Final Report: A Review of Generative Adversarial Networks in Networking Applications

Md Hasan Shahriar, and Muhammad Rehan Ali Khan
Department of Computer Science
Virginia Polytechnic Institute and State University
Arlington, VA 22203
{hshahriar, mrk2811}@vt.edu

Abstract

Generative adversarial networks (GAN) are one of the most promising inventions of the deep learning era. GAN has been popular in image processing applications and in recent years, gained traction in other domains such as cybersecurity, cyber physical systems (CPS) and networks. As more GAN papers are getting published, it is important to perform a comprehensive review of these papers to discuss use of GAN. In this paper, we present the most up-to-date review of GAN in cybersecurity, CPS and networks. We focus on analyzing the potential of GAN and its variants in cybersecurity, CPS and network domains while capturing a wide range of applications relevant to the subject. We find that GAN were used in solving various problems and are popular for intrusion detection and attack synthesis applications. We also find that most research have used the original GAN model as the base GAN variant to develop their application specific machine learning models.

1 Introduction

Generative adversarial networks (GAN) is one of the promising and emerging idea in AI and has already shown the light of evolution in modern technology. GAN consists of two neural network models, called generator and discriminator, that can learn the hidden correlation of the data features and the structure of the objects by playing an adversarial min-max game [1]. Among numerous impressive real-world applications of GAN, generating realistic photographs, photograph improving and editing, text to image translations, imputing missing data, video prediction, 3D object generation, etc., are notable. Moreover, recently GAN is extensively used in cybersecurity research to evaluate the vulnerability and improve the system's robustness. The challenges in cybersecurity applications can also be more efficiently solved using the AL/ML techniques. For example, the AI/ML-based intrusion detection systems have already outperformed the existing rule-based methods. However, the cybersecurity datasets are mostly imbalanced due to the limited amount of attack samples compared to the normal samples. Hence, we still have challenges in cybersecurity research. In such cases, GAN can play a vital role by generating synthetic (attack) data and help the models get trained more efficiently. Apart from this, there are several other applications where GAN were proven to outperform other traditional models.

The rising popularity of GAN has led to several prior reviews. The difference between previous studies and current work is summarized here:

- *GAN and its range of applications:* This paper expands upon a wider range of applications and categorize them into cybersecurity, CPS and networks domains.
- *Inclusion of recent works:* There are many comprehensive reviews done previously [2–6]. This paper presents a more updated version of previous reviews where the most recent GAN papers are included.

35th Conference on Neural Information Processing Systems (NeurIPS 2021), Sydney, Australia.

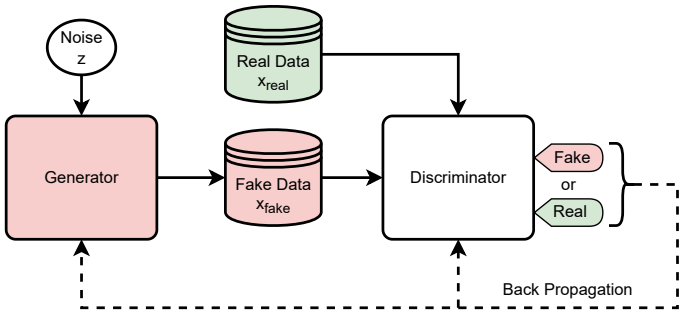


Figure 1: GAN basic architecture.

The rest of the report is organized as follows. We give a formal introduction of GAN and discuss its different variations in §2. We discuss applications of GAN in cybersecurity in §3. In §4, we review applications of GAN in CPS domain. In §5, we discuss applications of GAN in networks domain. In §6, we discuss our literature analysis, limitation of GAN in cyberspace, possibility of GAN in cyberspace and future direction. Finally, §7 presents the conclusion of our review.

2 Generative Adversarial Networks

GAN is a machine learning model that learns the distribution of the sample data, allowing it to generate data that resembles the data of the sample. Figure 1 shows a basic model of GAN. GAN introduced a novel way for training a generative model, where two 'adversarial' neural networks compete against each other by playing a min-max game. GAN achieves this task just by taking noise as an input and by simultaneously training two neural network models: generator and discriminator. Learning the distribution in this manner allows us to train the model in an unsupervised fashion, avoiding the need for data labeling. Also, it opens the door for new possibilities in applications where generation of synthetic samples or discriminative detection are maybe helpful. This paper will cover applications of GAN in the future sections.

