GPS Solutions (2021) 25:115
https://doi.org/10.1007/s10291-021-01154-7

ORIGINAL ARTICLE

Machine learning-based approach to GPS antijamming

Cheng-Zhen Wang[1] · Ling-Wei Kong[1] · Junjie Jiang[1] · Ying-Cheng Lai[1,2]

Received: 1 December 2020 / Accepted: 12 June 2021 / Published online: 19 June 2021

Abstract

A challenging and outstanding problem in applications that involve or rely on GPS signals is to mitigate jamming. We develop a machine learning-based antijamming framework for GPS signals. Three types of jamming signals are considered: continuous wave interference, chirp and pulse jamming. In addition, white Gaussian noise is assumed to be present. From the point of view of communication, information is encoded in the coarse/acquisition (C/A) code. Multiplying the jammed signal by a sinusoidal wave and integrating over one C/A code period leads to a jammed C/A code signal. To mitigate jamming, we study three types of machine learning methods: reservoir computing (echo state network), multi-layer perceptron, and long short-term memory networks (RNNs). A machine can be trained to learn and predict the signal directly or learn and predict jamming where the real signal can be obtained by removing the jammed component from the total received signal. For a high-frequency carrier (e.g., the standard 1575.42 MHz L1 carrier), learning and prediction can be made computationally efficiently on the C/A code signal. The main result is that machine learning can be effective for predicting and extracting weak GPS signals even in a strongly jammed/noisy environment where the jamming amplitude is three orders of magnitude stronger than the GPS signal. We find that the reservoir computing scheme is stable and performs well for all three types of jamming. The multi-layer perceptron is better for predicting the jamming signal than the GPS signal itself, and the long short-term memory networks work well but only for certain jamming types. In particular, with the direct signal prediction method, the bit error rate (BER) associated with reservoir computing (RC) remains at near-zero values (less than 1%) even for jamming signal ratio (JSR) up to 60 dB for the three types of jamming. The multi-layer perceptron (MLP) method breaks down when the JSR is larger than 20 dB for continuous wave interference (CWI) and pulse jamming, 45 dB for chirp jamming. The long short-term memory (LSTM) can perform very well for the chirp jamming with a near zero error rate and give BER larger than 10% when the JSR is around 40 dB for the CWI and pulse jamming. For the jamming prediction method (indirect method), these three machine learning methods perform well, with near-zero BER (less than 1%). Overall, the RC scheme is stable and performs well for three types of jamming. Besides, RC is fast compared to LSTM method, with much less running time.

Keywords GPS · Antijamming · Machine learning · Reservoir computing

Abbreviations

BER	Bit error rate
C/A	Code coarse/acquisition code
JSR	Jamming-to-signal ratio
LSTM	Long short-term memory
MLP	Multi-layer perceptron
PSD	Power spectral density
RC	Reservoir computing

✉ Ying-Cheng Lai
Ying-Cheng.Lai@asu.edu

[1] School of Electrical, Computer and Energy Engineering, Arizona State University, Tempe, AZ 85287, USA

[2] Department of Physics, Arizona State University, Tempe, AZ 85287, USA

Introduction

The global positioning system (GPS) has become an indispensable part of modern society with a large variety of civil and defense applications. The accuracy of navigation and tracking systems depends on the accuracy of received GPS signals which, due to their weak power, are vulnerable to external interference such as jamming and spoofing (Ioannides et al. 2016). Various methods have been proposed to mitigate GPS jamming (Ioannides et al. 2016), which include the adaptive filtering method (Borio et al. 2008; Mao et al. 2011; Chien et al. 2013), wavelet packet transform (Pardo et al. 2006; Mosavi et al. 2017), combined wavelet transform and filtering (Chen et al. 2016), wavelet-based correction (Mosavi et al. 2011), and artificial neural networks for interference rejection/suppression (Mao 2008; Mosavi and Shafiee 2016).

Previous works focused on the use of different filters or combining neural networks with filters for narrow band jamming. Here, we exploit machine learning to develop potential solutions to the GPS antijamming problem with narrow band and wide band jamming, especially reservoir computing, which is highly efficient and simple to construct. Recent years have witnessed an explosive growth of interest in machine learning because of its demonstrated superior capability in accomplishing complex tasks ranging from speech recognition (Hinton 2012) to playing Go (Silver et al. 2016). The basic principle underlying our study is that GPS antijamming can be viewed as a nonlinear signal prediction and classification problem that can be effectively solved using machine learning. Naturally, a jammed GPS signal is a mixture of jamming and GPS signal and, hence, if either the GPS signal or the jamming signal can be accurately predicted, the two can be separated from each other. The difficulty is that, often, jamming significantly overpowers the GPS signal, so it is critical to assess whether machine learning can be effective at predicting and separating two mixed signals of vastly different amplitudes. With this challenge in mind, we investigate the antijamming capability of three machine learning frameworks: reservoir computing (RC), multi-layer perceptrons (MLPs), and long short-term memory (LSTM) networks.

Reservoir computing

In chaotic time series and signal prediction, reservoir computing, a class of recurrent neural networks (RNNs), has stood out as a powerful paradigm, which is first proposed by Jaeger (2001) and subsequently used to predict nonlinear time series by Jaeger and Haas (2004) and even to predict large spatial temporally chaotic systems by Pathak et al. (2018). And recently, the role of the spectral radius is investigated by Jiang and Lai (2019), and even long time predictions of chaotic time series by feeding real data (Fan et al. 2020) and long-time prediction of phase information (Zhang et al. 2020). Reservoir computing has also been demonstrated to be effective at distinguishing and separating characteristically different chaotic signals (Carroll 2018; Krishnagopal et al. 2019).

Multi-layer perceptrons

Multi-layer perceptrons are classical, backpropagation-based artificial neural networks (Hertz et al. 1991). They represent the fundamental network architecture during the second wave of machine learning at the end of the last century. Due to the limitation of computational capability at that time, the number of hidden layers was typically quite small, e.g., one or two. In the current (third wave) of machine learning, the neural networks become "deep" in the sense that the number of hidden layers has increased dramatically, making sophisticated tasks such as recognition of images, handwritten characters and speech possible. The training of these deep neural networks is typically done with highly efficient, readily programmable, fast graphics processing units (GPUs) (LeCun et al. 2015).

Long short-term memory networks

LSTM networks are a class of unique RNNs, first introduced in 1997 to solve the gradient exploding and vanishing problem (Hochreiter and Schmidhuber 1997). The training of LSTM networks is typically accomplished with the conventional backpropagation through time. LSTM networks have been exploited to recognize the temporal order of separated events in noisy time series (Schmidhuber 2015), such as speech recognition (Graves 2013) and translation from one language to others (Sutskever et al. 2014).

