Channel Prediction and Transmitter Authentication
With Adversarially-Trained Recurrent
Neural Networks

KEN ST. GERMAIN (Graduate Student Member, IEEE), AND FRANK KRAGH
Department of Electrical and Computer Engineering, Naval Postgraduate School, Monterey, CA 93943, USA
CORRESPONDING AUTHOR: K. St. GERMAIN (e-mail: kenneth.stgermain@nps.edu)

ABSTRACT As wireless communications and interconnected networks become ubiquitous and relied upon, they must also remain secure. Advanced communication systems that use techniques to improve data throughput and minimize latency lend themselves to physical-layer authentication. The stochastic and dynamic nature of the wireless mobile channel provides features that can be extracted through deep learning. We propose a novel method to authenticate transmitters at the physical layer by leveraging channel state information to predict future channel impulse responses. Specifically, we compare the use of recurrent neural networks (RNNs) using long-short term memory (LSTM) and gated recurrent unit (GRU) cells with variations of a conditional generative adversarial network (CGAN) to authenticate transmitters in a mobile environment. Our evaluation shows that standalone RNNs using LSTM and GRU cells are adept at predicting future channel responses, however a CGAN-trained discriminator using GRU cells is able to match the authentication accuracy of a standalone network without using a predefined channel prediction error threshold. Using a discriminator trained by a CGAN with binary cross entropy loss in the discriminator and mean squared error loss in the generator, the neural network was able to authenticate at a 98.5% rate.

INDEX TERMS Channel prediction, channel state information, generative adversarial network, physical-layer authentication, recurrent neural networks.

I. INTRODUCTION

As 5TH generation (5G) mobile networks offer the expectation of high speed, low latency mobile connectivity, appropriate security mechanisms must also be considered. Improved data speeds and increased area coverage are attained while symbol error is minimized by employing multiple-input, multiple-output (MIMO) receiver/transmitter systems [1]. However, intrusions and attacks can be expected to counter the benefits of the networks without appropriate security. Computer network attacks continue to be reported, justifying improvement against a myriad of threats at the federal, state, and private levels [2], [3], [4], [5].

Prediction of channel characteristics allows for a variety of techniques to make efficient use of a wireless link [6], [7]. By applying adaptive measures such as changing transmitter power, modulation, channel coding, antenna diversity, etc., improved performance can be achieved between transmitter and receiver while ensuring symbol error rate remains at acceptable levels [8]. The result of wireless signal deterioration due to factors including fade, shadowing, scattering, and path loss can be characterized by channel state information (CSI). CSI estimation and prediction is crucial in adaptive systems [9] and has been a topic of much research. Notably, as communication systems have evolved and become more complex with the inclusion of MIMO antenna architectures, orthogonal frequency division multiplexing (OFDM) with multiple subcarriers, artificial neural networks have been shown to outperform traditional linear algorithms [10] resulting in several neural network-based solutions to channel prediction [11], [12], [13], [14].

In this paper, we leverage deep learning to predict the future characteristics of a channel and compare the prediction with ground truth to make an authentication decision. We explore physical-layer authentication and artificial neural
networks with the objective of correctly authenticating legitimate devices and denying authentication to illegitimate transmitters.

Key-based cryptography is the common technique for ensuring authentication, however the growing number, size, and complexity of ad-hoc self-organizing networks can result in user delays due to key distribution and management bottlenecks [15], [16]. Unfortunately, key-based systems still have vulnerabilities that a motivated adversary can exploit, and in some instances very little security [17] is gained at the expense of increased complication or worse quality of service [18]. Another drawback for cryptographic systems is the challenge of key distribution and management in a decentralized, dynamic, and heterogeneous network [16], [19]. Depending on the application, there are many networked systems that forego any protective measures at all. There are devices such as those in the Internet of Things (IoT) realm that do not use strong cryptographic techniques due to the competing constraints of power allocation, processing capability, and memory limitations [20]. When these devices connect to greater networks, they can become a tempting target to malicious actors. Even if initial authentication is achieved using cryptographic methods, physical-layer authentication for subsequent exchanges reduces the load on the upper layers in the Open Systems Interconnected (OSI) model. When authentication is performed at the physical layer, computational demand on the higher OSI layers is reduced. Physical-layer authentication systems that correctly deny authentication to illegitimate transmitters prevent an undue expenditure of processing and memory resources.

There are two main methods to characterize transmitters as either trusted or untrusted using features of the physical layer without the use of a pre-shared secret, cryptography, user-provided credentials, or higher OSI-layer processing [16], [21]. The first method uses unique transmitter hardware imperfections that materialize as radio frequency (RF) fingerprints [22], [23], [24]. Based on manufacturing processes and designs, the transmitted signal will be uniquely distorted from device to device, even if only slightly. The other main technique to identify a transmitter depends on the inherent randomness of the wireless multipath fading channel and relies upon the unique impulse or frequency response [25], [26], [27].

We propose a physical-layer authentication method that builds upon channel-based research. The elements of the CSI matrix are attributes of the fading channel and are therefore unique to the pairwise position of the receiver and transmitter in line-of-sight (LOS) and non-line-of-sight (NLOS) multipath environments. While there is merit in using the RF fingerprinting method in the first category, these characteristics are observable to a malicious actor and can be spoofed. Contrast with using the channel-based approach, an adversary cannot directly measure the CSI between two entities and create a transmission to mimic a legitimate signal. In dynamic conditions with a mobile transmitter, receiver, and/or significant reflective or absorbing objects, the CSI is also time-variant. Simulating a mobile channel, we use the magnitude of the CSI elements to identify transmitters that should be authenticated.