2.1 Architecture of GAN

In this section, we describe the two main parts of GAN in more detail i.e. the generator and discriminator. These are two neural network models that are combined to form a standard GAN model as shown in Figure 1.

Generator. The Generator is a neural network model that takes a noise vector as an input and attempts to generate an output that resembles the real sample. The generator then receives feedback from the discriminator. Loss function is computed and the generator learns through back-propagation. Analogously, a generator can be viewed as an artist who's trying to improve itself through discriminator's feedback. Besides, it can also be viewed as an art forger who's trying to fool the discriminator by generating realistic fake data. In short, a Generator's role is to capture the real data distribution, produce realistic data, fool the Discriminator with its produced data, and achieve high-performance by completion of the training process.

Discriminator. The Discriminator is also a neural network model that is responsible for classifying the input as real or fake. It has access to both: the real dataset as well as the output of the generator. Having those two inputs, the discriminator's job is predict if the data received is coming from generator(fake data) or does it belong to the actual real dataset(real data). Going with the same analogy mentioned earlier, when Generator is an artist the then Discriminator is a mentor guiding the artist. If Generator is an art forger, then Discriminator is the detective responsible for identifying the forgery. Either way, a Discriminator's role is always to predict if data is coming from Generator or from a real sample.

2.2 Training of GAN

In this section, we will briefly describe the training method used to train a GAN model along with the generator and discriminator. When training a GAN model, it is essential to train both generator and discriminator simultaneously where one never outperforms the other at any given time. A generative model G observes the data distribution of a training set and tries to generate synthetic data following the same distribution. Adversely, a discriminative model D works as a classifier that estimates if

Table 1: Different variations of GAN

Name	Types of Model	Contribution	Types of Data	Reference
Original GAN	Unsupervised	First GAN model	1D Data	[1]
DCGAN	Unsupervised	Convolution layers to generate image	1D Data	[7]
CGAN	Supervised	Ability to generate class specific data	1D Data + Condition	[8]
InfoGAN	Unsupervised	Another approach to CGAN using regularization	1D Data + Condition	[9]
ACGAN	supervised	Extension of CGAN, providing source of class label	1D Data + Condition	[10]
StackGAN	Unsupervised	High-quality images fron text description	1D Data + Condition	[11]
CycleGAN	Unsupervised	Image-to-image translation	2D Data	[12]
WGAN	Unsupervised	Stable training and faster convergence	2D Data	[13]
SSGAN	Semisupervised	Better samples for a imbalanced dataset	2D + Label	[14]
ProgressiveGAN	Unsupervised	Stable generation of high-quality images	2D Data	[15]
StyleGAN	Unsupervised	Control on the image synthesis	2D Data	[16]
BiGAN	Unsupervised	Feature learning/mapping capabilities	2D Data	[17]
BGAN	Semisupervised	Stable semisupervised GAN	2D Data	[18]

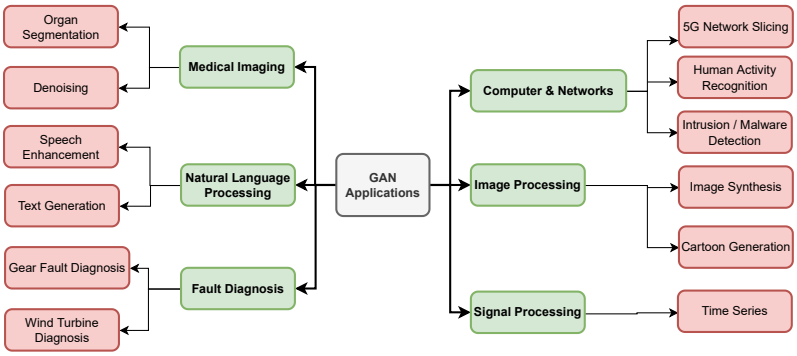


Figure 2: GAN application in various domains

data belongs to the training set or being generated by G. The generator G estimates the distribution p_g over training data x by building a mapping function from the noise distribution p_z to training distribution p_{data} presented as $G(z; \theta_g)$.