We test the three types of neural machines to extract the information encoded into weak GPS signals through suppression or removal of jamming. The performance of antijamming is measured by the accuracy of recovering the information-carrying binary sequence (GPS C/A code) from severely jamming signals. The main conclusion of this study is that machine learning is generally capable of extracting the information encoded in the GPS signals for both narrow- and wide-band jamming types. In particular, the performance of RC can sustain jamming-to-signal ratio up to 60 dB, i.e., the jamming amplitude is three orders of magnitude higher than the GPS signal amplitude. RC thus stands out as the best choice among the three types of neural machines for GPS antijamming. There are three achievements in this research. First, we utilize the three different machine learning methods to mitigate jamming and find that reservoir computing is accurate and saves time. Second, our methods are applicable to both narrow- and wide-band jamming types and can be effective in situations where the jamming signal ratio is up to 60 dB along with Gaussian noise. Third, we can predict binary C/A code based on noise C/A code without down converting the high-frequency jamming signals (the prediction of intermediate frequency signal after down converting using reservoir computing is presented in Supplementary materials).

In the following, we first give the basic equation for GPS signal generation and its power spectral density. We then briefly describe reservoir computing and articulate a machine learning framework to mitigate jamming. We consider three different types of jamming and use three different machine learning methods to mitigate jamming. The bit error rate (BER) is used to characterize antijamming performance. Finally, we present conclusions and discussions.

GPS signal simulation

The C/A code and navigation message modulated GPS signal can be written as

$$s(t) = [D(t) \cdot CA(t)] \sin(2\pi f_{L1} t + \theta) \tag{1}$$

where $\mathrm{D}(t) = \pm 1$ is the binary navigation data sent out from the satellite with frequency of 50 Hz, $\mathrm{CA}(t) = \pm 1$ represents the binary C/A code with frequency of 1.023 MHz, f_{L1} is the $L1$ carrier frequency (1575.42 MHz), and θ is the phase delay which is set to be 0. In the simultaneous presence of jamming and noise, the signal received at the antenna, $r(t)$, can be written as

$$r(t) \ = \ s(t) \ + \ j(t) \ + \ n(t) \tag{2}$$

where $j(t)$ is the jamming signal and $n(t)$ denotes the additive white Gaussian noise. To be concrete, we fix the power of Gaussian noise to be 30 dB and vary the jamming-to-signal ratio up to 60 dB.

We generate C/A code bits from GPS PRN 1–37, e.g., the 7th PRN (Tsui 2005). In particular, we keep the **1**'s in the PRN number unchanged while changing the **0**'s to **−1**'s. We modulate the C/A code repeatedly on the carrier. We also generate a sequence of 5 random numbers (±1) as navigation data to modulate the 102300 bits of C/A code. A schematic illustration of the GPS modulation process is shown on the left side of Fig. 1. To simulate a jammed and noisy environment, we add jamming and Gaussian noise into the GPS signal. At the receiving end, the signal is demodulated and then integrated as

$$\tilde{r}(t) \ = \ 2r(t) \sin(2\pi f_{L1} t + \theta) \tag{3}$$

$$r(k) \ = \ \frac{1}{T_{CA}} \int_{(k-1)T_{CA}}^{kT_{CA}} \tilde{r}(t) dt \tag{4}$$

for $k = 1, 2, \ldots$, where the demodulation sinusoidal signal in (3) has the same frequency and phase as the GPS carrier signal. The integration is carried out over one C/A code period T_{CA} (containing 1500 periods of the sinusoidal carrier wave) consecutively for the C/A binary code to be recovered. This procedure is schematically shown in Fig. 1. In the absence of jamming and Gaussian noise, the C/A code can be perfectly recovered via the integration. When both jamming and noise are present, direct integration of the contaminated signal will not give the correct C/A code, as illustrated on the right side of Fig. 1. We note that the carrier wave and the noise in Fig. 1 are schematic illustrations, not the real signals we study in this work.

We study three different types of jamming: continuous wave interference (CWI), chirp jamming signal with a sweeping frequency wave, and pulse jamming in the form of a discontinuous sinusoidal wave. Figure 2 shows the power spectral density (PSD) of the three types of jamming signals. We focus on the realistic case where jamming overpowers the GPS signal. For the case of CWI jamming, whose PSD consists of a pronounced narrow peak and a broad but weak spectral background, the peak value is much larger than that of the GPS signal, as shown in Fig. 2a. For chirp and pulse jamming signals that have a broad band power spectrum, the PSD of the GPS signal is "buried" completely inside that of the jamming, as shown in Figs. 2b, c, respectively.

Machine learning

To recover the C/A code from a jammed GPS signal, we apply machine learning to the integrated noisy data to predict the real binary C/A code. A convenient quantity to characterize the performance of antijamming is the bit error rate (BER) defined from the C/A code, where we set the code value to +1 (−1) if it is positive (negative). As an illustrative example, we use 102300 C/A noisy code bits (corresponding to five navigation bits) in total as input to the neural network. We use the first 40000 noisy C/A code bits along with the true C/A code to train the neural network, while the remaining C/A code bits are for testing the machine prediction.

A detailed description of the three machine learning methods is in the Supplementary Materials. Below, we give a simple description of reservoir computing. A schematic illustration of RC is shown in Fig. 3, where the neural machine consists of three components: (1) a linear input layer converting a low-dimensional (say M) input signal into a high (N) dimensional vector, (2) the reservoir network with N dynamical nodes driven by both the input and the interaction or coupling with the other reservoir nodes, and (3) a linear output layer that maps the high-dimensional reservoir network state vector into an L-dimensional vector signal.

There are two methods of training and prediction with the target signal to be the actual GPS or jamming signal, respectively. In the first method, we train the neural network with

