Secure Channel Reservation for Wireless Networks

By

Sang-Yoon Chang
Yih-Chun Hu

Technical Report
UILU-ENG-2010-2509

Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign

Urbana, Illinois
August 2010

Secure Channel Reservation for Wireless Networks

Sang-Yoon Chang Yih-Chun Hu
Department of Electrical and Computer Engineering
University of Illinois at Urbana-Champaign
Urbana, IL 61801
Email: {chang6,yihchun}@illinois.edu

Technical Report
August 9, 2010

***Abstract*—In reservation-based MAC protocols, adversaries that have compromised a node can perform an efficient denial-of-service attack by sending excessive reservation requests. Attackers, having thus prevented legitimate users from using some fraction of the bandwidth, can then use their power for jamming the legitimate transmissions instead of transmitting on the reserved channel. We propose a countermeasure which forces attackers to choose between the two attacks and restricts the optimal attacker behavior to physical-layer jamming, which in general is a weaker attack than over-reservation, when attackers are the minority of the network. Our work consists of a bandwidth allocation scheme that maximizes spectral efficiency and thus provides optimal performance and a channel coordination mechanism where users exchange and reach a consensus channel reservation in both centralized and distributed settings. By theoretical analysis and simulations, we demonstrate a substantial performance gain over the case where no countermeasure is utilized.**

I. Introduction

Wireless networks share a transmission medium. As demands for wireless communication increase, it is becoming important to utilize the communication medium more efficiently. To support transmissions from multiple users, the medium is divided into many communication channels. Typical channel access schemes are Time Division Multiple Access (TDMA), Frequency Division Multiple Access (FDMA), and Code Division Multiple Access (CDMA). These schemes interleave the use of transmission medium in time, frequency, and code, respectively. Since a data network is characterized by bursty arrivals, communication systems use a Medium Access Control (MAC) protocol to effectively coordinate the channel use of the network users; such protocols not only establish a link between a communicating transmitter-receiver pair but are also useful for helping transmitters to avoid each other to minimize interference. In order to avoid interference, these protocols are designed so that each channel is used by at most one user at any time. We say that a user *reserves* a channel prior to its data transmission when it notifies all the other users of its use of the channel.

We focus on a multi-channel environment, where the frequency spectrum is divided into multiple channels and many users compete for bandwidth, with power-limited attackers (however, our work can also be applied to single-channel TDMA systems with energy-limited attackers). We aim to design a spectrum channel allocation mechanism where we assign bandwidth to the network users to maximize the overall performance in the presence of malicious entities who perform Denial-of-Service (DoS) attacks. In particular, we are mainly concerned about *false reservation* attacks where an insider attacker (who compromised a legitimate network node) requests channel resource, i.e., bandwidth, with the intention of denying it to other users. This attack takes relatively small amount of attacker resources (to transmit control messages) and takes resources out of the network disproportionately to attacker effort. We consider jamming attack on legitimate transmissions as the attacker's best alternative attack; however, jamming is less efficient than false reservation since it requires more power consumption for attackers.

Our countermeasure for false reservation attack is two-fold: bandwidth allocation and channel coordination. First, we propose to allocate bandwidth to a user based on the power received from the user, and thus forcing attackers to emit power on the reserved channel to make future reservation requests. Then, we design a channel coordination scheme where all users agree on and distribute the bandwidth assignment. We begin by describing a centralized channel coordination scheme where there is a trusted authority, e.g., access point in WiFi, who coordinates the users' spectrum use. Afterwards, we devise a distributed scheme where the receivers reach a consensus to allocate bandwidth to users. Since it is hard to individually detect attackers and exclude attackers from contributing to the coordination process, a distributed scheme introduces another vulnerability which attackers take advantage of by sharing false information for coordination. We show that, with our countermeasure, the optimal DoS attackers' strategy becomes physical-layer jamming, as opposed to the more efficient false reservation attack, when attackers comprise the minority of the network. Our scheme not only successfully counters false reservation attack but also yields the optimal performance maximizing the aggregate rate of the network.

The rest of the paper is organized as follows. In Section II, we review previous work that deals with attacks on availability such as over-reservation for reservation-based MAC protocols and physical-layer jamming. Next, we establish the setup of our investigation in Section III. In Section IV, we present our threat model and assumptions about attackers. We introduce our secure channel reservation scheme in Section V and theoretically

analyze the performance and the attacker's optimal strategy in Section VI. Afterwards, we evaluate our scheme via simulations in Section VII and conclude our work in Section VIII.

II. Related Work

Our work considers a Denial-of-Service (DoS) attacker (capable not only of physical-layer jamming but also of sending bogus requests to reserve channel). Previous literature (e.g., [1]–[6]) describe an adversarial attacker who can send excessive reservation messages to prevent legitimate nodes from using the channel. Negi and Arjeswaran [4] consider an adversarial model similar to ours where attackers exploit MAC-layer vulnerabilities to be power efficient. Unlike our scheme, however, their scheme which revokes reservation if there is no data transmission assumes a detection scheme for malicious behaviors and places more restraints on attackers' power capabilities. Also, the effectiveness of the scheme is sensitive to parameter choices so that the reservation period and the detection period must be chosen wisely (thus requiring information about network topology).

Another form of DoS attack is channel jamming where adversaries inject noise to disrupt transmissions. Previous work [7]–[10] propose mechanisms for avoiding jamming, but, unlike our work, these approaches do not contemplate the possibility that jammers are compromised network participants and thus have access to some of the keys of the network nodes (in this paper, we assume that attackers only use the insider information for false reservation attack but not for channel jamming; we solve the intelligent jamming attack where attackers use insider information to facilitate more effective jamming on data transmissions in another orthogonal work that is currently under review). Also, in contrast to many prior jamming-aware MAC protocols, our work considers an attacker that is power-limited rather than energy-limited, and thus can jam all of the time.

