


Article

Adversarial Machine Learning for NextG Covert Communications Using Multiple Antennas

Brian Kim ¹, Yalin Sagduyu ² , Kemal Davaslioglu ³, Tugba Erpek ² and Sennur Ulukus ^{1,*}

¹ Department of Electrical and Computer Engineering, University of Maryland, College Park, MD 20742, USA; bkim628@umd.edu

² Virginia Tech, National Security Institute, Arlington, VA 24061, USA; ysagduyu@vt.edu (Y.S.); terpek@vt.edu (T.E.)

³ University Technical Services, Greenbelt, MD 20770, USA; kemal@ut-services.com

* Correspondence: ulukus@umd.edu

Abstract: This paper studies the privacy of wireless communications from an eavesdropper that employs a deep learning (DL) classifier to detect transmissions of interest. There exists one transmitter that transmits to its receiver in the presence of an eavesdropper. In the meantime, a cooperative jammer (CJ) with multiple antennas transmits carefully crafted adversarial perturbations over the air to fool the eavesdropper into classifying the received superposition of signals as noise. While generating the adversarial perturbation at the CJ, multiple antennas are utilized to improve the attack performance in terms of fooling the eavesdropper. Two main points are considered while exploiting the multiple antennas at the adversary, namely the power allocation among antennas and the utilization of channel diversity. To limit the impact on the bit error rate (BER) at the receiver, the CJ puts an upper bound on the strength of the perturbation signal. Performance results show that this adversarial perturbation causes the eavesdropper to misclassify the received signals as noise with a high probability while increasing the BER at the legitimate receiver only slightly. Furthermore, the adversarial perturbation is shown to become more effective when multiple antennas are utilized.

Keywords: deep learning; covert communications; signal classification; adversarial attack



Citation: Kim, B.; Sagduyu, Y.; Davaslioglu, K.; Erpek, T.; Ulukus, S. Adversarial Machine Learning for NextG Covert Communications Using Multiple Antennas. *Entropy* **2022**, *24*, 1047. <https://doi.org/10.3390/e24081047>

Academic Editor: Vaneet Aggarwal

Received: 8 June 2022

Accepted: 27 July 2022

Published: 29 July 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Copyright: © 2022 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Privacy is a fundamental problem in wireless communications due to the open and shared nature of wireless medium. An eavesdropper may overhear the communications intended between a transmitter and a receiver. The eavesdropper may pursue different objectives such as decoding transmissions or detecting whether there is an ongoing transmission, or not (e.g., for launching follow-up jamming attacks). The privacy of information regarding unapproved decoding has been extensively studied from both encryption-based security and information theory perspectives [1,2]. In this paper, we consider an eavesdropper that pursues the second objective, namely detecting an ongoing transmission for future adversarial purposes such as jamming to degrade the quality of communications.

Covert communications has been studied to hide information in noise where the main goal has been to reduce the signal-to-noise ratio (SNR) at the eavesdropper [3,4]. A fundamental bound has been demonstrated on the total transmit power over a given number of channel users while maintaining covert communications, generally known as the square-root law [5]; see also [6] for related work. In this paper, we study covert communications from an *adversarial machine learning* (AML) point of view. Overall, AML is an emerging field that studies machine learning (ML) in the presence of adversaries that may aim to manipulate the test and/or training pipelines of ML algorithms [7–9]. While the applications of AML have originated in the computer vision domain, there has been a growing interest in applying AML to wireless communications [10–12], including exploratory (inference) attacks [13,14], evasion (adversarial) attacks [15–33] and their extensions to secure and covert

communications against eavesdroppers [34–37], causative (poisoning) attacks [38–40], membership inference attacks [41,42], Trojan attacks [43], and spoofing attacks [44–47].

We consider an eavesdropper with a deep learning (DL)-based classifier to detect an ongoing transmission where this classifier achieves a high accuracy for distinguishing the received signals from noise. We introduce a *cooperative jammer* (CJ) that has been extensively used in the physical layer security literature [48–50]. In this paper, the CJ transmits signals over the air at the same time as the transmitter with the purpose of fooling the eavesdropper's classifier for covert communications. These signals from CJ corresponds to an evasion attack (or adversarial attack) in AML where evasion attacks have been used to manipulate wireless signal classification (in particular, modulation classification) [15–28], spectrum sensing [29], autoencoder communications [30], initial access [31], channel estimation [32], and power control [33]. In this paper, adversarial attack is used as a means of covert communications to prevent an eavesdropper from distinguishing an ongoing transmission from noise.

We use the CJ as the source of adversarial perturbation to manipulate the classifier at an eavesdropper into making classification errors. While a perturbation with high power level transmitted by the CJ can easily fool the classifier, it would also increase the interference and the bit error rate (BER) at the intended receiver to an unacceptable level. Therefore, an upper bound on the perturbation strength is imposed. A special case of our setting has been considered in [34], where the transmitter with a single antenna adds perturbations to its own signals to fool an eavesdropper with a modulation classifier while aiming to maintain its own communication performance. In this paper, our focus is on covert communications aided by a CJ, whose position can further boost the impact on the eavesdropper to classify received signal as noise while reducing the impact on the BER performance. Note that we only consider fooling a classifier into misclassifying a signal as noise since it is typically more demanding. Further, we extend the analysis to the use of *multiple antennas* at the CJ to generate multiple concurrent perturbations over different channel effects (subject to a total power budget) for better covert communications. This problem setting is different from computer vision applications of adversarial attacks that are limited to a single perturbation that is directly added to the input of a deep neural network (DNN). We assume that the CJ has multiple antennas to transmit adversarial perturbations against the eavesdropper and aims to decrease the probability of detection at the eavesdropper.

In this paper, we design a white-box attack at the CJ where the signal of the CJ is time-aligned with the transmitted signal and uses the maximum received perturbation power (MRPP) attack that was introduced in [20]. We propose different methods to allocate power among antennas at the CJ and to exploit the channel diversity. We first propose a genie-aided adversarial attack where the CJ selects one antenna to transmit the perturbation such that it would result in the worst classification performance depending on the channel condition over the entire symbol block (that corresponds to the input to the DNN at the receiver). Then, we consider transmitting with all the antennas at the adversary where the power allocation is based on the channel gains, either proportional or inversely proportional to the channel gains. Finally, we propose the elementwise maximum channel gain (EMCG) attack to utilize the channel diversity more efficiently by selecting the antenna with the best channel gain at the symbol level to transmit perturbations.

For the performance evaluation, we first consider a CJ with a single antenna using basic modulated signals (e.g., QPSK and 16-QAM), and then extend the setting to a more complicated 5G communication signal. Our results show that we can effectively hide these signals from an eavesdropper that uses a DL-based classifier to detect transmissions. Then, we use multiple antennas at the CJ to investigate the performance of multiple concurrent perturbations over different channel effects on the eavesdropper's classifier.

During simulations, the perturbation of the CJ is selected to minimize the strength of the perturbation subject to the condition of successfully fooling the eavesdropper and an upper bound on the perturbation power that can translate to limiting the BER at the receiver.

We show that Gaussian noise is not effective as an adversarial perturbation and develop an algorithm to optimize the perturbations for the CJ to enable covert communications, which we demonstrate for signals with different modulation types and 5G communications. Furthermore, we show that the EMCG attack outperforms other attacks and effectively uses the channel diversity provided by multiple antennas to cause misclassification at the receiver. This attack improvement remains effective regardless of the channel variance or correlation between channels, whereas the proportional to the channel gain (PCG) attack is greatly affected by the correlation between channels. Finally, we show that increasing the number of antennas at the adversary significantly improves the attack performance by better exploiting the channel diversity to craft and transmit adversarial perturbations.

In summary, our contributions are given as follows:

- We present how a CJ is used to make wireless communications covert by transmitting adversarial attack against the classifier of the eavesdropper.
- For a CJ equipped with multiple antennas, we investigate the use of multiple antennas to generate multiple concurrent perturbations over different channel effects against the eavesdropper. Furthermore, we propose different methods to utilize the channel diversity.
- With simulations, we show that the CJ can generate perturbation signals that cause misclassification at the eavesdropper for both basic modulated signals and sophisticated 5G signals, while the BER at the receiver is slightly affected.

