Noah: Keyed Noise Flooding for Wireless Confidentiality

Sang-Yoon Chang
Advanced Digital Sciences Center
Singapore 138632
sychg@adsc.com.sg

Jemin Lee
Singapore University of Technology and Design
Singapore 487372
jemin_lee@sutd.edu.sg

Yih-Chun Hu
University of Illinois at Urbana-Champaign
Urbana, IL 61801
yihchun@illinois.edu

ABSTRACT

Cryptographic protocols for confidentiality are oblivious to the unique challenges and advantages that wireless communication presents, mainly due to the open and public medium. We design a protocol at the wireless-specific physical and link layers and build a system that is information-theoretically secure against eavesdropping. Leveraging both friendly jamming and signal cancellation, Noah offers a novel keyed noise flooding protocol for wireless confidentiality. In contrast to prior work in wireless security, Noah protocol and its security properties are independent of the individual receiver's channel and do not require the channel link information (such as the channel condition and the antenna location) on the transmitter side. Thus, Noah supports multicast, taking advantage of the inherent broadcast nature of wireless medium, and defeats advanced channel-controlling eavesdroppers by making it impossible to physically separate the transmission and jamming. In this paper, we present the Noah protocol and provide fundamental insights in jamming and rate control for designing Noah.

1. INTRODUCTION

Wireless communication uses an open medium, which bypasses the physical medium establishment (typically in wires or optical fiber cables), makes the maintenance easier, and facilitates device mobility. Furthermore, it supports simultaneous communication in one-to-many communication (from single transmitter source to multiple receiver destinations), enabling more efficient delivery of messages than sharing a dedicated unicast link. However, the openness in wireless medium introduces security vulnerabilities. The medium access is more feasible than wired communication (where the attacker needs to physically tap the wire medium to breach the message integrity), as any wireless node equipped with radio hardware to capture the electromagnetic (EM) propagation is capable of receiving the transmitted message. Furthermore, the eavesdropping threat is entirely passive and leaves no trace evidence of breach.

A well-studied approach to enforce message integrity is to use cryptography. With pre-shared keys, the legitimate parties encrypt and decrypt their messages (which operations are performed at the application layer on the back-end of the devices). Attackers without the keys often resort to making series of guesses to retrieve the message out of the ciphertext, which consumes much more resources in computation and time. Thus, typical cryptographic approaches assume that the interested parties are computationally bounded. Despite the maturity of the field and the pervasive use in modern days, such cryptographic approaches are continuously facing challenges due to the development in computing.

We take a fundamentally different approach for wireless confidentiality and implement security at the antenna level by fuzzing the signal with jamming and disallowing the unauthorized eavesdroppers from receiving the signal. To contrast with cryptography, cryptanalysts operate to retrieve the plaintext given the ciphertext while our approach prevents the eavesdroppers/cryptanalysts from receiving the correct ciphertext. Thus, our scheme operates orthogonally to cryptographic mechanisms and offers integrity protection even when the eavesdroppers are computationally capable.

Our work offers a transmitter-receiver strategy for confidentiality. In specific, we incorporate *friendly jamming* at the transmitter (where artificial interference is used for beneficial reasons) and *signal cancellation* at the receiver (which cancels the signal by destructive interference at the analog domain or sample subtraction at the digital domain). Both techniques of friendly jamming and signal cancellation break the more conventional and well-studied models in their respective fields: in friendly jamming, the jamming source is not malicious, as is the case in prior jamming work that threatens communication availability; and signal cancellation breaks the additive signal and noise model by considering the destructive interference of EM signals. Thus, both fields are still young and the deployment limited. For instance, friendly jamming (or any intentional RF interference) is illegal in the US, and successful implementation of signal cancellation has begun to appear only recently, e.g., in full duplex work in a non-security context [1–3]. Due to the lack of implementation and deployment, we focus on making theoretical contributions and producing fundamental results that produce bases for designing our scheme.

In contrast to much prior work that studies friendly jamming and signal cancellation separately, we offer a coupled protocol leveraging both techniques. Furthermore, in contrast to other work that offers a sophisticated scheme tailormade to a particular receiver, we emphasize simplicity in the protocol design by making it receiver-independent and take advantage of the open medium in wireless by building a

Q2SWinet'15, November 02–06, 2015, Cancun, Mexico
 ISBN 978-1-4503-3757-1/15/11 ...$15.00.
DOI: http://dx.doi.org/10.1145/2815317.2815329.

multicast protocol to support multiple receivers. We further elaborate on the novelties of our work in Section 2.2.

We make an analogy to the narrative of Noah's Ark. Our protocol floods the channel space with noise signals (much like God in the story flooding the earth), and the selected authorized users (the living creatures selected to board the ark) nullify the noise by cancellation (the ark surviving the flood). Thus, we name our keyed multicast protocol *Noah*; the *Noah transmitter* floods the network (God) and the *Noah receivers* cancel the flooding effect (Noah's ark). A network of users, coexisting with other users, share a pre-shared information advantage in key and are authorized to access the communication; such network is called *Noah network*.

In this paper, we make four major contributions: first, we contrast with prior work in wireless confidentiality and present the Noah protocol; second, we construct a model that captures signal cancellation and friendly jamming (which advancements challenge the traditional jamming model); third, we show the optimality of our transmitter-receiver coupled strategy and the jamming design (although some results are the same as those from the traditional jamming model, this contribution is important as we base our analyses on a different model); fourth, we analyze the power and the rate control in a multicast scenario. The control over jamming (interference) power and the communication rate enables us to leverage the channel capacity and achieve information theoretic security. At the end, we present an optimal Noah design that supports multicast communication to the legitimate receivers while simultaneously defending against eavesdroppers who not only know the Noah transmitter-receiver's channel but are also capable of controlling their own channel gains or spaces. For clarity of presentation (e.g., to avoid unnecessary variables and introduce the necessary variables as they are used), we take a modular approach in developing our model and analyses; Section 6 builds on Section 5.

2. PRIOR WORK AND NOAH PRINCIPLES

In Section 2.1, we provide a literature review in signal cancellation and other nulling techniques (e.g., orthogonal channel space access in space or processing) and in advanced jamming (that goes beyond Gaussian jamming, which is the capacity-optimal choice when the strategy is chosen independent to that of the transmitter [4–7]). Then, in Section 2.2, we highlight the novelties of Noah and establish the principles that will dictate the design of Noah.