On the other hand, the discriminator D outputs $D(x)$, the probability that a particular sample is from the real data set. Both G and D are trained simultaneously, though one is kept constant when the other is being trained. The value function $V(G, D)$ is defined as follows:

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

The discriminator's parameters θ_d are updated to maximize both $\log D(x)$ and $\log(1 - D(G(z)))$, the above equation, whereas the generator's parameters θ_g are updated to minimize $\log(1 - D(G(z)))$. For achieving the optimal solution, both the models continually optimize themselves to reach Nash equilibrium. Throughout the training process, it is very important to maintain a balance in performance between the Generator and Discriminator since out performance of any one model will hinder the training progress of the other. But maintaining this balance is often challenging. Additionally, a GAN model could fail due to other challenges such as vanishing gradient problem and mode collapse problem. Overcoming these challenges and further improvement of GAN has been the main motivation for developement of new variants of GAN.

2.3 Variants of GAN

In the next section, we briefly discuss GAN variants and how they optimize GAN by overcoming common issues and improving upon the training process. Table 1 shows some of the variants of GAN along with their data input types and how they contribute towards improving the Original GAN model. Each GAN variants focus towards improving a specific aspect of GAN. For instance, CGAN and Info GAN allows the model to Generate synthetic data that belongs to a specific class as opposed to a random class for the sample data, providing more controlled GAN model. DCGAN is another variant that improves neural network learning process of image data by using convolution layers (instead of typical fully connected layers). ProgressiveGAN improves training time and image quality by gradually expending the neural network hidden layers, while stackGAN achieves the same task by utilizing hierarchical stack of conditional GAN. WGAN provides stable training and better convergence by using Wasserstein as the distance measure.

2.4 Applications of GAN

GAN has a broad range of applications across various fields. Figure 2 shows some of the applications in the domain of Medical imaging, Natural Language, Fault Diagnosis, Computer & Networks, Image Processing and Signal Processing. GAN applications can be mainly classified into two categories: task specific & domain specific applications. For task specific applications, GAN are extensively used for either synthetic data generation or to solve a discrimination problem. For instance, synthetic data is used to solve class imbalance problem by generating data belonging to a minority. Synthetic data is also used for anomaly detection [19, 20] where GAN is used to learn distribution of anomalous data. Other task specific GAN applications includes transfer learning [21], reinforcement learning, dimension reduction, and feature selection.

3 GAN in Cybersecurity

In this section, we discuss the literature related to the applications of GANs and their variants in cybersecurity. The reviews cover three main areas which are explained in the following subsections.

3.1 GAN for Attacks in Cybersecurity

GANs have the capability to learn the complex distribution and generate similar samples. The application of GANs in the generation of cyberattacks can be categorized as follows.

Adversarial Machine Learning Attack. Due to their ability to learn underlying threat patterns/features, machine learning is increasingly used in intrusion detection systems (IDS) to detect threats within computer networks. The disadvantage of ML-based models is that they are vulnerable to adversarial attacks when slight alterations in input features can lead to misclassifications. In [22], Shu et al. proposed a technique for generating adversarial attacks against ML-based IDS, utilizing active learning and GAN. The proposed model achieved a 98.86% success rate in evading the IDS model employing only 25 labeled data samples during model training. URL-based phishing attacks have been around for a while and it still constitutes a significant percentage of security incidents. The Machine Learning adversarial based attacks have potential to bypass current URL-based phishing detection techniques. In [23], AlEroud et al. proposed using GAN to synthesis examples of these adversarial phishing attacks. Results shows that the generate phishing examples can effectively fool both simple and sophisticated machine learning phishing detection models.

