Received 29 January 2024; revised 17 March 2024; accepted 15 April 2024. Date of publication 24 April 2024; date of current version 14 May 2024.

Digital Object Identifier 10.1109/OJCOMS.2024.3393023

Experimental Evaluation of Network-Controlled Physical-Layer Security Through Friendly Jamming

SAYED AMIR HOSEINI [1] (Member, IEEE), PARASTOO SADEGHI [2] (Senior Member, IEEE), FAYCAL BOUHAFS [1] (Senior Member, IEEE), NEDA ABOUTORAB [2] (Senior Member, IEEE), AND FRANK DEN HARTOG [1,3] (Senior Member, IEEE)

[1]School of Systems and Computing, University of New South Wales, Canberra, ACT 2610, Australia

[2]School of Engineering and Technology, University of New South Wales, Canberra, ACT 2610, Australia

[3]Network Engineering and Cybersecurity, University of Canberra, Canberra, ACT 2617, Australia

CORRESPONDING AUTHOR: S. A. HOSEINI (e-mail: s.a.hoseini@unsw.edu.au)

ABSTRACT In this paper, we present a real-life, cost-effective implementation of physical layer security (PLS) using friendly jamming (FJ) and the IEEE 802.11 technology. Our approach is based on a recent development in software-defined networking (SDN) called spectrum programming, where a network controller can execute an intelligent access point (AP) selection algorithm to connect the user station to the AP that provides the most secrecy while exploiting idle APs as jammers. Considering a system with two APs, our first contribution is a theoretical optimization of the power of FJ based on system power parameters, as well as distances between the two APs and the user station and the eavesdropper station. Our second contribution is demonstrating not only that PLS can be implemented with commercial-off-the-shelf Wi-Fi devices, but also that our theoretical network-centric approach allows for a significant increase of secrecy capacity and secrecy coverage by applying FJ. Our experiments show that the theoretical optimization of the transmit power of the jamming AP is valid in practice, effectively maximizing the throughput gap between the user and the eavesdropper. To our best knowledge, this is the first work linking information-theoretic optimization of FJ in PLS to a real-world implementation, which is compatible with Wi-Fi standards and devices.

INDEX TERMS Artificial noise, secrecy, physical-layer security, software-defined networking, programmable networks, friendly jamming, experimental.

I. INTRODUCTION

IN THE past two decades, we have become increasingly reliant on a range of wireless communication technologies. Via our smart devices, we almost constantly interact with Wi-Fi or cellular networks and transmit our financial or other sensitive data over wireless links on a daily basis. However, due to the broadcast nature of the wireless medium, our data is prone to eavesdropping and manipulation. Currently, the information transmitted over wireless links is mostly protected by encryption. Yet, the computational capabilities of adversaries are rapidly advancing, making encryption a less safe choice as time goes by. There have been several cyber attacks against wireless networks when attackers could eavesdrop or intercept a wireless network [1], [2], [3].

In this context, physical layer security (PLS) is a promising complementary measure of security for wireless communications. PLS utilizes the physical characteristics of wireless channels in order to securely transmit information [4]. The advantage of PLS is that it offers *information-theoretic security* and therefore, has the potential to provide perfect secrecy even if the eavesdroppers have unlimited computational power.[1] However, until recently, implementing practical and cost-effective PLS was a challenge [6]. While most of the proposed PLS techniques in the literature are theoretical and simulation-based, they also would require major signal

[1]Information-theoretic security, also known as perfect secrecy, refers to a concept in information theory that provides a level of security that is theoretically unbreakable even with adversaries having unlimited computational capabilities [5].

processing efforts that may not be compatible with current wireless standards or their commercial deployments.

In [7], [8], a practical PLS system using off-the-shelf equipment was shown to be realizable using a relatively new network-layer control technique called spectrum programming [9]. The system utilized the fact that often multiple wireless access points (AP) are available to either serve the legitimate station or produce a jamming signal and thanks to spectrum programming, it is now possible to execute AP selection algorithms in a way that is fast and completely transparent to the connecting device, which we refer to as intelligent AP selection. In [7], the legitimate station is always connected to the least beneficial AP to the eavesdropper, and in [10] the AP that maximizes the secrecy capacity for the legitimate station is selected. The secrecy capacity is the maximum information-theoretic channel capacity that a legitimate station can achieve under the condition of full secrecy while connected to a given AP [4].

In [11], we utilized the opportunities offered by network-enabled PLS using spectrum programming and introduced a novel secrecy capacity optimization framework, which combines intelligent AP selection as described in [10] with the creation of a friendly jamming (FJ)[2] [12], [13] signal by the not-selected AP. We considered a system with two APs, as this is the simplest yet non-trivial setting that allows one to obtain tractable theoretical conclusions and insights about the optimization of FJ and AP selection. The simulation results indicated that introducing an intelligently crafted FJ signal significantly improved secrecy in the network beyond what can be achieved with intelligent AP selection only. This was the first time the concepts of network-controlled intelligent AP selection of [9] and FJ were combined and supported by a single robust theoretical framework. In [14], we investigated our framework for a larger network with multiple APs, users and eavesdroppers. We employed reinforcement learning to optimize APs' transmit power that can work as user traffic source or jammer.

In this paper, we extend [11] by evidencing the real-life cost-effective applicability of the framework by experimental evaluations, as well as more advanced simulations taking into account small-scale path-loss effects. To the best of our knowledge, the current paper is the first of its kind to combine theory, simulations, and real-world experiments using commercial Wi-Fi technology to show the efficacy and robustness of PLS to eavesdropping via FJ in a wide range of system parameters. Specifically, we demonstrate that PLS can be achieved by using the IEEE 802.11 standard for the data stream as well as for creating the jamming signal. For that, we have extended the framework of [11] by taking into account constraints imposed by the standard, particularly regarding active interference management and the fact that FJ can only be created by generating vacuous traffic. The proposed solution is *cost-effective* in the sense that it uses existing commercial hardware and software for Wi-Fi technology with little to no modification. Since Wi-Fi products can be obtained relatively cheaply, the addition of Wi-Fi APs that can solely serve as jammers does not impose a great cost relative to the benefit they can provide in terms of enhancing network security.

The remainder of this paper is organized as follows. Section II provides a literature review on the subject. Section III introduces a basic model of the network-controlled Wi-Fi system, which is an extension of the standard-agnostic model as described in [11]. In Section IV, we discuss the proposed FJ approach and its associated power optimization. The simulation environment and results are presented in Section V. In Section VI, we present the experimental test-bed and correlate the numerical and experimental results. Finally, we summarize our findings and draw conclusions in Section VIII.

II. RELATED WORK

PLS techniques can be categorized into the following four groups: channel coding, channel control, power control, and artificial noise techniques. Channel coding introduces robust coding schemes and randomization in the transmitted signal to make it difficult for eavesdroppers to decode the intercepted signal [15], [16]. Channel control manipulates the radio channel parameters and monitors the channel to detect the presence of eavesdroppers [17], [18]. Power control techniques control transmission power and beams direction using Multiple-In-Multiple-Out (MIMO) antennas [19] to increase the secrecy capacity. Artificial noise techniques degrade the quality of the channel at the eavesdropper. Such techniques are particularly efficient in situations where the eavesdropper is closer to the source than the legitimate station. Early artificial noise contributions were based on the assumption that the channel state information (CSI) at both the legitimate station and eavesdropper is partially or not known [20], [21], [22], [23].

Works presented in [13] and [12] fall into the artificial noise category and propose to achieve PLS using two APs, namely AP_1 and AP_2. In this technique, when the legitimate station is communicating with either AP, the other AP generates a pre-determined signal transmitted to the eavesdropper in order to jam its radio channel. More recent artificial noise techniques include the use of intelligent reflecting surfaces [24] or non-orthogonal multiple access [25].

However, in addition to being limited to theoretical models, these contributions focus on providing link-level approaches to PLS, which has proven too difficult to implement [6]. In this context, we have already proposed in [10] and [7] a network-level PLS approach that is practical to realize using the concept of spectrum programming [9]. Inspired by software-defined networking (SDN), in this concept, a central controller offers an Application Programming

[2]FJ in this work refers to the scenario where a not-selected AP sends a jamming signal to interfere with the eavesdropper's reception at the same time when another AP serves and transmits the message signal to the legitimate station.