III. System Model

We consider a scenario in which there are T non-idle transmitters, which compose 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. 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. All users operate on open spectrum and communicate directly, i.e., no communication relies on a third node to relay the message to the final destination node. For our model, we also assume that all users are within transmission range of each other, so that any transmission is heard by every user. Thus, when two or more users operate on the same channel, they collide. However, users who operate on different frequency channels, i.e., non-overlapping portion of spectrum, do not interfere with each other. All data communication is unicast, whereas control packets are broadcasted as described in Section III-A.

All users have equal priorities for transmission and their contributions to the overall network performance are weighted equally. Thus, attackers do not target a specific group of users and their optimal jammer strategy becomes wideband jamming across the entire frequency band as detailed in Section IV. Assuming this optimal jammer strategy and that every portion of the spectrum is expected to be subject to equal amount of fading, legitimate users do not need to hop across frequencies to avoid narrowband interference, i.e., frequency hopping spread spectrum, which technique is typically used to counter jammming on narrowband users.

In order to prevent forgery of reservation messages, we authenticate control packets containing channel reservation information by cryptographically signing them. This not only eliminates spoofing attacks or forgery of packets but also provides non-repudiation (and thus all users who reserve channels are held accountable for their actions). We assume an offline third party that not only a priori distributes public key-private key pairs to all nodes in the network but also provides direct validation of an entity, e.g., via reverse lookup, to prevent sybil attack (where one entity fakes multiple identities).

A. Secure Broadcast

In order to reserve a channel and notify all the other users of the channel use, we require jamming-resistant broadcast. The literature contains proposals for secure broadcast [11]–[13]. Baird et al. [11] suggest the BBC coding algorithm, in which they encode data using indelible marks (so that jammers can not erase a message, even though they can decode it). Strasser et al. [12] propose Uncoordinated Frequency Hopping, in which users send and listen on random frequency channels without pre-shared keys in order to establish a spontaneous link. Chiang and Hu [13] use binary key tree scheme to detect and isolate each jammed key by introducing asymmetry of knowledge between the sender and any set of receivers in the network (so that no other nodes in the network have as much information as the sender). We can use any such protocols to broadcast our control messages to the network.

B. Channelization

In this paper, we diverge from the conventional slotted channelization approach (where the spectrum is consisted of channels with fixed bandwidth and static location). In particular, by allocating channels with varying bandwidth and center frequency, we can more effectively match the needs of the users when assigning bandwidth and increase our system's spectral efficiency.

Many researchers, in a non-security framework, already adopted the channelization approach with flexible boundaries for frequency channels. Yuan et al. [14] proposed a distributed spectrum allocation scheme where they dynamically adjust the operating frequency carrier, the occupancy time, and communication bandwidth. Bahl et al. [15] also proposes such a scheme in a cognitive radio environment (where the users have an additional restriction of being non-intrusive to the licensed users). Split Wideband Interferer Friendly Technology (SWIFT) [16] is designed for Ultra Wideband communication (UWB) users and enables them to operate on non-contiguous frequency band while avoiding the portion that is occupied by narrowband users. While allowing varying bandwidth and

non-contiguous access, Jello [17] devises a defragmentation scheme where users distributively rearrange their frequency use so that unoccupied frequency blocks are merged into a large contiguous range (effectively decreasing the guardband overhead). Unlike SWIFT and Jello, our scheme does not require the hardware capability of non-contiguous frequency access (However, as described in Section IV, we assume that attackers have such capability to describe the optimal attacker strategy).

C. Performance Metric

We use Shannon capacity as our performance metric. Whenever user i transmits to user j, it does so on a frequency channel that varies with time according to the frequency hopping pattern, pre-shared between user i and user j. At any point in time, the user transmits on frequency channel with bandwidth W_i and at carrier frequency f_i. Assuming a flat fading Gaussian channel with Gaussian signals, the capacity of the link $i \rightarrow j$ is:

$$\mathcal{R}_i = \int_{f_i - W_i/2}^{f_i + W_i/2} \log_2 \left[1 + \Lambda_{i,j}(f)\right] df \tag{1}$$

where $\Lambda_{i,j}$ is the SINR:

$$\Lambda_{i,j} = \frac{\gamma_{i,j}\widetilde{P}_i(f)}{N_0 + \sum_{\ell \neq i, \ell \in \mathcal{M}^c}[\gamma_{\ell,j}\widetilde{P_\ell}(f)] + \sum_{k \in \mathcal{M}}[\gamma_{k,j}\widetilde{P_k}(f)]} \tag{2}$$

In Equation 2, $\gamma_{a,b}$ is the channel gain between transmitter a and receiver b, N_0 is the power spectral density of noise, $\mathcal{M}^c$ are the indices of legitimate users, $\mathcal{M}$ are the indices of jammers, $\widetilde{P_x}(f)$ is the user x's *transmitted* power spectral density (the subscript x determines whether it is signal, unintentional interference, or malicious jamming power spectral density).

Since the rate performance is determined at the communication receiver, we reconstruct our performance metric using received power (as opposed to the transmitted power). First, we place power constraints to all users including attackers:

$$\gamma_{i,j} \cdot \int \widetilde{P}_i(f)\, df \leq P_{i,j}, \ \forall i \in \mathcal{T}$$

where $P_{i,j}$ indicates the upper bound for the *received* power of the signal from user i to user j. $P_{i,j}$ is a function of both $\widetilde{P}_i$ and $\gamma_{i,j}$ (which depends on the distance between the two users). For our analysis, we assume uniform channel gains across all channels, i.e., $\gamma_{i,j} = \gamma_{a,b} = \gamma, \ \forall i, \forall j, \forall a, \forall b$, and thus, $P_{i,j} = P_i, \ \forall j \in \mathcal{T} \cap \{i\}^c$ (defining P_i to be the *received* power corresponding to the maximum transmitting power of user i). This assumption yields a lower bound on the expected capacity, because of Jensen's Inequality and the fact that $\mathcal{R}_i$ is a convex function of γ (see Section III-D). Also, as $\mathcal{R}_i$ is a monotonically increasing function of P_i, the transmitter will emit at full power and maximize the signal power P_i. From Equation 1, this yields the expected capacity expression:

$$E[\mathcal{R}_i] \geq W_i \log_2 \left[1 + \frac{P_i}{N_0 \cdot W_i + \sum_{\ell \neq i, \ell \in \mathcal{M}^c} I_\ell \cdot P_\ell + \sum_{k \in \mathcal{N}} J_k \cdot P_k}\right] \tag{3}$$

where P_i is the transmitter i's signal power, I_ℓ is the amount of user ℓ's power that interferes with the transmitter's signal normalized with respect to the power constraint, P_ℓ, J_k is the attacker k's jamming power normalized to the power constraint, P_k (and thus, $J_k \cdot P_k = \gamma_{k,i} \cdot \int_{f_c - W_i/2}^{f_c + W_i/2} \widetilde{P_k}(f)\, df, \ \forall i \in \mathcal{T} \cap \{i\}^c$). We use the expression on the right-hand side of Equation 3 (which is worse than the actual capacity) for the performance of user i.

Our goal is to maximize the performance of the overall network. We introduce a network utility function, U that is the aggregate rate of the users:

$$U = \sum_{i \in \mathcal{T}} \mathrm{E}[\mathcal{R}_i] = \sum_{i \in \mathcal{M}^c} \mathrm{E}[\mathcal{R}_i] \tag{4}$$

The second equality comes from the fact that the attackers make no contribution to the network; they, in fact, aim to do the contrary and degrade the network performance as described in Section IV.

D. Jensen's Inequality

From Equation 3, we observe that our performance metric is convex with respect to attacker's emitted power and concave with respect to legitimate transmitter's signal power. We use this property to analyze the attacker behavior in Section IV and Section VI-C and our scheme in Section V-A. Here, we provide an overview and a brief intuition of Jensen's inequality. Jensen's inequality states that, given a function (in our case, network utility U) which is convex with respect to a variable input (attacker's jamming power $J_k \cdot P_k$), $E[U(J_k \cdot P_k)] \geq U(E[J_k \cdot P_k])$. A corollary to Jensen's inequality, relying on the concavity of our performance metric to signal power, yields that using the expected signal power across all channels results in maximum performance and is used for analyzing legitimate transmitter's strategy. Therefore, users will choose to emit on the expected power level (attackers to minimize network performance and legitimate users to maximize it). In a multi-channel environment, this corresponds to water-filling where users emit on each channel so that all channels have equal SINR, as opposed to focusing their power on a subset of channels. In a single-channel TDMA environment, Jensen's inequality yields that, given that you equally weigh the performance for all time (that is, no single time slot is more important than any other), users' choosing a single transmission strategy rather than varying their behaviors maximizes their impact on the performance.

IV. Attack Model

Malicious attackers aim to degrade the network performance. Thus, we consider an attacker that intends to minimize the utility function subject to its power constraint:

$$\text{minimize } U \text{ subject to } \gamma \int_f \widetilde{J_k}(f)\, df \leq P_k, \ \forall k \in \mathcal{M} \tag{5}$$

and that there is collusion among jammers. Thus, attackers learn and share all information, including the secret key for control packets, with one another through a secure, covert communication path. Also, attackers do not care more about

a user than any other; that is, they do not target a specific subset of users.

We are mainly concerned with two types of DoS attacks: false reservation (wasting network resources) and jamming (injecting noise to decrease reliability of communication). False reservation is the more efficient attack of the two, since it allows an attacker to make a big impact while using less power. Without any countermeasures, each attacker can send a short reservation request message and reserve a channel for an extended period of time (which is supposedly to be used for data transmission), preventing legitimate users from using the resource. This requires only small amount of power to deliver control packets (since whether the channel is used during reserved period is not checked or regulated) and attackers can use the majority of their power to jam and disrupt the communication of legitimate users. Therefore, attackers will first falsely reserve the bandwidth as much as possible, and then jam the rest of the transmissions on the frequency band that is being used by other users (as described in Section III-B, attackers are capable of accessing non-contiguous frequency band).

For the frequency band occupied by legitimate users, attackers need to decide whether to choose narrowband jamming or wideband jamming. We observe that R_i is a decreasing and convex function of $\widetilde{J_k}(f)$. Hence, by Jensen's inequality, the minimum value of its statistical expectation $E[R_i]$, under the constraint in Equation 5, is attained by choosing $E[\widetilde{J_k}(f)]$ for every frequency f. Thus, to minimize capacity, jammers will conduct wideband jamming across the channels that are being used by all legitimate users as opposed to targetting and jamming a specific set of users. SWIFT [16], as described in Section III-B, can be used for attackers' wideband jamming to avoid wasting jammer power on the portion of frequency band that they have already falsely reserved. Since attackers perform wideband jamming across all channels, legitimate users do not benefit from spreading the spectrum, e.g., via frequency hopping.

For each transmission period, all users need to agree on the same bandwidth allocation to be coordinated. In scenario where a trusted entity does not exist, all users need an algorithm to reach consensus. This introduces another attack where attackers attempt to shift the consensus to their advantages. This secondary attack on distributed channel coordination is discussed in Section V-C.

V. Secure Channel Reservation Scheme

We devise a countermeasure for false reservation attack that not only maximizes the spectral efficiency providing optimal performance but also forces the optimal attacker strategy to become jamming. Our scheme consists of two parts. We first design a bandwidth allocation scheme where we assign bandwidth to a user according to the observation of the received power from the user. Then, we devise a distributed channel coordination scheme where users agree on bandwidth allocation. A centralized coordination scheme, which we also study, does not require exchanges among users, since a trusted entity can broadcast the bandwidth allocation information according to its own observation.