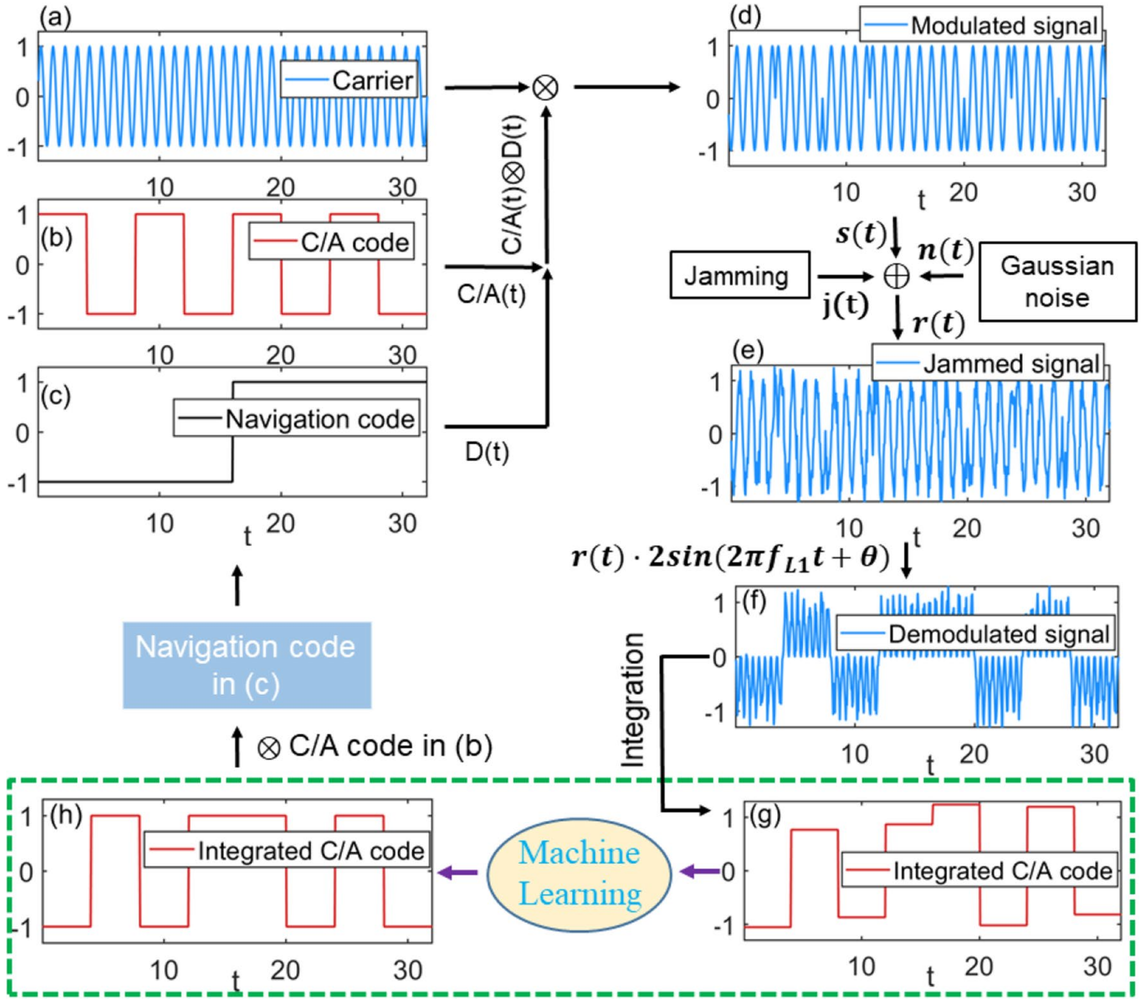


Fig. 1 Schematic illustration of GPS signal modulation, demodulation and machine learning-based antijamming. The left and right sides show the modulation and demodulation processes, respectively. In the modulation process, the L1 carrier is modulated by the binary C/A code CA(t) which itself is modulated by the binary navigation data D(t), giving the "pure" GPS signal $s(t)$. In the simultaneous presence of jamming $j(t)$ and Gaussian noise $n(t)$, at the receiving end, the signal is $r(t)$, and the jammed GPS signal is demodulated by the same carrier waveform and integrated to generate a deformed C/A code that provides the input to the neural machine for learning and prediction. Training of the neural network is accomplished with the deformed C/A code as input and the original, "clean" C/A code as the target. With a segment of actual deformed C/A code as input, a properly trained neural network generates the predicted C/A code, where the effects of jamming and noise are suppressed or even removed

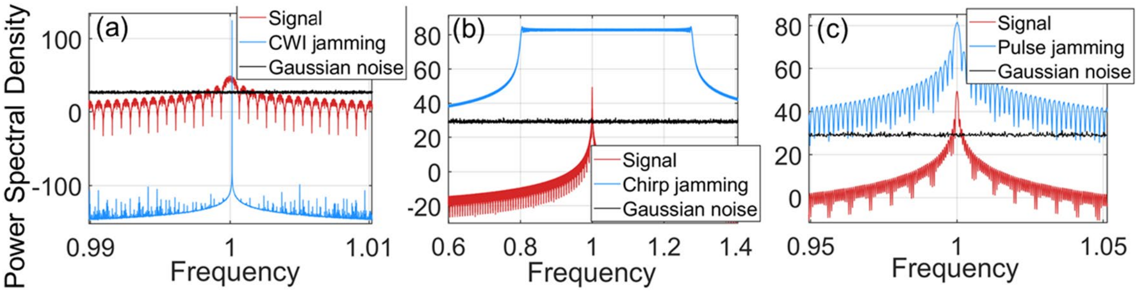


Fig. 2 Power spectral density (PSD) of modulated GPS carriers (red), additive white Gaussian noise (black), and three different types of jamming (blue): **a** CWI jamming; **b** chirp jamming; **c** pulse jamming. For weak GPS signals in general, the maximum value of its PSD is much smaller than that of jamming, as for CWI jamming in (**a**). For chirp and pulse jamming, the PSD of the GPS signal is "buried" completely inside that of jamming (**b**, **c**). The frequency axes are in units of the GPS carrier frequency f_{L1}

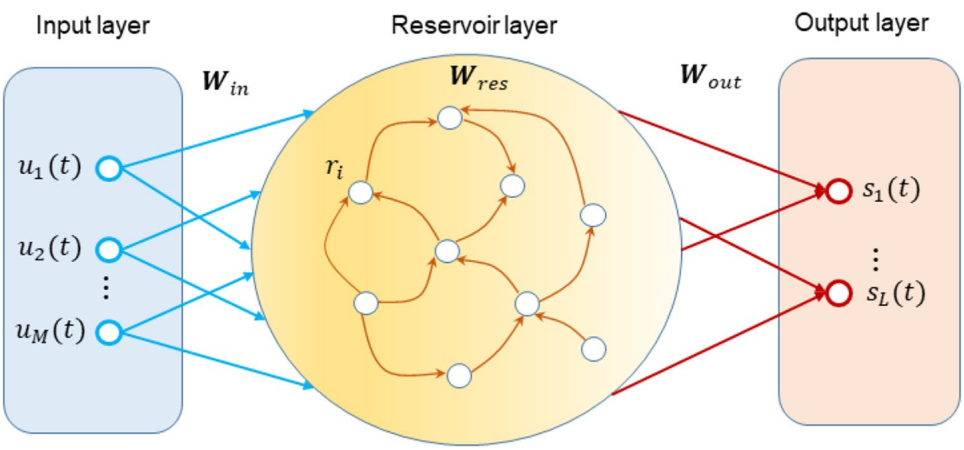


Fig. 3 Schematic illustration of reservoir computing for GPS antijamming

jammed and noisy GPS signal as inputs but with the actual GPS signal as the reference. In this case, what the network predicts is the actual GPS signal. For convenience, we name it the *GPS signal prediction or direct method*. In the second method, the reference signal is the jamming, so the neural network predicts the actual jamming, henceforth the term *jamming prediction or indirect method*. In this case, the GPS signal can be extracted by removing the predicted jamming signal from the original signal. Depending on the type of jamming, the performance of the two alternative methods can differ.

Machine learning-based antijamming scheme for GPS signals of high carrier frequency

For a high-frequency carrier such as $L1$, each bit of the C/A code contains 1540 cycles of carrier oscillation. Thus, it is computationally infeasible to use machine learning to directly predict the GPS waveform, as many sampled data points are needed for each bit of the C/A code. As explained in Fig. 1, for high-frequency GPS signals, machine learning is exploited to predict the C/A code. We test the antijamming capability of the three types of neural networks with three types of jamming and demonstrate that RC has the consistently best performance, rendering it desired as the choice for machine learning-based GPS antijamming.