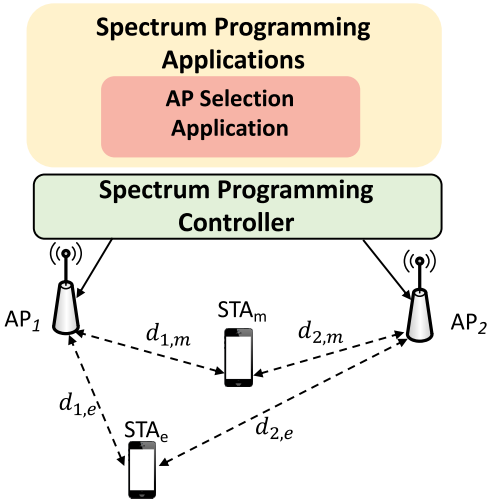


FIGURE 1. Network-level PLS: the controller helps the legitimate station STA_{meter} to associate with the AP that can provide the best secrecy capacity in the presence of an eavesdropper STA_e. Besides, the controller can assign FJ transmitter role to the idle AP with an appropriate jamming signal strength.

Interface (API) that allows to implement radio resources and connections management to achieve PLS.

In this work, we extend [7], [10], [11] as follows. The main novelty of our work compared to [7], [10] lies in enhancing communication secrecy by *combining* intelligent AP selection [7], [10] with network-controlled optimization of the power of the FJ signal. Similar to [13] and [12], we study a system with two APs, since it is a rich enough model to exhibit the fundamental performance gains from FJ power optimization. Furthermore, in this paper, we conduct an experimental evaluation of our proposed theoretical FJ power optimization in [11]. Notably, our proposed approach is compatible with current hardware and software implementation of commercial Wi-Fi devices. This is demonstrated in our extensive experimental evaluations with matching trends with the developed theory and simulations in terms of secrecy capacity improvement.

III. SYSTEM MODEL

Referring to Figure 1, a legitimate station (denoted by STA_m) aims to connect and receive information from a Wi-Fi network consisting of two APs (denoted by AP_1 and AP_2) in the presence of an eavesdropper (denoted by STA_e). We note, however, that the concept can be generalized to other wireless networks. A summary of the notations is presented in Table 1.

PLS can be theoretically achieved when the Shannon capacity of the legitimate channel is greater than the Shannon capacity of the eavesdropping channel (under several conditions as specified in [4]). In other words, a secrecy capacity greater than zero can result in PLS, where the secrecy capacity is defined as how much the legitimate channel capacity exceeds the eavesdropping capacity. Without loss of generality, we assume downstream traffic from one of the Wi-Fi APs to the legitimate station. This models situations

TABLE 1. Summary of notation and units.

AP_n	Either one of the APs (n is either 1 or 2)
STA_m	Legitimate station
STA_e	Eavesdropper station
W	Channel bandwidth, Hz
f_0	Operating center frequency, Hz
C	Speed of light, $\sim 3 \times 10^8$ meter per second
P_{t_n}	Transmit power of AP_n, Watt
$P_{t_n}^{\max}$	Maximum transmit power of AP_n, Watt
$d_{n,m}$	Distance between STA_m and AP_n, meter
$d_{n,e}$	Distance between STA_e and AP_n, meter
α	Path loss exponent (typical values are: $\alpha = 2$ for free space, $\alpha = 2.7 \sim 3.5$ for urban area, $\alpha = 1.6 \sim 1.8$ for indoor (line-of-sight))
$P_{0,n}$	Free-space received power from AP_n at reference distance d_0: $P_{0,n} = P_{t_n}(\frac{C}{4\pi f_0 d_0})^2$, Watt
P_n	Distance-corrected power used in capacity formulas: $P_n = P_{0,n} d_0^{\alpha}$, Watt.meter$^{\alpha}$
$\text{SINR}_{n,m}$	SINR at station STA_m when connected to AP_n
$\text{SINR}_{n,e}$	SINR at station STA_e when connected to AP_n
$I_{n,m}$	Interference experienced at STA_m, Watt
$I_{n,e}$	Interference experienced at STA_e, Watt
N_m	Noise experienced by STA_m, Watt
N_e	Noise experienced by STA_e, Watt
$C_{n,m}$	Channel capacity between AP_n and STA_m, bits/second
$C_{n,e}$	Channel capacity between AP_n and STA_e, bits/second

where privileged information is offered only for consumption by legitimate clients.

In this work, the AP selection mechanism suggested in [10] is employed to assign the AP that can provide the highest secrecy capacity to STA_m by exploiting the principles of PLS. It is assumed that the location of the APs, STA_m, and STA_e are known. The latter is hard to achieve when the eavesdropper is passive, but various proposals have been made in the literature to overcome this problem (see, e.g., [26]). In addition and in certain real-world situations, the physical premises of legitimate users are secure (for example in a secure building or an apartment unit). In these situations, it is fair to assume that the eavesdropper cannot be in a certain neighborhood of the user and one can use an estimate for the closest possible location the eavesdropper can get to the user. For simplicity of exposition, we will model the channel between the APs and both stations using a path loss model [27]. This model is rich enough to exhibit performance gains from FJ power optimization.

Let us assume that AP_n (n is either 1 or 2) is the considered candidate for downlink data transmission. The received power at STA_m and STA_e from AP_n is $P_n d_{n,m}^{-\alpha}$ and $P_n d_{n,e}^{-\alpha}$, respectively. Therefore, the Shannon capacity of the channel between AP_n and the legitimate station STA_m is given as

$$C_{n,m} = W \log\big(1 + \text{SINR}_{n,m}\big) = W \log\left(1 + \frac{P_n d_{n,m}^{-\alpha}}{I_{n,m} + N_m}\right), \quad (1)$$

where $\text{SINR}_{n,m}$ is the signal-to-interference plus noise ratio (SINR) at STA_m from AP_n. Similarly, the Shannon capacity of the channel between AP_n and the eavesdropper STA_e is

$$C_{n,e} = W\log\big(1+\text{SINR}_{n,e}\big) = W\log\left(1+\frac{P_n d_{n,e}^{-\alpha}}{I_{n,e}+N_e}\right), \quad (2)$$

where all logs are in base 2 and, therefore, capacities are measured in bits/s. The terms $I_{n,m}$ and $I_{n,e}$ measure the interference experienced at STA_m and STA_e, respectively, as further elaborated in Section IV.

The legitimate station STA_m can securely communicate with AP_n if $C_{n,m} > C_{n,e}$, which means the user experiences a better channel than the eavesdropper and can achieve secrecy capacity according to the PLS theory [4], [28]. The AP selection mechanism in [10] connects STA_m to the AP that provides the maximum secrecy capacity (i.e., maximum $C_{n,m} - C_{n,e}$ value among AP choices $n = 1$ or $n = 2$). The secrecy capacity is maximized by finding the solution

$$i = \arg\max_{n\in\{1,2\}} \big(C_{n,m} - C_{n,e}\big). \quad (3)$$

Therefore, AP_i is the selected AP for the transmission of information to STA_m. The other AP AP_j, $j \neq i$ is referred to as the "idle" AP.

IV. PROPOSED FRIENDLY JAMMING

In addition to employing the AP selection mechanism in Section III, the not-selected AP_j (or the idle AP) in (3) is used to generate an optimal FJ signal. The aim for the idle AP_j is to reduce the SINR experienced at STA_e as much as possible, which will in turn reduce the channel capacity of the eavesdropper ($C_{e,n}$) and, therefore, will improve the secrecy capacity of STA_m. However, the FJ signal may also affect the STA_m reception. Therefore in this section, we aim to find an optimal FJ power that maximizes secrecy capacity in addition to AP selection in (3). For ease of exposition, we assume that STA_e and STA_m have the same noise powers, i.e., $N = N_m = N_e$. We also assume that the *ambient* interference (without FJ generation) is zero. This will allow us to meaningfully evaluate the improvement due to optimal FJ generation compared to a baseline system (which is free from ambient/extra interference). Nonetheless, the method presented below can be extended to cater to the general case.

Given the above, the interference received by STA_m and STA_e from the FJ generating AP_j is $P_j d_{j,m}^{-\alpha}$ and $P_j d_{j,e}^{-\alpha}$, respectively. Therefore, we specify (1) and (2) as functions of P_i and P_j

$$C_{i,m}\big(P_i,P_j\big) = W\log\left(1+\frac{P_i d_{i,m}^{-\alpha}}{P_j d_{j,m}^{-\alpha}+N}\right), \quad (4)$$

$$C_{i,e}\big(P_i,P_j\big) = W\log\left(1+\frac{P_i d_{i,e}^{-\alpha}}{P_j d_{j,e}^{-\alpha}+N}\right). \quad (5)$$

