6.2.1 and 6.1.2, we discussed about our SDR-based testbed results, demonstrating that SecureMAC channelization scheme is practical and that both the individual and distributed channelization provide performance advantages over the naïve baseline strategy of identity-based channelization. In this section, to demonstrate the scalability of SecureMAC, we use MATLAB to simulate a more complicated network topology in a fading environment. To capture the game between the legitimate network and the attacker network, we vary the network parameters and study their effect on SecureMAC channelization. We simulate a network of 100 equal-power transmitters ($T = 100$), including M number of attackers, with an interference-free SNR of 15 dB, using a 20 MHz wide bandwidth. We model an AWGN channel with Rayleigh fading, which emulates a highly dynamic environment, such as in urban setting [36], [37].



(a) Individual channelization



(b) Distributed channelization



(c) Comparison between the attacker's optimal strategy ($\alpha = \hat{\alpha}$) and only jamming ($\alpha = 0$)

Fig. 5. Computer simulations.

Using the performance metric of network capacity limit in Equation (3), we analyze the *performance ratio* between the aggregate capacity limit of SecureMAC channelization and the aggregate capacity limit of the baseline performance. In particular, we use the performance ratio over the optimal baseline strategy, which is that attackers jam ($\alpha = 0$). The metric measures the improvement observed by each user. We also study the optimal attacker reactions to SecureMAC channelization and $\hat{\alpha}$ denotes the optimal power-splitting strategy.

Unsurprisingly, the rate performance suffers with increasing attackers' power capability M (the data presentation is omitted here). However, as seen in Fig. 5a, the individual channelization outperforms the baseline performance in all evaluated scenarios and does so more strongly with increasing attacker capability (performance ratio increases as M increases).

When M is small, attackers' optimal strategy is to jam with all their power ($\hat{\alpha} = 0$), which agrees with out SDR-based testbed studies. However, as the aggregate attacker power reaches and exceeds the aggregate legitimate user power, using some power to reserve channels, i.e., $\hat{\alpha} > 0$, becomes the optimal attacker strategy; this occurs when the attackers control more than 45 percent of the network's power capability. For example, in Fig. 5a, when attackers have as much power capability as the legitimate users, i.e., $M = 50$ out of $T = 100$, attackers will transmit on data channels with $\hat{\alpha} = 0.2$ of their power capability to obtain some valid channel reservations, and use $1 - \hat{\alpha} = 0.8$ of power to jam. The optimal attacker strategy diverges from $\alpha = 0$, since additional jamming has a logarithmic impact on network performance while reservations have a linear impact. Therefore, as attackers' power capabilities grow, the marginal impact of reserving and consuming bandwidth exceeds that of jamming legitimate transmissions.

In order to better compare the optimal attacker strategy and pure jamming, Fig. 5c, varies the fraction of attacker nodes in the network and studies the *suboptimality of pure jamming* by plotting the performance ratio between the optimal attacker strategy, $\alpha = \hat{\alpha}$, and that when attackers jam at full power, $\alpha = 0$. Thus, the metric indicates how much pure jamming underachieves the attacker's goal of degrading the network performance compared to the optimal power-splitting strategy. We observe that, when normal users outnumber malicious users, and thus legitimate user channels have sufficiently good quality, jamming ($\alpha = 0$) is an optimal or near-optimal strategy. In particular, $\hat{\alpha} = 0$ until about 45 percent of the network nodes are compromised, and there is only 2.5 percent difference in performance between $\alpha = 0$ and $\alpha = \hat{\alpha} = 0.2$ when half the nodes are malicious ($M = T - M = 50$). Therefore, in most practical scenarios (where attackers do not substantially outnumber legitimate users), $\alpha = 0$ is the optimal jammer strategy or is negligibly suboptimal.

The distributed channelization scheme performs worse but has similar properties to the individual channelization scheme. In Fig. 5b, we observe that the optimal attacker strategy diverges from $\alpha = 0$ in more scenarios than in the individual scheme due to the false information distribution threat. For example, when $M = 30$, $\alpha = 0.24$ is the optimal strategy for distributed scheme (Fig. 5b) whereas $\alpha = 0$ is the optimal attacker behavior in the centralized scheme (Fig. 5a). From Fig. 5c, pure jamming is optimal, i.e., $\hat{\alpha} = 0$, if less than 27 percent of network is compromised by attackers. Also, as discussed in Section 5.2, if $\frac{M}{T} \leq 0.5$, the attacker can take all of the bandwidth when $\alpha > 0$.