Continuous wave interference (CWI) jamming

CWI jamming can be written as (Mosavi and Shafiee 2016; Morales et al. 2019):

$$j(t) = \sum_{k=1}^{K} \sqrt{2P_{J_k}} \cos[2\pi(f_c \pm f_{\Delta_k})t + \theta_k] \tag{5}$$

where P_{J_k}, f_c, f_{Δ_k}, and θ_k stand for the power, central frequency (same as the L_1 frequency), frequency offset, and random phase of the k th tone, respectively. For convenience, we normalize the frequencies by setting $f_c = 1$. We choose the frequency offset to be $f_\Delta = (0, \pm 0.1, \pm 0.2) f_{CA}$ with f_{CA} being the frequency of the C/A code. The PSD plots for the signal, CWI jamming and Gaussian noise are shown in Fig. 2a, where the jamming to signal ratio (JSR) is 50 dB. Using the definition of decibel (dB), we have$10 \log_{10}\left(\frac{2P_{J_k}}{1}\right) dB = 50\ dB$, with the carrier amplitude set to one. In this way, we can obtain the CWI amplitude as $\sqrt{2P_{J_k}} \approx 316$. The Gaussian noise-to-signal ratio (NSR) is fixed to be 30 dB in all cases. As can be seen from Fig. 2a, about the central frequency, the jamming power is significantly larger than that of the GPS signal.

Figure 4a shows, for JSR = 50 dB, 20 bits of the values of the jammed, noisy C/A code, which fall in the range of $[-100, 100]$ and deviates significantly from the actual GPS C/A code. Without jamming mitigation, the information carried by the GPS signal is completely lost. Figures 4b–d present results with RC, MLP, and LSTM, respectively, where 20 bits of the machine learning predicted C/A code and the jammed C/A code with the three types of artificial neural networks are shown. For RC and LSTM, the direct, GPS prediction method is used. For MLP, the indirect jamming prediction method is adopted where the neural network is trained with the actual jamming signal as the target and is a self-evolving nonlinear dynamical system. With a short segment of the jammed and noisy GPS signal as the initial condition, the network generates continuous prediction of the jamming signal. Removing the predicted from the original jamming signal recovers the GPS signal. In all cases, the output state of the neural network agrees with the true C/A code remarkably well, effectively eliminating jamming and noise.

The prediction accuracy of the neural networks can be quantified by the BER associated with the C/A code.

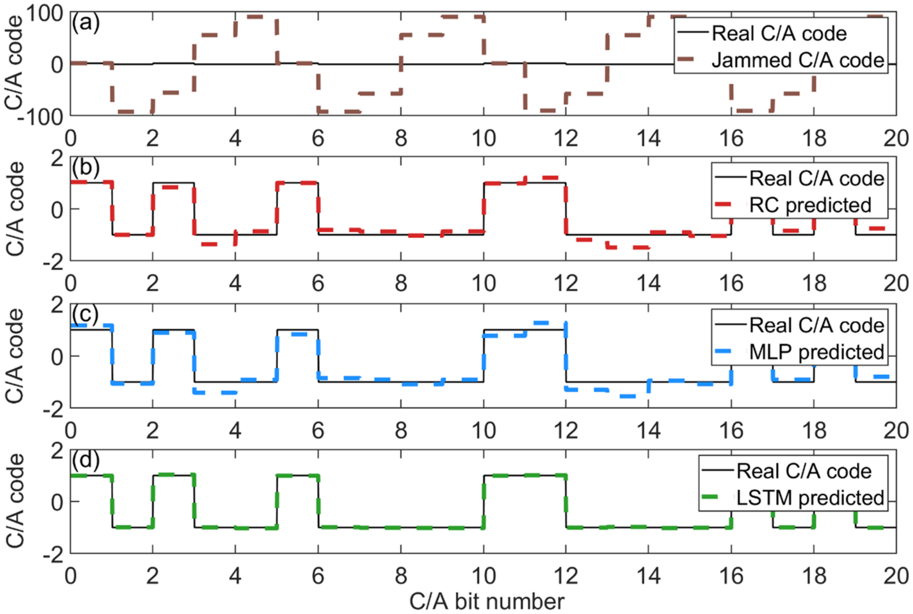


Fig. 4 Examples of jamming mitigation with three types of neural networks. The jamming type is CWI with JSR = 50 dB. **a** Twenty bits of jammed C/A code at the receiver end, in which the true GPS C/A code is deeply "buried" and the information with the communication is completely lost. **b**–**d** For RC, MLP, and LSTM, respectively, the predicted C/A code (dashed traces). The solid trace in each panel represents the true GPS C/A code. The direct, GPS signal prediction method is applied to RC (**b**) and LSTM (**d**), while the indirect, jamming prediction method is used for MLP (**c**), and the same convention holds for subsequent figures: Figs. 5 and 7

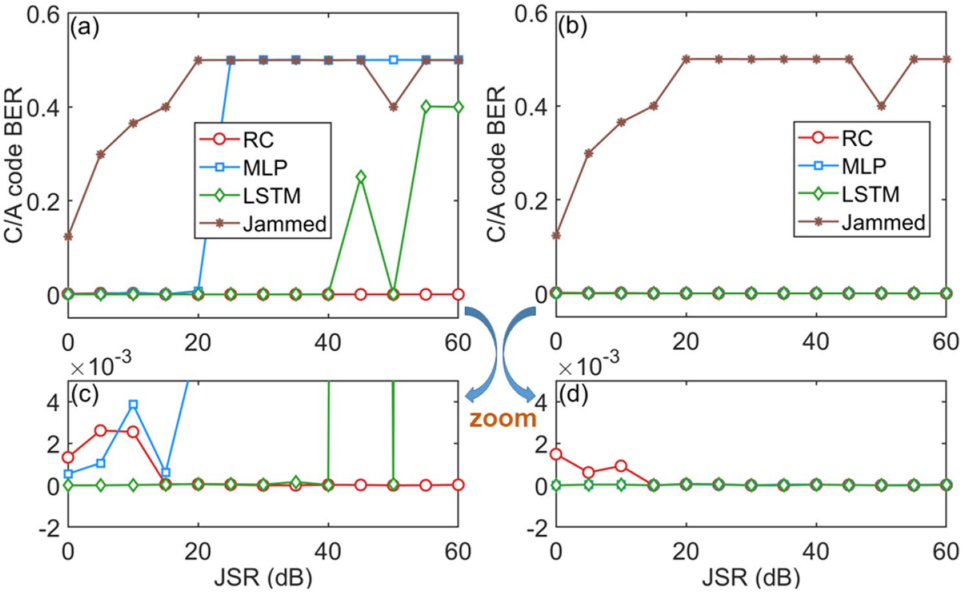


Fig. 5 Error rate with machine learning-based antijamming for CWI. **a** With the direct prediction method, the C/A code BER versus JSR for RC, MLP, and LSTM neural networks. Also shown is the BER associated with the jammed GPS signal without invoking machine learning. For JSR up to 60 dB, the BER with the RC neural network remains at near zero values. However, MLP and LSTM break at JSR about 20 dB and 40 dB, respectively. **b** The corresponding results with the indirect, jamming prediction method. In this case, the BER is near zero for RC and MLP for JSR up to 60 dB, indicating the effectiveness of machine learning-based GPS jamming mitigation