The rest of the paper is organized as follows. Section 2 describes the system model. Section 3 presents the white-box adversarial attacks when the CJ has one antenna. Section 4 introduces different methods to generate adversarial attacks when the CJ has multiple antennas. Section 5 presents the performance evaluation results. Section 6 concludes the paper.

2. System Model

We consider a wireless system that consists of a transmitter, a receiver, a CJ, and an eavesdropper as shown in Figure 1. The transmitter sends p complex symbols consecutively in time, $\mathbf{x} \in \mathbb{C}^p$, by mapping a binary input sequence $\mathbf{m} \in \{0, 1\}^l$. Specifically, $\mathbf{x} = g_s(\mathbf{m})$, where $g_s : \{0, 1\}^l \rightarrow \mathbb{C}^p$ and s represents the modulation type of the transmitter. Then, the transmitter's signal received at node j (either the receiver r or the eavesdropper e) is given by

$$\mathbf{r}_{tj} = \mathbf{H}_{tj}g_s(\mathbf{m}) + \mathbf{n}_{tj} = \mathbf{H}_{tj}\mathbf{x} + \mathbf{n}_{tj}, \quad j \in \{r, e\}, \quad (1)$$

where $\mathbf{H}_{tj} = \text{diag}\{h_{tj,1}, \dots, h_{tj,p}\} \in \mathbb{C}^{p \times p}$ and $\mathbf{n}_{tj} \in \mathbb{C}^p$ are the channel and complex Gaussian noise from the transmitter to node j , respectively. Upon receiving the signal \mathbf{r}_{tr} , the receiver decodes the message with the BER given by

$$P_e(\mathbf{m}, \mathbf{r}_{tr}) = \frac{1}{l} \sum_{i=1}^l \mathbb{I}\{m_i \neq \hat{m}_i\}, \quad (2)$$

where \hat{m}_i is a decoded bit and $\mathbb{I}\{\cdot\}$ is an indicator function.

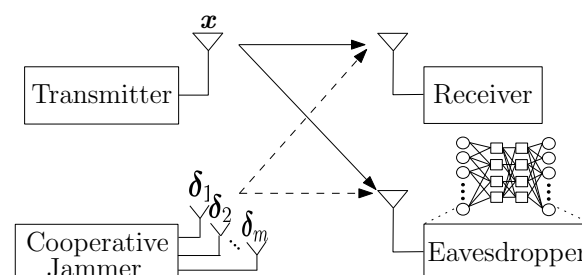


Figure 1. System model.

The eavesdropper tries to detect the existence of wireless transmission using a pre-trained DL-based classifier, namely a DNN, $f(\cdot, \theta) : \mathcal{X} \rightarrow \mathbb{R}^2$, where θ is the set of DNN parameters and $\mathcal{X} \subset \mathbb{C}^p$. An input $x \in \mathcal{X}$ is assigned a label $\hat{l}(x, \theta) = \arg \max_k f_k(x, \theta)$, where $f_k(x, \theta)$ is the output of a classifier f corresponding to the k th class.

To make communications between the transmitter and its receiver covert, the CJ with q antennas transmits perturbation signals $\delta_1, \delta_2, \dots, \delta_q \in \mathbb{C}^p$, where the i th antenna transmits δ_i , to cause misclassification at the eavesdropper by changing the label of the received signal r_{te} from *signal* to *noise*. Thus, if the transmitter transmits x , the received signal at node j is given by

$$r'_{tj}(\delta_1, \dots, \delta_q) = \mathbf{H}_{tj}x + \sum_{i=1}^q \mathbf{H}_{cij}\delta_i + n_{tj}, \quad j \in \{r, e\}, \quad (3)$$

where $\mathbf{H}_{cij} = \text{diag}\{h_{cij,1}, \dots, h_{cij,p}\} \in \mathbb{C}^{p \times p}$ is the channel from the i th antenna of the CJ to node j .

Since the perturbation signals from the CJ not only creates interference at the eavesdropper, but also at the receiver, the CJ determines its signals $\delta_1, \delta_2, \dots, \delta_q$ to cause misclassification at the eavesdropper using a fixed power budget P_{max} that also limits the BER at the receiver. Formally, the CJ first determines $\delta_1, \delta_2, \dots, \delta_q$ by solving the following optimization problem:

$$\begin{aligned} \arg \min_{\delta_i} \quad & \sum_{i=1}^q \|\delta_i\|_2^2 \\ \text{s.t.} \quad & \hat{l}(r_{te}, \theta) \neq \hat{l}(r'_{te}(\delta_1, \dots, \delta_q), \theta) \\ & \sum_{i=1}^q \|\delta_i\|_2^2 \leq P_{max}. \end{aligned} \quad (4)$$

The solution δ_i^* to (4) results in a BER, $P_e(\mathbf{m}, r'_{tr}(\delta_i^*))$, at the receiver that can be bounded to a target level by selecting P_{max} accordingly. Since solving (4) is difficult, different methods have been proposed in computer vision to approximate the adversarial perturbations such as the fast gradient method (FGM) [7]. The FGM is computationally efficient for crafting adversarial attacks by linearizing the loss function, $L(\theta, x, y)$, of the DNN classifier in a neighborhood of x where y is the label vector. This linearized function is used for optimization. In this paper, we consider a *targeted attack*, where the perturbation of the CJ aims to decrease the loss function of the label *noise* and cause a specific misclassification, from *signal* to *noise*, at the eavesdropper even though there is an actual transmission. We approach the problem from an AML point of view and aim to fool a target classifier, which is equivalent to hiding communications in noise from a wireless communications perspective. While designing the perturbation, we constrain the BER at the receiver to stay below a certain level while satisfying the power constraint at the CJ, as stated in the constraints of the optimization problem (4). We assume that the CJ collaborates with the transmitter and thus knows the transmitted signal from the transmitter.

3. Adversarial Perturbation for the CJ

In this section, we design the white-box perturbation for the CJ using a targeted FGM to solve (4). We first assume that the CJ has one antenna, $q = 1$. We will relax the assumption in Section 4. For the targeted attack, the CJ minimizes $L(\theta, r'_{te}(\delta), y^{target})$ with respect to δ where y^{target} is the one-hot-encoded desired target class. We fix y^{target} as *noise* label since the CJ always tries to add perturbation to fool the eavesdropper into misclassifying a received signal as noise. We use FGM to linearize the loss function as $L(\theta, r'_{te}(\delta), y^{target}) \approx L(\theta, r_{te}, y^{target}) + (\mathbf{H}_{ce}\delta)^T \nabla_x L(\theta, r_{te}, y^{target})$ and then minimize it by setting $\mathbf{H}_{ce}\delta = -\alpha \nabla_x L(\theta, r_{te}, y^{target})$, where α is a scaling factor to constrain the adversarial perturbation power to P_{max} . The details of determining the CJ's perturbation

signal are presented in Algorithm 1. After we obtain the δ that causes misclassification at the eavesdropper and satisfies the power constraint, we check the BER at the receiver. The perturbation power can further be adjusted to meet a target BER level. Specifically, if the BER level at the receiver is more important than fooling the eavesdropper, we can decrease the adversarial perturbation power. On the other hand, if fooling the eavesdropper is the priority, we can increase the adversarial perturbation power.

Algorithm 1: Generating the perturbation of the CJ

Inputs: input \mathbf{r}_{te} , desired accuracy ε_{acc} , power constraint P_{max} , and $L(\boldsymbol{\theta}, \cdot, \cdot)$.