A. Bandwidth Allocation

We assign bandwidth according to the observed received power, that is, the bandwidth assigned to a user is proportional to the amount of the user's received power. In other words, receiver only respects a user's channel request proportionally to the amount of power that user emits on the data channel. Therefore, an attacker needs to emit power on the (data) channel in order to make a valid bandwidth reservation request for the following transmission. Since attackers can not simply reserve a channel without emitting any power on it, as they could without a countermeasure scheme, their limited power capabilities force them to choose between reserving channels and jamming legitimate transmissions.

When attackers transmit on their reserved data channel and consume bandwidth, we do not distinguish them from legitimate users. Even though attackers' transmissions on their reserved channels do not contribute to the network performance, e.g., no meaningful messages, it is difficult to determine and detect bogus data packets before application layer. Therefore, we do not aim to identify attackers in our work.

We use received signal power and not the transmitted power to determine the amount of bandwidth because transmitted power estimation requires the estimation of channel states and distances between any transmitter-receiver pair, which is a difficult task and makes the scheme more complicated. More importantly, the actual SINR which determines capacity is computed on the receiver side and thus depends directly on the received signal power. In Section III-C, we constructed a rate expression for our performance metric, namely, Equation 3, that is a lower bound of the actual capacity and uses the received power level (as opposed to the transmitted power and the channel gains).

Suppose our bandwidth allocation scheme using observations on the received power results in $\overrightarrow{W^*}$ where its i'th element, W_i^* corresponds to the bandwidth assigned to user i. Since we do not want to waste bandwidth, we allocate the entire frequency band, i.e., $\sum_{i\in\mathcal{T}} W_i^* = W$. Now, we claim that our bandwidth allocation scheme also yields optimal performance (that is, it maximizes the network utility function, Equation 4) and provide a sketch of proof.

Claim 1:

$$\overrightarrow{W^*} = \underset{\{W_1,\ldots,W_T\}}{\operatorname{argmax}} U \implies W_i^* = W \cdot \frac{P_i^*}{P}, \ \forall i \in \mathcal{T} \qquad (6)$$

where P_i^* is the received signal power on the channel reserved by user i and P is the total network power on the reserved channels, i.e., $P = \sum_{i\in\mathcal{T}} P_i^*$

Proof: For simplicity of proof, we assume equal channel gain (γ) for all channels, equal noise power spectral density (N_0) over all frequency, and fixed strategy with respect to time for attackers (which we later show to be the optimal strategy in Section VI-C). We first study the case where all users who reserve and transmit on their reserved channels contribute to

the network utility function (i.e., attackers use all their power to jamming and none on reserving channels, which is the optimal jammer reaction to our scheme, i.e., $P_i^* = 0,\ \forall i \in \mathcal{M}$, as detailed in Section VII). Using Equations 1, 2, 4, we observe that U (which is a summation of $E[\mathcal{R}_i]$) is a concave function with respect to $\widetilde{P}_i(f)$ from Equation 1. Jensen's Inequality yields $E[U(\widetilde{P}_i)] \leq U(E[\widetilde{P}_i])$. Therefore, in order to maximize the expected utility function, the network needs to have constant power spectral density across the entire frequency bandwidth W, i.e., $\widetilde{P}_i(f) = \frac{P}{W}, \forall f$. Thus, users who have greater power capability needs to have proportionally greater bandwidth, yielding $W_i^* = W \cdot \frac{P_i^*}{P}$.

Now, we consider the case where attackers transmit on data channels and reserve bandwidth, i.e., $\exists i \in \mathcal{M},\ P_i^* \neq 0$. In this case, attackers are indistinguishable from legitimate users and the proof is the same as the case where attackers use all their power for jamming instead of transmitting on the reserved data channel. ■

B. Channel Coordination

The bandwidth allocation scheme in Section V-A is performed individually by each user. Before data transmission, all users need to agree on the same bandwidth allocation, which process we call *channel coordination*. Otherwise, their transmissions will overlap and cause collisions resulting in poor performance. In a centralized scheme, the trusted entity can simply broadcast its bandwidth assignment to the users.

However, in scenario where such trusted entity does not exist or is offline, we need to share the observations and reach consensus. After gathering all users' observations (assuming reliable delivery, secure broadcast, discussed in Section III-A, is used to exchange the values of every users' observations), users choose the median of the received power observations. Since all users choose median from the same set of values, they reach consensus. (the Byzantine General's Problem solution using signed messages [18] also solves the problem). We also propose a commit-and-reveal protocol that conceals the observation values until all values are exchanged and gathered by every users, which motivation and procedure is detailed in Section V-C. In this paper, we study the performance of both the centralized and the distributed scheme for bandwidth coordination.

C. Attack on Distributed Channel Coordination

Unfortunately, using median to reach consensus for distributed channel coordination is vulnerable to an attack where attackers attempt to distort the consensus to their advantages. Since attackers know each other, they can distort the median value by reporting favorable values (i.e., high received power) for fellow attackers and low received power for others. Due to variable channel conditions and channel fading, the reported observations of received power vary between all users and the consensus median value will be shifted towards the value that the attackers report. Also, the use of median introduces an additional constraint that must be placed on the number of attackers: $M < \frac{T}{2}$ (this constraint is not necessary in a centralized scheme); otherwise, the attackers outnumber legitimate users and has direct control over the median and thus the bandwidth allocation outcome.

Attackers that know legitimate users' received power observations know exactly what the median is and how much they can distort it. We hide the legitimate users' reports of received power values by committing the reported values and then revealing them after all reports are gathered. Using one-way hash function, a commit-and-reveal protocol conceals the power observations until all reports are broadcasted and gathered. In our protocol, the committed value is the hash of the received power and the corresponding hash function while the revealed value is the received power; only after all the committed values are broadcasted will users reveal the received power.