Machine learning has shown merit for problems with fluctuating data in dynamic settings [28] and regression problems have been successfully addressed using deep learning techniques [29]. Additional motivation for the use of deep learning is to more accurately model mobile channel effects over prior techniques. Features of the channel can be abstracted from raw data using deep learning algorithms [30] and then used to make an authentication decision. Deep learning with neural networks has been shown to meet challenges where a high level of accuracy is required, and especially if the samples contain high dimensionality [31]. In this paper we compare the use of recurrent neural networks (RNNs) to a generative adversarial network (GAN) for the task of predicting dynamic magnitude of the channel state information elements corresponding to a transmitter. Based on the difference between the predicted channel response and the actual channel response, a decision can be made to authenticate or deny authentication to the transmitter. The neural networks are provided with previous channel response measurements and are tasked to predict the value of the next response. We use long short-term memory (LSTM) or gated recurrent unit (GRU) cells to create RNNs. The GAN model also employs these LSTM or GRU cells and uses channel responses as conditional information in an architecture known as a conditional GAN (CGAN) [32].

- We propose a novel method for accomplishing channel prediction and physical-layer authentication for mobile devices. Specifically, our method uses a CGAN to predict the mobile MIMO channel response magnitudes.
- We propose two methods to authenticate at the physical layer:
  - A discriminator trained in an adversarial framework that can be used to authenticate or deny authentication.
  - Based on the difference from the predictive channel responses and the true channel response, a threshold based on mean squared error (MSE) can be used to grant or deny authentication.
- We compare the performance of our generative adversarial models to alternative recurrent neural networks.

In Section II, we discuss prior research. The channel model and channel prediction are addressed in Section III. Neural networks including the CGAN are presented in Section IV. The channel model simulation and results are presented in Section V and Section VI, respectively. Finally, we conclude and share additional areas of interest to investigate in Section VII. With regard to notation, vectors are denoted with bold lower-case letters, and matrices with bold upper-case letters.

II. RELATED WORK

Many researchers have used deep neural networks to successfully address mapping challenges using CSI. Authors have used the received CSI and known locations of wireless
transmitters as input to machine learning systems that are then used to accurately determine the position of the transmitters at a later time [33], [34], [35]. Additionally, there has been physical-layer authentication research based on CSI using spatial information and machine learning [36], [37], [38], [39]. Pan et al. showed that static environments, rich fading, and antennas separated by greater than a half wavelength improved authentication performance [39]. The methodology used in these works requires making CSI measurements in advance at various fixed locations within the test environments. Our proposal does not require such a survey of the operating environment, nor is it necessary for a location to be explicitly identified. By extracting mobile channel features through received CSI, we are able to make an authentication decision based on the output of adversarially-trained RNNs.

The GAN architecture adversarially trains a discriminator neural network against a generator neural network [40]. While GANs have provided breakthrough contributions in the image processing fields [41], [42], [43], there have been a variety of successes in using GANs to address challenges in the wireless arena as well. Li et al. [44] developed a GAN-trained generator network with convolutional layers to supplement previously collected data to improve the performance and reduce the labor in creating a MIMO CSI-based Wi-Fi localization system. The authors collected CSI from subcarriers in an IEEE 802.11n network and converted that information into amplitude feature maps. A GAN using deep convolutional neural networks created additional samples similar to the amplitude feature maps converted from the collected CSI data. A CGAN approach was used by Dong et al. in [45] for the purpose of channel prediction. A generator was trained to generate CSI samples based on pilot sequences and received signals and the discriminator was then tasked with differentiating between authentic and artificial CSI matrices conditioned on the pilots. While these papers made use of adversarially-trained networks, the architectures used were all feed-forward networks since the operating areas were relatively static. The present work makes use of mobile channel time-varying CSI measurements that are used as inputs to adversarially-trained RNNs. For a sequence of samples, a RNN uses the output obtained with the previous time step as part of the input to calculate the output for the next time step. RNNs have been shown to be successful with temporally correlated data.

Several works have explored the use of RNNs to predict channel characteristics such as Liu et al. [11] for narrowband prediction, and [46] where Ding et al. used a recurrent complex-valued neural network to improve prediction results. Wang et al. [47] used convolutional layers and RNNs to conduct physical-layer authentication with CSI in a stationary office environment. Jiang and Schotten [48] demonstrated the use of LSTM and GRU cells for improving channel prediction over previous RNNs. Roy et al. [49] used LSTM and GRU cells to classify transmitters, but instead of using received CSI, Roy used in-phase and quadrature time-series measurements. While our proposal uses RNNs consisting of LSTM and GRU cells to process time-series CSI data, our training architecture pits RNNs against each other in adversarial competition. By doing so we produce two neural networks: one that is able to predict channel characteristics, and the other that can discriminate between legitimate and illegitimate transmitters based on received CSI.

Distinguishing from previous research, we use adversarially-trained RNNs to not only predict future channel characteristics, but to create a binary classifier that provides an authentication decision based on received CSI. In our previous work [50], we incorporated LSTM and GRU cells into a CGAN architecture for transmitter authentication based on CSI. To the best of our ability and after a thorough search, we could find no other authors incorporating CGANs and RNNs for the purpose of channel prediction or physical-layer authentication. Our current proposal extends the ideas initially considered in [50] as we further develop the mechanisms that underpin the operation of adversarially-trained recurrent neural networks. We use the generator network from the CGAN for channel prediction to authenticate transmitters based on mobile channel conditions. The CGAN discriminator network is also used to authenticate transmitters by assessing the received impulse response conditioned on previously recorded channel responses. In this work, we explore various neural network loss functions and analyze the effects the loss functions have on channel prediction and discriminator accuracy. Additionally, we evaluate the performance of our newly-trained RNN models against the results of previously developed networks.

III. CHANNEL MODEL

Independent fading channels can be achieved when antennas are spaced greater than two wavelengths apart [6]. With modern and future communications using ever-higher carrier frequencies [51], the wavelength decreases proportionally and enables the use of MIMO schemes in handheld and mobile devices. Movement of the receiver, transmitter, and/or substantial objects within the multipath channel will result in variation of the channel response compared to the static case. Certainly for millimeter wave as well as gigahertz frequencies, independent channels can be encountered, even for wearable devices. The receivers can then differentiate transmitters based on received CSI and choose whether or not to authenticate.