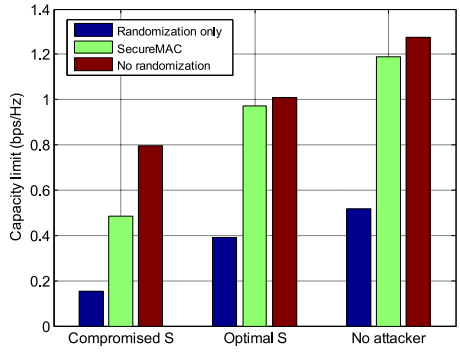
Unlike individual channelization, the distributed channelization can have worse performance than the baseline strategy as the number of attackers (M) increases, e.g., $M = 45$ in Fig. 5b. This reduced performance arises from the bandwidth advantage that comes from the false reporting attack, which grows quickly as M increases. As shown in Fig. 3, when $M = 45$, the attacker can reserve five times as much bandwidth than legitimate users if the same amount of power is used for reservation ($\beta = 5$). Therefore, as the number of attackers approaches that of legitimate users, the distributed channelization becomes less effective. However, the distributed bandwidth allocation only exhibits poor performance when the number of malicious users approaches 50 percent; before the scheme breaks down due to the false-reporting attack, it effectively prevents the false reservation. For example, even when 30 percent of nodes are attackers, the scheme provides nearly a 40 percent performance improvement over the baseline strategy.

6.2 Randomization and Coordination

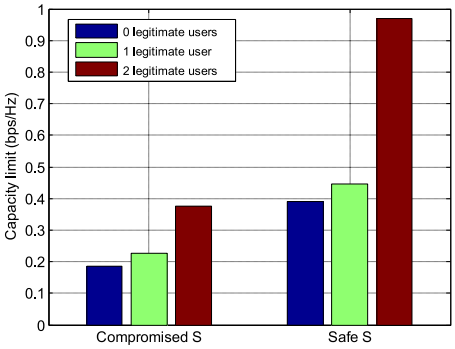
To isolate the behavior of randomization and coordination from channelization, we set each user's bandwidth to 0.25 of the total network bandwidth, and conduct our experiments with four users. Also, to capture the impact of the targeted jamming, we model the worst-case performance among the network users by focusing attacks on a single user, called *User 1*, and evaluating the performance of this user.

6.2.1 At Steady-State Handshaking

We compare the channel capacity of three schemes: the naïve frequency hopping ("randomization only"), our proposed



(a) Randomization only (naïve hopping), SecureMAC, and No randomization (fully orthogonal access)



(b) Varying handshaking lists. Safe S (right) excludes attacker and the compromised S (left) includes attacker

Fig. 6. SecureMAC randomization and coordination.

SecureMAC randomization and coordination, and the centralized scheme that offers fully orthogonal access, either by using no randomization or perfectly orthogonal randomization ("no randomization"). Because the behavior of each scheme depends on the handshaking list in use, we use three attacker strategies to represent different categories of handshaking list: an attacker that behaves like other legitimate users and contains its transmission within its reserved bandwidth (which we label "no attacker"), an attacker that reserves as much spectrum as it can and performs wideband jamming outside that spectrum, since the user uses the ideal handshaking list that excludes the attacker and includes all benign users (labelled "optimal S"), and an attacker that performs narrowband jamming on the highest-priority user, User 1 (labelled "compromised S"). For each type of transmission list, Fig. 6a shows the results of these three schemes under these three types of handshaking list.

SecureMAC is strong compared to and consistently outperforms the random frequency hopping; SecureMAC outperforms randomization-only by 129 percent when no attackers are present, and the performance advantage increases to over 148 percent in the presence of a malicious node, regardless of User 1's handshaking list strategy. Furthermore, SecureMAC compares well with the perfectly-orthogonal approach, which either does not defend against a reactive jammer (no-randomization) or requires very high overhead (to implement perfect orthogonality). The only case where SecureMAC performs notably worse than the perfectly orthogonal approach is when the handshaking list is compromised. Such lists are only used for a short time when the protocol is starting, and even then, SecureMAC's performance is about half-way between the current best practice of randomized frequency hopping and the very high-overhead no-randomization scheme; specifically, SecureMAC does 223 percent better than randomized frequency hopping, and no-randomization does 64 percent better than SecureMAC. However, by the steady-state with the optimal S, SecureMAC performs within 5 percent of the optimal performance of no-randomization, while imposing much less overhead and defending against reactive jammers.