The goal here is to find the optimal interference power transmitted from AP_j, i.e., the optimal P_j, to maximize the secrecy capacity of the downlink transmission from AP_i to STA_m. To that end, we fix the power for the main AP_i, P_i, and find the optimal P_j that maximizes $C_{i,m}(P_i,P_j) - C_{i,e}(P_i,P_j)$. In summary, to optimize secrecy in our system, we adopt a two-step approach. Firstly, we employ (3) to select the user and jammer APs. Subsequently, we determine the optimal P_j as follows

$$P_j^{\text{Optimal}} = \arg\max_{P_j} \quad C_{i,m}\big(P_i,P_j\big) - C_{i,e}\big(P_i,P_j\big),$$
$$\text{s.t.} \quad 0 \le P_j \le min\big\{P^{max}, P'_{\text{CCA}}\big\}, \quad (6)$$

while $P^{\max} := P_{t_j}^{\max}(\frac{C}{4\pi f_0 d_0})^2 d_0^{\alpha}$. Furthermore, the IEEE 802.11 standard defines a clear channel assessment (CCA) mechanism to indicate if the channel is not busy and ready for the transmitter [29], [30]. Hence, if the optimized jamming signal power is too high, it may stop the other AP that is associated with the user from transmitting payload traffic data. The standard defines a threshold of -82dBm $\approx$ 6.31 pW to detect Wi-Fi frames and also a threshold of -62 dBm $\approx$ 0.63 nW to detect any RF signal in the channel. Our proposed FJ signal generation should clearly avoid the above threshold. Let $P_{\text{CCA}} = 0.63$ nW be the CCA threshold to avoid, d_{12} be the distance between AP_1 and AP_2, and $P'_{\text{CCA}} = P_{\text{CCA}} d_{12}^{\alpha}$ be the distance-corrected term for the CCA threshold used in capacity formulas. Overall, $\min\{P^{\max}, P'_{\text{CCA}}\}$ signifies the maximum (distance-corrected) power allowed to be used for FJ generation, by taking into account the maximum transmit power of AP_j and the CCA threshold.

After some algebraic manipulations, we obtain the detailed equation for secrecy capacity as follows[3]

$$C_{i,m}\big(P_i,P_j\big) - C_{i,e}\big(P_i,P_j\big) = W\log\left(\frac{P_j d_{i,m}^{\alpha} + N d_{i,m}^{\alpha} d_{j,m}^{\alpha} + P_i d_{j,m}^{\alpha}}{P_j d_{i,m}^{\alpha} + N d_{i,m}^{\alpha} d_{j,m}^{\alpha}} \times \frac{P_j d_{i,e}^{\alpha} + N d_{i,e}^{\alpha} d_{j,e}^{\alpha}}{P_j d_{i,e}^{\alpha} + N d_{i,e}^{\alpha} d_{j,e}^{\alpha} + P_i d_{j,e}^{\alpha}}\right). \quad (7)$$

To simplify, let us refer to the argument inside the logarithmic term as $f(P_i,P_j)$. Therefore, $C_{i,m}(P_i,P_j) - C_{i,e}(P_i,P_j)$ can simply be expressed as

$$C_{i,m}\big(P_i,P_j\big) - C_{i,e}\big(P_i,P_j\big) = W\log\big(f(P_i,P_j)\big), \quad (8)$$

where $f(P_i,P_j)$ is given by

$$f\big(P_i,P_j\big) = \frac{{P_j}^2 A + P_j B + P_i P_j C + P_i D + K}{{P_j}^2 A + P_j B + P_i P_j E + P_i F + K}, \quad (9)$$

and A, B, C, D, E, F and K are defined as follows:

$$A = d_{i,m}^{\alpha} d_{i,e}^{\alpha},$$
$$B = N d_{i,e}^{\alpha} d_{j,e}^{\alpha} d_{i,m}^{\alpha} + N d_{i,m}^{\alpha} d_{j,m}^{\alpha} d_{i,e}^{\alpha},$$
$$C = d_{j,m}^{\alpha} d_{i,e}^{\alpha},$$
$$D = N d_{i,e}^{\alpha} d_{j,e}^{\alpha} d_{j,m}^{\alpha},$$

[3] See [11] for more detailed derivations in this section.

$$E = d_{i,m}^{\alpha} d_{j,e}^{\alpha},$$
$$F = N d_{i,m}^{\alpha} d_{j,m}^{\alpha} d_{j,e}^{\alpha},$$
$$K = N^2 d_{i,m}^{\alpha} d_{j,m}^{\alpha} d_{i,e}^{\alpha} d_{j,e}^{\alpha}. \tag{10}$$

The partial derivative of f with respect to P_j is

$$\frac{\partial f}{\partial P_j} = \frac{P_j^2 a + P_j b + c}{P_j{}^2 A + P_j B + P_i P_j E + P_i F + K}, \tag{11}$$

where a, b and c are defined as

$$a = 2P_i AE + P_i AC - 2P_i AC - P_i AE,$$
$$b = 2P_i AF - 2P_i AD,$$
$$c = P_i BF + P_i^2 FC + P_i KC - P_i BD - P_i^2 ED - P_i KE.$$

This results in two quadratic solutions of $\frac{\partial f}{\partial P_j} = 0$ by $Q_j^{1,2}$. Note that $Q_j^{1,2}$ may be negative or go above $P^{\max}$. Therefore, we need to adjust the above two solutions, $Q_j^{1,2}$, according to the physical system constraints:

$$P_j^k = \min\left\{\max\left\{Q_j^k, 0\right\}, \min\left\{P^{\max}, P'_{\text{CCA}}\right\}\right\}, \quad k = 1, 2. \tag{12}$$

Hence, the optimal FJ power solution is the one among the two candidates that gives the best secrecy capacity $C_{i,m} - C_{i,e}$. That is,

$$P_j^{\text{Optimal}} = \arg \max_{k \in \{1,2\}} W \log\left(f\left(P_i, P_j^k\right)\right). \tag{13}$$

V. SIMULATION SETUP AND RESULTS

We simulated the proposed algorithm in MATLAB to evaluate the performance. Specifically, the simulated network is assumed to be a 2.4 GHz Wi-Fi network. Nonetheless, the concept can be generalized to other wireless networks. Four Wi-Fi configurations are set up: a) a normal Wi-Fi configuration where STA_m is associated with the nearest AP, equivalently the highest SINR, regardless of the eavesdropper's location; b) the smart AP configuration based on [10] where STA_m is associated to AP_i that provides the highest secrecy capacity according to (3); c) the enhanced smart AP configuration where the idle AP AP_j generates FJ to increase the secrecy of communication between STA_m and AP_i according to (13); and d) the enhanced smart and FJ where transmitters carry out CCA and avoid transmitting if there is at least -62 dBm interference.

An 80×80 map is considered in our simulation where the positions are represented in meter. The two APs are located at positions $(25, 40)$ and $(55, 40)$ and operate at $f_0 = 2.4$ GHz. While the FJ optimization is done according to the distance-based model in Section IV, the simulated channel is modeled as a Rician channel with a Rician K-factor of 4 to model channel fading in the presence of a Line-of-Sight signal [31]. We simulate 1e6 channel samples and show the mean ergodic capacity as channel capacity. However, due to system-level constraints, AP selection cannot be performed too frequently. Therefore, we use the mean ergodic capacity computed using (3) to select the associated AP. The AP associated with STA_m uses a fixed transmit power of $P_{t_i} = 50$ milli Watt. When the idle AP_j is used to introduce FJ, we assume $P_{t_j}^{\max} = 50$ milli Watt. The noise power at both STA_m and STA_e is $N = N_m = N_e = -70$ dBm $= 10^{-10}$ Watt. A path loss exponent of $\alpha = 2$ and a reference distance $d_0 = 1$ meter are assumed for the entire map. Next, we perform a simulation in which STA_m is held in a fixed location at $(55, 15)$, and we vary the STA_e's locations, for the four configurations a) to d) as described earlier in this section. Subsequently, we calculate the eavesdropping capacity $C_{i,e}$, the secrecy capacity $C_{i,m} - C_{i,e}$, and the coverage ratio, which is the ratio of the area with positive secrecy capacity to the total area of the map. The results are visualized as a map in Figure 2 and Figure 3.

Figure 2(a) is the case for normal Wi-Fi. It shows that STA_m is always associated with AP_2 since it receives a stronger signal from this AP no matter where eavesdropper STA_e is located. However, when STA_e is located closer to AP_2 than STA_m, there would be no secrecy capacity. This area is shown with the white color. For this scenario, Figure 3(a) illustrates the secrecy capacity map for eavesdroppers and the dark blue area represents no secrecy. For other locations of STA_e, the secrecy capacity is greater than 0 (zero). Figure 2(b) and 3(b) then show the results for the smart AP configuration where the user station STA_m is associated with the AP that can provide higher secrecy capacity [10]. In this case, the location of STA_e matters and it can be observed depending on the location of the eavesdropper the stationary STA_m may be associated with AP_1 or AP_2. This reduces the no-secrecy area by 40% compared to normal Wi-Fi, which shows the effectiveness of the algorithm in [10]. But there is still a large white area in Figure 2(b) (or dark blue area in Figure 3(b)) where the eavesdropper can capture the entire STA_m communication. The results for our proposed FJ algorithm are shown in Figure 2(c) and Figure 3(c). Now, secrecy capacity can be achieved almost everywhere. STA_m is associated to the same AP as in the smart AP configuration, but the FJ helps to reduce the eavesdropper capability. Interestingly from Figure 2(c) and 2(d), we can see that in certain locations where there is an eavesdropper present, for instance at (40,50), STA_m is associated with AP_1 instead of the closer AP, i.e., AP_2. In such a scenario, the eavesdropper is situated closer to both APs than the legitimate user, but thanks to jamming secrecy can be achieved.