Malicious Traffic Generation. Despite the prevalence of machine learning algorithms in cybersecurity, recent research has found that adversarial examples can degrade their performance. At present, there are still limited studies on adversarial ML in cybersecurity. In [24], Zhang et al. proposed BFAM, a brute-force type attack, to evaluate the robustness of the machine learning classifiers against adversarial examples. To have a comprehensive evaluation of the attack performance of their proposed method, they synthesized adversarial examples against three common domains: host intrusion detection systems, Android malware detection systems, and network intrusion detection systems. Their results showed that BFAM was able to synthesize adversarial examples against any detection framework and hence worked as an effective tool to evaluate the effectiveness of the defense. In [25], Cheng et al. proposed a similar GAN-based method for synthesizing real traffic flows such as ICMP Pings, DNS queries, and HTTP web requests. The generated network traffic was able to create legitimate request to the services and received response. Cyber intrusion activities has become so diverse and complex that it is often confusing for the analysts and researchers to determine the action and intent of the attack. In [26], Sweet et al. proposed WGAN to synthesis these attacks. The attack synthesis will help with learning the behaviour of the intrusion attacks, paving the way for more proactive cyber threat analysis.

Denial of service (DoS) attack is becoming ubiquitous with the increasing number of connected devices as the form of IoT. Detecting DoS traffic is very challenging as it looks benign as a trace but becomes malicious considering multiple traces together. In [27], Yan et al. proposed DoS-WGAN, a WGAN-based architecture with gradient penalty can generate stealthy DoS traffic, evading the existing network security defense techniques, such as traffic classifiers, where the detection rate drops to 47.6% from 97.3%. Moreover, Even though software-defined networks (SDN) are widely used in modern new legitimate requests is challenging to create attack responses, scenarios, or even intrusion detection rules applicable to SDN dynamic environments. In [28], AlEroud et al. proposed a GAN-based method to generate synthetic data targetting SDN, which can be utilized at the SDN level for more generalized training in attack generation and detection. Proactive cyber security still

remains an open challenge as cyber attack data is often not available for study. In [29], Sweet et al. employed two variants of GAN for artificial cyber alert synthesis.

Malware Generation. GANs are also utilized to generate malwares. In [30], Hu et al. proposed MalGAN, which can generate malware examples against a black box detection algorithm. The discriminator network is considered as the substitution model of the targeted black detection box model. On the other hand, the generator model learns to craft intelligent adversarial samples taking advantage of the leveling skill of the black-box model. Thus, taking advantage of the black-box model, both the generator and the discriminator learn simultaneously and eventually fool with adversarial malware.

Self Adapting Malware Self-adapting is an essential feature of any smart device. To adapt to the host environment, the device first needs to learn it and adopt those parameters to flow. This is applicable for both the adversary and the defender. For example, a malicious user would try to mimic the pattern of the regular network pattern to hide its packets. On the other hand, a smart IPS should always be updated with the normal data's dynamic pattern, which would reduce the false positive rate. With this motivation, Rigaki et al. proposed a GAN-based network traffic generator that learns the traffic patterns of the legitimate applications and produces network traffic for malware, which can easily bypass the trained IPS [31]. They showed the GAN-assisted framework was able to learn the Facebook chat network traffic and adapt the Command and Control (C2) channel behavior. They also adopted a novel feedback mechanism of the malware and GANs to adapt depending on the IPS blocking state.

3.2 GAN for Defense in Cybersecurity

Schlegl et al. paved the way to apply GAN in anomaly detection [32]. Their work was on tomography images but motivated other domain experts to utilize the same in their own domains. The works on GAN in cyber defense are discussed from the following perspectives:

Data Privacy. 5G networks are up-to-date communication platforms, which are experiencing a fast booming in implementation. The increasing volumes of sensitive user data, most importantly, location, are being reported and shared using 5G networks for various purposes. Any published data that contains location and trajectory will always be vulnerable to malicious attacks from adversaries. Because 5G signal towers primarily cover a short-range, there are still potential privacy leakage threats if they share original data. To address this issue, in [33], Qu et al. proposed developed a GAN enhanced location privacy protection model that virtually masks the users' location and even trajectory information. They used posterior sampling to meet differential privacy requirements, generating subsets of data from end devices. Then, a set of full-size synthetic data is generated using a modified version of the classic GAN algorithm. The synthetic data generated by this proposed model can ensure location privacy protection, data utility, and prediction accuracy.