Initialize: $\varepsilon \leftarrow 0, \varepsilon_{max} \leftarrow \sqrt{P_{max}}, \varepsilon_{min} \leftarrow 0$.

$$\boldsymbol{\delta}_{norm} = \frac{\nabla_{\mathbf{x}} L(\boldsymbol{\theta}, \mathbf{r}_{te}, \mathbf{y}^{target})}{(\|\nabla_{\mathbf{x}} L(\boldsymbol{\theta}, \mathbf{r}_{te}, \mathbf{y}^{target})\|_2)}.$$

while $\varepsilon_{max} - \varepsilon_{min} > \varepsilon_{acc}$ **do**

$$\varepsilon_{avg} \leftarrow (\varepsilon_{max} + \varepsilon_{min})/2$$

$$\mathbf{x}_{adv} \leftarrow \mathbf{r}_{te} - \varepsilon_{avg} \boldsymbol{\delta}_{norm}$$

if $\hat{l}(\mathbf{x}_{adv}) == \text{noise}$ **then** $\varepsilon_{min} \leftarrow \varepsilon_{avg}$

else $\varepsilon_{max} \leftarrow \varepsilon_{avg}$

end

$$\varepsilon^* = \varepsilon_{max}, \boldsymbol{\delta}^{jam} = -\varepsilon^* \boldsymbol{\delta}_{norm}$$

4. Adversarial Perturbations Using Multiple Antennas at the CJ

In this section, we present different methods to utilize q antennas at the CJ to improve the performance of the adversarial attack against the eavesdropper. Note that the adversary can allocate power differently to each antenna and increase the channel diversity by using multiple antennas. In this paper, we apply the targeted MRPP attack in [20], which has been developed from the attack in [15] by accounting for additional channel effects.

4.1. Single-Antenna Genie-Aided (SAGA) Attack

We first begin with an attack where the CJ allocates all the power to only one antenna for the entire symbol block of an input to the classifier at the eavesdropper as shown in Figure 2a. In this attack, we assume that the CJ is aided by a genie and thus knows in advance the best antenna out of q antennas that causes a misclassification. Then, the genie-aided CJ puts all the power to that one specific antenna to transmit the adversarial perturbation against the eavesdropper.

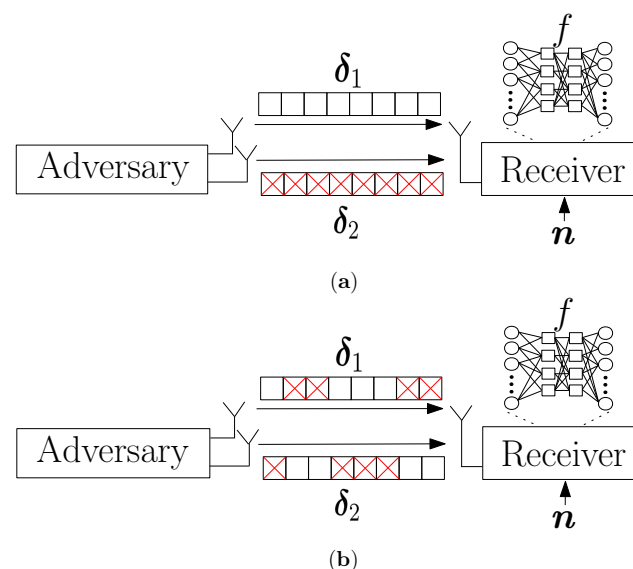


Figure 2. Illustration of (a) SAGA attack and (b) EMCG attack.

4.2. Proportional to Channel Gain (PCG) Attack

To exploit the channel with the better channel gain, the CJ allocates more power to better channels. Specifically, the power allocation for the i th antenna is proportional to the channel gain $\|\mathbf{h}_{c_{ie}}\|_2$, where $\mathbf{h}_{c_{ie}} = [h_{c_{ie},1}, \dots, h_{c_{ie},p}]^T$, using weight $w_i = \frac{\|\mathbf{h}_{c_{ie}}\|_2}{\sum_{j=1}^q \|\mathbf{h}_{c_{je}}\|_2}$, $i = 1, \dots, q$. The adversarial perturbation that is transmitted by each antenna is generated using the MRPP attack as before and transmitted with the power allocated to each antenna. The detailed algorithm is presented in Algorithm 2.

Algorithm 2: PCG attack

Inputs: input \mathbf{r}_{te} , desired accuracy ε_{acc} , power constraint P_{max} , and model of the classifier $L(\boldsymbol{\theta}, \cdot, \cdot)$.

Initialize: $w_i = \frac{\|\mathbf{h}_{c_{ie}}\|_2}{\sum_{j=1}^q \|\mathbf{h}_{c_{je}}\|_2}$, $i = 1, \dots, q$.

$\varepsilon_{max} \leftarrow \sqrt{P_{max}}$, $\varepsilon_{min} \leftarrow 0$.

for $i = 1$ **to** q **do**

$\delta_i = \frac{\mathbf{H}_{c_{ie}}^* \nabla_{\mathbf{x}} L(\boldsymbol{\theta}, \mathbf{r}_{te}, \mathbf{y}^{target})}{(\|\mathbf{H}_{c_{ie}}^* \nabla_{\mathbf{x}} L(\boldsymbol{\theta}, \mathbf{r}_{te}, \mathbf{y}^{target})\|_2)}$

end

while $\varepsilon_{max} - \varepsilon_{min} > \varepsilon_{acc}$ **do**

$\varepsilon_{avg} \leftarrow (\varepsilon_{max} + \varepsilon_{min})/2$

$\mathbf{x}_{adv} \leftarrow \mathbf{x} - \varepsilon_{avg} \sum_{i=1}^q w_i \mathbf{H}_{c_{ie}} \delta_i$

if $\hat{l}(\mathbf{x}_{adv}) == \text{noise}$ **then** $\varepsilon_{min} \leftarrow \varepsilon_{avg}$

else $\varepsilon_{max} \leftarrow \varepsilon_{avg}$

end

$\varepsilon^* = \varepsilon_{max}$

$\delta_i = w_i \varepsilon^* \delta_i$ for $\forall i$

4.3. Inversely Proportional to Channel Gain (IPCG) Attack

In contrast to the PCG attack, the CJ allocates more power to weak channels to compensate for the loss over the weak channels, i.e., inversely proportional to the channel gain. The perturbations that are transmitted by each antenna are generated using the MRPP attack and the power for each antenna is determined to be inversely proportional to the channel gain. The algorithm is the same as Algorithm 2 except that w_i changes to be inversely proportional to the channel, i.e., $w_i = \frac{1}{\|\mathbf{h}_{c_{ie}}\|_2} \frac{1}{\sum_{j=1}^q \frac{1}{\|\mathbf{h}_{c_{je}}\|_2}}$, $i = 1, \dots, q$.

4.4. Elementwise Maximum Channel Gain (EMCG) Attack

Unlike the previous attacks that considered the channel gain of the channel vector with dimension $p \times 1$ as a way to allocate power among antennas, the EMCG attack considers the channel gain for each time instance to fully utilize the channel diversity as shown in Figure 2b. First, the CJ compares the channel gains elementwise and selects one antenna that has the largest channel gain at each instance. Specifically, the CJ finds and transmits with the antenna $j^* = \arg \max_{j=1, \dots, q} \{\|h_{ar_{j,t}}\|_2\}$ that has the largest channel gain at instance t . Furthermore, a virtual channel $h_{vir,t}$ at instance t is defined as the channel with the largest channel gain among antennas which is $h_{ar_{j^*,t}}$. Then, the adversary generates the perturbation δ^{vir} with respect to $\mathbf{h}_{vir} = [h_{vir,1}, \dots, h_{vir,p}]^T$ using the MRPP attack and transmits each element of δ^{vir} with the antenna that has been selected previously. The details are provided in Algorithm 3.

Algorithm 3: EMCG attack

Inputs: input r_{te} , desired accuracy ε_{acc} , power constraint P_{max} , and model of the classifier $L(\theta, \cdot, \cdot)$.
Initialize: $k \leftarrow \mathbf{0}^{p \times 1}$, $\delta_i \leftarrow \mathbf{0}^{p \times 1}$ for $\forall i$.
for $i = 1$ **to** p **do**
 $h_{vir,i} = \max\{\|h_{c_1e,i}\|_2, \dots, \|h_{c_me,i}\|_2\}$
 $k[i] = \arg \max\{\|h_{c_1e,i}\|_2, \dots, \|h_{c_me,i}\|_2\}$
end
Virtual channel: $\mathbf{H}_{vir} = \text{diag}\{h_{vir,1}, \dots, h_{vir,p}\}$
 $\varepsilon_{max} \leftarrow \sqrt{P_{max}}$, $\varepsilon_{min} \leftarrow 0$
 $\delta = \frac{\mathbf{H}_{vir}^* \nabla_{\mathbf{x}} L(\theta, r_{te}, \mathbf{y}^{target})}{(\|\mathbf{H}_{vir}^* \nabla_{\mathbf{x}} L(\theta, r_{te}, \mathbf{y}^{target})\|_2)}$
while $\varepsilon_{max} - \varepsilon_{min} > \varepsilon_{acc}$ **do**
 $\varepsilon_{avg} \leftarrow (\varepsilon_{max} + \varepsilon_{min})/2$
 $\mathbf{x}_{adv} \leftarrow \mathbf{x} - \varepsilon_{avg} \mathbf{H}_{vir} \delta$
 if $\hat{l}(\mathbf{x}_{adv}) == \text{noise}$ **then** $\varepsilon_{min} \leftarrow \varepsilon_{avg}$
 else $\varepsilon_{max} \leftarrow \varepsilon_{avg}$
end
 $\varepsilon^* = \varepsilon_{max}$
 $\delta^{vir} = \varepsilon^* \delta$
for $i = 1$ **to** p **do**
 $\delta_{k[i]} = \delta^{vir}[i]$
end
Transmit $\delta_i, i = 1, \dots, q$