An attacker detection scheme using thresholds can prevent attackers from reporting extremely big or small values. However, even with a scheme that hides the legitimate users' reports (that we described in the pervious paragraph), such threshold-based detection 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 being detected. Not only is a threshold-based detection scheme ineffective but it can also degrade the performance due to false positives; such a detection scheme will mostly detect unintentional outliers (who are legitimate) and may degrade the future performance by punishing benign users. Therefore, we do not consider such detection schemes.

Even though the attack of distorting coordination outcome is inherent in a distributed algorithm (where attackers contribute to the outcome) since it is difficult to determine which users are attackers and all reported observations are weighted equally when reaching consensus, a more sophisticated algorithm (as opposed to using the median) for distributed channel coordination scheme may be able to reduce attackers' advantage. We leave the design of such a protocol as future work.

VI. Theoretical Analysis

Our problem reduces to two-party scenario between *legitimate user network* (consisting of users who wish to maximize network utility) and *attacker network* (with malicious entities who want to degrade network performance). This is not only because we assume cooperative behaviors among benign users and collusion among attackers, but also because our bandwidth allocation depends only on the received power.

Our bandwidth allocation assigns bandwidth proportional to the power level and depends on the power capabilities of the legitimate/attacker network but not on the number of users/attackers. For our analysis, we connect the two variables by assuming that all users have the same power constraints. In other words, all individual users, including attackers, have the same power constraints, $\bar{P}$, 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 $\frac{T-M}{M}$, and we control the power capabilities of the two groups by varying the number of users (T) and attackers (M). Also, all legitimate users i have the same

rate performance since they have the same power capabilities and attackers care equally about all users. We denote the capacity of individual users with $\mathcal{R}_c$, i.e., $\mathcal{R}_i = \mathcal{R}_c,\ \forall i \in \mathcal{T}$, for *centralized* scheme, and with $\mathcal{R}_d$, i.e., $\mathcal{R}_i = \mathcal{R}_d,\ \forall i \in \mathcal{T}$, for *distributed* scheme. For simplicity of analysis, we introduce a variable α (normalized to the power emitted) that indicates the portion of attackers' power that they will transmit on data channels to perform false reservation attack and decrease bandwidth, and thus, $1-\alpha$ portion of power will be used for jamming other channels, i.e., $J_k = 1-\alpha,\ \forall k \in \mathcal{M}$.

A. Capacity for Centralized Scheme

A centralized scheme does not need an explicit channel coordination mechanism (i.e., exchanging control packets among all network users) since a trusted entity (which is known to be non-malicious) can assign bandwidth to users corresponding to its observations. In this section, we study the network performance of our centralized scheme. Since the attacker network uses $(\alpha \cdot \bar{P} \cdot M)$ amount of power for false reservation (and $[(1-\alpha)\cdot \bar{P}\cdot M]$ amount of power for jamming), the amount of bandwidth that a legitimate user is able to reserve is $W_i = \frac{W}{T-M+M\alpha}$ where the denominator $T-(1-\alpha)M$ indicates the number of valid reservations made. This reduces Equation 3 into the following:

$$\mathcal{R}_c = \frac{W}{T-M+M\alpha}\cdot \log_2\left[1+\frac{\text{SNR}}{\frac{T}{T-M+M\alpha}+\frac{M(1-\alpha)}{(T-M)}\text{SNR}}\right]$$

Since $U_c = (T-M)\cdot \mathcal{R}_c$,

$$U_c = \frac{(T-M)\cdot W}{T-M+M\alpha}\cdot \log_2\left[1+\frac{\text{SNR}}{\frac{T}{T-M+M\alpha}+\frac{M(1-\alpha)}{(T-M)}\text{SNR}}\right]$$

B. Capacity for Distributed Scheme

When we lack a trusted authority, we need to coordinate bandwidth allocation among users. We study the capacity performance under our channel coordination scheme using median detailed in Section V-B. We also consider the attack described in Section V-C where attackers report less received power if the signal originated from a legitimate user (thus providing some disadvantage to the legitimate user) and more received power if it originated from a colluding attacker (advantageous to the attacker). The bandwidth advantage that an attacker will have over a legitimate user is denoted with β; as discussed in Section V-C, attackers can reserve more bandwidth than legitimate users with the same amount of power, i.e., $\beta \geq 1$, since attackers know each other while legitimate users do not know who are malicious. Figure 1 plots β, the ratio ot the expected amount of bandwidth an attacker can reserve to that of a leigimtate user when they use the same amount of power, while assuming Rayleigh fading. The number of attackers, and thus the number of their reports, affect the distorted median of the received power which directly correlates to bandwidth. Under such attack, a legitimate user's bandwidth for its data

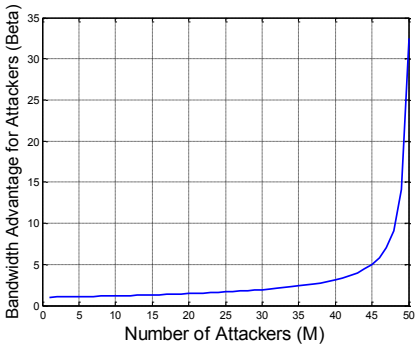


Fig. 1. Ratio between attacker's bandwidth and legitimate user's bandwidth under the attack on distributed channel coordination. $T = 100$.

communication becomes $T-(1-\alpha\beta)M$, yielding per-user performance ($\mathcal{R}_d$) and the network performance (U_d) of:

$$\mathcal{R}_d = \frac{W}{T-M+M\alpha\beta}\cdot \log_2\left[1+\frac{\text{SNR}}{\frac{T}{T-M+M\alpha\beta}+\frac{M(1-\alpha)}{(T-M)}\text{SNR}}\right]$$

$$U_d = \frac{(T-M)\cdot W}{T-M+M\alpha\beta}\cdot \log_2\left[1+\frac{\text{SNR}}{\frac{T}{T-M+M\alpha\beta}+\frac{M(1-\alpha)}{(T-M)}\text{SNR}}\right]$$

Compared to our centralized scheme, our distributed scheme yields more bandwidth to attackers (by the amount of β) when they reserve channels.