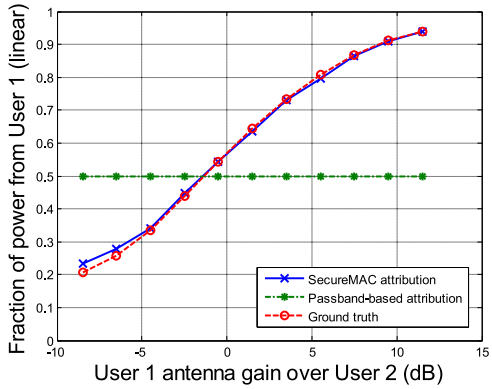


Fig. 7. Power attribution (overlapping channel case).

6.2.2 *The Effect of Handshaking List Decision*

To study the effect of the handshaking list decisions, we compare the capacity performance of SecureMAC coordination as the size of the handshaking list varies and as we include or exclude the attacker from the handshaking list. Fig. 6b plots the results. Because the collision-free bandwidth is increasing in the number of legitimate users in the handshaking list, we see improved performance with increasing handshaking list size. When the handshaking list is safe, we observe a 4 and 30 percent increase in collision-free bandwidth as we move from no coordination to coordination with one and two benign nodes, respectively. The capacity using the ideal handshaking list outperforms both the naïve frequency hopping (without handshaking) and the naïve scheme of sharing the control message with all registered users (including attackers) by 149 and 159 percent, respectively.

6.3 Physical-Layer Power Attribution

In this section, for simplicity of the presentation and since we study a physical-layer phenomenon, we have two transmitters transmitting at the same time and sharing the medium. Our implementation samples one hop in each round. We compare our power attribution scheme, the simple *passband-based* power attribution (which, to attribute power within a frequency band, filters each band and evenly divides the power between the users who reserved the band), and the *ground truth* (which assumes a priori knowledge about the exact transmission waveform that leaves the transmitter antenna and by using soft correlation with the signal at the receiver antenna). We study two scenarios: one in which the reserved channels do not overlap and another in which reserved channels completely overlap, only the latter of which is shown in Fig. 7. Any scenario is a linear combination of these two scenarios. Compared to the ground truth, our attribution scheme and passband observation both provide good performance and follow the ground truth attribution's behavior when the channels have no overlap; both schemes

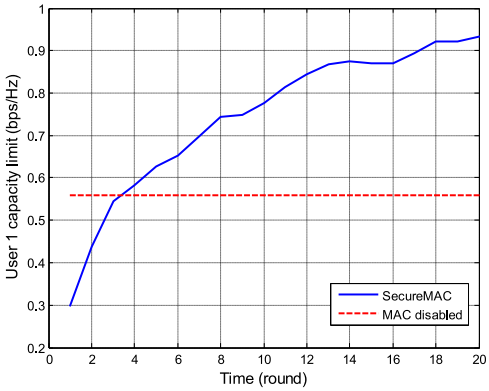


Fig. 8. Capacity over time.

perform well because the entire signal power in the passband originates from a single sender. However, when the two users choose completely overlapping channels (after randomization and coordination), the passband observation observes the same channel for each user and divides the power in half, resulting in equal power attributions for each user, regardless of the actual power. Our scheme uses the actual waveform transmitted and is much more accurate; as seen in Fig. 7, across all relative powers studied (in the x-axis), the maximum error in our power attribution is 0.56 dB while the maximum error in passband attribution is 3.86 dB. Also, because passband attribution gives a constant 50 percent attribution to each user, the error in relative power increases as the difference in transmission power level increases.

6.4 SecureMAC Convergence

We now combine the components evaluated above to study SecureMAC's performance over rounds (SecureMAC updates itself, including the channelization and the handshaking list, every round as discussed in Section 4.1).[4] In particular, we study the per-user capacity over rounds under two MAC choices: SecureMAC and the Nash equilibrium, the latter of which is the prior state-of-the-art and outperforms other suboptimal schemes (discussed and evaluated in Section 6.2). Under the Nash equilibrium, each node disables the MAC handshaking and accesses the entire bandwidth all of the time. The results are shown in Fig. 8. On the vertical axis is the User 1 capacity, averaged across the entire network bandwidth (including the bandwidth on which User 1 does not transmit), and on the horizontal axis is the number of elapsed rounds.