5. Simulation Results

We analyzed the success of covertness achieved by CJ's perturbation at the eavesdropper and the corresponding effect on the BER at the receiver. We first assumed that the CJ only had one antenna to analyze the impact of the CJ on the eavesdropper. Then, we increased the number of antennas at the CJ to observe the performance when multiple antennas are used with different methods. We compared this perturbation with random Gaussian noise transmitted by the CJ. Furthermore, we changed the location of the CJ to investigate the effects of topology and channel.

5.1. Simulation Settings

We assumed that the binary source data were generated independently and uniformly at the receiver. The classifier at the eavesdropper was a convolutional neural network (CNN). The input to the CNN was of two dimensions (2, 16) corresponding to 16 in-phase/quadrature (I/Q) data samples. The CNN consisted of a convolutional layer with kernel size (1, 3), a hidden layer with dropout rate 0.1, a rectified linear unit (ReLU) activation function at the convolutional and hidden layers and a softmax activation function at the output layer that provides the label *signal* or *noise*. We applied a backpropagation algorithm with the Adam optimizer to train the CNN using cross-entropy as the loss function. The CNN was implemented in Keras with the TensorFlow backend. We assumed that the eavesdropper already knew the signal type that was used at the transmitter. Thus, the classifier at the eavesdropper was only trained with two labels, *signal* and *noise*. For each signal type, we trained a separate classifier using different datasets, where 20,000 symbols were generated and split into blocks of 16 I/Q symbols. The channel between the nodes had path-loss effects and Rayleigh fading such that the channel gain from node i to node j was $h_{ij} = \left(\frac{d_0}{d_{ij}}\right)^\gamma h_{i,j}$, where d_{ij} is the distance from node i to j , d_0 is the reference distance, $h_{i,j}$ is Rayleigh fading between node i to j , and γ is the path loss exponent. We set $d_0 = 1$ and $\gamma = 2.8$ throughout the simulations. Note that there was only a path loss component in the channels for the simulations with CJ for the case of one antenna.

We used the perturbation-to-noise ratio (PNR) metric from [15] that captures the relative perturbation power at the CJ with respect to the noise and measured how the increase in the PNR affected the accuracy of the classifier at the eavesdropper. As the PNR increases, the perturbation generated by the CJ is more likely to be detected by the eavesdropper and increases the BER at the receiver.

5.2. Performance Evaluation of CJ with One Antenna for Signals with Different Modulations

We first assumed that the CJ only had one antenna, $q = 1$, and aimed to hide signals with a fixed modulation scheme, namely QPSK or 16QAM, used by the transmitter using Algorithm 1. Note that we used only Algorithm 1 since the CJ only had a single antenna. The first topology that we considered was $d_{cr} = d_{ce} = 1$. In Figure 3, we show how the perturbation signal generated by the CJ affects the classifier at the eavesdropper. The x -axis is the PNR (measured in dB) and the y -axis is the success of covertness (measured in percentage) that indicates the success of making wireless communications covert, namely the likelihood that the eavesdropper classifies a signal plus perturbation as noise. We observe that as the SNR of the signal increases, the CJ needs more perturbation power to cause misclassification at the eavesdropper. Furthermore, the 16QAM-modulated signal is more susceptible to adversarial perturbation than the QPSK-modulated signal, since it is more difficult to distinguish the 16QAM-modulated signal from the noise for the same SNR. Furthermore, we observe that the success of covertness suddenly increases after some PNR value for both modulation types. On the contrary, the Gaussian noise based perturbation has negligible effect on the classifier for all SNR values. We further observe that the Gaussian noise with more power decreases the success of covertness when the SNR of 16-QAM modulated signal is 3 dB. The reason is the Gaussian noise strengthens the noise which makes the received signal at the eavesdropper resemble the strength of the signal, thus the classifier at the eavesdropper classifies the received signal as signal.

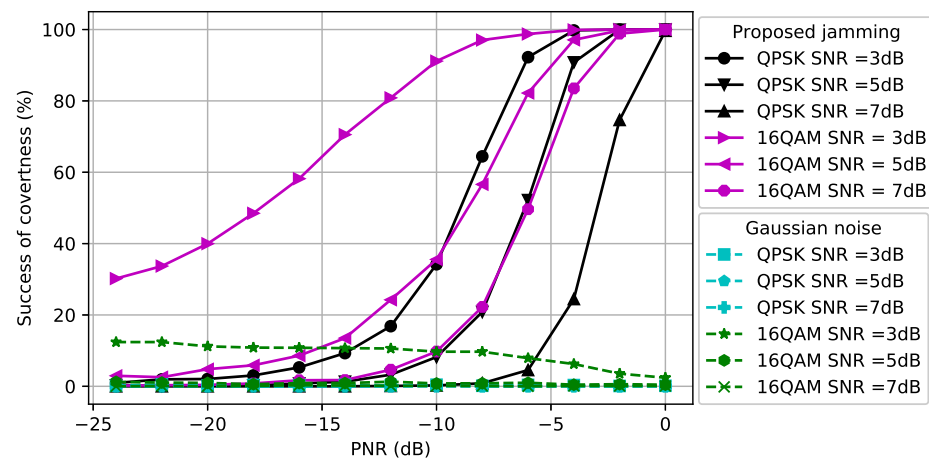


Figure 3. Success of covertness at the eavesdropper when $d_{ce} = d_{cr} = 1$.

In Figure 4, we consider $d_{cr} = 1.5$ and $d_{ce} = 0.5$ (namely, the distance between the CJ and the receiver is increased and the distance between the CJ and the eavesdropper is decreased compared to Figure 3). As the SNR of the signal increases, the CJ requires more power to cause misclassification at the eavesdropper, as we also observed in Figure 3. Due to the reduced path loss effect between the CJ and the eavesdropper, less power is required to cause misclassification compared to Figure 3. This result motivates the use of AML instead of conventional jamming (e.g., [51]) to attack an eavesdropper.

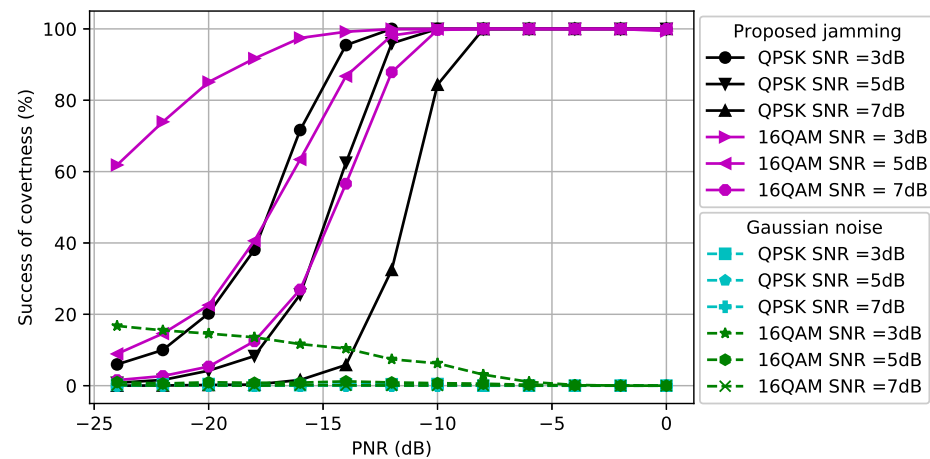


Figure 4. Success of covertness at the eavesdropper when $d_{ce} = 0.5$ and $d_{cr} = 1.5$.