C. Attacker Reaction to Our Scheme

Our scheme, detailed in Section V, forces attackers to either reserve a channel (to waste bandwidth) or jam the other users' transmissions (to cause interference) by requiring power use on data channels to validate their future requests for bandwidth. In this section, we explore the optimal attacker strategy given our channel reservation scheme. Namely, we claim and show that attackers will use a deterministic strategy (rather than a mixed strategy where they vary α with respect to time) in order to minimize the network utility. To incorporate the dependence on time, we define $\mathcal{U}$ to be the aggregate network utility over time, i.e., $\mathcal{U} = \sum_t U_t$ where U_t is the network performance (expressed in Equation 4) at time t. We also define α_t to be the amount of power attackers use to reserve a channel rather than jamming at time t.

Claim 2: Given $\hat{\alpha}$ that yields minimum U, $\alpha_t = \hat{\alpha},\ \forall t$ yields the minimum network performance, $\mathcal{U}$.

Proof: We use the network utility function expression, Equation 7, for centralized scheme in this proof (the proof for distributed scheme follows the same procedure). From Equation 7, both $\frac{(T-M)\cdot W}{T-M+M\alpha}$ and $\log_2\left[1+\frac{\text{SNR}}{\frac{T}{T-M+M\alpha}+\frac{M(1-\alpha)}{(T-M)}\text{SNR}}\right]$ 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, $\alpha_t = E[\hat{\alpha}] = \hat{\alpha},\ \forall t$ yields the minimum network performance, $\mathcal{U}$. ■

VII. Simulation Evaluations

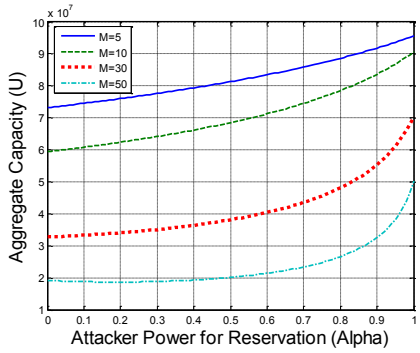
In this section, we simulate the bandwidth allocation and the channel coordination scheme that we discussed in Section V under Rayleigh fading. To show the performance of our scheme, we compare it to the case when there is no countermeasure and the conventional slotted channelization approach is used when dividing the bandwidth, (i.e., frequency band is divided equally into multiple channels that have fixed center frequency), which we define to be the *baseline performance* (we assume that all the slotted channels are utilized, e.g., the frequency band is divided into the same number as users). For baseline performance, as detailed in Section IV, attackers reserve channels without consuming power and use all their power to jam the rest of the legitimate transmissions (we assume that control packets are considerably smaller than data packets, so that the power required to transmit control packets are negligible compared to that for data packets). Thus, baseline performance itself varies with the power capability of the attacker network, M. In our simulations, in addition to the aggregate capacity performance of our scheme, we show the *capacity gain*, which is defined to be the aggregate capacity of our scheme divided by the aggregate capacity of the baseline performance. Thus, the number of legitimate users who contribute to the network performance $(T - M)$ becomes irrelevant for capacity gain and the metric corresponds to the gain of an individual user's performance over the case when there is no countermeasure.

As pointed out in Section VI, the power capabilities of the two parties, i.e., legitimate user network and attacker network, affects the network performance for our bandwidth allocation scheme. When analyzing our simulation plots, we observe that attacker network has a power capability of $\frac{M}{T}$ out of the entire power consumption of the network while legitimate user's is $\frac{T-M}{T}$. We first study the centralized scheme in Section VII-A and then the distributed scheme in Section VII-B. The parameters we use are: $T = 100$ transmitters, SNR (without interference) $= 15$dB, $W = 20$MHz and the number of malicious entities, M, are varied and specified in the plots.

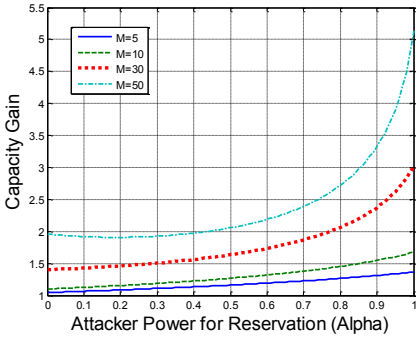
A. Centralized Scheme

Figure 2(a) plots the network rate performance (expressed in Equation 4) in bits per second with respect to the attacker strategy, specifically, α, which determines how much power attackers will use to make valid reservations for bandwidth. We observe that, when the power capability of the attacker network is smaller than that of the legitimate user network, attackers' wideband jamming with all their power, i.e., $\alpha = 0$, is more destructive to the network than consuming power to transmit on data channels and effectively reserving bandwidth. Thus, the optimal attacker strategy, which we denote with $\hat{\alpha}$, is to jam with all of its power, i.e., $\hat{\alpha} = 0$. Also, the network performance increases with the amount of power attackers use for transmitting on reserved channels, α.