2.1 Related Work in Jamming and Nulling

Researchers traditionally studied jamming as a threat to wireless availability where jammers inject noise to degrade the channel quality [8–11]. However, some study a more sophisticated threat to cancel the victim's transmission by injecting highly synchronized signals to cause destructive interference at the receiver antenna [4, 12–16]. Although such attack is information-theoretically optimal (unless the attacker's power is significantly less than the victim's power) [4], the precise synchronization requirement in time and frequency makes the attack difficult without the legitimate transmitter's cooperation and limits its feasibility (e.g., static and slow-fading environment). As a result, the analysis of such cancellation-based jamming attacks has largely remained within theory [4, 12, 13] and in-computer simulations [14–16].

In contrast to the traditional malicious use, jamming has recently began garnering attention to facilitate wireless integrity. In *friendly jamming*, jamming is used for benign purposes [17–28] and challenges the more conventional principle that jammers are malicious (which principle is also reflected by the policy where many countries such as the US forbid the radio transmission of artificial interference by law). The benign nature of the jamming also makes the implementation of cancellation-based jamming more feasible than the case of using it for malicious purposes, since it motivates cooperation to facilitate synchronization between the jammer and the legitimate parties. To realize the nulling effect at the legitimate receiver, wireless researchers use diversity in multiple antennas (from the transmitter or the receiver) [17–19], in third-entity parties (outside of the transmitter and receiver) [20, 21], or in both multiple antennas and third-party helpers [22, 23]. Noah does neither; it is based on single antenna and does not require an external node to facilitate security. Since Noah does not rely on spatial diversity for its security properties, it is not vulnerable to threats that leverage the diversity information, which threat has shown to be effective against the aforementioned friendly jamming schemes [24]. In Section 2.2, we further discuss the advantages of our approach over the state-of-the-art that relies on multiple antennas/entities.

Qin et al. [25] offers an OFDM-based friendly jamming scheme that uses a *single* antenna chain. However, much like other precoding-based MIMO work, their jamming requires the channel information of the receiver, and the scheme is vulnerable when the eavesdropper is within the null space of the jammer's channel. In contrast, Noah uses after-channel postcoding at the receiver for jamming cancellation, which does not require the feedback of the receiver's channel information to the transmitter and makes the jamming and signal transmission inseparable to any eavesdropper.

There are other friendly jamming approaches performing omnidirectional jamming without nulling or signal cancellation [26, 29, 30], which approaches are simpler but experience more interference and noise at legitimate receivers than the aforementioned cancellation-based schemes and Noah. Such non-cancellation based friendly jamming has also been used for other applications such as physical-layer key sharing between a transmitter and a receiver [31, 32]; our contributions are orthogonal to these work since we build on pre-established keys and assume multicast with multiple receivers; building on a keyed network enables our scheme to achieve greater security and overcome a more advanced attacker who has greater control in channel and processing. Others have used such technology for access control [20, 27, 28] where unauthorized transmission is jammed, often disabling the channel altogether (even for legitimate users), but our aim is to establish message integrity of the transmissions and thus the focus is on passive eavesdropping threats.

2.2 Noah's Design Principles and Novelties

Much prior work in Section 2.1 offers modular design. By having the jamming cancellation implemented toward the end of the transmitter (as is done in prior work) or the beginning of the receiver (as is done in Noah), the jamming cancellation schemes support generality in physical layer designs; the security measure of jamming cancellation is independent to and can be built on any logical mappings of modulation and coding. Noah also shares this attribute.

However, Noah's jamming scheme differs from prior work in two aspects: it only requires single antenna and the cancellation is based on postcoding at the receiver (i.e., the cancellation is implemented after the channel and at the receiver).

These features offer many advantages in the system design over the prior work in literature, such as:

Hardware Noah's single-antenna design lessens the radio hardware requirements, as there is no need for multiple antennas or external entities for facilitation. This lightweight nature consequentially offers easier setup and wider adoption potentials.

Control communication Noah transmitter does not require the legitimate receiver's channel information (the medium access control information, the antenna's spatial location, the link state information in amplitude and phase, etc.).[1] Thus, it can bypass the prerequisite process of the transmitter learning the receiver's channel information. Otherwise, a typical method is via direct feedback, which requires an additional communication overhead from the receiver to the transmitter (Noah still requires a training process, so that the *receiver* learns about its own channel). Bypassing such step can especially reduce the overhead load in environments with greater fluctuation in channel (fading).

Security Noah provides additional security. In addition to reducing the feasible threat space by bypassing the channel feedback, Noah transmitter's single-antenna structure mixes the jamming and the desired message signal and makes them physically inseparable. Thus, threats on confidentiality that uses spatial diversity to separate the signals, e.g., [24], are infeasible.

Multicast Noah supports one-to-many communication. Prior schemes rely on transmitter precoding and thus all transmissions are tailor-made to the receiver's states. In contrast, Noah has the transmitter sending receiver-independent signals and the receiver implementing jamming cancellation. Thus, Noah can take advantage of the inherently broadcast nature of wireless and support one-to-many communication.

3. SYSTEM MODEL

We use radio communication for transferring digital information (e.g., computer bits) from one source transmitter to one or multiple receivers. The source data, denoted by x, has finite entropy, e.g., it has discrete distribution with finite alphabet size (possible values), and is processed at the physical layer to be converted into electromagnetic (EM) signal waveform, suitable for air propagation. Since RF communication relies on EM field propagation, multiple signals arriving at the antenna superpose with each other.

We consider an environment where there is a single source transmitter and multiple receivers and eavesdroppers, e.g., downlink. A *network* constructs a trusted domain where the members exclusively share a key k, and all members in the network are the intended recipients, or the *legitimate receivers*, of the transmitter's communication. When the network uses Noah protocol for confidentiality, we call it *Noah network*. Any receivers outside of the network does not have the key k and has no legitimate access to the communication. The *attackers* nevertheless are interested in x and eavesdrop to learn about x. The message data x and the pre-shared key k are independent. It is standard that security researchers build their schemes on a priori established information advantage within the trusted domain, e.g., the secrecy of k. For instance, a key can be established at bootstrapping through Diffie-Hellman exchange or physical-layer key sharing [31,32] and its randomness amplified by a pseudo-random generator. Furthermore, by Kerckhoff's principle, the attackers know the processing chain of the transmitter and the corresponding decoding strategy. Thus, the only disadvantage of the unauthorized attackers comes from the secrecy of k.

All receivers (legitimate receivers and attackers) are synchronized and use the same channel. Thus, the network integrity does not rely on random channel access schemes in time, frequency, and space (e.g., beamforming) although such schemes can operate orthogonally and provide an additional layer of defense. Furthermore, Noah does not rely on processing-based spreading techniques such as direct sequence spread spectrum (DSSS) due to its inherent spreading cost, typically incurred either in frequency, time or both [10, 15]. In other words, Noah is efficient in its channel resource use (as it does not spread the spectrum, which process reserves and uses more frequency bandwidth or time than the actual goodput delivery requires) and is broadcast friendly (as it does not limit its transmission to some spatial domain).