Furthermore, Figure 3(d) illustrates implementing the CCA mechanism and limiting the FJ to an upper threshold to avoid jamming the associated AP's transmitter (i.e., AP_1).

Figure 4 demonstrates the optimized FJ power for AP_j to enhance the secrecy capacity and coverage. Figure 4(b) shows that the FJ power is capped to about 8 dBm to keep the received jamming power below the CCA threshold of

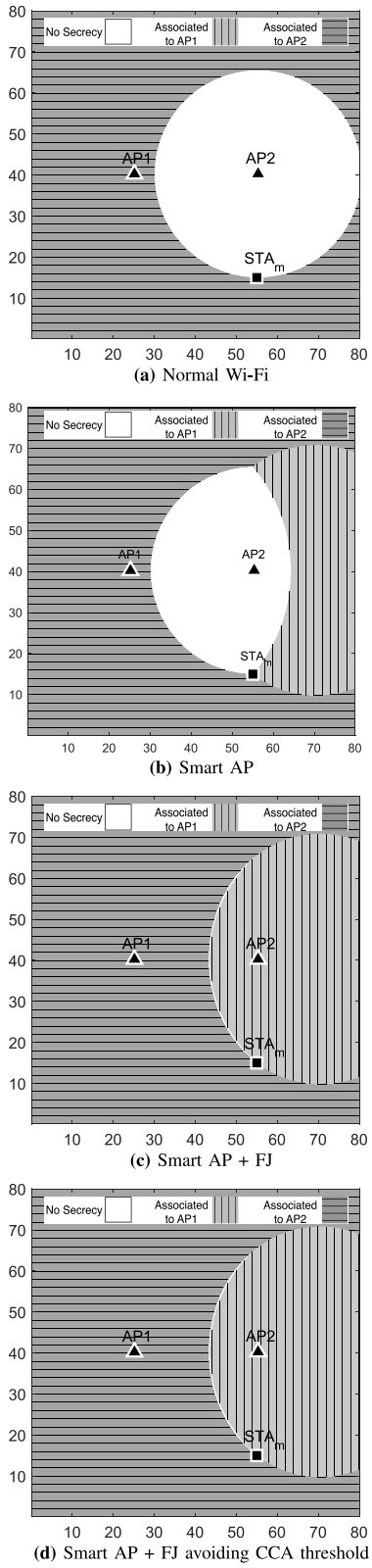


FIGURE 2. Association maps for different locations of STA_e, STA_m is located at position (55, 15) for 4 simulated configurations.

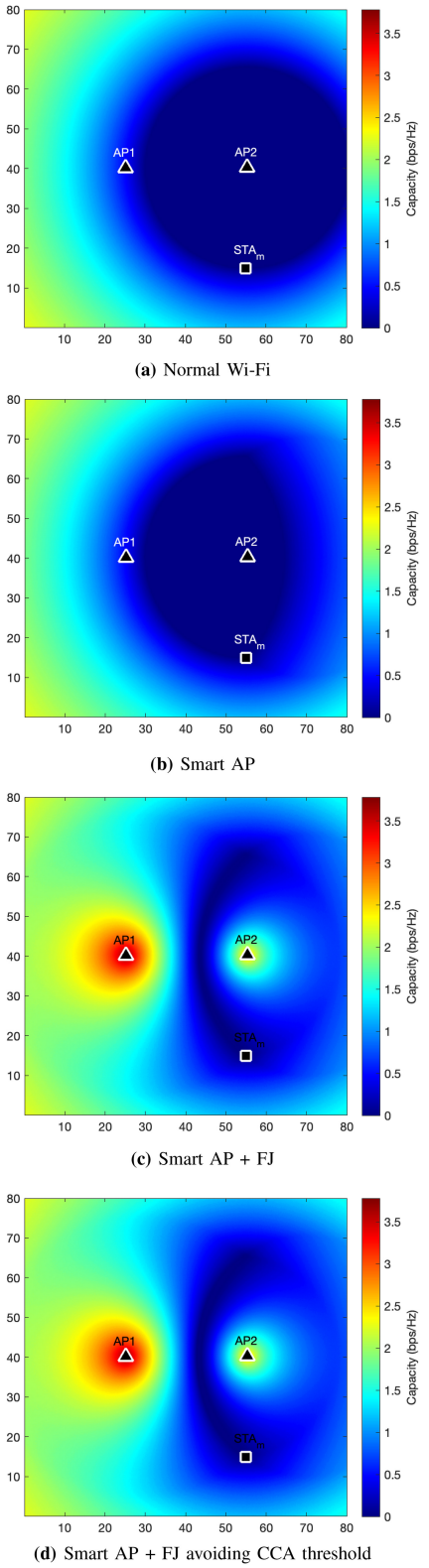


FIGURE 3. Secrecy capacity for different locations of STA_e, STA_m is located at position (55, 15) for 4 simulated configurations.

−62 dBm at the associated AP. In our simulations, given a constant transmit power of 17 dBm for AP_i, the optimized FJ power of AP_j is about 5-10 dBm for most potential locations of the eavesdropper. When the eavesdropper is situated at the edge area of the map, it is possible to achieve optimal secrecy without using any jamming.

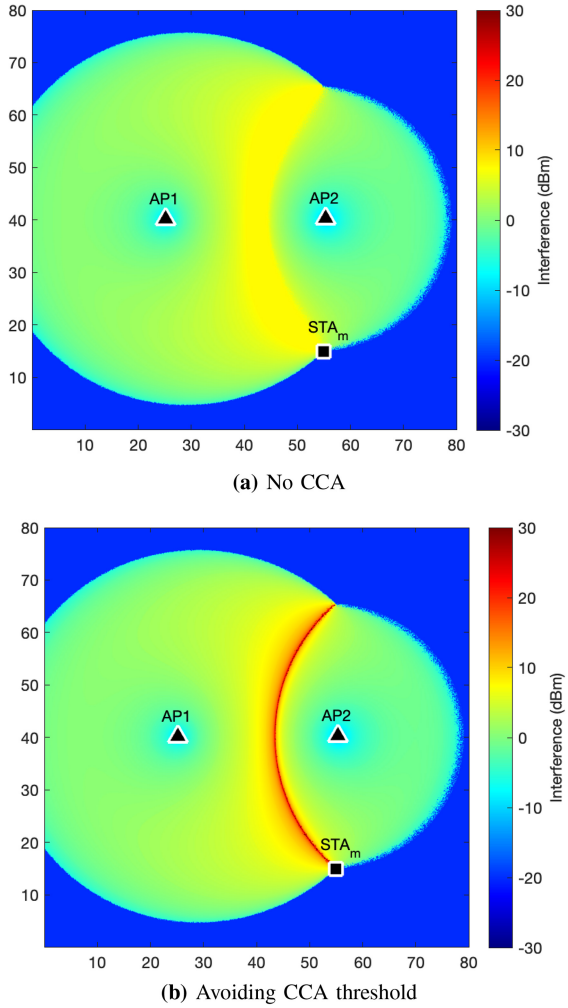


FIGURE 4. The optimized transmit power of the idle AP as FJ for different locations of STA_e.

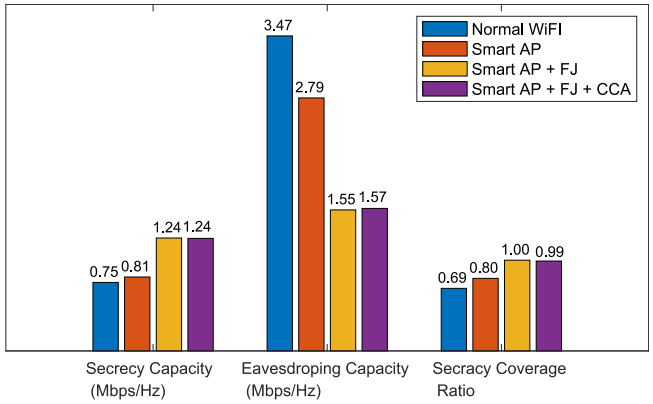


FIGURE 5. The average secrecy capacity for STA_m in bps/Hz, the average secrecy coverage ratio, and the average eavesdropper's capacity. The results are averaged over 10,000 locations for STA_m. The colors indicate the Wi-Fi configuration.