SecureMAC's expected performance increases because it quickly prevents attackers that do not use reserved spectrum from obtaining exclusive access to spectrum in future rounds (the attacher begins with 16.7 percent of the bandwidth, less than 25 percent because randomization generates some collisions, but by the tenth round, the attacker has less than 1 percent of the bandwidth) and because it converges to the ideal handshaking list (due to sampling random handshaking list every round, which overhead is omitted here but studied in [14], [30]). SecureMAC's performance is monotonically increasing, and, by round four, outperforms the Nash equilibrium strategy, which has constant performance in time. By round 20, SecureMAC reaches 95 percent of the steady-state performance of 0.982 bps/Hz, which outperforms the Nash equilibrium of wideband transmission by 76 percent.

4. The length of the round (including the update decision) is a systems parameter and can be in the order of tens of milliseconds or much longer, depending on the fading/mobility, as has been studied in [14], [30].

7 Conclusion

This paper studies the inherent vulnerabilities of MAC against attackers who have the credentials of legitimately registered users. Threats that have been left unresolved in such environments include false reservation injection, false feedback distribution, and intelligent jamming. Our scheme defends against such threats using a combination of four mechanisms: channelization that allocates bandwidth based on the usage in previously reserved spectrum, randomization to defend against reactive and outsider jamming, coordination to resolve collisions caused by randomization, and power attribution to make future MAC control decisions. Our evaluations show that, in practical scenarios, both centralized and distributed versions of our work are successful in nullifying the attackers' advantages of compromising the network while having the benign users retain the benefit of user collaboration in MAC. In particular, in our implementation environment, our work outperforms security-oblivious MAC with entity-fair channelization by 159 percent, FHSS (without coordination) and entity-fair channelization by 149 percent, and the Nash equilibrium of wideband access by 76 percent.

Acknowledgments

This study is partially supported by NSF under Contract No. NSF CNS-0953600 and by the Human-Centered Cyber-physical Systems Programme at the Advanced Digital Sciences Center from Singapore's Agency for Science, Technology and Research (A*STAR). This paper is an extended version of the work published at IEEE CNS, Florence, Italy, September, 2015 [1] and the technical report that supplements the conference publication [2]. The authors extended the previous work by studying a comprehensive threat model on MAC (including the new MAC-aware jamming which has a more devastating impact than an attacker jamming the non-reserved channels) and consequently upgrading the scheme, especially the coordination component. They also provide more in-depth insights and analyses than the conference publication. Section 2.2 outlines the contribution scope of this paper.

References

[1] S.-Y. Chang, Y.-C. Hu, and Z. Liu, "Securing wireless medium access control against insider denial-of-service attackers," in *Proc. IEEE Conf. Commun. Netw. Security*, 2015, , pp. 370–378.

[2] S.-Y. Chang and Y.-C. Hu, "Secure channel reservation for wireless networks," (2010). [Online]. Available: https://www.ideals.illinois.edu/bitstream/handle/2142/17098/2010–2509_Chang.pdf?sequence=2

[3] R. Etkin, A. Parekh, and D. Tse, "Spectrum sharing for unlicensed bands," *J. Selected Areas Commun.*, vol. 25, no. 3, pp. 517–528, 2007.

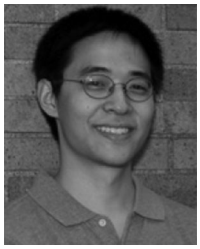
[4] J. Chiang and Y. Hu, "Dynamic jamming mitigation for wireless broadcast networks," in *Proc. 27th Conf. Comput. Commun.*, 2008, pp. 1211–1219.

[5] L. Li, S. Zhu, D. Torrieri, and S. Jajodia, "Self-healing wireless networks under insider jamming attacks," in *Proc. IEEE Conf. Commun. Netw. Security*, Oct. 2014, pp. 220–228.

[6] Z. Liu, H. Liu, W. Xu, and Y. Chen, "Exploiting jamming-caused neighbor changes for jammer localization," *IEEE Trans. Parallel Distrib. Syst.*, vol. 23, no. 3, pp. 547–555, Mar. 2012.