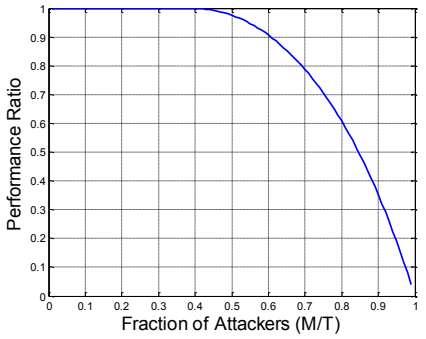
On the other hand, when attackers have comparable amount of or more power capabilities than the legitimate user network,



(a) Network performance



(b) Individual user's performance gain



(c) Performance difference between optimal attacker strategy ($\alpha = \hat{\alpha}$) and only jamming ($\alpha = 0$)

Fig. 2. Simulations for Centralized Scheme ($T = 100$)

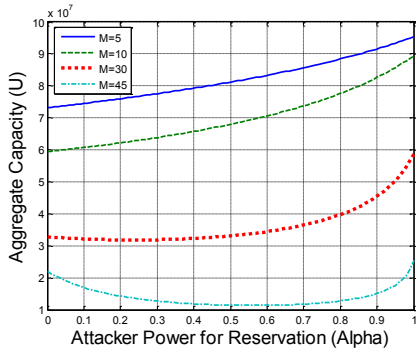
$\hat{\alpha} > 0$ (and using some power to reserve channels) becomes the optimal attacker strategy. For example, in Figure 2(a), when attackers have as much power capability as the legitimate users, i.e., $M = 50$ out of $T = 100$, $\hat{\alpha} = 0.2$ attackers will transmit on data channels with $\hat{\alpha} = 0.2$ of their power capabilities (for valid channel reservations and bandwidth consumptions) and use the rest of the power $1 - \hat{\alpha} = 0.8$ to jam the rest of the channels where legitimate users transmit on. The optimal attacker strategy diverges from $\alpha = 0$, since attackers' impact on the network grows logarithmically with respect to the attackers' jamming power while the impact of reserving channels grow linearly. Therefore, as attackers' power capabilities grow, their impact of reserving and consuming bandwidth outgrows that of jamming legitimate transmissions as attackers have more power to use.

In Figure 2(c), to compare the optimal attacker strategy and pure jamming, we plot the performance ratio between the case when optimal attacker strategy (that minimizes the network performance) is used, i.e., $\alpha = \hat{\alpha}$, and when attackers jam at full power, i.e., $\alpha = 0$, with respect to the fraction of attacker nodes in the network. We observe that, when malicious users are less in numbers than normal users and have less power to emit than legitimate users (and thus channel link has sufficiently good quality, i.e., sufficiently high SNR), either $\hat{\alpha} = 0$ or the performance between $\alpha = \hat{\alpha}$ and $\alpha = 0$ yields minimal difference. For example, from Figure 2(c), $\hat{\alpha} = 0$ until about 45% of the network nodes are compromised and there is only 2.5% difference in performance between $\alpha = 0$ and $\alpha = \hat{\alpha} = 0.2$ when $M = T - M = 50$. Therefore, in most practical scenarios (where attackers do not overwhelm the network by substantially outnumbering legitimate users and are capable of providing too low quality of channel links), $\alpha = 0$ is the optimal jammer strategy or yields negligible difference to the optimal strategy.

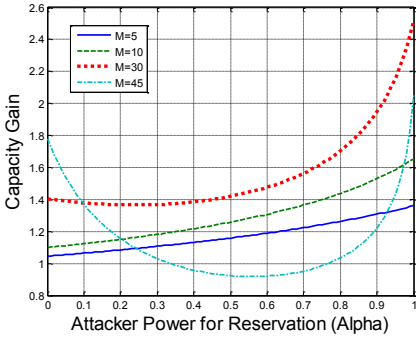
In Figure 2(b), we compare our scheme to the baseline performance by plotting capacity gain. Our scheme not only outperforms the baseline performance for all possible scenarios (capacity gain is always greater than one) but also provides more resistance to attacks as the attackers' capability grow (capacity gain increases as M increases); the network performance degrades much more quickly as the attackers have more power without our scheme.

B. Distributed Scheme

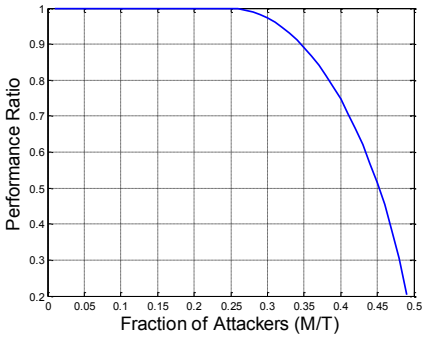
Our distributed scheme evaluation yields similar properties to those of our centralized scheme. However, from Figure 3(a) in which we show our distributed scheme's aggregate capacity performance in bits per second and from Figure 3(b) in which we plot the capacity gain, we observe that optimal attacker strategy diverges more from $\alpha = 0$ than the centralized scheme due to the attack on coordination process described in Section V-C; attackers have more motivations to reserve channels since they gain more bandwidth advantage (denoted as β and studied in our analysis in Section VI) when they reserve channels. For example, when $M = 30$, $\alpha = 0.24$ is the optimal strategy for distributed scheme (Figure 3) whereas $\alpha = 0$ is the



(a) Network performance



(b) Individual user's performance gain



(c) Performance difference between optimal attacker strategy ($\alpha = \hat{\alpha}$) and only jamming ($\alpha = 0$)

Fig. 3. Simulations for Distributed Scheme ($T = 100$)

optimal attacker behavior in the centralized scheme (Figure 2). Figure 3(c) compares the performance of the optimal attacker strategy ($\alpha = \hat{\alpha}$) and only jamming ($\alpha = 0$) by plotting the ratio of the corresponding network rate performance between the two strategies ($\frac{M}{T} \leq 0.5$ as detailed in V-C). From the plot, $\hat{\alpha} = 0$ if less than 27% of network users are compromised by attackers.

The additional vulnerability created by distributively coordinating bandwidth allocation information also causes a decrease in performance gain over that of baseline performance (as shown in Figure 3(b)) compared to the simulations for centralized scheme. Nevertheless, our distributed scheme always outperforms baseline performance.