A. CHANNEL STATE INFORMATION

The effect of channel conditions on the received signal, CSI, is represented as a time varying matrix \( H(t) \). The wideband channel model describing \( H(t) \) is a tapped delay line

\[
H(t) = \sum_{i=1}^{L} A_i \delta(t - \tau_i) \tag{1}
\]

where each \( A_i \) is an \( N \times M \) matrix of circularly symmetric complex-valued Gaussian random variables, \( \tau_i \) is the path
delay and \( L \) is the total number of delays [52]. The amount of receiver antennas is \( N \), while the total transmitter antennas is \( M \). Fig. 1 shows the representation of the channel and the aggregate of CSI matrices sampled from \( t = 1 \) to \( t = t_\Sigma \). Each of the elements within \( H, h_{n,m} (1 \leq n \leq N, 1 \leq m \leq M) \), are independent complex circularly symmetric Gaussian random variables.

In a dynamic environment, the CSI matrix, \( H(t) \), changes for every sample time, where \( t_\Sigma \in \{t_1, t_2, \ldots, t_S\} \) and \( S \) is the number of samples. Likewise, the magnitude of each CSI element, \( |h_{n,m}|_{N \times M} \), changes. Following Jiang and Schotten in their work in channel prediction [53], we will use the magnitude of the CSI elements to discern the transmitter to be authenticated using the intuitive notion that magnitude will change more slowly than the phases. We construct a time-varying channel gain tensor, \( \hat{Q}(t) = [h_{n,m}(t_s)]_{N \times M \times S} \) where we further decompose the CSI elements into a two-dimensional matrix,

\[
\hat{Q} = \begin{bmatrix}
|h_{1,1}(t_1)| & |h_{1,1}(t_2)| & \ldots & |h_{1,1}(t_S)| \\
|h_{1,2}(t_1)| & |h_{1,2}(t_2)| & \ldots & |h_{1,2}(t_S)| \\
\vdots & \vdots & \ddots & \vdots \\
|h_{N,M}(t_1)| & |h_{N,M}(t_2)| & \ldots & |h_{N,M}(t_S)|
\end{bmatrix}
\]  

(2)

where \( \hat{Q} \) is a time-series representation of the channel gain matrix where one dimension is time, and the other dimension is spatial. Each column in (2) is a vector representation of the magnitude of the CSI elements for a particular channel sample.

### B. CHANNEL PREDICTION

The time-series channel gain matrix, \( \hat{Q} \), is obtained by measuring the magnitude of the CSI elements within \( H(t) \). This can be accomplished through pilot symbols where the complex value of the symbol is known a priori by the receiver. Pilots symbols can be extracted from dedicated pilot channels in an OFDM framework or in the preamble of a transmitted packet. We consider a fast-fading channel, we assume channel variations from symbol to symbol are correlated for a short time, consistent with mobile channel measurements [6].

We achieve channel prediction by first measuring a sequence of \( S \) impulse responses from a series of received transmissions, and then forecasting the next sequence of predictions, \( P \). For example, consider Fig. 2(a) and Fig. 2(b), where a sequence of \( S \) received impulse responses are measured, and \( P \) impulse responses are predicted. This illustrates a single-input single-output communication system with a CSI matrix of dimension \( 1 \times 1 \). Increasing the number of receiver and transmitter antennas likewise increases the dimensions of \( H(t) \). Although there will be correlation for each of the individual CSI element magnitudes in time, we expect different CSI elements to have independent channel gains.

### IV. RECURRENT NEURAL NETWORKS

For a sequence of samples, a RNN uses the output obtained with the previous timestep as part of the input used to calculate the output for the next timestep as shown in Fig. 3. In this example, \( x, h \), and \( o \) are time-series vectors respectively representing the input, hidden layer state, and the output of the network. The neural network weight matrices are given by \( U, V \), and \( W \). The hidden layer state is also an output from the current cell to the next cell and is calculated as \( h_t = g_1(U \cdot x_t + V \cdot h_{t-1}) \), while the output is \( o_t = g_2(W \cdot h_t) \), where \( g_1 \) and \( g_2 \) are activations that may include functions such as sigmoid or hyperbolic tangent as defined by

\[
\text{sigmoid} := \sigma(z) = \frac{1}{1 + e^{-z}}
\]

(3)

\[
\text{hyperbolic tangent} := \tanh(z) = \frac{e^z - e^{-z}}{e^z + e^{-z}}.
\]

(4)

RNNs can be beneficial when the sequential samples are not independent from one another and has applications for time-series prediction [54] and anomaly detection [55]. The RNN architectures we will use consist of the variations of LSTM and GRU cells illustrated in Fig. 4.

**A. LSTM**

LSTM cells addressed the exploding of gradient problem of previous RNNs [56]. The current input vector, \( x_t \), is concatenated with the output vector of the previous LSTM cell,
The output of the generative model is a function of a random variable and the neural network weights in $G$. The output of $D$ is a probability that the sample is “Fake” (0.0) or “Real” (1.0). In our application, legitimate trusted transmitters should be labeled as “Real” and illegitimate untrusted transmitters should be labeled as “Fake”.

The GAN minimax value function, from Goodfellow et al. [40], is given by

$$\min_G \max_D V(D, G) = \mathbb{E}_{x \sim p_{data}(x)} \left[ \log D(x) \right] + \mathbb{E}_{z \sim p_z(z)} \left[ \log (1 - D(G(z))) \right]$$

where $D(x)$ is the output of the discriminative model when $x$ is a “Real” sample from the training dataset, and $D(G(z))$ is the discriminator output when the input is a “Fake” sample created by the generator.