[7] R. Pickholtz, D. Schilling, and L. Milstein, "Theory of spread-spectrum communications–a tutorial," *IEEE Trans. Commun.*, vol. 30, no. 5, pp. 855–884, May 1982.
[8] M. Simon, J. Omura, R. Scholtz, and B. Levitt, *Spread Spectrum Communications Handbook*. New York, NY, USA: McGraw-Hill, Mar. 1994.
[9] L. Baird, W. Bahn, M. Collins, M. Carlisle, and S. Butler, "Keyless jam resistance," in *Proc. IEEE SMC Inf. Assurance Security Workshop*, Jun. 2007, pp. 143–150.
[10] M. Strasser, S. Capkun, C. Popper, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," *Proc. IEEE Symp. Security Privacy*, May 2008, pp. 64–78.
[11] W. Xu, W. Trappe, and Y. Zhang, "Channel surfing: Defending wireless sensor networks from interference," in *Proc. 6th Int. Conf. Inf. Process. Sensor Netw.*, 2007, pp. 499–508.
[12] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan, "Understanding and mitigating the impact of rf interference on 802.11 networks," in *Proc. Conf. Appl. Technol. Archit. Protocols Comput. Commun.*, 2007, pp. 385–396.
[13] J. H. Reed and M. Lichtman, *Letter Response to FirstNet Conceptual Network NOI (Docket No. 120928505250501; RIN 0660XC002)*, Nov. 2012.
[14] S.-Y. Chang, Y.-C. Hu, and N. Laurenti, "SimpleMAC: A jamming-resilient MAC-layer protocol for wireless channel coordination," in *Proc. 18th Annu. Int. Conf. Mobile Comput. Netw.*, 2012, pp. 77–88, https://www.ntia.doc.gov/files/ntia/va_tech_response.pdf
[15] S.-Y. Chang, Y.-C. Hu, J. Chiang, and S.-Y. Chang, "Redundancy offset narrow spectrum: Countermeasure for signal-cancellation based jamming," in *Proc. 11th ACM Int. Symp. Mobility Manag. Wireless Access*, 2013, pp. 51–58. [Online]. Available: http://doi.acm.org/10.1145/2508222.2508233
[16] J. Bellardo and S. Savage, "802.11 Denial-of-service attacks: Real vulnerabilities and practical solutions," in *Proc. 12th Conf. USENIX Security Symp.*, Aug. 2003, pp. 2–2.
[17] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A secure on-demand routing protocol for ad hoc networks," *Wireless Netw.*, vol. 11, no. 1, pp. 21–38, 2005.
[18] R. Negi and A. Rajeswaran, "DoS attacks on a reservation based MAC protocol," in *Proc. IEEE Int. Conf. Commun.*, 2005, pp. 3632–3636.
[19] V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial of service attacks at the MAC layer in wireless ad hoc metworks," in *Proc. MILCOM*, 2002, pp. 1118–1123.
[20] Y.-C. Tung, S. Han, D. Chen, and K. G. Shin, "Vulnerability and protection of channel state information in multiuser mimo networks," in *Proc. ACM SIGSAC Conf. Comput. and Commun. Security*, 2014, pp. 775–786. [Online]. Available: http://doi.acm.org/10.1145/2660267.2660272
[21] D. Liu and P. Ning, "Establishing pairwise keys in distributed sensor networks," in *Proc. 10th ACM Conf. Comput. Commun. Security*, 2003, pp. 52–61. [Online]. Available: http://doi.acm.org/10.1145/948109.948119
[22] W. Du, J. Deng, Y. S. Han, and P. K. Varshney, "A pairwise key pre-distribution scheme for wireless sensor networks," in *Proc. 10th ACM Conf. Comput. Commun. Security*, 2003, pp. 42–51. [Online]. Available: http://doi.acm.org/10.1145/948109.948118
[23] H. Chan, A. Perrig, and D. Song, "Random key predistribution schemes for sensor networks," in *Proc. Symp. Security Privacy*, May 2003, pp. 197–213.
[24] C. Shannon, "A mathematical theory of communication," *Bell Syst. Technical J.*, vol. 27, pp. 623–656, 1948.
[25] C. E. Shannon, "Communication in the presence of noise," in *Proc. Institute Radio Engineers*, 1949, pp. 10–21.
[26] J. Jensen, "Sur les fonctions convexes et les inégalités entre les valeurs moyennes," *Acta Mathematica*, vol. 30, no. 1, pp. 175–193, Dec. 1906. [Online]. Available: http://dx.doi.org/10.1007/BF02418571