Next, for every configuration above, we calculated the average secrecy capacity and the average eavesdropper's capacity for all possible locations of STA_e. Let STA_m and STA_e be located at (x_m, y_m) and (x, y), respectively. The channel capacity of STA_m and STA_e can then be represented as $C_{i,m}(x, y|x_m, y_m)$ and $C_{i,e}(x, y|x_m, y_m)$, respectively, where $x, y \in \{1, 2, \ldots, Z\}$, i.e., we vary the location of STA_e in steps of 1 meter in horizontal or vertical directions. This yields the average secrecy capacity

$$E\big(C_{sec,m}\big) = \frac{1}{Z^2}\sum_{x=1}^{Z}\sum_{y=1}^{Z}\big(C_{i,m}(x, y|x_m, y_m) - C_{i,e}(x, y|x_m, y_m)\big), \quad (14)$$

with $Z = 80$. Furthermore, the average eavesdropping capacity is calculated as

$$E(C_e) = \frac{1}{Z^2}\sum_{x=1}^{Z}\sum_{y=1}^{Z} C_{i,e}(x, y|x_m, y_m). \quad (15)$$

Figure 5(b) presents the average secrecy capacity for STA_m, the average secrecy coverage ratio, and the average eavesdropper's capacity calculated using (14) and (15). The results are obtained by averaging over 10,000 locations for STA_m. The Wi-Fi configuration is specified by color. The results indicate that the observations made from figure 3 can be generalized to other locations of STA_m. The results also suggest that incorporating FJ significantly improves the average secrecy capacity and reduces the average eavesdropper's capacity. Moreover and notably, it can be observed that the region where no secrecy can be achieved has reduced to a negligible area. Also, it can be observed that implementing CCA and limiting FJ power accordingly has only a little effect.

VI. EXPERIMENTAL SETUP

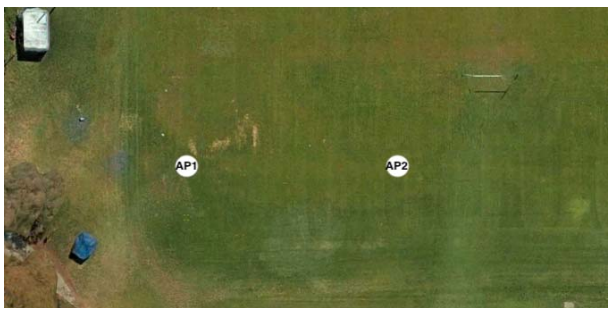
We experimentally evaluated our PLS-based FJ technique with the aim of validating the simulation results shown in Section V. We deployed an outdoor testbed consisting of two off-the-shelf Wi-Fi routers (Netgear AC1750) acting as APs and two HP laptops acting as STAs, with one laptop acting as STA_m and the other as STA_e. Both STAs are also equipped with external ALFA wireless USB adapters (AWUS036NHA).

To make APs transmit FJ signals, we generate Wi-Fi traffic on the channel adjacent to the legitimate traffic channel. Our measurements indicate that the transmitted signal, with a 20 MHz bandwidth, is received on the adjacent channel with a 1 to 2 dB of attenuation. This is consistent with findings reported in the literature [32]. For the sake of simplicity, we used a receiver as the destination for jamming traffic in our experiment. Moreover, it is also possible to propagate Wi-Fi jamming frames through the air without a receiver.

Both APs had their firmware replaced with OpenWRT 19.07 and can act as sources for data or jamming traffic. The built-in wireless adapter on STA_m is utilized as the sink for legitimate traffic, while an Android phone is used as the sink for jamming traffic. We run Iperf3 to generate a downlink UDP stream. Iperf packet size is set to 1400 Bytes and the

(a) Test-bed equipment in the field.

(b) AP locations in scenarios 1 and 2.



(c) AP locations in scenarios 3 and 4.

FIGURE 6. Test-bed equipment and AP locations in UNSW, Canberra Campus.

bandwidth is set to 70 Mbps which maximizes throughput in our setup. IEEE 802.11g [29] and 2.4GHz band are used for this experiment.

The tests consisted of four scenarios at two different locations: the Rugby Pitch and one of the car parks of the University of New South Wales (UNSW), Canberra Campus as shown in Figure 6. Figure 7 shows the exact location of devices and all coordinates are expressed in meter. The scenarios are very similar to the ones simulated in Section V. While the distance between APs is 30 meter in scenarios 1 and 2, it is reduced to 20 meter in scenarios 3 and 4. In all four scenarios, AP_1 is selected as serving AP for legitimate station STA_m since it provides higher secrecy capacity according to (3). The transmit power of AP_1 is set to 15 dBm while the transmit power of AP_2 (jammer) is set to different levels from 0 dBm to 25 dBm. For each jamming power level, we repeat every test 5 times where each test lasts for 5 seconds. While AP_1 is sending the UDP stream to the STA_m on channel 3, ALFA cards on both the user and eavesdropper stations are used to capture data on the same channel (i.e., channel 3) using Wireshark. This would let us have a fair comparison of the user and eavesdropper capability to capture all packets including retransmitted frames.

For each test, we measured the number of legitimate traffic data packets that were captured by both STA_m and STA_e. We used the measurements to calculate the throughput at each station and then calculated the difference in throughput to determine the packet capture success rate at STA_e. We repeated each test five times and we then calculated the average and standard deviation of these measurements. We obtained system gain from the experiments, which includes antenna gain and system loss at both transmitter and receiver and adjusted the communication link parameters of the simulation accordingly.

VII. RESULTS

For every scenario 1-4, we present the results in Figure 8 to 11 in three different ways. The reason for that is that secrecy capacity as calculated in the previous section is difficult to measure in a real experiment: in real experiments, received signal strengths can be measured quite easily, but which part of that signal strength is noise (or interference) and which part is genuine signal is difficult to distinguish. Throughputs, however, are easy to capture. Fortunately, we recently found that secrecy capacity and the difference between the throughputs of the legitimate user and eavesdropper are surprisingly well correlated [33]. Verifying the results of our simulation by our experimental data has, therefore, merely become a matter of scaling. We have done so in three different ways, and the figures show that the experiments validate the model well, regardless of which scaling method is chosen. Note that the jamming technique in our experiments is discontinuous in time and hence, differs from the assumed continuous jamming in theory. Nevertheless, both theoretical secrecy capacity and experimental throughput reach their maximum values with the same level of FJ power.

Figure 8 to 11 (a), on the left-hand side, show the average measured throughput at the legitimate user, at the eavesdropper, and the difference between the two average throughputs, for different jamming powers. The error bars present the standard deviation of 5 independent tests. To compare the experimental results with the simulation results, we added the secrecy capacity obtained from the simulation to the plots. We scaled the secrecy capacity to the difference of the average throughputs using a Linear Weighted Least-SQuare (WLSQ1) fitting routine which resulted in the bps/Hz scale on the right-hand side y-axis in these plots. More specifically, if we denote the left y-axis limit by L_{LY} and the right y-axis by L_{RY}, we scale the right-hand side y-axis by $L_{RY} = (L_{LY} - \nu)/\mu$, with ν and μ being the scaling parameters. WLSQ1 brings about both y-axes having the same origin at zero by setting $\nu = 0$ and finding μ by $\arg\min_\mu \sum_{t=1}^{n} \omega_t |d\theta_t - \mu C_t|^2$. t represents the index of

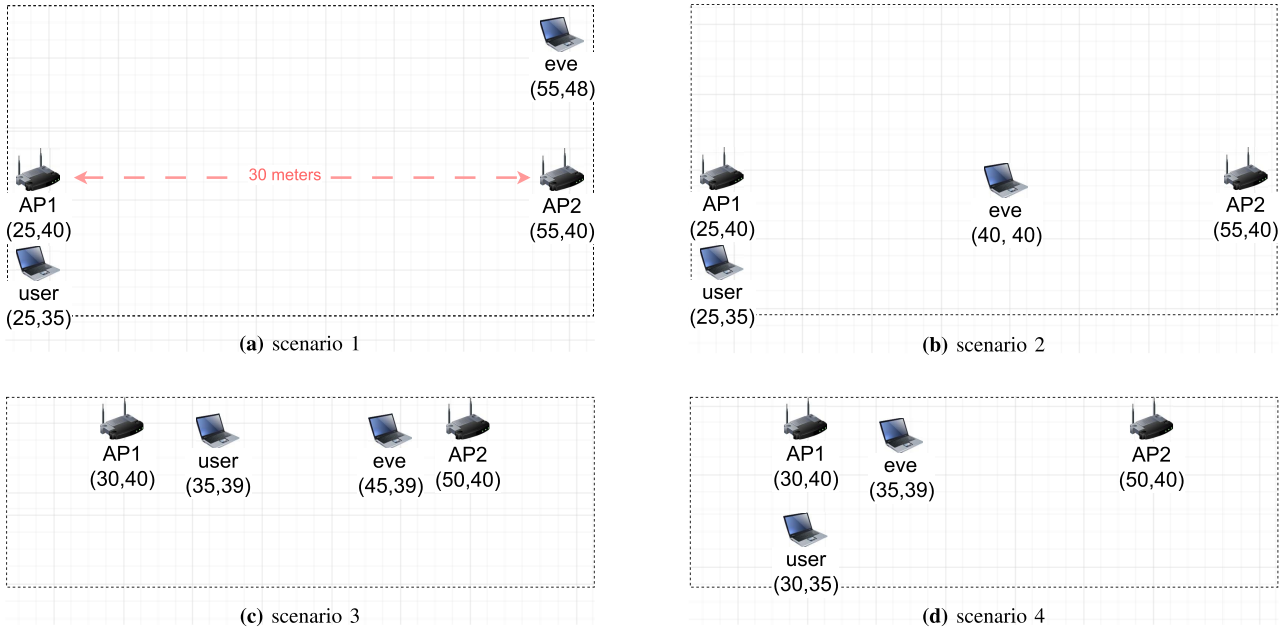


FIGURE 7. Measurement scenarios. Eavesdropping station STA_e is referred to as "eve" while user station STA_m is "user".