For the CGAN, we also provide conditional information to the discriminator and generator. The conditional information is the previous magnitudes of the CSI elements associated with $t_0 \in \{t_1, t_2, \ldots, t_S\}$. The vector $q(t)$ is the magnitude of the CSI elements at time $t_0$, and $\hat{Q} = \{q(t_1), q(t_2), \ldots, q(t_S)\}$. The output of the discriminator is the probability that $X$ is the channel gain matrix composed of channel gain vectors at time $t_0 \in \{t_{S+1}, t_{S+2}, \ldots, t_{S+P}\}$, given the previous channel gain matrix, $\hat{Q}$. The number of future channel measurements is $P$, while the number of historic channel measurements is $S$. The generator output, $G(z|\hat{Q})$ is a channel gain matrix approximating $X$, given that $\hat{Q}$ was the matrix composed of previous channel gain vectors. Latent points from a random noise distribution are used to create the vector $z$. Therefore, (13) becomes

$$\min_G \max_D V(D, G) = \mathbb{E}_{X \sim p_{data}(x)} \left[ \log D(X|\hat{Q}) \right] + \mathbb{E}_{z \sim p_z(z)} \left[ \log (1 - D(G(z|\hat{Q}))) \right]$$

where $G$ produces $G(z|\hat{Q})$ and $D$ calculates $D(X|\hat{Q})$ and $D(G(z|\hat{Q}))$. Fig. 5 illustrates a CGAN during training. Using (14), the loss functions should be minimized for
the discriminator and generator are

\[
J^{(D)}_{\text{minimax}} = -\mathbb{E}_{X \sim p_{\text{data}}(X)} \left[ \log D(X|\bar{Q}) \right] - \mathbb{E}_{z \sim p_{z}(z)} \left[ \log \left( 1 - D(G(z|\bar{Q})) \right) \right]
\]

\[
J^{(G)}_{\text{minimax}} = \mathbb{E}_{z \sim p_{z}(z)} \left[ \log \left( 1 - D(G(z|\bar{Q})) \right) \right]
\]

(15)

where \(J^{(D)}_{\text{minimax}}\) is the sign-opposite of (14), since the result of \(J^{(D)}_{\text{minimax}}\) should be minimized, and (14) calls for the discriminator network to maximize the value function. The term containing \(D(X|\bar{Q})\) from (14) is omitted from \(J^{(G)}_{\text{minimax}}\) in (15) since the generator is not connected to the discriminator while the samples from the dataset, \(X\), are being processed by the discriminator.

Alternative loss functions can also be used for the discriminator and generator networks. In this work, we use the loss functions in (15) and also train networks in a CGAN framework using a mean squared error (MSE) loss for the generator network. In [60], Mao et al. introduced the least squares generative adversarial network (LSGAN) in order to address the issue of vanishing gradients while training GANs by applying a MSE loss to the discriminator. To see if the accuracy of the discriminator and generator changes with alternative loss functions to the vanilla cross entropy loss for both networks, we also use the loss functions from [60] as shown in

\[
J^{(D)}_{\text{MSE}} = \mathbb{E}_{X \sim p_{\text{data}}(X)} \left[ (D(X|\bar{Q}) - 1)^2 \right]
\]

\[
+ \mathbb{E}_{z \sim p_{z}(z)} \left[ (D(G(z|\bar{Q}) - 0)^2 \right]
\]

\[
J^{(G)}_{\text{MSE}} = \mathbb{E}_{z \sim p_{z}(z)} \left[ (D(G(z|\bar{Q})) - 1)^2 \right].
\]

(16)

Additionally, we’ll train the CGAN with a hybrid of loss functions: the binary cross entropy (BCE) loss in (15) for the discriminator, and use a MSE loss for the generator, as shown in

\[
J^{(D)}_{\text{hybrid}} = -\mathbb{E}_{X \sim p_{\text{data}}(X)} \left[ \log D(X|\bar{Q}) \right] - \mathbb{E}_{z \sim p_{z}(z)} \left[ \log \left( 1 - D(G(z|\bar{Q})) \right) \right]
\]

\[
J^{(G)}_{\text{hybrid}} = \mathbb{E}_{z \sim p_{z}(z)} \left[ (D(G(z|\bar{Q})) - 1)^2 \right].
\]

(17)

By using the MSE loss in the generator based on [60], we reduce the chance that vanishing gradients will prevent the network from reaching the highest quality generated CSI samples. That is, when the discriminator easily determines the generator output to be “Fake”, \(D(G(z|\bar{Q}))\) is close to zero. Near zero, the magnitude of the MSE gradient is greater than the magnitude of the BCE gradient. The larger gradient magnitude will create a bigger update to the neural network weights, subsequently resulting in the distribution of generator outputs quickly approaching \(p_{\text{data}}(X)\). By using BCE loss in the discriminator, we hope to train a binary classifier that quickly converges to an optimum state. The BCE loss has a greater penalty for misclassifications when compared to MSE loss and since we use BCE loss in the discriminator with this hybrid approach, we also avoid problems with converging on non-optimal local minima when using MSE loss for binary classification [29].

V. SIMULATION

In this section, we discuss the system model and the architecture of the neural networks under consideration. We continue with our evaluation methodology and discuss how we will use the neural networks to make an authentication decision.

A. SYSTEM MODEL

We consider an independent and identically distributed \(2 \times 2\) MIMO Rayleigh multipath fading channel with path delay profile shown in Table 1. The path delay profile is specified by the extended vehicular A (EVA) model in [61]. The power spectral density used is the Clarke model [62], with a maximum Doppler shift of 70 Hz. We simulated our channel with a 10 kHz sample rate and scaled the amplitude of the CSI elements \([0,1]\). To train the networks, 60% of the samples were used for training and the remainder was reserved for testing. Fig. 6 shows the magnitude of the CSI elements and the partitioning of the dataset.

The training and testing data was sequenced so that each input sample consisted of \(S\) time steps and four amplitude features. The target variable for training and testing was likewise sequenced so that each sample consisted of \(P\) future time steps and four amplitude features.

B. NEURAL NETWORK DEVELOPMENT

The RNNs we considered were composed of LSTM cells or GRU cells. The Adam optimizer [63] was used and to avoid overfitting, all the networks used a recurrent Dropout [64] of
of the concatenation of GRU CGAN generators had a conditional input consisting of previous channel response vectors, \( Q \). The LSTM and GRU CGAN generators had a conditional input consisting of the concatenation of \( Q \) and a random seed tensor, \( z \). The seed tensor was composed of latent points from \( U(0, 1) \). The discriminator input is either the target variable from the dataset or a channel gain matrix created by the generator, \( G(\tilde{z}|\tilde{Q}) \). A summary of the architecture of the neural networks is shown in Table 2.