At the same time, the current trend in applying machine learning in cybersecurity domains is hindered by low-fidelity, obfuscated, and limited-sized datasets. To resolve this problem, Le et al. proposed CyberGAN, a GAN network, to produce high-fidelity and large-scale novel challenging attack datasets, merging the latent features of both the normal and attack data [34]. Their approach solves the privacy issue related to sharing the original proprietary dataset, enabling intruders to infer other sensitive information. Hence, the GAN-generated synthetic dataset is generalized and comes with high fidelity that solves the privacy and the limitation of the publicly available dataset issue. CyberGAN generated dataset found compelling on machine learning algorithms for cybersecurity applications, such as intrusion detection. The algorithm is implemented on three different datasets, showing the efficacy and effectiveness of the proposed model.

Intrusion Detection System. The most common and most promising application of GANs are in the intrusion detection systems (IDS) applications. Both the knowledge of the generator and discriminator can be utilized to detect unknown or anomalous pattern in the data. In [35], Shahriar et al. proposed G-IDS, a GAN-based intrusion detection system for an imbalanced dataset. The GAN, which is defined as a data synthesizer module, works on the top of the IDS to generate more synthetic examples for the class with a lower detection rate due to limited training samples. A controller module determines the class with a lower detection rate and asks GAN to generate more samples. At the same time, instead of blindly adding the GAN-generated samples to the original dataset, the controller module checks if those samples are contributing to the IDS detection rate or

not. The synthetic data are added only if there is a performance boost up in IDS, which ensures the continuous improvement of the final dataset and the IDS. There are few other works proposing the similar approaches. In [36], Merino et al. used GAN to generate the synthetic data to solve the data imbalance problem. Usama et al. utilized GAN to create new attacks and train IDS on the augmented data to make it more robust [37]. In [38], Sedjelmaci et al. proposed an attack detection and decision framework to accurately detect smart and impactful attacks. They improved the accuracy while reducing the detection latency. In [39], Huang et al. proposed IGAN-IDS, another GAN-assisted IDS for the imbalanced dataset, where GAN generates new instances for the minority IDS is trained on them to detect those rarely seen classes. Experiments on three different datasets against 15 other methods showed IGAN-IDS robust and outperformed other approaches. In [40], De et al. proposed FID-GAN, an unsupervised strategy to detect cyber-attacks in CPSs. Unlike others, they consider two types of losses: discrimination and reconstruction losses, which require mapping data samples to the latent space. Their framework outperforms other baselines approach with respect to both detection rate and latency.

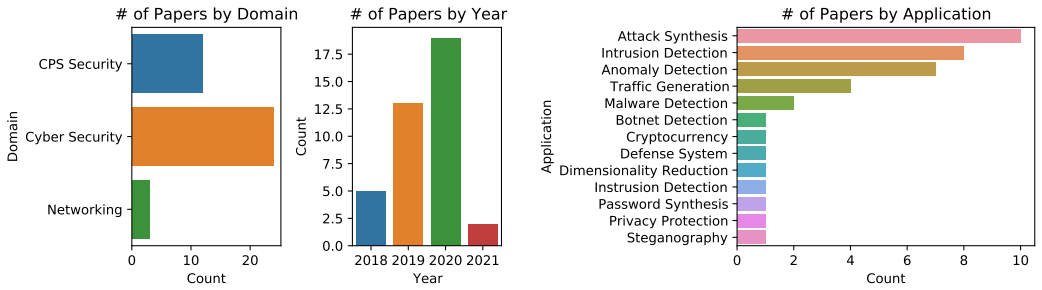
As the modern power grid becomes smarter, automated, and intelligent, developing a robust defense against emerging attacks becomes another challenge. In [41], Ying et al. proposed another GAN-based framework to tackle the imbalanced dataset problem for IDS and improves the detection rate by 4%. In [42], Li et al. proposed an intrusion detection system, called MAD-GAN, for multivariate series data of critical CPS using LSTM and GAN. The authors trained the unsupervised deep learning models (LSTM-RNN) on the multivariate time-series data using a moving window to learn the Spatio-temporal relationship among different features. Later in the test case, they utilized the reconstruction error from the generator and the discrimination error from the discriminator to find the ultimate anomaly score of the sample test data. The evaluation result shows MAD-GAN outperforms the existing unsupervised algorithms and can detect anomalies in time-series data effectively. Anomaly detection in system logs has become increasingly significant as it is essential for preventing system breakdown. Current detection approaches only concentrate on the anomaly detection in a high-level granularity of logs (i.e., session) instead of detecting log-level anomalies which weakens the efficiency of responding anomalies and the diagnosis of system failures. Therefore in [43], Xia et al. proposed LogGAN, a sequence-based GAN that detects anomalies based on system log patterns. In [44], Zhang et al. proposeda BiGAN-based network intrusion detection system using real dataset and showed the feasibility and comparison analysis.