Reliability of Communications

The BER performance at the receiver for different modulation types and SNR values is compared in Figure 5 when $d_{cr} = d_{ce} = 1$. We observe that the BER of the 16QAM-modulated signals is more susceptible to the adversarial perturbation signal than the BER of QPSK-modulated signals. The reason is that since the 16QAM transmits more bits than the QPSK per symbol, the distances between constellation points are smaller, which leads to a larger BER for a given SNR. Moreover, as the SNR increases, the average BER decreases as expected. For the CJ with the proposed adversarial perturbation, we observe that the BER curve saturates after some PNR value because the successful perturbation signal can be generated using less power than the maximum power that the CJ can use. Figure 5 can be used as a guideline to determine the maximum PNR to satisfy the BER requirement at the receiver. For example, to meet the target BER of 0.15 for a QPSK-modulated signal, the PNR is selected to be at most -8 dB when the SNR is 3 dB and the resulting success of covertness is 65%. Furthermore, we observe that the Gaussian noise based perturbation results in a lower BER than the adversarial perturbation in the low PNR regime. However, the BER gap between these two CJ schemes decreases when the PNR increases, and the adversarial perturbation results in a smaller BER in the high PNR region.

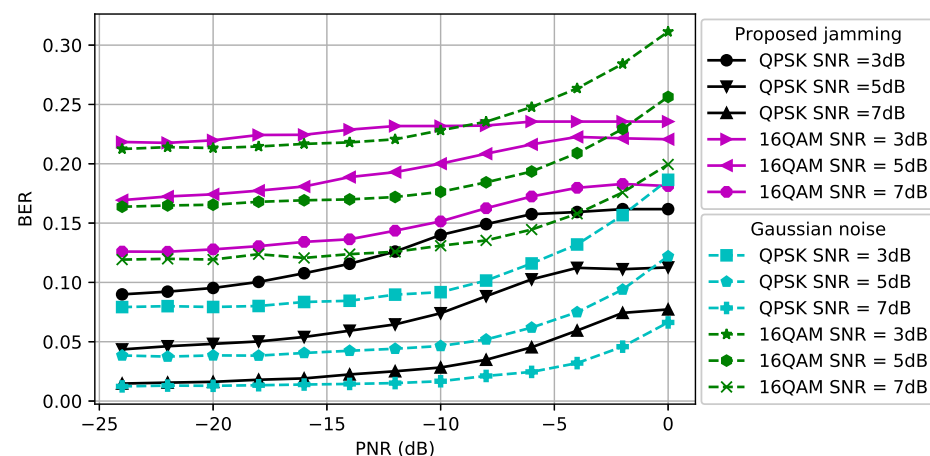


Figure 5. BER at the receiver when $d_{ce} = d_{cr} = 1$.

The BER performance at the receiver for different modulation types and SNR values is compared in Figure 6 when $d_{cr} = 1.5$ and $d_{ce} = 0.5$. We observe that the BER gap between the Gaussian noise and adversarial perturbation for the same SNR value decreases due to the increased path loss effect between the CJ and the receiver. Thus, the CJ can create a perturbation signal that causes misclassification with higher success without increasing the BER further if the location of the CJ is closer to the eavesdropper. This result motivates the control of the CJ positions to fool a target classifier while protecting the BER performance of the intended receiver.

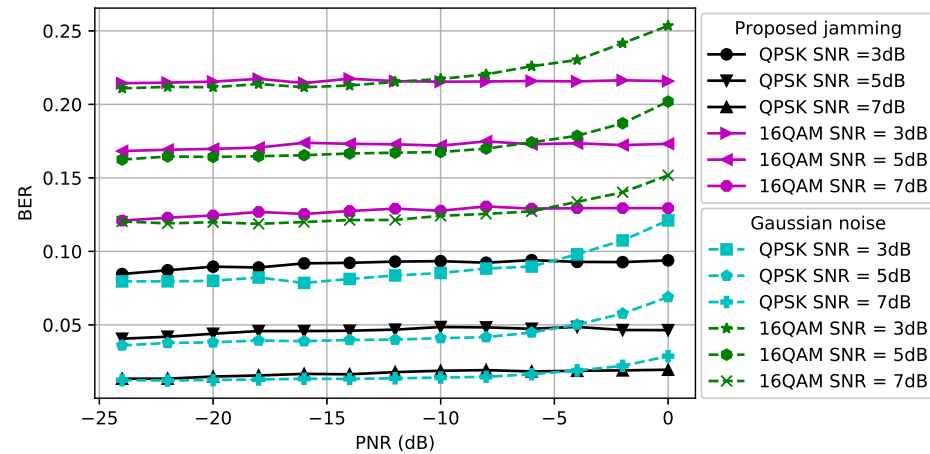


Figure 6. BER at the receiver when $d_{ce} = 0.5$ and $d_{cr} = 1.5$.

5.3. Performance Evaluation for 5G Communications

As a full-fledged waveform to hide, we considered the 5G physical layer communications where a 5G user equipment (UE) transmits a 5G uplink signal to a base station (gNodeB) in the presence of the perturbation from the CJ. MATLAB's 5G toolbox was used to generate 5G signals that included the transport (uplink shared channel, UL-SCH) and physical channel. The transport block was segmented after the cyclic redundancy check (CRC) addition and low-density parity-check (LDPC) coding was used as forward error correction. The output codewords were QPSK-modulated as an example. Next, the generated resource grid was OFDM-modulated with inverse fast Fourier transform and cyclic prefix (CP) addition operations where the subcarrier spacing was 15 kHz. The target code rate was set to $\frac{820}{1024}$ and the output I/Q samples were stored after the signal passed through the channel. The eavesdropper attempted to distinguish the received signals from noise, whereas the receiver attempted to decode the received signals by removing the CP and performing FFT, channel equalization, QPSK demodulation, LDPC, and CRC decoding operations.

5.3.1. Covertness of Communications

The success of covertness for 5G communications is considered in Figure 7. As in the previous figures for QPSK-modulated signals and 16QAM-modulated signals, the proposed perturbation outperforms the Gaussian noise significantly in the high-PNR region for 5G signals. Furthermore, we observe that more power is needed for the CJ to fool the classifier at the eavesdropper when the distance between the CJ and the eavesdropper increases.

5.3.2. Reliability of Communications

The BER for 5G communications is shown in Figure 8. When $d_{ce} = d_{cr} = 1$ and the SNR is 5 dB, the Gaussian noise based perturbation has a higher BER performance compared to the proposed perturbation and a similar result is also observed for other SNR values. Note that the adversarial perturbation by the CJ not only increases the success of covertness, but also has less effect on the BER performance of the receiver compared to

the Gaussian noise based perturbation for 5G communication signals. We further observe that the Gaussian noise based perturbation results in a higher BER than the proposed adversarial perturbation when $d_{ce} = 0.5$ and $d_{cr} = 1.5$.

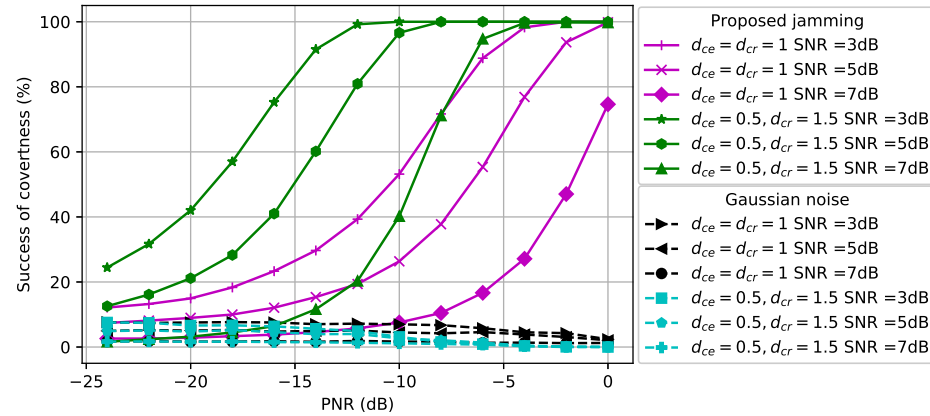


Figure 7. 5G communications covertness performance at the eavesdropper.