[27] H. Rahul, N. Kushman, D. Katabi, C. Sodini, and F. Edalat, "Learning to share: Narrowband-Friendly wideband networks," in *Proc. ACM SIGCOMM Conf. Data Commun.*, Aug. 2008, pp. 147–158.
[28] P. Bahl, R. Chandra, T. Moscibroda, R. Murty, and M. Welsh, "White space networking with wi-fi like connectivity," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 39, no. 4, pp. 27–38, 2009.
[29] L. Yang, W. Hou, L. Cao, B. Y. Zhao, and H. Zheng, "Supporting demanding wireless applications with frequency-agile radios," in *Proc. 7th USENIX Conf. Networked Syst. Des. Implementation*, 2010, pp. 5–5.
[30] S. Y. Chang, Y. C. Hu, and N. Laurenti, "Simplemac: A simple wireless MAC-layer countermeasure to intelligent and insider jammers," *IEEE/ACM Trans. Netw.*, vol. 24, no. 2, pp. 1095–1108, Apr. 2016.
[31] G. V. Crosby, L. Hester, and N. Pissinou, "Location-aware, trust-based detection and isolation of compromised nodes in wireless sensor networks," *Int. J. Netw. Security*, vol. 12, no. 2, pp. 107–117, 2011.
[32] D. N. C. Tse, "Optimal power allocation over parallel gaussian broadcast channels," *Proc. IEEE Int. Symp. Inf. Theory*, 1997, Art. no. 27.
[33] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Trans. Program. Languages Syst.*, vol. 4, no. 3, pp. 382–401, 1982.
[34] B. Przydatek, D. Song, and A. Perrig, "SIA: Secure information aggregation in sensor networks," in *Proc. 1st Int. Conf. Embedded Networked Sensor Syst.*, 2003, pp. 255–265. [Online]. Available: http://doi.acm.org/10.1145/958491.958521
[35] R. C. Merkle, "A digital signature based on a conventional encryption function," in *Proc. Conf. Theory Appl. Cryptographic Techn. Advances Cryptology*, 1988, pp. 369–378. [Online]. Available: http://dl.acm.org/citation.cfm?id=646752.704751
[36] B. Sklar, "Rayleigh fading channels in mobile digital communication systems. i. characterization," *IEE Commun. Magazine*, vol. 35, no. 7, pp. 90–100, Jul. 1997. [Online]. Available: http://dx.doi.org/10.1109/35.601747
[37] D. Chizhik, J. Ling, P. W. Wolniansky, R. A. Valenzuela, N. Costa, and K. Huber, "Multiple-input-multiple-output measurements and modeling in manhattan," *IEEE J. Selected Areas Commun.*, vol. 21, no. 3, pp. 321–331, Apr. 2003.
[38] P. Murphy, A. Sabharwal, and B. Aazhang, "Design of WARP: A flexible wireless open-access research platform," in *Proc. 14th Eur. Signal Process. Conf.*, Sep. 2006, pp. 53–54.
[39] C. Tellambura and V. Bhargava, "Unified error analysis of DQPSK in fading channels," *Electron. Lett.*, vol. 30, no. 25, pp. 2110–2111, Dec. 1994.
[40] T. Tjhung, C. Loo, and N. Secord, "BER performance of DQPSK in slow Rician fading," *Electron. Lett.*, vol. 28, no. 18, pp. 1763 –1765, Aug. 1992.

Sang-Yoon Chang received the BS and PhD degrees from the Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign (UIUC), in 2007 and 2013, respectively. He is an assistant professor in the Computer Science Department, University of Colorado Colorado Springs (UCCS). His research focuses on designing secure systems in wireless networks and cyber-physical systems. He worked as a postdoctoral fellow at the Advanced Digital Sciences Center (ADSC) before joining UCCS. He is a member of the IEEE.



Yih-Chun Hu received the BS degree in computer science and pure mathematics from the University of Washington, Seattle, in 1997 and the PhD degree in computer science from Carnegie Mellon University, Pittsburgh, Pennsylvania, in 2003. He is an associate professor in the Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, Urbana. His research interests include security in networked systems, with particular interest in the areas of wireless, cyberphysical systems, and medical systems. After receiving the PhD degree, he worked as a postdoctoral researcher with the University of California, Berkeley. He is a member of the IEEE.