Defense Against Adversaril ML Attack. Recently used deep learning models for defense systems could be compromised by introducing a small yet carefully designed pertubation into the training datasets. Additionally, It is important to have a system that is robust to existing adversarial attacks as well as future and unseen adversarial attacks within the specified threat model. In [45], Taheri et al. proposed a technique using Pix2pix conditional GAN to generate unseen adversarial examples and understand the transformations between adversarial and clean data.

Botnet Traffic Detection. One of the most formidable cybersecurity threats is botnet, which can be used to launch large-scale attacks on critical infrastructures. In [46], Yin et al. proposed BotGAN, a framework that utilizes GAN to detect botnets, augmenting the original detection model. The generative model in the framework continuously generates 'fake' samples to assist the original detection model to improve the performance.

Decentralized IDS for IoT Devices. IoT devices are being used in mission-critical and real-time applications. However, such devices are becoming the favorite target of adversaries due to their remote, and low capability features. To defense against such attacks, IDS are implemented in each of the decentralized IoT devices. The data generated by only one device might not be sufficient to train it's own IDS. On the other hand, sharing the critical information, such as health and financial data, raises privacy concerns. Researchers are proposing GAN-based decentralized IDSs for each of the devices to tackle this conflicting issue, where the devices share their masked data/implicit information with other nearby devices/central controllers. In [47], Ferdowsi et al. proposed such a distributed IDS for IoT devices where each device has its discriminator, share a common central generator talking to IoT devices. The discrete discriminators and the central generator learn together implicitly, utilizing all the datasets from different IoT devices.

Password Generation. Authenticating with passwords is the most popular method, mainly because it's easy to implement, doesn't require special hardware or software, and is familiar to users and developers. The leaks of multiple password databases indicate that users usually opt for easy-to-guess



(a) Number of papers by domain and year

(b) Number of papers by application

Figure 3: Number of papers on GAN in cyberspace in different categories.

passwords, primarily composed of standard strings (e.g., password, 123456, iloveyou) and variants thereof. Password guessing tools like John the Ripper or HashCat can help determine weak passwords. Such tools have some limitations as they depend on the heuristics, testing hundreds of highly probable passwords. In [48], Hitaj et al. proposed PassGAN, a novel approach based on GAN to address these shortcomings. PassGAN guesses high-quality passwords without relying on manual password analysis; instead, it learns the distribution of real passwords from actual password leaks and generates high-quality guesses. Additionally, PassGAN is capable of matching 51

Steganography. Steganography can be often used for malicious acitivties such as phishing attacks. Therefore it is important to find ways to crack them. In [49], Khan et al. proposed CycleGANs model with pre-trained Pix2pix as a starting point. This model was able to crack LSB steganography algorithm with a significant success.