We assume correct training and channel estimation, so that the receiver learns about the channel from the source transmitter to itself. Noah performs and updates channel estimation for every coherence interval in time, frequency, and space to limit the fading effect, and the channel distribution remains intact during the transmission of x. For instance, OFDM is used for flat fading in frequency, and known preamble signals can be sent for every coherence time and space. Such assumptions are standard in signal cancellation, described in Section 2.1, or other interference alignment work, e.g., collaborative MIMO. Noah, by design, is easier to achieve such feats than prior work since it does not require the training at the transmitter, as described in Section 2.2.

We evaluate Noah based on the security gain over the unauthorized eavesdroppers and the rate performance in channel capacity. Since Noah injects interference by jamming, the interference power (relative to the transmission signal's power) plays a key role. To capture this, we use the widely-studied channel capacity C, as it is strongly correlated with the signal-to-interference-and-noise ratio (SINR). Even though our analyses holds for any performance metric (or any expression of the channel capacity) that is strictly increasing with SINR, we use the Shannon capacity for our multicast analysis. We later show the optimality in Gaussian jamming and motivate using the Shannon capacity in Section 5. For multicast, we observe the sum aggregate rate.

We introduce R to be the transmitter's information transmission rate. By definition, the channel capacity C provides a fundamental upper bound on the reliable information transmission rate R. For confidentiality, we control R in the Noah transmitter while assuming packet-based encoding and decoding, so that the receiver can either receive the packet correctly or incorrectly. For example, undersampling (such as focusing only on every other samples) and receiving those samples correctly does not yield any information about the packet message. The control in R enables us to ensure confidentiality, as we will see in Section 6.

The rate control assumes the worst-case receiver channel information even though it does not require the individual receiver's channel information. This lower bound effectively defines the Noah's *secure transmission range* and the scope of Noah's communication, as any receiver with worse channel

[1] As discussed in Section 3, the Noah's rate and power control makes use of the lower bound of the receivers' channel gains, which can be set as a system parameter. However, it does not require the information of the individual receivers.

than the bound cannot reliably communicate with the Noah transmitter. Because it determines the multicast transmission rate, this bound affects the performance of all the legitimate receivers, and thus we set it as a system parameter to define the Noah network, i.e., the Noah network receivers operate within the Noah's secure transmission range. The dynamic control of the Noah transmission range (such as the feedback-based power and rate control and the tradeoff analysis between the aggregate performance and the lowest receiver performance) and the use of network-layer protocols such as multi-hop relaying and flooding (e.g., to communicate to the receivers who move outside of the Noah transmission range) are beyond the scope of this paper.

4. NOAH SCHEME

Noah incorporates friendly jamming at the transmitter and signal cancellation at the receivers. As discussed in the design principles (Section 2.2), the transmission is independent of the receiver's channel (allowing multicast), and Noah is implemented toward the end of the processing chain (the transmitter adds jamming at the later processing end and the receiver cancels the jamming at the earlier front end).

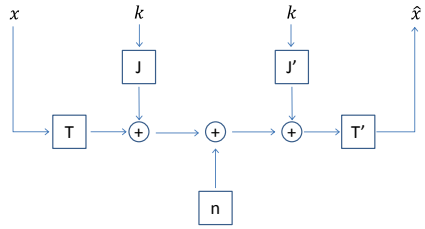
4.1 Transmitter's Jamming

Even though random jamming is typical in wireless security, Noah jamming design presents further challenges because the jamming signal needs to be securely shared within the Noah network prior to its transmission. In other words, without knowing k, the jamming signal should be random in distribution p and retain the information entropy of k (to make it difficult for the unauthorized eavesdroppers to guess k and the cancellation signal); and with k, jamming signal needs to be deterministic. To incorporate randomness, the jamming signal needs to be chosen out of a certain distribution, pre-agreed within the Noah network. Suppose this distribution is p. Noah does not rely on the secrecy of p. (Section 5 later shows that the Noah transmitter will flood Gaussian noise for jamming, i.e., $p \sim \mathcal{N}(0, P_J)$, where $\mathcal{N}$ is the Gaussian distribution and P_J is the jamming power.) To satisfy the jamming requirements, Noah users first use k to generate a normalized Uniform random variable; the mapping is deterministic and injective, and the randomness comes from the entropy of k. Then, the spacings between the variable values are adjusted by applying F^{-1} where F is the CDF of p, so that the likelihood of the values are equal.

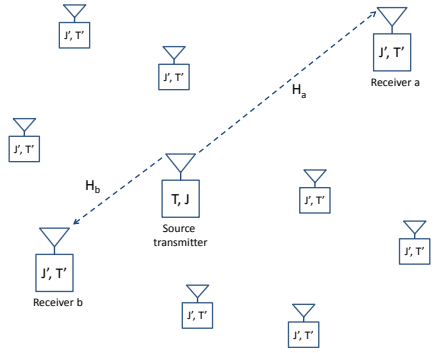
As the two-step mappings are public information by Kerckhoff's principle, the security of Noah (e.g., the randomness of Noah jamming) depends on the strength of k. For instance, if k has an entropy level that is as great as the size of the physical-layer samples produced by the Noah transmitter, then Noah can effectively realize a one-time pad. If we have further channel resources, e.g., greater power budget to overwhelm the message delivery, then we can devise a scheme to realize perfect security. Such development (e.g., placing assumptions on k and other resources for greater security strength) is beyond the scope of this paper.

4.2 Receiver's Cancellation

Noah receiver cancels the jamming signal at the sample level. For instance, with training and channel estimation (Section 3), proof-of-concept implementation work (for full duplex radios in a non-security context) has demonstrated signal cancellation in both analog and digital domains [1–3]. In particular, Bharadia et al. [3] offers a single-antenna



(a) Additive noise (n), the transmitter strategy (T and J), and the receiver's (J' and T') for Section 5



(b) Channel diversity for multiple receivers for Section 6 (the channel links are only drawn for Receiver a and Receiver b for sample representatives)

Figure 1: Theoretical models

based cancellation and achieves cancellation at the thermal noise level at about -174 dBm/Hz. To achieve such feat for multicast scenario, all receivers locally incorporate dynamic feedback-based differential control with known jamming signal as their references. For instance, to achieve tight phase synchronization, Noah receivers can use PLL with differential VCO. The synchronization error (e.g., PLL is not aggressive enough) and self-interference can be captured in our noise model in Section 5.1.