For the standalone LSTM and GRU networks, the loss function used was MSE,

\[
\text{MSE} = \frac{1}{T} \sum_{t=1}^{T} e_t \\
e_t = \frac{1}{NM} \sum_{n,m} (Q_{n,m} - \hat{Q}_{n,m})^2
\]

where \( T \) is the number of samples, \( Q \) is the true value for the channel gain tensor at each time, \( t_p \), and \( \hat{Q} \) is the networks’ predicted value for each \( t_p \). The element-wise mean squared error between \( Q \) and \( \hat{Q} \) for sample \( i \) is \( e_t \). The CGANs use the loss functions described in (15), (16), (17).

**C. EVALUATION CRITERIA**

To assess relative performance, we used MSE between the predicted channel gain and the true channel gain as our metric. MSE is favored as a metric since it is sensitive to mean absolute error and root mean squared error when the error is large. After training, we evaluated the MSE produced by the standalone networks and the generator networks from the CGANs. After gathering MSE measurements for the simulated channel, we established a threshold, \( MSE_T \) for authentication. That is, when

\[
\text{MSE} \leq MSE_T \rightarrow \text{authenticate}, \\
\text{MSE} > MSE_T \rightarrow \text{do not authenticate}. \quad (19)
\]

If the error between the predicted and actual channel measurement is less than or equal to the threshold, the transmitter should be authenticated. Otherwise, the transmission should be denied authentication.

Since the CGANs train a discriminator and a generator, we can also use the discriminator to make the authentication decision. The discriminator output will indicate whether the input is “Real” or “Fake”. Because the discriminator is trained on the channel gain profile shown in Fig. 6, these samples should be assessed as “Real”. We created additional channel responses representing four other transmitters using the same EVA power delay profile shown in Table 1. There were 395 samples in each group of channel responses. The samples from these new profiles were not seen by the networks before testing and represent illegitimate transmitters that the discriminator should assess as “Fake”. Regarding the authentication decision, if the discriminator output for the sample is “Real,” we authenticate, and if discriminator output is “Fake” we do not authenticate.

**VI. RESULTS**

In this section, we present the results of our simulations applying the BCE loss from (15), the MSE loss from (16), and the hybrid loss from (17) to the CGAN networks. The standalone LSTM and GRU networks both use the MSE loss in (18).

Both the standalone RNN and CGAN-based RNN methods of channel prediction showed very high accuracy in our MIMO mobile channel environment. To this point, when measuring MSE, we found that converting MSE to dB units was necessary to get a better sense of the error, since the MSE was such a small value. That is, MSE(dB) = 10log(MSE). To make an authentication decision based on channel prediction, we required a threshold to determine if the received CSI is likely to be from a transmitter that should be authenticated. Because of the threshold, high channel prediction accuracy is required so that legitimate transmitters are authenticated and illegitimate transmitters are denied authentication.

With \( S = 5 \), \( P \) is increased from 1 to 10, allowing the networks to predict future MIMO channel response magnitudes. With our 10 kHz sample rate, the amount of time elapsed for every prediction step, \( P \), is 100 \( \mu \)s. Except for \( P = 1 \) where the CGAN-GRU predicted the channel better than any other network configuration, the standalone networks performed better than the generator networks in the CGANs, achieving the least amount of error as shown in Fig. 7.

The superior performance of the standalone alone networks compared to their CGAN counterparts can at least be partially attributed to the difficulty in training GANs. Evaluation of adversarially-trained neural networks is difficult without human intervention [65], [66]. This is not the case for the standalone networks, as the single network can be monitored for signs of convergence and optimal training. Additionally, the purpose of the CGANs is not solely to create a network for channel prediction, but also to produce a discriminator to identify legitimate and illegitimate transmitters based on received CSI. Therefore, the training of the generator and discriminator needs to be balanced so that one network does not dominate the other, again resulting in vanishing gradients. Both the generator and discriminator are monitored, and performance is expected to vary as training continues and both networks mutually improve.

---

**TABLE 2: Neural networks architecture.**

| Input Layer | Hidden Layer | Output Layer |
|-------------|--------------|--------------|
| Input       | LSTM         | Output       |
| LSTM        | LSTM         | Output       |
| LSTM        | LSTM         | Output       |
| LSTM        | LSTM         | Output       |

For example, Table 2 shows the architecture of the neural networks. The LSTM and GRU networks were trained with a conditional input consisting of previous channel response vectors, \( Q \). The LSTM and GRU CGAN generators had a conditional input consisting of the concatenation of \( Q \) and a random seed tensor, \( z \). The seed tensor was composed of latent points from \( U(0, 1) \). The discriminator input is either the target variable from the dataset or a channel gain matrix created by the generator, \( G(\tilde{z}|\tilde{Q}) \). A summary of the architecture of the neural networks is shown in Table 2.
We applied (19) with $S = 5$ and $P = 1$ for $MSE_T$ values $-50 \, \text{dB} \leq MSE_T \leq -20 \, \text{dB}$ to determine which transmitter’s channel gain profile to authenticate. Although accuracy increases for all networks up to $MSE_T$ of $-25 \, \text{dB}$ as shown in Fig. 8, false positives begin to arise at $-25 \, \text{dB}$ and greater, which would allow illegitimate transmitters to authenticate. At $-30 \, \text{dB}$, there are no false positives, as shown in the upper right quadrants of Fig. 9(a) through Fig. 9(d). As shown in Fig. 8, the standalone GRU network was the most accurate in authenticating from channel prediction, achieving 98.1% accuracy. The generator from the CGAN-GRU using BCE loss was the next-best configuration, reaching 96.2% accuracy in Fig. 8(a).