Representative results are shown in Fig. 5, where BER is plotted versus JSR. In particular, Fig. 5a shows, with the GPS prediction method (direct method), the C/A BER versus JSR for the three types of neural networks: RC, MLP, and LSTM. For comparison, the significant BER with the jammed GPS signal for almost all values of JSR is also shown (the brown trace). It can be seen that the performance of MLP and LSTM breaks at JSR ≈ 20 dB and JSR ≈ 40 dB, respectively, where the BER starts to increase dramatically from near-zero values. However, the BER associated with RC remains at near-zero values (less than 0.3%) even for JSR up to 60 dB, suggesting the relatively strong antijamming capability of RC neural networks. The corresponding results with the jamming prediction method (indirect method) are shown in Fig. 5b, where the BER with RC and MLP remains at near-zero values for JSR up to 60 dB. Figures 5c and 4d show magnification of the BER values near zero in Figs. 5a, b, respectively. We see that, for the direct prediction case, RC has the lowest error rate (less than 0.3%) and, for the indirect situation, the error rate of the three machine learning methods is less than 0.2%, with MLP performing slightly better than RC. For RC, MLP and LSTM, the indirect prediction method has smaller errors due both to the sinusoidal nature of the jamming and its large signal magnitude, which facilitate machine learning-based prediction.

Chirp jamming

Chirp jamming is generated by sweeping the signal frequency linearly over a certain range for a certain time period, after which the process restarts at the initial frequency. The chirp jamming signal in the time interval $0 \le t < T_{swp}$(the first sweeping period) can be written as (Morales et al. 2019; Chen et al. 2016)

$$j(t) = \sqrt{2P_J}\sin\left(2\pi f_c t + \pi\frac{f_{\max} - f_{\min}}{T_{swp}}t^2 + \theta_J\right) \qquad (6)$$

where P_J is the jamming power, f_c is the starting frequency of the sweep (same as the carrier frequency), $f_{\min}$ and $f_{\max}$ are the minimum and maximum frequencies of a single sweep, and T_{swp} is the sweep period, i.e., the time it takes for the jammer to sweep from $f_{\min}$ to $(f_{\max} + f_{\min})/2$. The signal repeats itself in subsequent sweeping periods. In our simulation, we set $f_c = 0.8$, $T_{swp} = 9T_{CA}$ with T_{CA} being the C/A code period, $f_{\min} = f_c$, and $f_{\max} = 1.6f_c$. The corresponding PSD profiles for the signal, chirp jamming and Gaussian noise are shown in Fig. 2b for JSR = 50 dB. The PSD of the jamming exhibits a plateau in the approximate frequency range [0.8, 1.25]. In the entire frequency range, jamming completely overpowers the GPS signal.

Figure 6 shows representative output C/A code without and with machine learning. In particular, Fig. 6a shows 20 bits of the jammed C/A code without applying machine learning-based antijamming for JSR = 50 dB. This output C/A code does not agree with the true code, signifying complete loss of information carried by the GPS signal. In contrast, when machine learning is activated to mitigate jamming, the output C/A code agrees well with the true one, as shown in Figs. 6b–d for the three types of neural networks: RC, MLP, and LSTM, respectively. For the results with RC and LSTM [Figs. 6b, d, respectively], the neural network predicts the GPS signal, while the jamming signal is predicted for MLP and the GPS signal is obtained by taking away the predicted jamming signal from the original jammed GPS signal [Fig. 6c].

Figures 7a, b show BER versus JSR for the two jamming mitigating cases of predicting directly the GPS signal and predicting the jamming signal, respectively. Results for the case without applying machine learning are also included, where the C/A code BER increases from near zero values when JSR exceeds about 20 dB. For the direct prediction approach, MLP can resist jamming up JSR = 40 dB, but both RC and LSTM have practically zero errors for JSR up to 60 dB, as shown in Fig. 7a. For indirect prediction, both RC and MLP are effective at removing jamming, as shown in Fig. 7b. Figure 7c, d is magnification of the BER values near zero in Fig. 7a, b, respectively. It can be seen that, for the direct prediction case, the maximum error rate for RC is less than 2%, and the errors with LSTM are essentially zero. For the indirect case, the errors associated with the

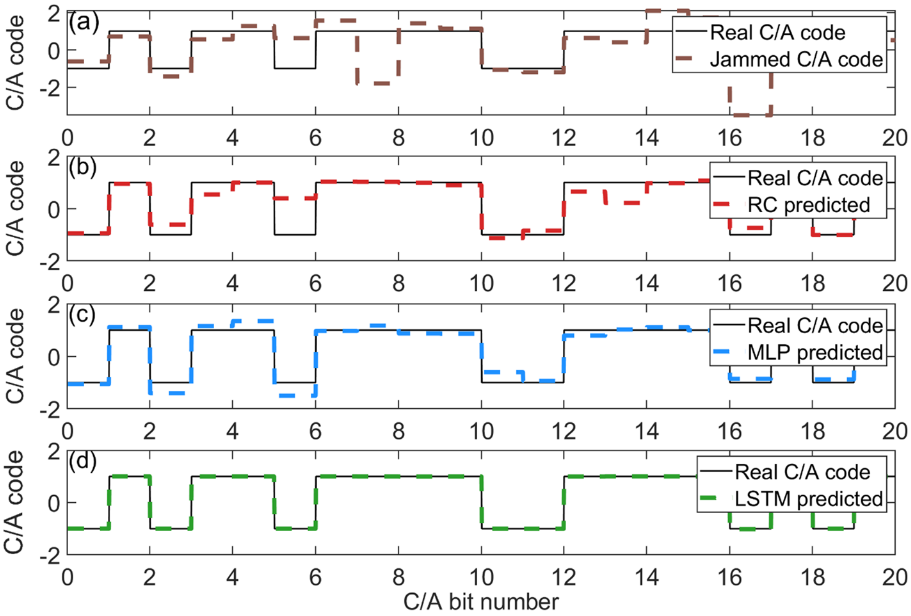


Fig. 6 Mitigation of chirp jamming with three types of neural networks. The value of JSR is 50dB and the jamming completely overpowers the GPS signal because the PSD of the latter is significantly lower than that of jamming in the entire frequency range. **a** Twenty bits of jammed C/A code (dashed trace) at the receiver end, which does not match the true C/A code (solid trace). **b–d** For RC, MLP, and LSTM, respectively, the predicted C/A code (dashed traces) versus the true C/A code (the solid traces), with a reasonable agreement between them for the three types of neural networks