5. JAMMING AND NULLING ANALYSIS

In this section, we study the optimal transmitter-receiver strategy for the jamming and the cancellation design. While we define *jamming* to mean any artificial RF interference, we show here that the optimal jamming is to imitate the channel *noise* in Gaussian. Even though Gaussian jamming to inject noise-like signals is standard in wireless security [5, 6, 18, 33], our model significantly diverges from the traditional wireless jamming model and needs careful investigation for the jamming design. The two key differences between our model and the traditional model are that 1) jamming is to help the cause of the legitimate network, and 2) the source signal and the jamming signal originate from the same transmitter. Due to these key differences, we carefully study the transmitter-receiver design in this section even though the end results of our theoretical analysis concur with the prior literature using the more traditional jamming models.

To further motivate our analysis, we compare and contrast our model with a related model in correlated jamming [4, 7, 12]. In correlated jamming model, the malicious jammer has the a priori access to the data x and the capability to utilize x for generating J. Even though the optimal jam-

ming strategy is to perform correlated jamming that cancels the source transmission signal at the receiver's antenna, the study of correlated jamming has largely been left as a theoretical exercise [4, 12, 13, 15] and deemed with limited practical applications [14] because it is difficult for a remote attacker to achieve the access to x in advance due to causality (both signal generation and travel takes time). In contrast, in our model, a Noah transmitter is capable of using x to generate J since the transmitter self-jams and both signal generations for message delivery and jamming happen within the same entity. Therefore, Noah may choose to utilize x to generate J. Nevertheless, in this section, we prove the ineffectiveness of using x for jamming control.

5.1 Theoretical Model

We consider signal superposition and adopt additive interference and noise model. As depicted in Figure 1(a), the transmitter takes scalar zero-mean source symbol x, processes it with a mapping of T (which focuses solely on effectively delivering x, e.g., $T = T(x)$), and adds jamming signal of J. The transmission experiences channel noise n in Gaussian distribution with zero mean (e.g., because of numerous noise sources). After the propagation through the wireless channel, the receiver adds J' and then maps it via function T' to an estimate of x, $\hat{x}$ (for instance, it is common to have $T' = T^{-1}$, so that $\hat{x} = x$ if $n = 0$). The mappings of T, J, J', and T' are for control (i.e., the transmitter-receiver pair is free to choose them), given that they are deterministic and assume non-zero processing delay for causality. In addition, T, J, J', and T' are lossless (in information), and the entropy remains the same from the function mapping, e.g., $\mathcal{H}(J(\alpha)) = \mathcal{H}(\alpha)$ and $\mathcal{H}(J(\alpha, \beta)) = \mathcal{H}(\alpha, \beta) = \mathcal{H}(\alpha) + \mathcal{H}(\beta) - \mathcal{I}(\alpha; \beta)$, where $\mathcal{H}(\cdot)$ is the entropy of the variable within the parenthesis. The estimate, $\hat{x}$ (or x) is not known until the sequential mappings are complete. The message x is random and uniformly distributed (which maximizes the information content), and thus $\mathcal{H}(x) = \log_2 \mathcal{A}$ bits, where $\mathcal{A}$ is the alphabet size of x. By Kerckhoff's principle, T, J, J', and T' are known, and Noah relies solely on the pre-shared key k for security, i.e., k is only shared within the Noah network. The key k is independent to both x and n, as discussed in Section 3; in fact, x, k, and n are mutually independent.

5.2 Main Results

In this section, we show that the transmitter's jamming imitates wireless noise in Gaussian and the receiver will cancel the jamming. This coupled transmitter-receiver strategy simultaneously achieves the optimal performance for Noah users, which means the strategy performs as well as or better than any other transmitter-receiver strategy. Our result holds regardless of the eavesdropper's strategy (for example, the eavesdropper can know and control the transmitter-eavesdropper channel [24]). We first establish the optimality of the receiver's jamming cancellation in Lemma 1. Then, in Lemma 2, we show that the transmitter does not utilize x (for example, to perform correlated jamming [4, 14, 15]) while assuming cancellation for the receiver strategy. Lastly, in Lemma 3, we reduce our problem into the standard jamming problem of degrading the channel quality and establish that the optimal transmitter strategy is Gaussian jamming and to imitate channel noise. The lemmas yield Theorem 1.

LEMMA 1. *At the Noah receiver, $J' = -J$ is the optimal strategy in SINR, and it is feasible if J is a function of k and k only, i.e., $J = J(k)$ and $\mathcal{H}(J|k) = 0$.*

PROOF. If $J = J(k)$ and $\mathcal{H}(J|k) = 0$, the receiver receives $T(x) + J(k) + n$ and adds J', which results in $T(x) + J(k) + n + J'(k)$. Since $J(k) + J'(k)$ is interference and its power is non-negative, the physical SINR to decode x is maximized when the interference $J + J'$ is minimized in amplitude. Since the Noah receiver knows both the transmitter's strategy of J (public information) and k (privately shared information within the Noah network), $J' = -J(k)$ is feasible, which yields $J + J' = 0$ and achieves the maximum SINR. □

Lemma 1 is valid if the corresponding source transmitter (Noah transmitter) chooses the jamming strategy J such that J is only controlled by k. However, since the transmitter self-jams (in fact, T and J originate from not only the same processer but also the same antenna), it can choose to use both x and k to control J, i.e., $J = J(k, x)$ and $\mathcal{H}(J) = \mathcal{H}(k) + \mathcal{H}(x)$ (since k and x are independent). Using both x and k yields greater entropy in J, i.e., $\mathcal{H}(J(k, x)) - \mathcal{H}(J(k)) = \mathcal{H}(x) > 0$. Nevertheless, we show the ineffectiveness of using x to control J for wireless confidentiality and conclude that $J = J(k)$ and $\mathcal{I}(J; x) = 0$ in Lemma 2.[2] We first define *security gain* which will be used in the proof.

Definition Given the received signal $T + J + n$, the *security gain* of the legitimate users over the unauthorized users is the increase in information obtained from having the authorization (knowing k) over not having the authorization (not knowing k) in the estimation of x, i.e., $\mathcal{H}(x|T + j + n) - \mathcal{H}(x|T + j + n, k)$.