In addition to authenticating based on channel prediction and applying a MSE threshold, the CGAN-trained discriminators can be used for authentication. For $S = 5$ and $P = 1$, Fig. 10 shows the confusion matrices for the CGAN-LSTM and CGAN-GRU discriminator networks using BCE loss, MSE loss, and the hybrid loss. Compared to the MSE authentication method, the CGAN-GRU trained with the hybrid loss improves its authentication performance from 96.2% to 98.5% as shown in Fig. 10(f). This matches the authentication accuracy of the standalone GRU while still preventing any illegitimate transmitters from authenticating.

In Fig. 7 and Fig. 8, we see that the GRU-enabled RNNs performed better than the LSTM RNNs for channel prediction. It appears then, that the GRU-enabled RNNs are more suited to this task than those with LSTM cells. We also believe that this dataset of received MIMO CSI samples is also more appropriate for the discriminator in the CGAN-GRU than the discriminator in the CGAN-LSTM. When we compare the CGAN discriminator performance, we see that the CGAN-GRU trained with hybrid loss in Fig. 10(f) had the highest accuracy, followed by the CGAN-GRU trained with MSE loss in Fig. 10(d). The LSTM and GRU CGANs that used BCE loss performed about the same as we see in
FIGURE 10. Confusion matrices for discriminators performing authentication trained through (a) CGAN-LSTM with BCE loss, (b) CGAN-GRU with BCE loss, (c) CGAN-LSTM with MSE loss, (d) CGAN-GRU with MSE loss, (e) CGAN-LSTM with hybrid loss, and (f) CGAN-GRU with hybrid loss.

Figs. 10(a) and 10(b). Among the CGAN-trained discriminators using LSTM cells, regardless of loss function applied, we see that they all had similar test results as shown in the confusion matrices in Figs. 10(a), 10(c), and 10(e). However, depending on which loss function was applied, the CGAN-GRU discriminators had substantially different results as shown in Figs. 10(b), 10(d), and 10(f). The combination of a discriminator trained with BCE loss and a generator trained with MSE loss produced the most accurate CGAN-GRU discriminator but did not produce the most accurate CGAN-LSTM discriminator as shown in Fig. 10. The BCE loss in the discriminator applied a larger loss penalty when the discriminator misclassified a CSI sample compared to the penalty if MSE loss was used. This larger penalty encourages larger changes to the neural network weights in the discriminator, resulting in greater output changes and improved accuracy. Additionally, the MSE loss function in the generator was used to prevent stalling of the generator network. Early on in training, the generator is not expected to produce CSI samples that match those from the dataset, however, after only a few training iterations the discriminator is able to assess the difference between the samples in the dataset and the random outputs from the untrained generator. Therefore, $D(G(z|\hat{Q}))$ will be near zero. The gradient magnitude near zero in the BCE loss function is relatively small compared to the larger gradient magnitude of the MSE function. If BCE loss is used in the generator and the discriminator output is near zero, the weights of the generator will not have large updates and the generator will continue producing samples that the discriminator can easily assess as “Fake”. Thus, the generator will not improve very much, nor will the discriminator have an opportunity to get better at recognizing spoofed CSI samples that are nearly the same as the legitimate samples from the dataset. However, with MSE loss applied to the generator, the larger gradient magnitude produces a large change to the generator network weights. This encouraged the generator to create more realistic samples earlier on in training, and in turn, forced the discriminator to be more precise in extracting the relevant features of the input to more accurately classify the given sample.

While the standalone GRU-based RNN achieved the lowest error for channel prediction, the CGAN-GRU discriminator trained with the hybrid loss had the best authentication accuracy performance by a narrow margin. The advantage to using a discriminator trained in a CGAN-GRU architecture over the standalone RNN model is that the discriminator automatically determines the boundaries and features of received CSI from the legitimate transmitter. This was done without manual intervention or examining test results to determine an appropriate value for $MSE_T$. By taking advantage of deep learning and adversarial training, the discriminator implicitly discovered a threshold that was used to determine the discriminator output.

Although we have no false positive results using $MSE_T = -30$ dB or the CGAN discriminators as shown in Fig. 9 and Fig. 10, respectively, this does not suggest that an illegitimate transmitter will always be denied authentication. However, as seen in our results, all 1,580 testing samples were correctly categorized as “Fake”, implying the probability of inadvertently authenticating an illegitimate transmitter is on the order of 0.001 or less.

VII. CONCLUSION

In this work, we explored various RNN architectures to make authentication decisions at the physical layer in a mobile MIMO multipath channel. Alternative loss functions for the CGAN networks were also explored with BCE outperforming MSE in an LSGAN configuration and a hybrid loss where the discriminator used BCE and the generator used MSE. Varying the amount of channel responses and channel prediction time, regression performance was measured using mean square error against the ground truth. Using a MSE threshold of $-30$ dB, and without any false positive errors, the standalone GRU network achieved the highest authentication performance at 98.1%, followed by the CGAN-GRU at 96.2% accuracy. Using a CGAN-trained discriminator with a hybrid loss function, the network was able to authenticate at a 98.5% rate. Whether constructed as part a standalone network or incorporated into a CGAN architecture, the RNNs using GRU cells outperformed RNNs using LSTM cells for channel prediction. Due to the higher accuracy in channel prediction, for the task of predicting channel responses and classifying whether or not a transmitter should
be authenticated, architectures using GRU cells were superior to networks that used LSTM cells. The CGAN networks, particularly the CGAN-GRU, performed well compared to the standalone networks, encouraging further research and hyperparameter optimization.

Future work includes application of the methods in this paper to multi-carrier channels as well as classifying a variety of time-series channel gain profiles to enable multiple transmitter authentication. Additionally, more experimentation will be performed with GRU and LSTM RNNs under various dataset sizes and sample dimensions to determine the optimum network configuration for specific applications.

REFERENCES

[1] A. Sibille, C. Oestges, and A. Zanella, MIMO: From Theory to Implementation. Boston, MA, USA: Elsevier, 2011.