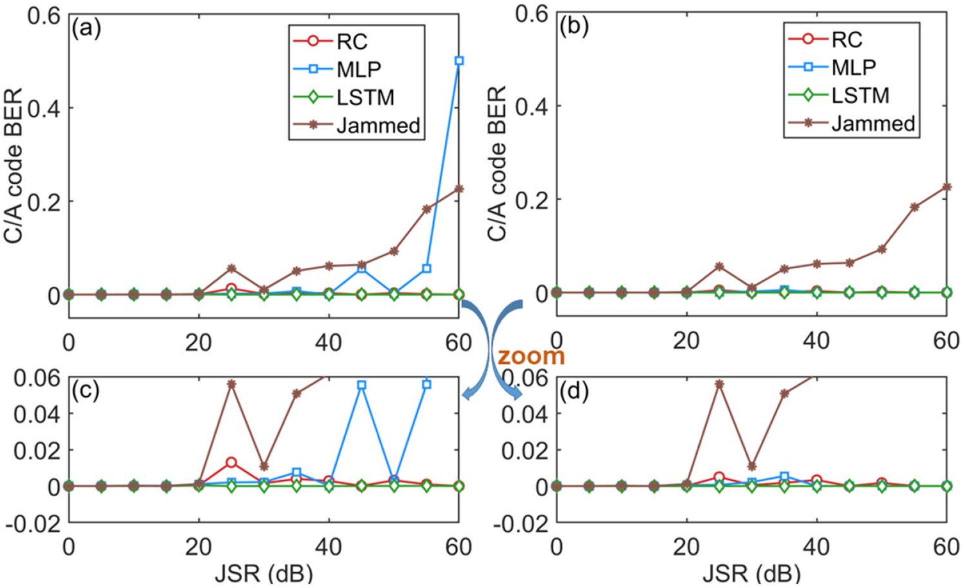


Fig. 7 Error rate with machine learning-based anti-chirp jamming. **a** C/A code BER versus JSR for direct prediction of GPS signal using RC, MLP, and LSTM. The case without invoking machine learning (original jammed signal) is also included. **b** C/A code BER versus JSR with the indirect method of predicting the jamming signal. (**c**, **d**) Magnification of near-zero BER values for (**a**, **b**), respectively. For both direct and indirect methods, among the three types of networks, RC stands out as the best neural machine with low BER

three machine learning methods are near zero in the range of jamming level tested.

Pulse jamming

For pulse jamming, the signal is active during the duty cycles, which can be expressed as (Morales et al. 2019; Elezi et al. 2019a, 2019b):

$$j(t) = \begin{cases} \sqrt{2\mathrm{P_J}}\sin(2\pi \mathrm{f_c}t), & \text{for } n\mathrm{T} \le t < (n+1/2)T \\ 0, & \text{otherwise} \end{cases} \quad (7)$$

for $n = 0, 1, \ldots$, where T is the repetition period, the duty cycle is 50%, P_J and f_c are the power and frequency of the jamming signal with f_c being the carrier frequency. We set $T = 0.8T_{CA}$, where T_{CA} is the period of the C/A code. The PSD profiles for the signal, pulse jamming and Gaussian noise are displayed in Fig. 2c for JSR = 50dB(corresponding to $\sqrt{2P_J} = 316$ and unity carrier amplitude). The PSD of the pulse jamming is wide and covers that of the GPS signal.

For pulse jamming, the performance of the three types of neural networks is exemplified in Fig. 8, with the behavior of BER versus JSR shown in Fig. 9. As for the case of CWI and chirp jamming, among the three types of machines, overall, RC exhibits the lowest error rate

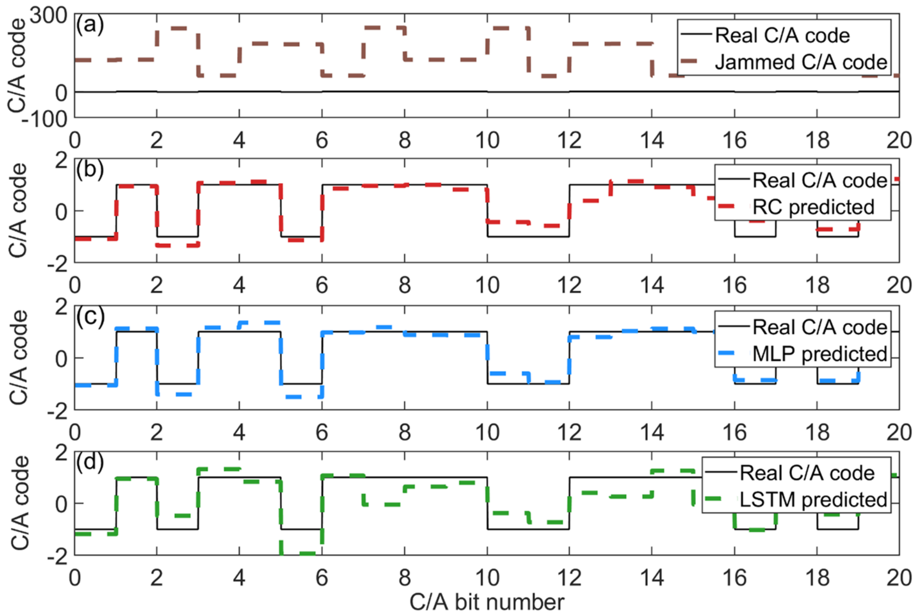


Fig. 8 Mitigation of pulse jamming with three types of neural networks. As shown in Fig. 2, for JSR = 50dB, jamming completely overpowers the GPS signal in the entire frequency range. **a** Twenty bits of jammed C/A code (dashed trace), which deviate significantly from those of the actual C/A code (solid trace). **b–d** For RC, MLP, and LSTM, respectively, the predicted C/A code (dashed traces) versus the true C/A code (the solid traces), where the binary codes associated with them agree with each other