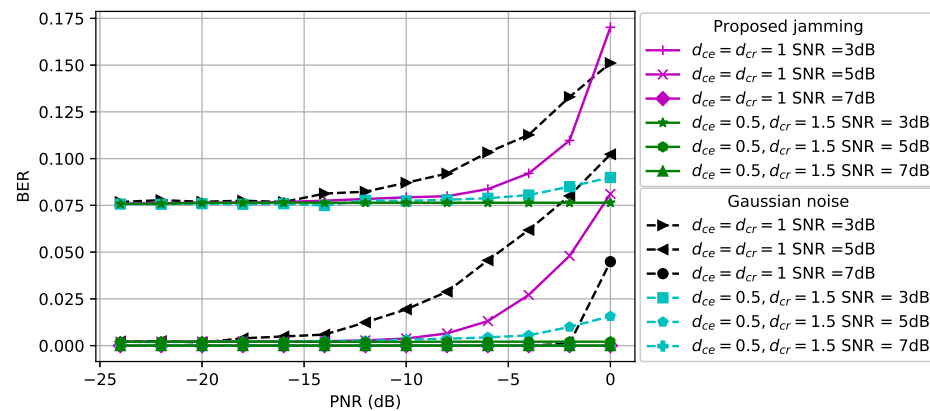


Figure 8. 5G communications BER performance at the receiver.

5.4. Performance Evaluation of CJ with Multiple Antennas

Next, we analyzed the performance of the CJ with multiple antennas when a QPSK-modulated signal was used at the transmitter. Note that the channel between the CJ and the receiver and the channel between the CJ and the eavesdropper had Rayleigh fading. Note that $h_{i,j} \sim \text{Rayleigh}(0, 1)$ if specified otherwise. Figure 9a presents the success of covertness when the CJ transmits an adversarial perturbation with $q = 2$ antennas using the different attack methods introduced in Section 4. We observe that all different methods using multiple antennas outperform the attack generated by the CJ with one antenna. Furthermore, randomly selecting one antenna at the CJ performs worst among attacks using multiple antennas and the performance of the IPCG attack is similar to the performance of the PCG attack. Moreover, the EMCG attack outperforms other attacks by fully utilizing the channel diversity.

Figure 9b presents the BER performance of different attack methods. We observe that the CJ using one antenna gives the largest BER whereas the PCG and IPCG attacks give the smallest BER. Furthermore, the EMCG attack gives a moderate BER increase while successfully making communications covert.

The performance of the CJ with different number of antennas is presented in Figure 10a. As the number of the antennas at the CJ increases, the success of covertness also increases suggesting that using more antenna at the CJ helps the covertness of communications. Furthermore, the BER decreases when more antennas are used at the CJ as we can see from

Figure 10b. Therefore, using more antennas at the CJ is always beneficial for communications in terms of covertness and BER when the EMCG attack is used at the CJ.

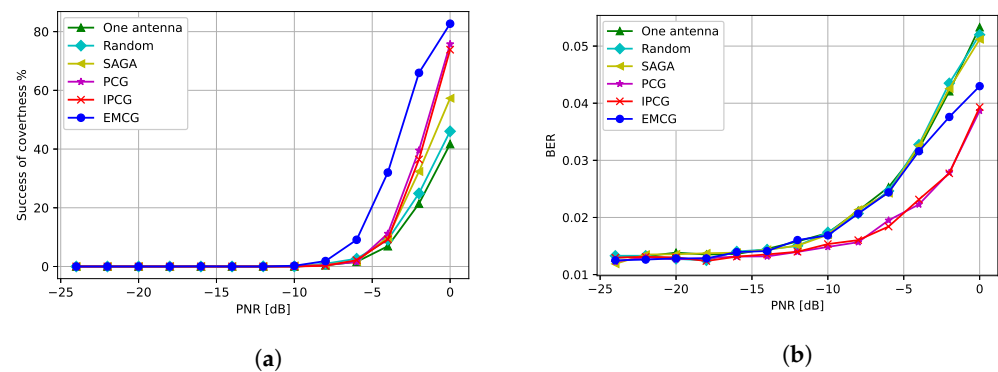


Figure 9. Performance when CJ has $q = 2$ antennas: (a) success of covertness and (b) BER at the receiver.

Next, we varied the SNR levels to analyze how the SNR affected the covertness and the BER in Figure 11a,b. As expected, the CJ needs a higher PNR to fool the eavesdropper when the SNR is high. Furthermore, we observe that the BER slightly increases when the PNR increases and the BER is higher for a lower SNR.

Finally, we increased the variance of the Rayleigh fading between the CJ and the eavesdropper to analyze the effect of the channel on the covertness of communications. In Figure 12a, we observe that a lower PNR is needed to fool the eavesdropper when the variance of the Rayleigh fading is high. Furthermore, as a consequence of using a lower PNR at the CJ, a higher variance of Rayleigh fading results in a lower BER at the receiver.

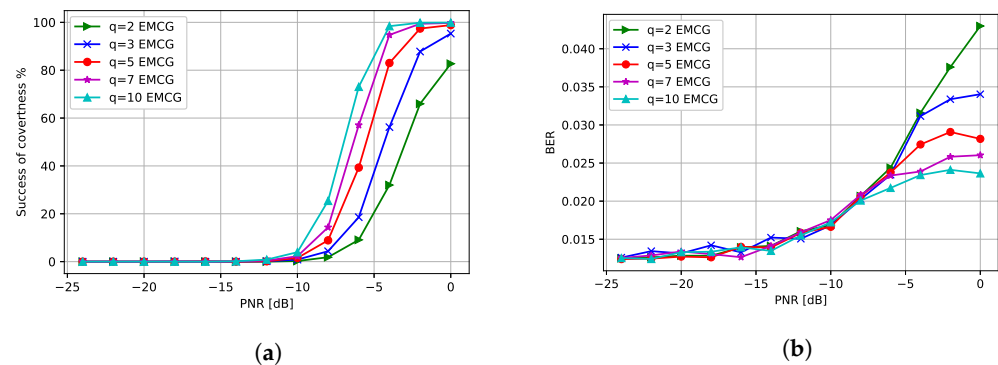


Figure 10. Performance with different number of antennas at the CJ: (a) success of covertness and (b) BER at the receiver.

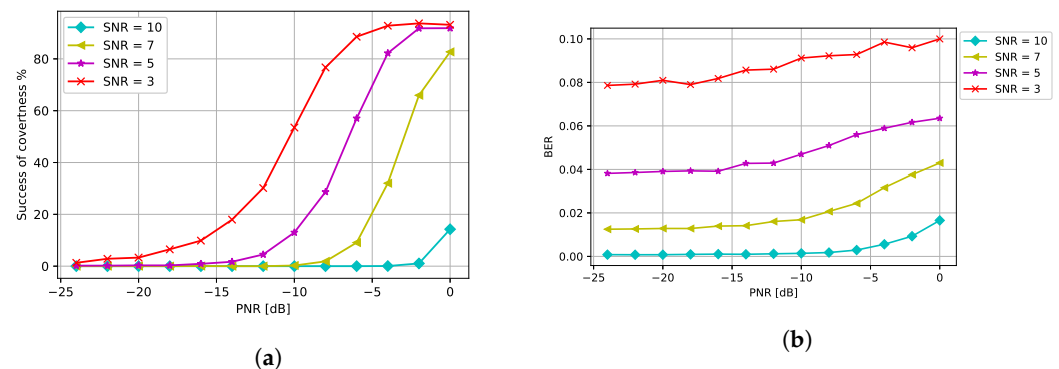


Figure 11. Performance with respect to different SNR levels: (a) success of covertness and (b) BER at the receiver.