[2] L. Ferrari, ‘The Rabyten of Death’ Cyberattack Against DoD Looms, DISA Director Warns. Accessed: Jan. 9, 2020. [Online]. Available: https://wwwdefense.gov/ExploreNews/Article/Article/1414146/the-rabyten-of-death-cyberattack-against-dod-looms-disa-director-warns

[3] F. Konkel. (2018). Pentagon Thwarts 36 Million Email Breach Attempts Daily. [Online]. Available: https://www.nextgov.com/cybersecurity/201801/pentagon-thwarts-36-million-email-breach-attempts-daily/145149

[4] S. Gallagher. Hacker’s Paradise: Louisiana’s Ransomware Disaster Far From Over—Arts Technica. Accessed: Jan. 9, 2020. [Online]. Available: https://arstechnica.com/information-technology/2019/11/hackers-paradise-louisiana-s-ransomware-disaster-far-from-over

[5] (2019). Hackers Demand $14 Million From Nursing Homes in Ransomware Attack. [Online]. Available: https://www.cbsnews.com/news/hackers-ransomware-nursing-homes-14-million/

[6] W. C. Jakes, Microwave Mobile Communications. New York, NY, USA: Wiley, 1974.

[7] A. Duel-Hallen, “Fading channel prediction for mobile radio adaptive transmission systems,” Proc. IEEE, vol. 95, no. 12, pp. 2299–2313, Dec. 2007.

[8] A. Duel-Hallen, S. Hu, and H. Hallen, “Long-range prediction of fading signals,” IEEE Signal Process. Mag., vol. 17, no. 3, pp. 62–75, May 2000.

[9] L. Hanzo, C. H. Wong, and M. S. Yee, Adaptive Wireless Transceivers. Chichester, U.K.: Wiley, Feb. 2002. [Online]. Available: http://doi.wiley.com/10.1002/047084776X

[10] X. Gao, J. Tankulicen, and S. Ovaska, “Comparison of linear and neural network-based power prediction schemes for mobile DS/CDMA systems,” in Proc. Veh. Technol. Conf. (VTC), vol. 1, Apr. 1996, pp. 61–65.

[11] W. Liu, L.-L. Yang, and L. Hanzo, “Recurrent neural network based narrowband channel prediction,” in Proc. IEEE 63rd Veh. Technol. Conf., vol. 5, May 2006, pp. 2173–2177.

[12] C.-K. Wen, W.-T. Shih, and S. Jin, “Deep learning for massive MIMO CSI feedback,” IEEE Wireless Commun. Lett., vol. 7, no. 5, pp. 748–751, Oct. 2018.

[13] W. Jiang and H. D. Schotten, “Deep learning for fading channel prediction,” IEEE Open J. Commun. Soc., vol. 1, pp. 320–332, 2020.

[14] C. Luo, J. Ji, Q. Wang, X. Chen, and P. Li, “Channel state information prediction for 5G wireless communications: A deep learning approach,” IEEE Trans. Netw. Sci. Eng., vol. 7, no. 1, pp. 227–236, Jan.–Mar. 2020.

[15] R. Fantacci, L. Maccari, T. Pecorella, and F. Frosali, “Analysis of secure handover for IEEE 802.1x-based wireless ad hoc networks,” IEEE Wireless Commun., vol. 14, no. 5, pp. 21–29, Oct. 2007.

[16] X. Wang, P. Hao, and L. Hanzo, “Physical-layer authentication for security enforcement: Current challenges and future developments,” IEEE Commun. Mag., vol. 54, no. 6, pp. 152–158, Jun. 2016.

[17] S. Fluhrer, I. Mantin, and A. Shamir, “Weaknesses in the key scheduling algorithm of RC4,” in Proc. 4th Annu. Workshop Sel. Areas Cryptogr., 2001, pp. 1–24.

[18] D. Menasce, “QoS issues in Web services,” IEEE Internet Comput., vol. 6, no. 6, pp. 72–75, Nov./Dec. 2002.
[42] K. Armanious et al., “MedGAN: Medical image translation using GANs,” *Comput. Med. Imag. Graph.*, vol. 79, Nov. 2019, Art. no. 101684. [Online]. Available: http://www.sciencedirect.com/science/article/pii/S0895719719300990

[43] J. Bao, D. Chen, F. Wen, H. Li, and G. Hua, “CVAE-GAN: Fine-grained image generation through asymmetric training,” in *Proc. IEEE Int. Conf. Comput. Vis.* (ICCV), Oct. 2017, pp. 2764–2773.

[44] Q. Li et al., “AF-DCGAN: Amplitude feature deep convolutional GAN for fingerprint construction in indoor localization systems,” *IEEE Trans. Emerg. Topics Comput. Intell.*, early access, Nov. 5, 2019, doi: 10.1109/ETT.2019.2948058.

[45] Y. Dong, H. Wang, and Y.-D. Yao, “Channel estimation for one-bit multiuser massive MIMO using conditional GAN,” *IEEE Commun. Lett.*, vol. 25, no. 3, pp. 854–858, Mar. 2021.

[46] T. Ding and A. Hirose, “Fading channel prediction based on combination of complex-valued neural networks and chirp Z-transform,” *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 25, no. 9, pp. 1686–1695, Sep. 2014.

[47] Q. Wang, H. Li, D. Zhao, Z. Chen, S. Ye, and J. Cai, “Deep neural networks for CSI-based authentication,” *IEEE Access*, vol. 7, pp. 123026–123034, 2019.

[48] W. Jiang and H. D. Schotten, “Recurrent neural networks with long short-term memory for fading channel prediction,” in *Proc. IEEE 91st Veh. Technol. Conf. (VTC-Spring)*, May 2020, pp. 1–5.

[49] D. Roy, T. Mukherjee, M. Chatterjee, and E. Papilio, “RF transmitter fingerprinting exploiting spatio-temporal properties in raw signal data,” in *Proc. 18th IEEE Int. Conf. Mach. Learn. Appl. (ICMLA)*, Boca Raton, FL, USA, Dec. 2019, pp. 89–96.

[50] K. S. Germain and K. Kragh, “Mobile physical-layer authentication using channel state information and conditional recurrent neural networks,” in *Proc. IEEE 93rd Veh. Technol. Conf. (VTC-Spring)*, Helsinki, Finland, Apr. 2021.