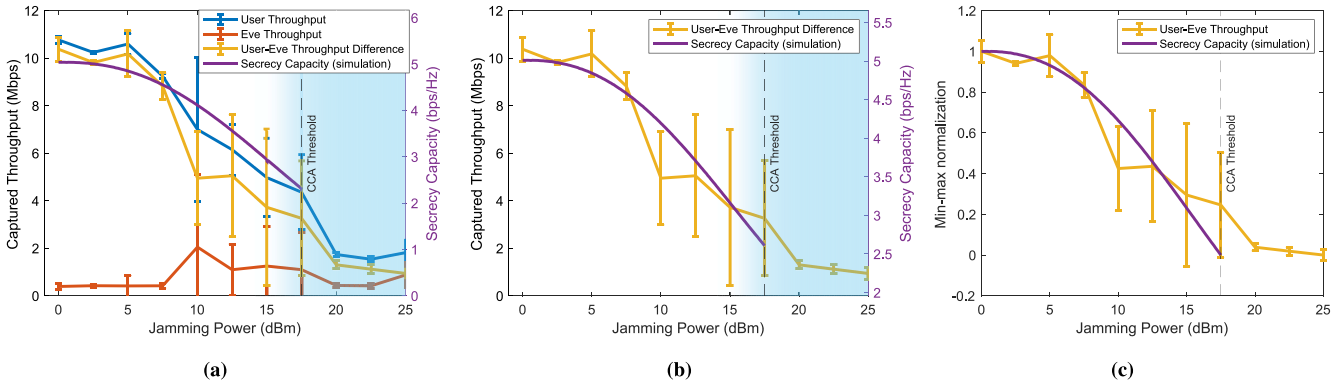


FIGURE 8. Results for scenario 1. The eavesdropper is far from the user station and increasing the jamming power reduces the throughput gap and secrecy capacity. a) all experimental and simulation results; the right-hand y-axis is scaled by WLSQ1. b) experimental throughput gap and simulation-based secrecy capacity; the right-hand y-axis is scaled by WLSQ2. c) min-max normalization of the experimental throughput gap and simulation-based secrecy capacity.

jamming power points on the x-axis, and $d\theta_t$ is the difference between the average captured throughputs. ω_t is the inverse of the standard deviation in the captured throughputs, and C_t is the secrecy capacity obtained from the simulation. This scaling assumes complete proportionality between secrecy capacity and the difference in average throughputs at all times.

Figure 8 to 11 (b), in the center, show the difference between the two average throughputs and the secrecy capacity obtained from the simulation, but the latter now scaled using a different WSLQ routine, namely the MATLAB *lscov* function, which we refer to in the plots as WSLQ2. We scale the right-hand side y-axis by $L_{RY} = (L_{LY} - \nu)/\mu$ where μ and ν are obtained by $\arg\min_{\mu,\nu} \sum_{t=1}^{n} \omega_t |d\theta_t - \mu C_t - \nu|^2$. This routine provides a (for the eye) better fit than WSLQ1, but with both y-axes having different origins. It allows for some level of disproportionality between secrecy capacity and the difference in average throughputs, which is still in line with the findings in [33].

It is important to note that when increasing the jamming power of AP_2, the received power of jamming at the AP_1 will eventually approach the CCA threshold of -62 dBm. Since the channel is non-deterministic and subject to random fluctuations, each frame may be received with a different SNR. Fortunately, Wireshark can record the signal strength of each Wi-Fi frame for the selected hardware in this experiment. So, we measured the received signal strength at AP_1 for different levels of jamming power to obtain the empirical cumulative distribution function (CDF). This is visualized as a blue shading in Figure 8 to 11 (a) and (b). Also, a vertical dashed line is plotted where the average received signal strength of the jamming signal is greater than or equal to the CCA threshold. We have not calculated the secrecy capacity for jamming powers greater than (on

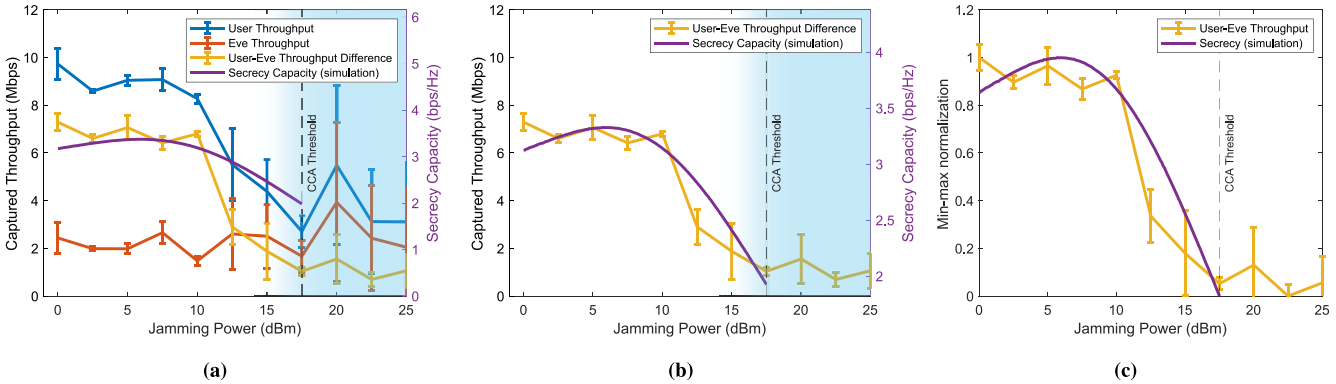


FIGURE 9. Results for scenario 2. Both experiment and simulation show the most effective range of 3-10 dBm of jamming power. a) all experimental and simulation results; the right-hand y-axis is scaled by WLSQ1. b) experimental throughput gap and simulation-based secrecy capacity; the right-hand y-axis is scaled by WLSQ2. c) min-max normalization of the experimental throughput gap and simulation-based secrecy capacity.

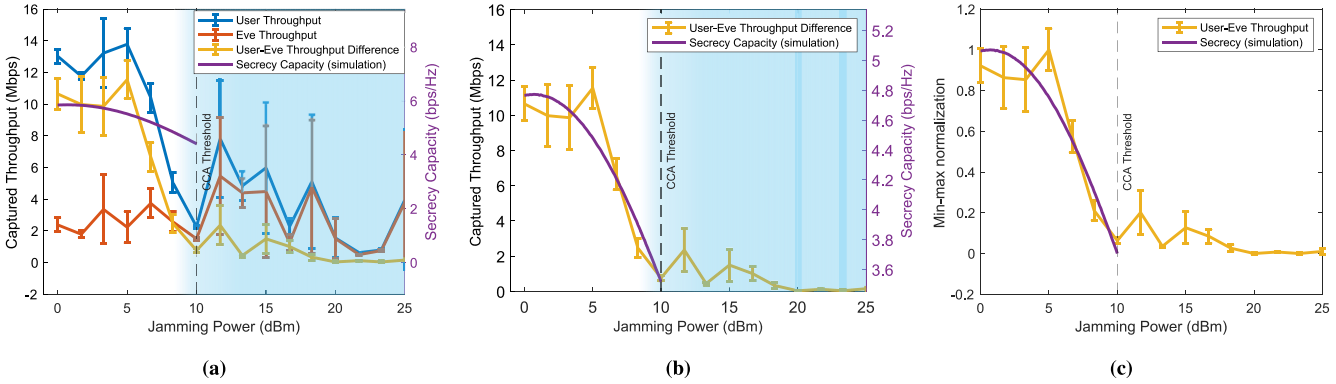


FIGURE 10. Results for scenario 3. Both experiment and simulation show the most effective range of 0-4 dBm of jamming power. a) all experimental and simulation results; the right-hand y-axis is scaled by WLSQ1. b) experimental throughput gap and simulation-based secrecy capacity; the right-hand y-axis is scaled by WLSQ2. c) min-max normalization of the experimental throughput gap and simulation-based secrecy capacity.