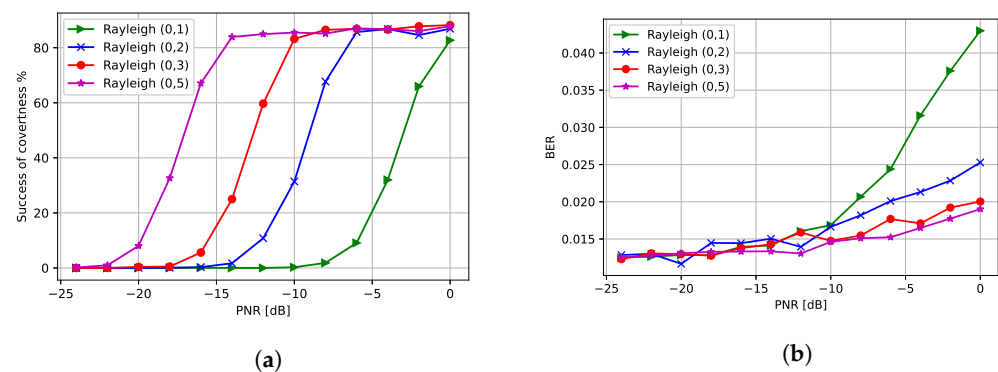


Figure 12. Performance with respect to different Rayleigh fading variances: (a) success of covertness and (b) BER at the receiver.

6. Conclusions

We considered a wireless communications system in which a CJ with multiple antennas transmits perturbation signals to fool a DL-based classifier at the eavesdropper into classifying the ongoing transmissions as noise. Following the AML approach, the CJ was designed to generate the perturbation signal with different methods. For both basic modulated signals and sophisticated 5G signals, we showed that the CJ could generate a perturbation signal that caused misclassification at the eavesdropper (from *signal* to *noise*) with high success, while the BER at the receiver was only slightly affected. Furthermore, we showed that by adding more antennas at the CJ always improved the attack performance and lowered the BER when the EMCG attack was used. These results demonstrate that wireless communications can be successfully kept covert when multiple antennas are used at the CJ by allocating the transmit power efficiently.

Author Contributions: Conceptualization, B.K., Y.S., K.D., T.E. and S.U.; methodology, B.K., Y.S., K.D., T.E. and S.U.; software, B.K., K.D. and T.E.; validation, B.K., Y.S., K.D., T.E. and S.U.; formal analysis, B.K., Y.S., K.D., T.E. and S.U.; investigation, B.K., Y.S., K.D., T.E. and S.U.; resources, B.K., Y.S., K.D., T.E. and S.U.; data curation, B.K., Y.S., K.D., T.E. and S.U.; writing—original draft preparation, B.K., Y.S., K.D., T.E. and S.U.; writing—review and editing, B.K., Y.S., K.D., T.E. and S.U.; visualization, B.K., Y.S., K.D., T.E. and S.U.; supervision, S.U.; project administration, S.U. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable

Data Availability Statement: Not applicable.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Yener, A.; Ulukus, S. Wireless Physical-Layer Security: Lessons Learned From Information Theory. *Proc. IEEE* **2015**, *103*, 1814–1825. [\[CrossRef\]](#)
2. Schaefer, R.F.; Boche, H.; Poor, H.V. Secure communication under channel uncertainty and adversarial attacks. *Proc. IEEE* **2015**, *103*, 1796–1813. [\[CrossRef\]](#)
3. Bloch, M.R. Covert communication over noisy channels: A resolvability perspective. *IEEE Trans. Inf. Theory* **2016**, *62*, 2334–2354. [\[CrossRef\]](#)
4. Wang, L.; Wornell, G.W.; Zheng, L. Fundamental limits of communication with low probability of detection. *IEEE Trans. Inf. Theory* **2016**, *62*, 3493–3503. [\[CrossRef\]](#)
5. Bash, B.A.; Goeckel, D.; Towsley, D.; Guha, S. Hiding information in noise: Fundamental limits of covert wireless communication. *IEEE Commun. Mag.* **2015**, *12*, 26–31. [\[CrossRef\]](#)
6. Mukherjee, P.; Ulukus, S. Covert bits through queues. In Proceedings of the IEEE Conference on Communications and Network Security (CNS), Philadelphia, PA, USA, 17–19 October 2016; pp. 626–630.

7. Kurakin, A.; Goodfellow, I.; Bengio, S. Adversarial examples in the physical world. In Proceedings of the International Conference on Learning Representations (ICLR), Toulon, France, 24–26 April 2017.
8. Shi, Y.; Sagduyu, Y.E.; Grushin, A. How to steal a machine learning classifier with deep learning. In Proceedings of the IEEE Symposium on Technologies for Homeland Security (HST), Boston, MA, USA, 25–26 April 2017.
9. Vorobeychik, Y.; Kantarcioglu, M. Adversarial machine learning. *Synth. Lect. Artif. Intell. Mach. Learn.* **2017**, *12*, 1–169.
10. Adesina, D.; Hsieh, C.C.; Sagduyu, Y.E.; Qian, L. Adversarial machine learning in wireless communications using RF data: A review. *arXiv* **2020**, arXiv:2012.14392.
11. Sagduyu, Y.E.; Shi, Y.; Erpek, T.; Headley, W.; Flowers, B.; Stantchev, G.; Lu, Z. When wireless security meets machine learning: Motivation, challenges, and research directions. *arXiv* **2020**, arXiv:2001.08883.
12. Liu, J.; Nogueira, M.; Fernandes, J.; Kantarci, B. Adversarial Machine Learning: A Multilayer Review of the State-of-the-Art and Challenges for Wireless and Mobile Systems. *IEEE Commun. Surv. Tutor.* **2022**, *24*, 123–159. [[CrossRef](#)]
13. Shi, Y.; Sagduyu, Y.E.; Erpek, T.; Davaslioglu, K.; Lu, Z.; Li, J. Adversarial Deep Learning for Cognitive Radio Security: Jamming Attack and Defense Strategies. In Proceedings of the IEEE International Communications Conference (ICC) Workshop on Machine Learning in Wireless Communications, Kansas City, MO, USA, 20–24 May 2018.
14. Erpek, T.; Sagduyu, Y.E.; Shi, Y. Deep learning for launching and mitigating wireless jamming attacks. *IEEE Trans. Cogn. Commun. Netw.* **2019**, *5*, 2–14. [[CrossRef](#)]
15. Sadeghi, M.; Larsson, E.G. Adversarial attacks on deep-learning based radio signal classification. *IEEE Commun. Lett.* **2019**, *8*, 213–216. [[CrossRef](#)]
16. Bair, S.; Delvecchio, M.; Flowers, B.; Michaels, A.J.; Headley, W.C. On the Limitations of Targeted Adversarial Evasion Attacks Against Deep Learning Enabled Modulation Recognition. In Proceedings of the ACM WiSec Workshop on Wireless Security and Machine Learning (WiseML), Miami, FL, USA, 15–17 May 2019.
17. Flowers, B.; Buehrer, R.M.; Headley, W.C. Evaluating adversarial evasion attacks in the context of wireless communications. *arXiv* **2019**, arXiv:1903.01563.
18. Kokalj-Filipovic, S.; Miller, R. Targeted Adversarial Examples against RF Deep Classifiers. In Proceedings of the ACM WiSec Workshop on Wireless Security and Machine Learning (WiseML), Miami, FL, USA, 15–17 May 2019.
19. Kokalj-Filipovic, S.; Miller, R.; Vanhoy, G.M. Adversarial Examples in RF Deep Learning: Detection and Physical Robustness. In Proceedings of the IEEE Global Conference on Signal and Information Processing (GlobalSIP), Ottawa, ON, Canada, 11–14 November 2019.
20. Kim, B.; Sagduyu, Y.E.; Davaslioglu, K.; Erpek, T.; Ulukus, S. Over-the-Air Adversarial Attacks on Deep Learning Based Modulation Classifier over Wireless Channels. In Proceedings of the Conference on Information Sciences and Systems (CISS), Princeton, NJ, USA, 18–20 March 2020.
21. Kim, B.; Sagduyu, Y.E.; Davaslioglu, K.; Erpek, T.; Ulukus, S. Channel-Aware Adversarial Attacks Against Deep Learning-Based Wireless Signal Classifiers. *IEEE Trans. Wirel. Commun.* **2022**, *21*, 3868–3880. [[CrossRef](#)]
22. Kim, B.; Sagduyu, Y.E.; Davaslioglu, K.; Erpek, T.; Ulukus, S. Adversarial attacks with multiple antennas against deep learning-based modulation classifiers. In Proceedings of the IEEE Global Communications Conference (Globecom), Taipei, Taiwan, 7–11 December 2020.
23. Kim, B.; Sagduyu, Y.E.; Erpek, T.; Davaslioglu, K.; Ulukus, S. Channel Effects on Surrogate Models of Adversarial Attacks against Wireless Signal Classifiers. In Proceedings of the IEEE International Conference on Communications (ICC), Montreal, QC, Canada, 14–23 June 2021.
24. Lin, Y.; Zhao, H.; Tu, Y.; Mao, S.; Dou, Z. Threats of Adversarial Attacks in DNN-Based Modulation Recognition. In Proceedings of the International Conference on Computer Communications (INFOCOM), Toronto, ON, Canada, 6–9 July 2020.
25. Restuccia, F.; D'Oro, S.; Al-Shawabka, A.; Rendon, B.C.; Chowdhury, K.; Ioannidis, S.; Melodia, T. Generalized wireless adversarial deep learning. In Proceedings of the ACM Workshop on Wireless Security and Machine Learning (WiseML), Virtual, 13 July 2020.
26. Hou, T.; Wang, T.; Lu, Z.; Liu, Y.; Sagduyu, Y. IoTGAN: GAN Powered Camouflage Against Machine Learning Based IoT Device Identification. In Proceedings of the IEEE International Symposium on Dynamic Spectrum Access Networks (DySPAN), Virtual, 13–15 December 2021.
27. Sahay, R.; Love, D.J.; Brinton, C.G. Robust automatic modulation classification in the presence of adversarial attacks. In Proceedings of the 2021 55th IEEE Annual Conference on Information Sciences and Systems (CISS), Baltimore, MD, USA, 24–26 March 2021; pp. 1–6.
28. Seo, J.; Park, S.; Kang, J. Adversarial, yet Friendly Signal Design for Secured Wireless Communication. In Proceedings of the 2021 IEEE Wireless Communications and Networking Conference (WCNC), Nanjing, China, 29 March–1 April 2021; pp. 1–7.
29. Shi, Y.; Erpek, T.; Sagduyu, Y.E.; Li, J. Spectrum Data Poisoning with Adversarial Deep Learning. In Proceedings of the IEEE Military Communications Conference (MILCOM), Los Angeles, CA, USA, 29–31 October 2018.
30. Sadeghi, M.; Larsson, E.G. Physical adversarial attacks against end-to-end autoencoder communication systems. *IEEE Commun. Lett.* **2019**, *23*, 847–850.
31. Kim, B.; Sagduyu, Y.; Erpek, T.; Ulukus, S. Adversarial Attacks on Deep Learning Based mmWave Beam Prediction in 5G Furthermore, Beyond. In Proceedings of the IEEE Statistical Signal Processing Workshop (SSP), Rio de Janeiro, Brazil, 11–14 July 2021.