LEMMA 2. *At the transmitter, generating J by utilizing x (i.e., $\mathcal{I}(J; x) > 0$) offers no security gain over using k only.*

PROOF. We use contradiction to prove that utilizing x offers no additional security gain and that the randomness of J is limited by $\mathcal{H}(k)$. Let's suppose the receiver strategy of $J' = -J$ (Lemma 1) and the transmitter strategy of $J = J(k, x)$ offers additional security gain over the case of using $J = J(k)$. By causality, the receiver does not know x when its antenna(s) receives the signal. However, a receiver could attempt to estimate x via some $\tilde{x}$; $\tilde{x}$ is independent of k since x and k are independent, and $\tilde{x} \neq \hat{x}$ because of causality and processing delay. Suppose a Noah receiver can use $\tilde{x}$ to realize $J' = -J$, i.e., it can find $\tilde{x}$ such that $J' = -J(k, \tilde{x})$ to cancel the jamming signal; otherwise, $J' \neq -J$. Then, since $\tilde{x}$ does not rely on the secrecy of k, the attacker without k can also find such $\tilde{x}$, and therefore any security gain from using $\tilde{x}$ to generate J and J' is null. Thus, by contradiction, the network's security gain over an eavesdropper does not increase by using x to control J. □

Now, we design Noah's jamming to disrupt eavesdropping.

LEMMA 3. *At the transmitter, J in Gaussian is optimal in C, given $J' = -J$ (Lemma 1) and $J = J(k)$ (Lemma 2).*

PROOF. From Lemma 1, the receivers within the network cancels J, making its design moot to them. However, its design affects the security against an unauthorized eavesdropper (who does not have the key k and thus experiences random J). Our problem reduces into the legitimate transmitter worsening its channel link to the eavesdropper. With Guassian n, Lemma 2 (independence between J and x and thus no correlated jamming), and general T, it is known that Guassian J minimizes the channel capacity [5,6] and the minimum squared error (MSE) [4, 7]. □

[2] In contrast, if the jamming source is malicious, $J = J(k, x)$ (correlated jamming) is the optimal strategy [4, 12, 13, 15].

THEOREM 1. *The coupled transmitter-receiver strategy of Gaussian jamming in J and the exact jamming cancellation of $J' = -J$ is optimal in legitimate user's SINR and offers positive security gain against an unauthorized eavesdropper.*

PROOF. The three lemmas combined proves Theorem 1. □

We provide a transmitter-receiver coupled strategy that provides security gain for the authorized network and the optimality in channel capacity (and MSE). It also adheres to our design principles in Section 2.2 and supports a modular design that provides generality in implementation by having T decoupled with J and k. (If we were to control T for implementing security, as opposed to having T given as in here, a joint optimization design using T and J is possible.)

6. MULTICAST ANALYSIS

6.1 Theoretical Model

In this section, we study multicast (where one source transmitter delivers messages to multiple receivers). While we largely build on the model in Section 5.1 (in which we focused on wireless unicast), we now incorporate spatial diversity with variable channels across the receivers to study a multi-user environment. The set of the legitimate receivers in the Noah network is denoted with $\mathcal{N}$, i.e., if $i \in \mathcal{N}$, then the receiver i is an intended recipient of the source transmission. In contrast, any user outside of the network, i.e., $i \notin \mathcal{N}$, is unauthorized to receive the transmission. As depicted in Figure 1(b), any receiver i will experience a channel effect of H_i, which is a channel gain in *power* where $H_i < 1$, $\forall i$ [3]. As established in Section 5, the source user transmits two independent signals in T and J, and its total transmitter power is $P_T + P_J$, where P_T is the power used for the transmission of the message $T(x)$ and P_J is that for the security-enforcing jamming. In turn, the receiver i receives a power of $H_i(P_T+P_J)$. The total power budget of the transmitter is P, i.e., $P_T + P_J \leq P$, and the noise power is σ_n^2. The processed version of x, T and the jamming signal, J are independent, as established in Section 5.2. As discussed in Section 3, the source transmitter transmits its message x at a rate of R, and by definition of C_i, if $R \leq C_i$, then there exists a transmitter-receiver strategy that enables reliable communication for the transmitter and the receiver i, and if $R > C_i$, reliable communication is impossible. To capture this, we introduce receiver i's communication rate (R_i') as:

$$R_i' = \begin{cases} R, & \text{if } R \leq C_i \\ 0, & \text{if } R > C_i \end{cases}$$

According to Theorem 1 in Section 5, Noah receivers cancel jamming whereas the other unauthorized receivers experience random jamming, and the artificial jamming is Gaussian due to its optimality. As discussed in Section 4.2, Noah receiver suppresses self-interference from fading and achieves perfect cancellation incurring the lower bound in cancellation noise, which is the receiver noise floor of σ_n^2; Bharadia et al. [3] also demonstrates signal cancellation that achieves the thermal noise level on a radio-based implementation. Thus, the SINR and the capacity in bps per Hz, respectively, are:

$$\text{SINR}_i = \begin{cases} \frac{H_i P_T}{2\sigma_n^2}, & \text{if } i \in \mathcal{N} \\ \frac{H_i P_T}{H_i P_J + \sigma_n^2}, & \text{if } i \notin \mathcal{N} \end{cases} \quad (1)$$

$$C_i = \log(1 + \text{SINR}_i), \ \ \forall i \quad (2)$$

Noah receivers ($i \in \mathcal{N}$) effectively nullify jamming and their performances are independent of P_J.

Our optimization problem is to maximize the aggregate communication rate performance by controlling P_T and P_J:

$$\begin{aligned} \underset{P_T, P_J}{\text{maximize}} \quad & \sum_{i \in \mathcal{N}} R_i' \\ \text{subject to} \quad & P_T + P_J \leq P \\ & R > C_e, \ \ \exists e \notin \mathcal{N}, C_e \geq C_j, \forall j \notin \mathcal{N} \\ & R \leq C_i, \ \ \forall i \in \mathcal{N} \end{aligned} \quad (3)$$

The first constraint is the transmitter's power budget; the second constraint is to enforce security and prevent any unauthorized eavesdropper from correctly decoding the message (by definition, e is the most capable receiver outside of the Noah network: $e = \text{argmax}_{i \notin \mathcal{N}} C_i$); the third constraint is to accommodate all authorized receivers in the Noah network (i.e., all Noah network receivers must have channels which capacity exceeds the transmission rate R). The last two constraints ensure that there is a strictly positive *secrecy rate*, which is the difference between the Noah user's channel capacity and the eavesdropper's [18, 22, 26, 30].

Our work is secure against *any* eavesdropper that coexists with the Noah transmitter; if there is one eavesdropper that can breach the integrity of the message, then the protocol is not secure. Thus, we consider attackers that have control over their channels and the worst-case scenario for the Noah network. In specific, we assume the best-case channel condition H for the unauthorized eavesdroppers who coexist with the Noah network on the same channel, as discussed in Section 3. This strong threat model is in contrast to some prior work in wireless confidentiality that places limitations on the attackers' channel conditions and assume that the attackers' channel conditions are known to the legitimate party. For instance, precoding approaches to separate the channel space between legitimate receivers and the eavesdroppers are popular [17, 18, 21, 22, 25], which approaches are ineffective if the eavesdroppers coexist with the receivers in the channel space (for instance, for spatial beamforming-based schemes, the eavesdroppers can not be in between the transmitter and the legitimate receiver). Our analysis is not only robust to eavesdroppers having full control over its H and are freely moving around but it is also valid for threat models that can afford diversity for better performance such as eavesdroppers having multiple antennas and multiple colluding attackers (with perfect coordination), as seen in Section 6.3.