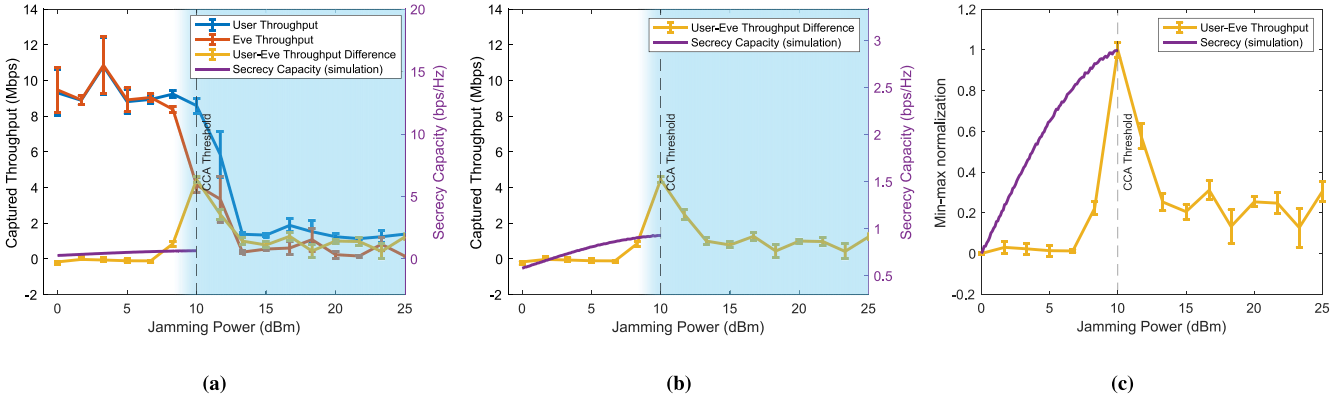


FIGURE 11. Results for scenario 4. Where the user station and eavesdropper are equidistant from the AP_1, a jamming power of less than 5 dBm allows the eavesdropper to capture all user traffic. But, increasing the jamming power results in a better throughput gap and secrecy capacity, subject to the limitation of the CCA threshold. a) all experimental and simulation results; the right-hand y-axis is scaled by WLSQ1. b) experimental throughput gap and simulation-based secrecy capacity; the right-hand y-axis is scaled by WLSQ2. c) min-max normalization of the experimental throughput gap and simulation-based secrecy capacity.

the right-hand side of) the CCA threshold because, in theory, AP_1 stops transmitting when AP_2 keeps the channel busy and a continuous jamming signal stronger than CCA threshold is received at AP_1. Said otherwise, in that regime our theory is not applicable. However, in the experiments, the jamming frames are not continuous signals and we show the throughput results for better understanding. The effect of jammer on the transmitter can be observed on the left side of the CCA line when the throughput drops sharply.

Figure 8 to 11 (a) show that, in most scenarios, increasing the jamming power affects both the user and eavesdropper and reduces the throughput on both stations. This is in line with the results of the simulations presented in Section V

that show the optimal jamming power is typically around 0-5 dBm. Additionally, when the jamming power exceeds the CCA threshold at the AP_1, AP_1 stops transmitting data frames, resulting in a low difference between the user and eavesdropper throughputs. This causes the graphs to fluctuate or have relatively large error bars in the shaded area.

Figure 8 to 11 (c), on the right-hand side, show the Min-Max normalization of the difference between the average throughputs of the legitimate user and eavesdropper as well as the secrecy capacity obtained from the simulations. This is a visualization of the trend in both graphs and can show for what FJ transmit power the maximum capacity or throughput difference can be achieved.

In scenario 4, we placed the user and eavesdropper stations at the same distance from AP_1. This means the eavesdropper has the same chance to successfully capture legitimate traffic as the legitimate user, with the same channel conditions in the absence of jamming. Thus, it is observed in Figure 11 that, initially, for low jamming power, the eavesdropper can capture nearly all packets that are destined for the user station. Therefore, the optimal jamming power is higher than that in the other scenarios. Both simulated secrecy capacity and experimental throughput show an optimum jamming power of about 10 dBm. Note that a negligible negative throughput *difference* means that the eavesdropper had a slightly better channel during the test. The individual user or eavesdropper throughputs are always positive.

VIII. CONCLUSION AND FUTURE WORK

In this paper, we showed how a coordinated PLS-aware Wi-Fi network can significantly improve the secrecy of the system and reduce the eavesdropping capability in the coverage area, thanks to the optimized generation of FJ by an idle AP (or an AP with multiple radios). Although we do not directly measure the theoretical concept of secrecy capacity, the system can create such a large difference between throughput obtained by users versus potential eavesdroppers, that relatively simple additional coding in the physical or higher layers is able to achieve perfect security of the Wi-Fi network in the physical layer. Furthermore, we showed that commercial off-the-shelf APs can act as jammers in the network to achieve secrecy without having to violate the standard. This realizes a cost-effective solution as no standard modification is required and existing devices in the market are compatible with this framework. Finally, the paper shows that the proposed jamming optimization is effective and matches with experimental results even though a simple free-space propagation model is used for theoretical derivations.

In order to obtain a tractable theoretical optimization framework and demonstrate the proof of concept, a small network of two APs, one user, and one eavesdropper was studied in this paper. However, most networks in the real world are much larger. While the theoretical approach is conceptually extensible to larger networks, it is unclear whether closed-form optimal solutions can be obtained. Therefore, a more complex optimization approach was employed in our recent work [14] to find the best jamming power and tune the APs' transmit powers. Reference [14] stops at the simulation level and large-scale experiments to verify the results in real-world are left as future work. Moreover, the novel idea of using Wi-Fi APs as jammers can be improved further to create a more continuous jamming stream over the air without necessarily having a dedicated sink. The jamming setup used in this work relied on normal Wi-Fi traffic to generate a jamming signal. Nevertheless, this implementation is not perfect as it cannot keep the channel constantly busy. Therefore, some modifications to the software and hardware are necessary. This is achievable by driver enhancement in the AP operating system and more intelligent programming of the spectrum by more advanced utilization of our wireless SDN architecture.

REFERENCES

[1] I. Dacosta, S. Chakradeo, M. Ahamad, and P. Traynor, "One-time cookies: Preventing session hijacking attacks with stateless authentication tokens," *ACM Trans. Internet Technol.*, vol. 12, no. 1, pp. 1–24, 2012.

[2] D. J. Fehér and B. Sandor, "Effects of the WPA2 KRACK attack in real environment," in *Proc. IEEE 16th Int. Symp. Intell. Syst. Inform. (SISY)*, 2018, pp. 000239–000242.

[3] N. Sayfayn and S. Madnick, "Cybersafety analysis of the maroochy shire sewage spill (preliminary draft)," Cybersecurity Interdisciplinary Systems Laboratory (CISL), Massachusetts Institute of Technology, Cambridge, MA, USA, Working Paper, 2017.

[4] A. D. Wyner, "The wire-tap channel," *Bell Syst. Tech. J.*, vol. 54, no. 8, pp. 1355–1387, 1975.

[5] C. E. Shannon, "Communication theory of secrecy systems," *Bell Syst. Tech. J.*, vol. 28, no. 4, pp. 656–715, 1949.

[6] K. S. Ryland, "Software-defined radio implementation of two physical layer security techniques," Ph.D. dissertation, Dept. Electr. Eng., Virginia Tech, Blacksburg, VA, USA, 2018.

[7] S. A. Hoseini, F. Bouhafs, and F. den Hartog, "A practical implementation of physical layer security in wireless networks," in *Proc. IEEE 19th Annu. Consum. Commun. Netw. Conf. (CCNC)*, 2022, pp. 1–4.

[8] S. A. Hoseini, F. den Hartog, and F. Bouhafs, "Realizing physical layer security with common off-the-shelf WiFi equipment," in *Proc. IEEE 20th Consum. Commun. Netw. Conf. (CCNC)*, 2023, pp. 935–936.

[9] F. Bouhafs et al., "Wi-5: A programming architecture for unlicensed frequency bands," *IEEE Commun. Mag.*, vol. 56, no. 12, pp. 178–185, Dec. 2018.

[10] F. Bouhafs, F. den Hartog, A. Raschella, M. Mackay, Q. Shi, and S. Sinanovic, "Realizing physical layer security in large wireless networks using spectrum programmability," in *Proc. IEEE Glob. Telecommun. Conf. (Globcom) Workshops*, 2020, pp. 1–6.

[11] S. A. Hoseini, P. Sadeghi, F. Bouhafs, N. Aboutorab, and F. D. Hartog, "Network-controlled physical-layer security: Enhancing secrecy through friendly jamming," in *Proc. 27th IEEE Symp. Comput. Commun. (ISCC)*, 2022, pp. 1–7.