32. Hou, T.; Wang, T.; Lu, Z.; Liu, Y.; Sagduyu, Y. Undermining Deep Learning Based Channel Estimation via Adversarial Wireless Signal Fabrication. In Proceedings of the ACM Workshop on Wireless Security and Machine Learning (WiseML), San Antonio, TX, USA, 16–19 May 2022.
33. Kim, B.; Shi, Y.; Sagduyu, Y.E.; Erpek, T.; Ulukus, S. Adversarial Attacks against Deep Learning Based Power Control in Wireless Communications. In Proceedings of the IEEE Globecom Workshops (GC Wkshps), Madrid, Spain, 7–11 December 2021.
34. Hameed, M.Z.; Gyorgy, A.; Gunduz, D. Communication without interception: Defense against modulation detection. In Proceedings of the IEEE Global Conference on Signal and Information Processing (GlobalSIP), Ottawa, ON, Canada, 11–14 November 2019.
35. Hameed, M.Z.; György, A.; Gündüz, D. The best defense is a good offense: Adversarial attacks to avoid modulation detection. *IEEE Trans. Inf. Forensics Secur.* **2020**, *16*, 1074–1087. [\[CrossRef\]](#)
36. Kim, B.; Sagduyu, Y.E.; Davaslioglu, K.; Erpek, T.; Ulukus, S. How to Make 5G Communications “Invisible”: Adversarial Machine Learning for Wireless Privacy. In Proceedings of the Asilomar Conference on Signals, Systems, and Computers, Pacific Grove, CA, USA, 1–4 November 2020.
37. Kim, B.; Erpek, T.; Sagduyu, Y.E.; Ulukus, S. Covert Communications via Adversarial Machine Learning and Reconfigurable Intelligent Surfaces. In Proceedings of the IEEE Wireless Communications and Networking Conference (WCNC), Austin, TX, USA, 10–13 April 2022.
38. Sagduyu, Y.E.; Erpek, T.; Shi, Y. Adversarial Deep Learning for Over-the-Air Spectrum Poisoning Attacks. *IEEE Trans. Mob. Comput.* **2021**, *20*, 306–319. [\[CrossRef\]](#)
39. Luo, Z.; Zhao, S.; Lu, Z.; Xu, J.; Sagduyu, Y.E. When Attackers Meet AI: Learning-Empowered Attacks in Cooperative Spectrum Sensing. *IEEE Trans. Mob. Comput.* **2022**, *21*, 1892–1908. [\[CrossRef\]](#)
40. Luo, Z.; Zhao, S.; Lu, Z.; Sagduyu, Y.E.; Xu, J. Adversarial machine learning based partial-model attack in IoT. In Proceedings of the ACM Workshop on Wireless Security and Machine Learning (WiseML), Virtual, 13 July 2020.
41. Shi, Y.; Davaslioglu, K.; Sagduyu, Y.E. Over-the-air membership inference attacks as privacy threats for deep learning-based wireless signal classifiers. In Proceedings of the ACM WiSec Workshop on Wireless Security and Machine Learning (WiseML), Virtual, 16–19 May 2020.
42. Shi, Y.; Sagduyu, Y. Membership inference attack and defense for wireless signal classifiers with deep learning. *IEEE Trans. Mob. Comput.* **2022**. [\[CrossRef\]](#)
43. Davaslioglu, K.; Sagduyu, Y.E. Trojan Attacks on Wireless Signal Classification with Adversarial Machine Learning. In Proceedings of the IEEE DySPAN Workshop on Data-Driven Dynamic Spectrum Sharing, Newark, NJ, USA, 11–14 November 2019.
44. Shi, Y.; Davaslioglu, K.; Sagduyu, Y.E. Generative adversarial network for wireless signal spoofing. In Proceedings of the ACM Workshop on Wireless Security and Machine Learning (WiseML), Miami, FL, USA, 15–17 May 2019.
45. Shi, Y.; Davaslioglu, K.; Sagduyu, Y.E. Generative adversarial network in the air: Deep adversarial learning for wireless signal spoofing. *IEEE Trans. Cogn. Commun. Netw.* **2021**, *7*, 294–303. [\[CrossRef\]](#)
46. Karunaratne, S.; Krijestorac, E.; Cabric, D. Penetrating RF Fingerprinting-based Authentication with a Generative Adversarial Attack. In Proceedings of the IEEE International Conference on Communications (ICC), Montreal, QC, Canada, 14–23 June 2021.
47. Sagduyu, Y.E.; Erpek, T.; Shi, Y. Adversarial Machine Learning for 5G Communications Security. In *Game Theory and Machine Learning for Cyber Security*; John Wiley & Sons: New York, NY, USA, 2021; pp. 270–288.
48. Tekin, E.; Yener, A. The general Gaussian multiple-access and two-way wiretap channels: Achievable rates and cooperative jamming. *IEEE Trans. Inf. Theory* **2008**, *54*, 2735–2751. [\[CrossRef\]](#)
49. Xie, J.; Ulukus, S. Secure Degrees of Freedom of Multiuser Networks: One-Time-Pads in the Air via Alignment. *Proc. IEEE* **2015**, *103*, 1857–1873. [\[CrossRef\]](#)
50. Bassily, R.; Ekrem, E.; He, X.; Tekin, E.; Xie, J.; Bloch, M.R.; Ulukus, S.; Yener, A. Cooperative Security at the Physical Layer: A Summary of Recent Advances. *IEEE Signal Process. Mag.* **2013**, *30*, 16–28. [\[CrossRef\]](#)
51. Sagduyu, Y.E.; Berry, R.A.; Ephremides, A. Jamming games in wireless networks with incomplete information. *IEEE Commun. Mag.* **2011**, *49*, 112–118. [\[CrossRef\]](#)