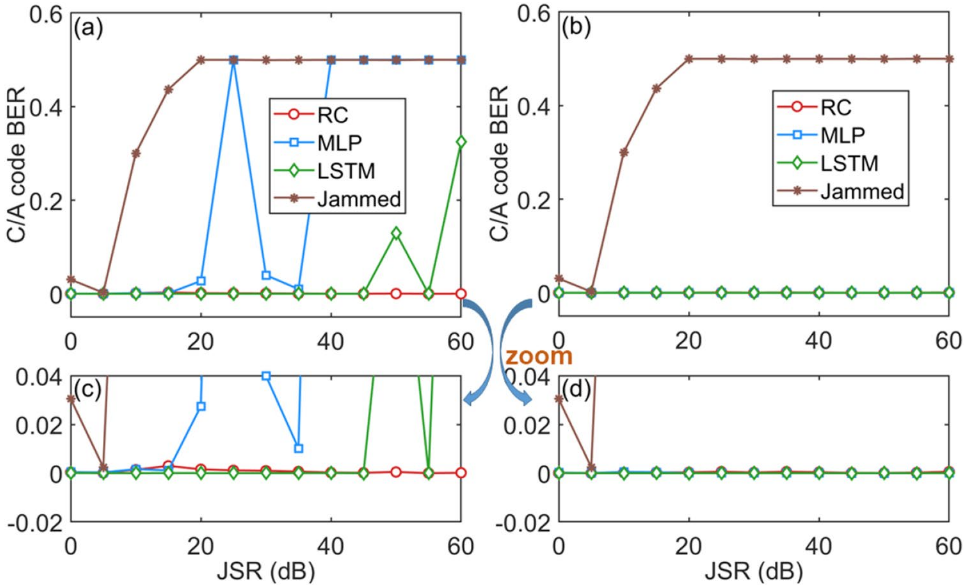


Fig. 9 Error rate with machine learning for mitigating pulse jamming. **a** C/A code BER versus JSR for direct prediction of GPS signal with RC, MLP, and LSTM. The case without invoking machine learning (original jammed signal) is also included. The error with MLP is large for JSR larger than about 20 dB. The maximum level of jamming with which LSTM can cope is about 40 dB. For RC, the BER is near zero for JSR up to 60 dB. **b** C/A code BER versus JSR with the indirect method of predicting the jamming signal. In this case, both RC and MLP perform well. (**c**, **d**) Magnification of near-zero BER values in (**a**, **b**), respectively. As for CWI and chirp jamming, RC exhibits the best antijamming performance among the three types of neural networks

for both direct and indirect prediction methods. RC thus stands out as the best choice for mitigating pulse jamming at the high carrier frequency.

A comparison of the BER for different machine learning methods for direct signal prediction and jamming prediction (indirect method) at JSR = 60 dB is shown in Table 1.

Parameter setting

Reservoir computing

In our simulations, we fix the number of network nodes to be 200. In the case of chirp jamming, we use the embedding with input data dimension being 21 and the delay between each input being the length of one C/A code. We employ the Bayesian optimization method (Snoek et al. 2012) to set the hyperparameters.

Multi-layer perceptrons

In our study, we use three hidden layers with the number of nodes being 165, 20, 7 respectively. The batch size is 8, the input dimension is 45, and the training epoch is 35. The activation functions of all the hidden layers are the sigmoid function in Keras and the activation function of the output layer is the hyperbolic tangent function.

Long short-term memory networks

We construct and train the LSTM RNN using the Pytorch (Paszke et al. 2019) package in Python. The RNN has 200 artificial neurons and training is accomplished with 39000 short signal sequences, where $n = 1000$ for each short

Table 1 Bit error rate for different machine learning methods at JSR = 60 dB

	Jammed (%)	RC direct (%)	MLP direct (%)	LSTM direct (%)	RC indirect (%)	MLP indirect (%)	LSTM indirect (%)
BER CWI	50	0.003	50	40	0.002	0.003	0.003
BER chirp	22.7	0.0003	50.1	0	0	0.002	0
BER pulse	50	0.02	50	32.5	0.06	0.003	0.005

sequence. The detailed description of the three different machine learning models is in the Supplementary Materials.

Conclusion

Intentional jamming on GPS signals represents a serious threat to many applications that rely on GPS for communication. To mitigate jamming is thus of interest, but there are two outstanding challenges: (a) the GPS signals are typically weak while the jamming power may be orders of magnitude higher and (b) the frequency band of jamming may completely overlap with that of the GPS signal. In the field of signal processing, extracting a weak signal "buried" deeply inside the jamming in both time and frequency domains is an unsolved problem.

We have developed a machine learning framework for GPS antijamming. The basic idea is to train an artificial neural network so that it can recognize and learn the "climate" of the GPS signals through training. Especially, assuming that sufficient samples of "clean" GPS signals are available, we input the jammed GPS signal into the neural network with the output target as the corresponding clean GPS signal. During the learning phase, the neural network adjusts its parameters until convergence is reached. A well-trained neural network should be able to predict or pick out the original GPS signal embedded in jamming, thereby achieving the goal of separating GPS signal from jamming and consequently removing it. Alternatively, a neural network can be trained with the jamming signal as the target. In this case, the predicted signal is jamming, which, when being subtracted from the jammed signal, gives the GPS signal. This alternative approach is meaningful only when a certain amount of the actual jamming signal is known. We have tested three types of neural machines: RC, MLP, and LSTM with both signal extraction approaches. The general finding is that, among the three types of machines, RC stands out as the best candidate for GPS antijamming, where the information carrying GPS signal can be reliably and accurately retrieved from a jammed signal even when the jamming-to-signal ratio is 60 dB, i.e., when the jamming amplitude is three orders of magnitude stronger than the GPS signal.

We have studied machine learning-based antijamming for high GPS carrier frequencies. For high carrier frequency, machine learning is incorporated into the stage of binary C/A code obtained by integrating the jammed GPS waveform. This is necessary because predicting the actual GPS waveform, in this case, is computationally prohibitive. We have demonstrated that machine learning can be effective even in the presence of strong white Gaussian noise. That is, in this high-frequency case, even when the received jammed GPS signal is noisy, at the level of binary C/A code, the influence of noise can be filtered out by machine learning, providing another reason for advocating the use of machine learning in GPS antijamming.

Discussion

It is necessary to determine the jamming type in an application, which can be achieved, e.g., by checking the GPS signal power or analyzing the frequency spectrum. Once the jamming type is known, the corresponding jamming data can be used for machine learning and prediction. Another issue is that learning needs to be performed at certain jamming strength, whereas in reality, the strength may depend on time. A possible solution is to train a series of neural networks, each for a particular value of the jamming strength, and to choose the one that matches the jamming strength of the incoming signal.

A difficulty arises for intermediate carrier frequency when one attempts to employ machine learning to predict the actual GPS waveform. In this case, without noise, machine learning can be quite effective at mitigating strong jamming, as we have demonstrated in the Supplementary Materials. However, the presence of Gaussian noise can significantly degrade the antijamming capability. In nonlinear systems, one well studied approach to suppressing white noise is through stochastic resonance, a phenomenon in which the presence of internal or external noise in a nonlinear system can enhance the response of the system output. A potential approach to addressing the difficulty with predicting the GPS waveform for intermediate carrier frequency in a jammed and noisy environment is to combine machine learning with a stochastic-resonance-based method—a promising case that deserves to be studied systematically.

Supplementary Information The online version contains supplementary material available at https://doi.org/10.1007/s10291-021-01154-7.

Acknowledgements We thank Dr. Arje Nachman from Air Force Office of Scientific Research for motivating us to study the problem of GPS antijamming. This work was supported by the Vannevar Bush Faculty Fellowship program sponsored by the Basic Research Office of the Assistant Secretary of Defense for Research and Engineering and funded by the Office of Naval Research through Grant No. N00014-16-1-2828.

Data availability The datasets generated during and/or analyzed during the current study are available from the corresponding author on reasonable request.