[12] J. P. Vilela, M. Bloch, J. Barros, and S. W. McLaughlin, "Wireless secrecy regions with friendly jamming," *IEEE Trans. Inf. Forensics Security*, vol. 6, pp. 256–266, 2011.

[13] M. L. Jorgensen, B. R. Yanakiev, G. E. Kirkelund, P. Popovski, H. Yomo, and T. Larsen, "Shout to secure: Physical-layer wireless security with known interference," in *Proc. IEEE Glob. Telecommun. Conf. (Globcom)*, 2007, pp. 33–38.

[14] S. A. Hoseini, F. Bouhafs, N. Aboutorab, P. Sadeghi, and F. d. Hartog, "Cooperative jamming for physical layer security enhancement using deep reinforcement learning," in *Proc. IEEE Glob. Telecommun. Conf. (Globcom) Workshops*, 2023, pp. 1838–1843.

[15] W. K. Harrison, J. Almeida, M. R. Bloch, S. W. McLaughlin, and J. Barros, "Coding for secrecy: An overview of error-control coding techniques for physical-layer security," *IEEE Signal Process. Mag.*, vol. 30, no. 5, pp. 41–50, Sep. 2013.
[16] W. K. Harrison and S. W. McLaughlin, "Physical-layer security: Combining error control coding and cryptography," in *Proc. IEEE Int. Conf. Commun.*, 2009, pp. 1–5.
[17] C. Sperandio and P. G. Flikkema, "Wireless physical-layer security via transmit precoding over dispersive channels: Optimum linear eavesdropping," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, vol. 2, 2002, pp. 1113–1117.
[18] X. Li and E. P. Ratazzi, "MIMO transmissions with information-theoretic secrecy for secret-key agreement in wireless networks," in *Proc. IEEE Mil. Commun. Conf. (MILCOM)*, 2005, pp. 1353–1359.
[19] X. Chen, D. W. K. Ng, W. H. Gerstacker, and H.-H. Chen, "A survey on multiple-antenna techniques for physical layer security," *IEEE Commun. Surveys Tuts.*, vol. 19, no. 2, pp. 1027–1053, 2nd Quart., 2017.
[20] S. Liu, Y. Hong, and E. Viterbo, "Practical secrecy using artificial noise," *IEEE Commun. Lett.*, vol. 17, no. 7, pp. 1483–1486, Jul. 2013.
[21] P.-H. Lin, S.-H. Lai, S.-C. Lin, and H.-J. Su, "On secrecy rate of the generalized artificial-noise assisted secure beamforming for wiretap channels," *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1728–1740, Sep. 2013.
[22] S.-H. Tsai and H. V. Poor, "Power allocation for artificial-noise secure MIMO precoding systems," *IEEE Trans. Signal Process.*, vol. 62, no. 13, pp. 3479–3493, Jul. 2014.
[23] X. Zhang, X. Zhou, and M. R. McKay, "On the design of artificial-noise-aided secure multi-antenna transmission in slow fading channels," *IEEE Trans. Veh. Technol.*, vol. 62, no. 5, pp. 2170–2181, Jun. 2013.
[24] S. Hong, C. Pan, H. Ren, K. Wang, and A. Nallanathan, "Artificial-noise-aided secure MIMO wireless communications via intelligent reflecting surface," *IEEE Trans. Commun.*, vol. 68, no. 12, pp. 7851–7866, Dec. 2020.
[25] C. Gong, X. Yue, Z. Zhang, X. Wang, and X. Dai, "Enhancing physical layer security with artificial noise in large-scale NOMA networks," *IEEE Trans. Veh. Technol.*, vol. 70, no. 3, pp. 2349–2361, Mar. 2021.
[26] A. Chaman, J. Wang, J. Sun, H. Hassanieh, and R. Roy Choudhury, "Ghostbuster: Detecting the presence of hidden eavesdroppers," in *Proc. 24th Annu. Int. Conf. Mobile Comput. Netw.*, 2018, pp. 337–351.
[27] A. Goldsmith, *Wireless Communications*. Cambridge, U.K.: Cambridge Univ. Press, 2005.
[28] H. V. Poor and R. F. Schaefer, "Wireless physical layer security," *Proc. Nat. Acad. Sci.*, vol. 114, no. 1, pp. 19–26, 2017.
[29] *IEEE Standard for Information Technology—Local and Metropolitan Area Networks—Specific Requirements– Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications: Further Higher Data Rate Extension in the 2.4 GHz Band*, IEEE Standard 802.11g-2003 (Amendment to IEEE Std 802.11, 1999 Edn. (Reaff 2003) as amended by IEEE Standards 802.11a-1999, 802.11b-1999, 802.11b-1999/Cor 1-2001, 802.11d-2001), 2003, pp. 1–104.
[30] *IEEE Standard for Information Technology–telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks–Specific Requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Enhancements for High-Efficiency WLAN*, IEEE Standard 802.11ax-2021 (Amendment to IEEE Standard 802.11-2020), 2021, pp. 1–767.
[31] S. Zhu et al., "Probability distribution of Rician *K*-factor in urban, suburban and rural areas using real-world captured data," *IEEE Trans. Antennas Propag.*, vol. 62, no. 7, pp. 3835–3839, Jul. 2014.
[32] E. G. Villegas, E. Lopez-Aguilera, R. Vidal, and J. Paradells, "Effect of adjacent-channel interference in IEEE 802.11 WLANs," in *Proc. 2nd Int. Conf. Cogn. Radio Oriented Wireless Netw. Commun.*, 2007, pp. 118–125.
[33] R. Ranji, U. Javed, B. Boltjes, F. Bouhafs, and F. den Hartog, "Optimizing wireless network throughput under the condition of physical layer security using software-defined networking enabled collaboration," in *Proc. IEEE 20th Consum. Commun. Netw. Conf. (CCNC)*, 2023, pp. 1–6.

SAYED AMIR HOSEINI (Member, IEEE) received the B.Sc. degree in electronic engineering from the Isfahan University of Technology, Iran, in 2008, the M.Sc. degree in electronics and communication engineering from the Amirkabir University of Technology (Tehran Polytechnic), Iran, in 2011, and the Ph.D. degree in computer science and engineering from the University of New South Wales in 2017. He is an Associate Lecturer with the School of Systems and Computing, The University of New South Wales (Canberra). His research interests includes wireless communications, beyond 5G, and physical layer security.

PARASTOO SADEGHI (Senior Member, IEEE) received the bachelor's and master's degrees in electrical engineering from the Sharif University of Technology, Tehran, Iran, in 1995 and 1997, respectively, and the Ph.D. degree in electrical engineering from the University of New South Wales (UNSW) Sydney, in 2006.

She is currently a Professor with the School of Engineering and Technology, UNSW Canberra. She has coauthored around 200 refereed journal articles and conference papers. Her research interests include information theory, communications theory, data privacy, index coding, and network coding. From 2016 to 2019, she served as an Associate Editor for the IEEE TRANSACTIONS ON INFORMATION THEORY. In 2022, she was selected as a Distinguished Lecturer of the IEEE Information Theory Society.

FAYCAL BOUHAFS (Senior Member, IEEE) received the Ph.D. degree in computer science from Liverpool John Moores University, U.K. He is a Senior Lecturer with the School of Systems and Computing, The University of New South Wales Canberra. Before, he served as an Assistant Professor of Wireless Communications and Networking. Since 2015, he acted as a Technical Lead for H2020 Project Wi-5. His research interests revolve around spectrum congestion, radio resource management, and beyond 5G communications and architecture.

NEDA ABOUTORAB (Senior Member, IEEE) received the Ph.D. degree in electrical engineering from the University of Sydney, Australia, in 2012. She is currently an Associate Professor with the School of Engineering and Technology, The University of New South Wales, Canberra, Australia. From 2012 to 2015 and before joining the University of New South Wales, she was a Postdoctoral Research Fellow with the Research School of Engineering, The Australian National University. Her research interests include index coding, network coding, wireless communications, and physical layer security.

FRANK DEN HARTOG (Senior Member, IEEE) received the M.Sc. degree from the Eindhoven University of Technology and the Ph.D. degree in physics from Leiden University. He is a Professor with the University of Canberra, Australia, where he holds the Cisco Research Chair of Critical Infrastructure. He is also an Adjunct Fellow with The University of New South Wales in Canberra. He specializes in complex wireless networked systems research and analysis, with a particular interest in the Internet of Things and cyber-physical systems. From 2003 to 2016, he was a Senior Scientist with the Netherlands Organisation for Applied Scientific Research TNO and studied Future Internet architectures and heterogeneous consumer networking. Before joining TNO, he worked for the Dutch incumbent telecommunications operator KPN, where he pioneered the home networking and IoT research area.