Furthermore, in contrast to the centralized scheme, we observe that the capacity gain can decrease as the number of attackers (M) increases in the distributed scheme. For example, $M = 45$ yields smaller capacity gain than $M = 5$ in Figure 2(a) for some α. This phenomenon is due to the fact that the attack on distributed channel coordination results in the attacker bandwidth reservation advantage, which grows rapidly with respect to M, dominating the performance when there are many attackers. As shown in Figure 1, $M = 45$ results in attacker capable of reserving five times as much bandwidth than legitimate users if the same amount of power were used for reservation, i.e., $\beta = 5$. Therefore, as the number of attackers grows close to that of legitimate users, our distributed scheme becomes less effective (attackers have total control over the scheme if they have as many as or are greater in number than legitimate users as detailed in Section V-C). However, our distributed scheme works well when there are many more legitimate users than attackers.

VIII. Conclusion & Future Work

This paper studies a multi-channel environment with DoS adversaries who not only reserve bandwidth without the intention of using it but also jam legitimate transmissions. Our countermeasure consists of a bandwidth allocation scheme based on the observations of received power and a channel coordination protocol that enables all users to reach a consensus for bandwidth allocation. We study both centralized and distributed scenarios and prove that our bandwidth allocation scheme is designed for the optimal performance. Our evaluations yield that, in practical scenarios, our scheme either restricts optimal attacker behavior to jamming (as opposed to falsely reserving channels, which is generally the more efficient attack) or yields very close performance to when attackers only jam, and provides considerable gain over the case where there is no countermeasure in all situations.

We leave some problems for future work. Instead of using median to reach a consensus for channel coordination, we can devise a more sophisticated protocol that minimizes the impact of attacks on channel coordination. Also, all values that are reported and exchanged for received power observations contribute equally to the coordination outcome. Techniques from reputation systems can be used to establish more trust to users who have been more responsible about their past channel reservations. Furthermore, in a totally distributed setting, i.e., a trusted offline third party for key setup and identity validation is not available, we can devise a computation-based scheme (such as that proposed by Juels and Brainard [19]) to distribute keys a priori and to counter sybil attack. Finally, overhead analysis and evaluations using hardware experiments will add more practicality to the scheme.

References

[1] J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," in *USENIX Security Symposium*, August 2003.

[2] K. Bian and J. M. Park, in *Proceedings of the 2006 US-Korea Conference on Science, Technology and Entrepreneurship (UKC2006)*.

[3] Y. Hu, A. Perrig, and D. Johnson, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," *Wireless Networks*, vol. 11, no. 1, pp. 21–38, 2005.

[4] R. Negi and A. Rajeswaran, "Dos attacks on a reservation based mac protocol," in *IEEE ICC*, 2005.

[5] V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial of Service Attacks at the MAC Layer in Wireless Ad Hoc Networks," in *MILCOM*, vol. 2, 2002, pp. 1118–1123.

[6] D. J. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applcations to 802.11b and other networks," in *IEEE MILCOM*, 2006.

[7] G. Alnifie and R. Simon, "A multi-channel defense against jamming attacks in wireless sensor networks," in *Q2SWinet '07: Proceedings of the 3rd ACM workshop on QoS and security for wireless and mobile networks*. New York, NY, USA: ACM, 2007, pp. 95–104.

[8] W. Xu, W. Trappe, and Y. Zhang, "Channel surfing: defending wireless sensor networks from interference," in *IPSN '07: Proceedings of the 6th international conference on Information processing in sensor networks*. New York, NY, USA: ACM, 2007, pp. 499–508.

[9] R. Gummadi, D. Wetherall, B. Greenstein, and S. Seshan, "Understanding and mitigating the impact of rf interference on 802.11 networks," in *SIGCOMM '07: Proceedings of the 2007 conference on Applications, technologies, architectures, and protocols for computer communications*. New York, NY, USA: ACM, 2007, pp. 385–396.

[10] A. Wood, J. Stankovic, and G. Zhou, "DEEJAM: Defeating Energy-Efficient Jamming in IEEE 802.15. 4-based Wireless Networks," in *Sensor, Mesh and Ad Hoc Communications and Networks, 2007. SECON'07. 4th Annual IEEE Communications Society Conference on*, 2007, pp. 60–69.

[11] L. Baird, W. Bahn, M. Collins, M. Carlisle, and S. Butler, "Keyless jam resistance," in *Information Assurance and Security Workshop, 2007. IAW '07. IEEE SMC*, June 2007, pp. 143–150.

[12] M. Strasser, S. Capkun, C. Popper, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," *Security and Privacy, 2008. SP 2008. IEEE Symposium on*, pp. 64–78, May 2008.

[13] J. Chiang and Y. Hu, "Dynamic Jamming Mitigation for Wireless Broadcast Networks," in *INFOCOM 2008. The 27th Conference on Computer Communications. IEEE*, 2008, pp. 1211–1219.

[14] Y. Yuan, P. Bahl, and R. Chandra, "Knows: Kognitiv networking over white spaces," *IEEE DySpan*, pp. 416–427, 2007.

[15] P. Bahl, R. Chandra, T. Moscibroda, R. Murty, and M. Welsh, "White space networking with wi-fi like connectivity," *SIGCOMM Comput. Commun. Rev.*, vol. 39, no. 4, pp. 27–38, 2009.

[16] H. Rahul, N. Kushman, D. Katabi, C. Sodini, and F. Edalat, "Learning to Share: Narrowband-Friendly Wideband Networks," in *ACM SIGCOMM 2008*, Seattle, WA, August 2008.

[17] L. Yang, W. Hou, L. Cao, B. Y. Zhao, and H. Zheng, "Supporting Demanding Wireless Applications with Frequency-agile Radios," in *Proc. of NSDI*, 2010.

[18] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," *ACM Trans. Program. Lang. Syst.*, vol. 4, no. 3, pp. 382–401, 1982.

[19] A. Juels and J. Brainard, "Client puzzles: A cryptographic countermeasure against connection depletion attacks," in *Proceedings of the Networks and Distributed System Security Symposium*, 1999.