References

Borio D, Camoriano L, Presti LL (2008) Two-pole and multi-pole notch filters: a computationally effective solution for GNSS interference detection and mitigation. IEEE Syst J 2(1):38–47

Carroll TL (2018) Using reservoir computers to distinguish chaotic signals. Phys Rev E 98:052209

Chen YE, Chien YR, Tsao HW (2016) Chirp-like jamming mitigation for GPS receivers using wavelet- packet-transform-assisted adaptive filters. In: 2016 International computer symposium (ICS), IEEE, pp 458–461

Chien YR (2013) Design of GPS antijamming systems using adaptive notch filters. IEEE Syst J 9(2):451–460

Elezi E, Çankaya G, Boyacı A, Yarkan S (2019) A detection and identification method based on signal power for different types of electronic jamming attacks on GPS signals. In: 2019 IEEE 30th annual international symposium on personal, indoor and mobile radio communications (PIMRC), IEEE, pp 1–5

Elezi E, Çankaya G, Boyacı A, Yarkan S (2019) The effect of electronic jammers on GPS signals. In: 2019 16th international multi-conference on systems, signals & devices (ssd), IEEE, pp 652–656

Fan H, Jiang J, Zhang C, Wang X, Lai YC (2020) Long-term prediction of chaotic systems with machine learning. Phys Rev Res 2:012080

Graves A, Mohamed AR, Hinton G (2013) Speech recognition with deep recurrent neural networks. In: 2013 IEEE international conference on acoustics, speech and signal processing, IEEE, pp 6645–6649

Hertz J, Krogh A, Palmer RG (1991) Introduction to the theory of neural computation. Addison- Wesley Publishing Company, Redwood City, California

Hinton G et al (2012) Deep neural networks for acoustic modeling in speech recognition. IEEE Sig Proc Mag 29(6):82–97

Hochreiter S, Schmidhuber J (1997) Long short-term memory. Neural Comp 9(8):1735–1780

Ioannides RT, Pany T, Gibbons G (2016) Known vulnerabilities of global navigation satellite systems, status, and potential mitigation techniques. Proc IEEE 104(6):1174–1194

Jaeger H (2001) The "echo state" approach to analysing and training recurrent neural networks-with an erratum note. Bonn Germany German National Res Center Info Technol GMD Tech Report 148(34):13

Jaeger H, Haas H (2004) Harnessing nonlinearity: Predicting chaotic systems and saving energy in wireless communication. Science 304(5667):78–80. https://doi.org/10.1126/science.1091277

Jiang J, Lai YC (2019) Model-free prediction of spatiotemporal dynamical systems with recurrent neural networks: role of network spectral radius. Phys Rev Res 1:033056

Krishnagopal S, Girvan M, Ott E, Hunt B (2020) Separation of chaotic signals by reservoir computing. Chaos 30:023123. https://doi.org/10.1063/1.5132766

LeCun Y, Bengio Y, Hinton G (2015) Deep Learning Nature 521(7553):436

Mao WL (2008) Novel srekf-based recurrent neural predictor for narrowband/FM interference rejection in GPS. AEU-Inter J Electron Commun 62(3):216–222

Mao WL, Ma WJ, Chien YR, Ku CH (2011) New adaptive all-pass based notch filter for narrowband/fm antijamming GPS receivers. Cir Syst Sig Process 30(3):527–542

Morales Ferre R, de la Fuente A, Lohan ES (2019) Jammer classification in GNSS bands via machine learning algorithms. Sensors 19(22):4841

Mosavi M, Shafiee F (2016) Narrowband interference suppression for GPS navigation using neural networks. GPS Solu 20(3):341–351

Mosavi MR (2011) Wavelet neural network for corrections prediction in single-frequency GPS users. Neur Proc Lett 33(2):137–150

Mosavi MR, Rezaei MJ, Pashaian M, Moghaddasi MS (2017) A fast and accurate antijamming system based on wavelet packet transform for GPS receivers. GPS Solu 21(2):415–426

Pardo E, Rodriguez-Hernandez MA, Perez-Solano JJ (2006) Narrowband interference suppression using undecimated wavelet packets in direct-sequence spread-spectrum receivers. IEEE Trans Sig Process 54(9):3648–3653

Paszke A et al (2019) Pytorch: An imperative style, high-performance deep learning library. Preprint at arXiv:1912.01703

Pathak J, Hunt B, Girvan M, Lu Z, Ott E (2018) Model-free prediction of large spatiotemporally chaotic systems from data: a reservoir computing approach. Phys Rev Lett 120:024102

Schmidhuber J (2015) Deep learning in neural networks: an overview. Neu Net 61:85–117

Silver D, Huang A, Maddison CJ, Guez A, Sifre L, Van Den Driessche G, Schrittwieser J, Antonoglou I, Panneershelvam V, Lanctot M et al (2016) Mastering the game of Go with deep neural networks and tree search. Nature 529(7587):484

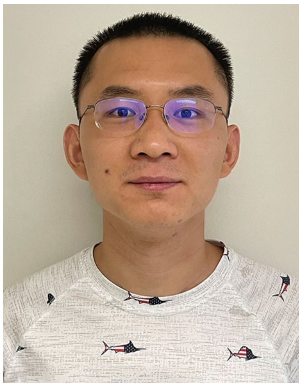
Snoek J, Larochelle H, Adams RP (2012) Practical Bayesian optimization of machine learning algorithms. Preprint at arXiv:1206.2944

Sutskever I, Vinyals O, Le Q (2014) Sequence to sequence learning with neural networks. Preprint at arXiv:1409.3215

Tsui JBY (2005) Fundamentals of global positioning system receivers: a Software Approach, vol 173. Wiley, Hoboken

Zhang C, Jiang J, Qu SX, Lai YC (2020) Predicting phase and sensing phase coherence in chaotic systems with machine learning. Chaos 30:083114

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.



Cheng-Zhen Wang is currently a Ph.D. candidate in electrical engineering at Arizona State University, USA. He obtained his B.Sc. and master's degree in physics in 2013 and 2016, both at Lanzhou University, China. His current research focuses on electronic transport and scattering in two-dimensional Dirac materials and machine learning-based physics.

Ling-Wei Kong is currently a Ph.D. candidate in the Department of Electrical Engineering at Arizona State University, USA. He obtained his B.Sc. degree at the University of Science and Technology of China in 2017. His current research mainly focuses on solving problems in nonlinear dynamics and complex systems using machine learning methods.

Junjie Jiang is currently a Postdoctoral Associate at the Center for neural science, New York University. He obtained his B.Sc. degree at Lanzhou University in 2014. He received his Ph.D. degree from the School of Electrical, Computer, and Energy Engineering, Arizona State University, in 2020. His current research mainly focuses on understanding complex systems and artificial intelligence systems.

Ying-Cheng Lai is currently ISS Endowed Professor of Electrical Engineering, Arizona State University. He received a Ph.D. degree in Physics from the University of Maryland at College Park in 1992. He is a Fellow of the American Physical Society, a Pentagon Vannevar Bush Faculty Fellow, a Foreign Member of the National Academy of Sciences and Letters of Scotland, a Foreign Member of the Academy of Europe, and a Fellow of the American Association for the Advancement of Science. His current research interests are Nonlinear Dynamics, Complex Networks, Machine Learning, Quantum Transport, Graphene Physics, Biological Physics, and Signal Processing.