6.2 Main Results

In this section, we solve the optimization problem in (3) and show that Noah is capable of secure communication for *all* network receivers in the presence of unauthorized eavesdroppers that have control over their channel links. We specifically focus on the worst-case Noah receiver and the best-case attacker. Without loss of generality, $l = \text{argmin}_{i \in \mathcal{N}} C_i$ (l is the worst-case *legitimate* Noah receiver) and

[3]The electromagnetic wave propagation through air experiences power loss via diffraction, reflection, absorption, etc.; even in open free space, there is loss from the natural expansion of the RF wave front. Even though multipath propagation makes $H \geq 1$ possible, such channel phenomenon is rare, as the amplification from multipath is quickly outweighed by the aforementioned attenuation factors. Nevertheless, Section 6.3 provides analysis for such cases of $H \geq 1$.

$e = \text{argmax}_{i \notin \mathcal{N}} C_i$ (e is the most capable unauthorized *eavesdropper*). For example, eavesdroppers know the location of the source transmitter antenna and can move close to it.

THEOREM 2. *For given H_l and σ_n^2, and in the presence of eavesdroppers that can control H_e, the following provides a strategy in P_J, P_T, P, and R that solves the problem in* (3)*:*

$$P_J = (\tfrac{2}{H_l} - 1)\sigma_n^2,$$
$$P > P_J,$$
$$P_T = P - P_J,$$
$$R = \log\left(1 + H_l \frac{P + \sigma_n^2 - \frac{2\sigma_n^2}{H_l}}{2\sigma_n^2}\right) - \epsilon, \quad \exists \epsilon > 0 \tag{4}$$

PROOF. We focus on the secrecy capacity between l and e, $C_l - C_e$. Because $z > C_e \Leftrightarrow z > C_j$, $\forall j \notin \mathcal{N}$ by definition of e, and C is injective and monotonic with P_T, P_J, and H for Noah users (Equation 2), focusing on the two users l and e is equivalent to solving the many-user conditions in (3).

$C_l - C_e > 0 \;\Leftrightarrow\; C_l > C_e$ yields feasibility:

$$\begin{aligned} C_l > C_e &\iff \text{SINR}_n > \text{SINR}_e \\ &\iff \frac{H_l P_T}{2\sigma_n^2} > \frac{H_e P_T}{H_e P_J + \sigma_n^2} \\ &\iff \frac{P_J}{\sigma_n^2} > \frac{2}{H_l} - \frac{1}{H_e} \end{aligned} \tag{5}$$

The first equivalence comes from C increasing with SINR; the second equivalence comes from Equation 1; and the third equivalence is obtained by linear algebra. Since the attacker has control over its channel, it can approach very closely to the source transmitter and maximize H_e, i.e., $H_e \to 1$ (and $\frac{1}{H_e} \to 1$). This choice of $H_e \to 1$ is the attacker's best strategy, as C_e is increasing with H_e (Equation 2 has a positive derivative for all possible values of H_i, $\forall i \notin \mathcal{N}$). From Equation 5, we obtain the lower bound of JNR$=\frac{P_J}{\sigma_n^2}$ that provides strictly positive secrecy capacity and is independent of H_e:

$$\frac{P_J}{\sigma_n^2} \geq \frac{2}{H_l} - 1 \;\Rightarrow\; C_l > C_e \tag{6}$$

In the optimization in (3), C_l is the upper bound of R. Since $\forall i \in \mathcal{N}$, C_i increases with P_T (as seen in Equation 2), we fully utilize the transmission power budget, i.e., $P_T = P - P_J$, and minimize P_J from Equation 6 by choosing $P_J = (\frac{2}{H_l} - 1)\sigma_n^2$. Thus, $P_T = P - (\frac{2}{H_l} - 1)\sigma_n^2 = P + \sigma_n^2 - \frac{2\sigma_n^2}{H_l}$. Then, from Equation 2:

$$C_e = \log\left[1 + \frac{H_e(P + \sigma_n^2 - \frac{2\sigma_n^2}{H_l})}{(\frac{2H_e}{H_l} - H_e + 1)\sigma_n^2}\right] \tag{7}$$

Since C_e is increasing with H_e, the upper bound of C_e can be obtained by $H_e \to 1$:

$$C_e < \lim_{H_e \to 1} C_e = \log\left[1 + H_l \frac{(P + \sigma_n^2 - \frac{2\sigma_n^2}{H_l})}{2\sigma_n^2}\right] \tag{8}$$

The right-hand side of Equation 8 corresponds to the capacity of worst-case Noah, i.e., $\lim_{H_e \to 1} C_e = C_l$. Thus, $C_e < C_l$ and there exists $R = \log\left(1 + H_l \frac{P + \sigma_n^2 - \frac{2\sigma_n^2}{H_l}}{2\sigma_n^2}\right) - \epsilon, \;\; \exists \epsilon > 0$ that satisfies $C_e < R < C_l$. Such R, with $P_J = (\frac{2}{H_l} - 1)\sigma_n^2$ and $P_T = P + \sigma_n^2 - \frac{2\sigma_n^2}{H_l}$, solves the problem in (3). □

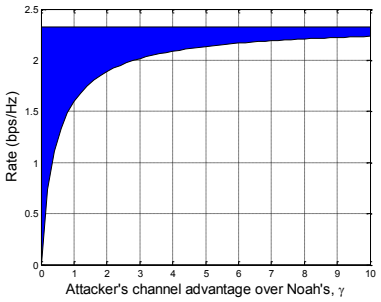


Figure 2: Rate feasible region when H_e is not known

Theorem 2 provides a solution for the Noah transmitter's power and rate control that ensures both confidentiality against eavesdroppers and delivery to all Noah receivers, i.e., $\forall i \notin \mathcal{N}$, $R_i' = 0$ and $\forall i \in \mathcal{N}$, $R_i' = R = C_l - \epsilon = \log\left[1 + H_l \frac{(P + \sigma_n^2 - \frac{2\sigma_n^2}{H_l})}{2\sigma_n^2}\right] - \epsilon$, $\exists \epsilon > 0$. The analysis is independent and robust to the eavesdropper's channel conditions, h_e.