[51] D. Fang, Y. Qian, and R. Q. Hu, “Security for 5G mobile wireless networks,” *IEEE Access*, vol. 6, pp. 4850–4874, 2018.

[52] K. Yu and B. Ottersten, “Models for MIMO propagation channels: A review,” *Wireless Commun. Mobile Comput.*, vol. 2, no. 7, pp. 653–666, 2002. [Online]. Available: https://onlinelibrary.wiley.com/doi/abs/10.1002/wcm.78

[53] W. Jiang and H. D. Schotten, “Neural network-based channel prediction and its performance in multi-antenna systems,” in *Proc. IEEE 88th Veh. Technol. Conf. (VTC-Fall)*, Aug. 2018, pp. 1–6.

[54] J. T. Connor, R. D. Martin, and L. E. Atlas, “Recurrent neural networks and robust time series prediction,” *IEEE Trans. Neural Netw.*, vol. 5, no. 2, pp. 240–254, Mar. 1994. [Online]. Available: http://doi.org/10.1109/72.279188

[55] T. J. O’Shea, T. C. Clancy, and R. W. McGwier, “Recurrent neural radio anomaly detection,” Nov. 2016. [Online]. Available: http://arxiv.org/abs/1611.00301

[56] S. Hochreiter and J. Schmidhuber, “Long short-term memory,” *Neural Comput.*, vol. 9, no. 8, pp. 1735–1780, Nov. 1997. [Online]. Available: https://www.mitpressjournals.org/doi/abs/10.1162/neco.1997.9.8.1735

[57] K. Cho et al., “Learning phrase representations using RNN encoder–decoder for statistical machine translation,” in *Proc. Conf. Empir. Methods Nat. Lang. Process. (EMNLP)*, Oct. 2014, pp. 1724–1734. [Online]. Available: https://www.aclweb.org/anthology/D14-1179

[58] R. Jozefowicz, W. Zaremba, and I. Sutskever, “An empirical exploration of recurrent network architectures,” in *Proc. 32nd Int. Conf. Int. Conf. Mach. Learn.*, vol. 37, 2015, pp. 2342–2350.

[59] J. Chung, C. Gulcehre, K. Cho, and Y. Bengio, “Empirical evaluation of gated recurrent neural networks on sequence modeling,” in *Proc. NIPS Workshop Deep Learn.*, Dec. 2014.

[60] X. Mao, Q. Li, H. Xie, R. Y. K. Lau, Z. Wang, and S. P. Smolley, “Least squares generative adversarial networks,” in *Proc. IEEE Int. Conf. Comput. Vis.* (ICCV), Oct. 2017, pp. 2813–2821.

[61] Evolved Universal Terrestrial Radio Access (E-UTRA); User Equipment (UE) Radio Transmission and Reception, 3GPP Standard TS 36.101, 2020. [Online]. Available: https://www.3gpp.org

[62] R. H. Clarke, “A statistical theory of mobile-radio reception,” *Bell Syst. Techn. J.*, vol. 47, no. 6, pp. 957–1000, Jul./Aug. 1968.

[63] D. P. Kingma and J. Ba, “Adam: A method for stochastic optimization,” in *Proc. 3rd Int. Conf. Learn. Represent. (ICLR)*, Dec. 2014. [Online]. Available: http://arxiv.org/abs/1412.6980

[64] N. Srivastava, G. Hinton, A. Krizhevsky, I. Sutskever, and R. Salakhutdinov, “Dropout: A simple way to prevent neural networks from overfitting,” *J. Mach. Learn. Res.*, vol. 15, no. 56, pp. 1929–1958, 2014. [Online]. Available: http://jmlr.org/papers/v15/srivastava14a.html

[65] T. Salimans, I. Goodfellow, W. Zaremba, V. Cheung, A. Radford, and X. Chen, “Improved techniques for training GANs,” in *Advances in Neural Information Processing Systems 29*, D. D. Lee, M. Sugiyama, U. V. Luxburg, I. Guyon, and R. Garnett, Eds. Red Hook, NY, USA: Curran Assoc., Inc., 2016, pp. 2234–2242. [Online]. Available: http://papers.nips.cc/paper/6125-improved-techniques-for-training-gans.pdf

[66] L. Theis, A. V. D. Oord, and M. Bethge, “A note on the evaluation of generative models,” Apr. 2016. [Online]. Available: http://arxiv.org/abs/1511.01844

KEN ST. GERMAIN (Graduate Student Member, IEEE) received the B.S.E.E. degree from the University of Nebraska, Lincoln, NE, USA, in 2000, the M.S.E.E. degree in 2005, and the M.S. degree in space operations from the Naval Postgraduate School, Monterey, CA, USA, in 2013, where he is currently pursuing the Ph.D. degree with the Department of Electrical and Computer Engineering.

He received his commission in the United States Navy in 2000 as a Cryptologic Warfare Officer. He continues to serve with the Department of Electrical and Computer Engineering, Naval Postgraduate School. His research interests include communications and cyber warfare.

FRANK KRAGH received the B.S.E.E. degree from the California Institute of Technology, Pasadena, CA, USA, in 1986, the M.S.E.E. degree from the University of Central Florida, Orlando, FL, USA, in 1990, and the Ph.D. degree in electrical engineering from the Naval Postgraduate School, Monterey, CA, USA, in 1997.

From 1998 to 2001, he served the Department of Defense as a Government Research Engineer and as a Government Contractor. From 2001 to 2003, he served as the Deputy Chief Engineer (Research and Development) for the Communications Programs Directorate of the Space and Naval Warfare Systems Command (currently Naval Information Warfare Systems Command). He is currently an Associate Professor with the Electrical and Computer Engineering Department, Naval Postgraduate School. He teaches courses in the areas of software defined radio, digital communications, and forward error correction coding. His research interests include data mining, cognitive systems, signals intelligence, software defined radio, multiple-input multiple-output communications systems, and modulation and coding.

974   VOLUME 2, 2021