REMARK 1. *Attackers' using amplifiers to increase the received power level does not help their performances as they increase not only the signal power P_T but also the interference P_J and noise power δ_n^2, much like how analog amplifiers at receivers generally do not increase noise resistance.*

6.3 Advanced Threats Breaking Channel Bounds

We let attackers dictate their channel conditions in Section 6.2, e.g., attackers can freely move around. In this section, we consider further advanced threats of eavesdroppers, even though they may be impractical, and show that our analyses still holds. The results further strengthen Noah's security properties (the legitimate Noah users, on the other hand, are not as advanced as the eavesdroppers and are bound to the model constraints). Specifically, we establish that both increased processing (oversampling) and multiple antennas do not help the eavesdroppers (which analyses are omitted here due to space constraints) and then consider an attacker that breaks the channel bound of $H < 1$.

The attackers were operating under the natural bound of wireless channel propagation in Section 6.2. Here, we study the cases where attackers can break these bounds. In specific, the eavesdroppers have an ideal channel and are capable of (channel-)noiseless amplification in the channel path, making $H_e > 1$ possible. Even against such an advanced eavesdropper (the Noah users still assume the natural wireless channel, e.g., $H_l < 1$), Noah still provides positive secrecy capacity because both T and J come from the same antenna and are physically inseparable. In such scenario, the attacker's optimal strategy would be to maximize its channel gain, i.e., $H_e \to \infty$. Then, the Noah transmitter strategy of $P_J = \frac{2\sigma_n^2}{H_l}$, $P_T = P - \frac{2\sigma_n^2}{H_l}$, and $R = \log\left[1 + H_l \frac{P - \frac{2\sigma_n^2}{H_l}}{2\sigma_n^2}\right] = C_l - \epsilon, \; \exists \epsilon > 0$ solves the optimization in (3). Relative to the case of channel attenuation ($H_e \leq 1$), the SINR decreases by $\frac{P - \frac{2\sigma_n^2}{H_l}}{P + \sigma_n^2 - \frac{2\sigma_n^2}{H_l}}$.

6.4 Numerical Results

We study the *per-user* performance since there is one source transmitter, and to study the behavior with varying H_e, we

introduce $\gamma = \frac{H_e}{H_l}$, the attacker's advantage in channel over Noah's. For instance, if $\gamma < 1$, the attacker has worse channel than the Noah receiver. For numerical results, the channel gain of the Noah user l is: $H_l = -21.1$ dB $= \frac{1}{128}$. The power-budget-to-noise-ratio (PNR) is: PNR $= 25.1$ dB $= 320$. When we do not require security and all the power budget is used for transmission, i.e., $P_T = P$ and $P_J = 0$, then the SNR of some arbitrary user i is the product of PNR and H_i, i.e., SNR $= H_i \cdot$ PNR. For a baseline performance, we define R'_0 as the achievable rate when no security is implemented, i.e., $P_J = 0$; in this setting, $R'_0 = 2.585$ bps/Hz. This is the case when Noah jamming is disabled and the communication has no protection against potential eavesdroppers. If H_e is known to the Noah users, then Noah users can leverage the H_e information for better performance. For instance, if $\gamma < 1$, jamming is unnecessary ($P_J = 0$) for confidentiality with $R = R' = R'_0$.

However, in a more realistic scenario, e.g., with physically moving attackers, Noah users do not know about the eavesdropper's channel condition H_e as eavesdropping is passive. Then, Noah needs to choose its parameters conservatively to ensure security, as it can not adapt its control to H_e. As a consequence of conservative parameter choices, the performance suffers, e.g., even when $\gamma < 1$, the rate now only achieves 90% of the R'_0 performance or lower. Figure 2 shows the feasible region for Noah's rate, R', for secure communication with γ; legitimate receivers outside of these regions will not receive the communication. As γ increases, it has less flexibility in R'; the feasible region converges to a point as H_e approaches the upper bound, i.e., $H_e \to 1$.

7. CONCLUSION

Noah incorporates the techniques of friendly jamming and signal cancellation to achieve wireless confidentiality. By providing a coupled transmitter-receiver strategy (jamming at the transmitter and cancellation at the receiver) and basing the scheme on single-antenna transmission, Noah makes the jamming and the signal transmission inseparable and realizes stronger security properties than the state-of-the-art schemes, defeating threats that not only know and use the information about the Noah transmitter-receiver channel link for eavesdropping but are also capable of controlling their own channel gains or spaces. For the Noah protocol design, we establish that the capacity-optimal choice is to imitate channel noise for jamming (hence noise flooding) and study the parameter control and the rate performances via theoretical analyses. At the end, Noah provides a multicast channel that supports delivery to the network users while defeating any eavesdropper coexisting on the medium.

8. ACKNOWLEDGEMENTS

This work is supported in part 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) and the Temasek Research Fellowship.

9. REFERENCES

[1] M. Jain, J. I. Choi, T. Kim, D. Bharadia, S. Seth, K. Srinivasan, P. Levis, S. Katti, and P. Sinha, "Practical, real-time, full duplex wireless," in *Proceedings of the 17th Annual International Conference on Mobile Computing and Networking*, ser. MobiCom '11. New York, NY, USA: ACM, 2011, pp. 301–312. [Online]. Available: http://doi.acm.org/10.1145/2030613.2030647

[2] M. Duarte and A. Sabharwal, "Full-duplex wireless communications using off-the-shelf radios: Feasibility and first results," in *Signals, Systems and Computers (ASILOMAR), 2010 Conference Record of the Forty Fourth Asilomar Conference on*, Nov 2010, pp. 1558–1562.

[3] D. Bharadia, E. McMilin, and S. Katti, "Full duplex radios," in *Proceedings of the ACM SIGCOMM 2013 Conference on SIGCOMM*, ser. SIGCOMM '13. New York, NY, USA: ACM, 2013, pp. 375–386. [Online]. Available: http://doi.acm.org/10.1145/2486001.2486033

[4] T. Basar, "The Gaussian test channel with an intelligent jammer," *IEEE Trans. Info. Theory*, vol. 29, no. 1, pp. 152–157, Jan. 1983.

[5] I. Shomorony and A. S. Avestimehr, "Worst-case additive noise in wireless networks," *CoRR*, vol. abs/1202.2687, 2012. [Online]. Available: http://dblp.uni-trier.de/db/journals/corr/corr1202.html#abs-1202-2687

[6] S. N. Diggavi and T. M. Cover, "The worst additive noise under a covariance constraint," *IEEE Trans. Inf. Theory*, vol. 47, no. 7, pp. 3072–3081, Nov. 2001.

[7] E. Akyol, K. Rose, and T. Basar, "On optimal jamming over an additive noise channel," *CoRR*, vol. abs/1303.3049, 2013.

[8] 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.

[9] 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.

[10] S.-Y. Chang, Y.-C. Hu, and N. Laurenti, "SimpleMAC: a jamming-resilient MAC-layer protocol for wireless channel coordination," in *Proceedings of the 18th annual international conference on Mobile computing and networking*, ser. Mobicom '12, 2012, pp. 77–88.

[11] S.-Y. Chang, Y.-C. Hu, and Z. Liu, "Securing Wireless Medium Access Control Against Insider Denial-of-Service Attackers," in *Proceedings of the Conference on Communications and Netork Security*, ser. CNS '15. IEEE, 2015.

[12] A. Kashyap, T. Basar, and R. Srikant, "Correlated jamming on MIMO Gaussian fading channels," in *IEEE ICC*, vol. 1, Jun. 2004, pp. 458–462.

[13] M. Medard, "Capacity of correlated jamming channels," in *Allerton Conference on Communications, Computing and Control*, Monticello, IL, USA, 1998.

[14] C. Pöpper, N. O. Tippenhauer, B. Danev, and S. Capkun, "Investigation of signal and message manipulations on the wireless channel," in *Proceedings of the 16th European conference on Research in computer security, ESORICS '11*. Berlin, Heidelberg: Springer-Verlag, 2011, pp. 40–59.

[15] S.-Y. Chang, Y.-C. Hu, J. Chiang, and S.-Y. Chang, "Redundancy offset narrow spectrum: Countermeasure for signal-cancellation based jamming," in *Proceedings of the 11th ACM International Symposium on Mobility Management and Wireless Access*, ser. MobiWac '13. New York, NY, USA: ACM, 2013, pp. 51–58. [Online]. Available: http://doi.acm.org/10.1145/2508222.2508233

[16] Y. Hou, M. Li, R. Chauhan, R. M. Gerdes, and K. Zeng, "Message integrity protection over wireless channel by countering signal cancellation: Theory and practice," in *Proceedings of the 10th ACM Symposium on Information, Computer and Communications Security*, ser. ASIA CCS '15. New York, NY, USA: ACM, 2015, pp. 261–272. [Online]. Available: http://doi.acm.org/10.1145/2714576.2714617

[17] M. Schulz, A. Loch, and M. Hollick, "Practical known-plaintext attacks against physical layer security in wireless MIMO systems," in *Proceedings of NDSS*. Internet Society, 2014.

[18] R. Negi and S. Goel, "Secret communication using artificial noise," in *Vehicular Technology Conference, 2005. VTC-2005-Fall. 2005 IEEE 62nd*, vol. 3, Sept 2005, pp. 1906–1910.

[19] B. Zhang, Q. Zhan, S. Chen, M. Li, K. Ren, C. Wang, and D. Ma, "Priwhisper: Enabling keyless secure acoustic communication for smartphones," pp. 1–1, 2014.

[20] W. Shen, P. Ning, X. He, and H. Dai, "Ally friendly jamming: How to jam your enemy and maintain your own wireless connectivity at the same time." in *IEEE Symposium on Security and Privacy*. IEEE Computer Society, 2013, pp. 174–188.

[21] S. Sankararaman, K. Abu-Affash, A. Efrat, S. D. Eriksson-Bique, V. Polishchuk, S. Ramasubramanian, and M. Segal, "Optimization schemes for protective jamming," in *Proceedings of the Thirteenth ACM International Symposium on Mobile Ad Hoc Networking and Computing*, ser. MobiHoc '12. New York, NY, USA: ACM, 2012, pp. 65–74. [Online]. Available: http://doi.acm.org/10.1145/2248371.2248383

[22] S. Goel and R. Negi, "Guaranteeing secrecy using artificial noise," *Wireless Communications, IEEE Transactions on*, vol. 7, no. 6, pp. 2180–2189, June 2008.

[23] S. Gollakota, H. Hassanieh, B. Ransford, D. Katabi, and K. Fu, "They can hear your heartbeats: non-invasive security for implantable medical devices," in *Proceedings of the ACM SIGCOMM 2011 conference*. New York, NY, USA: ACM, 2011, pp. 2–13.

[24] N. Tippenhauer, L. Malisa, A. Ranganathan, and S. Capkun, "On limitations of friendly jamming for confidentiality," in *Security and Privacy (SP), 2013 IEEE Symposium on*, May 2013, pp. 160–173.

[25] H. Qin, Y. Sun, T.-H. Chang, X. Chen, C.-Y. Chi, M. Z. 0001, and J. W. 0001, "Power allocation and time-domain artificial noise design for wiretap ofdm with discrete inputs," *CoRR*, vol. abs/1302.2330, 2013.

[26] J. Vilela, M. Bloch, J. Barros, and S. McLaughlin, "Friendly jamming for wireless secrecy," in *Communications (ICC), 2010 IEEE International Conference on*, May 2010, pp. 1–6.

[27] F. Xu, Z. Qin, C. Tan, B. Wang, and Q. Li, "IMDGuard: Securing implantable medical devices with the external wearable guardian," in *INFOCOM, 2011 Proceedings IEEE*, April 2011, pp. 1862–1870.

[28] M. Wilhelm, I. Martinovic, J. B. Schmitt, and V. Lenders, "Wifire: A firewall for wireless networks," *SIGCOMM Comput. Commun. Rev.*, vol. 41, no. 4, pp. 456–457, Aug. 2011. [Online]. Available: http://doi.acm.org/10.1145/2043164.2018518

[29] J. Lee, H. Shin, and M. Z. Win, "Secure node packing of large-scale wireless networks," in *Proc. IEEE Int. Conf. Commun.*, Ottawa, Canada, Jun. 2012, pp. 815–819.

[30] A. Rabbachin, A. Conti, and M. Z. Win, "The role of aggregate interference on intrinsic network secrecy," in *Proc. IEEE Int. Conf. Commun.*, Ottawa, Canada, Jun. 2012, pp. 3548–3553.

[31] S. Gollakota and D. Katabi, "Physical layer wireless security made fast and channel independent," in *INFOCOM, 2011 Proceedings IEEE*, April 2011, pp. 1125–1133.

[32] A. Arora and L. Sang, "Dialog codes for secure wireless communications," in *Information Processing in Sensor Networks, 2009. IPSN 2009. International Conference on*, April 2009, pp. 13–24.

[33] G. T. Amariucai, S. Wei, and R. Kannan, "Gaussian jamming in block-fading channels under long term power constraints," in *Proceedings of IEEE Internation Symposium on Information Theorey (ISIT)*, Nice, Italy, Jun. 2007, pp. 1001–1005.