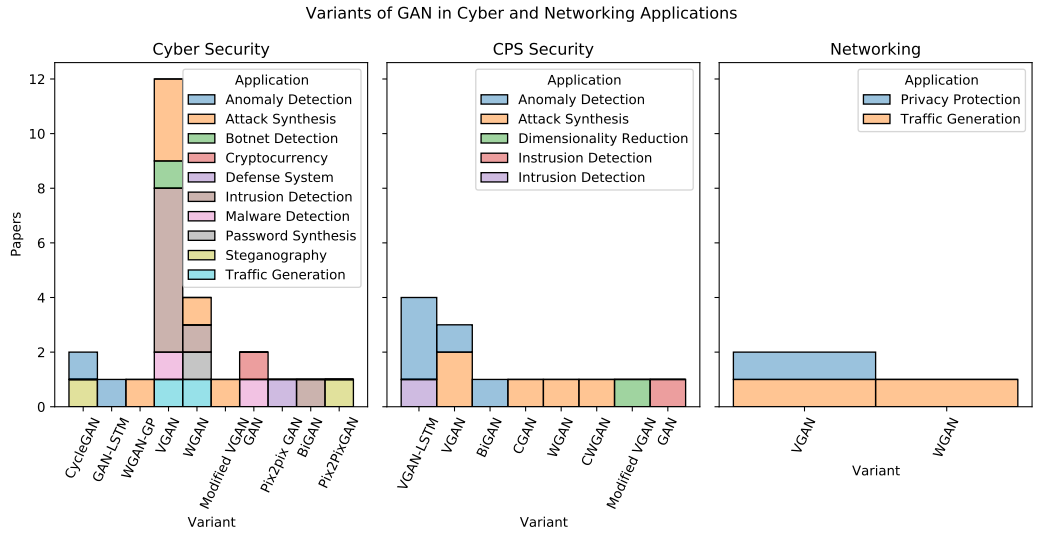


Figure 4: Adoption of GANs' variants in cyberspace from different domains and applications.

4 GAN in Cyber-physical Systems

In this section, we summarize applications of GAN in the cyber-physical systems domain.

4.1 GAN for Attacks in Cyber-physical Systems

In this section, we discuss the techniques of using GAN to attack CPS.

False Data Injection Attack Generation. False data injection (FDI) attacks are one of the damaging threats against any control system. FDI attack vectors are calculated following the targeted system's topology to remain stealthy to the conventional bad data detection algorithms. In [50], Ahmadian et

al. proposed a GAN-based false data injection attack generation framework, which can generate false measurement data satisfying the system topology and leading to an increase in the power generation cost. Even though they implemented the framework on power grids, it can be implemented on any networked control system. In [51], Mohammadpourfard et al. utized CGAN to learn the power grid topology and the distribution of the measrements and synthesized attack vectors that can mislead the bad data detection algorithm.

4.2 GAN for Defense in Cyber-physical Systems

Cyber-physical systems monitor a process by collecting measurement sensor readings, understanding the patterns, and making control decisions based on the context. Safety-critical cyber-physical systems, for example, smart grids, autonomous cars, industrial control systems, etc., make a decision in real-time for safe and reliable performance. Nowadays. AI and ML are becoming core features of such technologies. Moreover, an advanced intruder can also exploit the same level of AI/ML skills to attack the system or take control over it. The bad data detection (BDD) algorithm looks for abnormal patterns in the sensory data stream and filters out the anomalies. However, the existing and conventional BDD algorithm has proven ineffective against stealthy advanced attacks. An attacker can utilize GAN to generate realistically sensory data that follows the system topology and historical distribution and inject them into the safety-critical CPS. Such attacks would be challenging to defend against unless the system also has a GAN-enabled IDS to detect the advanced attacks. Moreover, while building an IDS, GAN can also help preserve privacy while generating realistic synthetic data that mimic historical data distribution. Thus, instead of sharing the actual data that may cause a breach of privacy, GAN-generated data can be shared among different stakeholders to build a unified defense technique [52]. In the following part we discuss the applications of GAN in defense for CPS.

Anomaly Detection. With the emergence of IoT, the Cyber-Physical Systems (CPSs) are getting more complex. This is because larger number of devices are autonomously communicating with each other over networks. The increase in complexity makes CPS prone to cyber-attacks which cannot be addressed using conventional detection tenchniques. In [53], Li et al. proposed GAN-AD, a GAN-based Anomaly Detection method that uses GAN's trained Descriminator to detect anomalies in the system. GAN-AD is able capture the non-linear correlations amongst the time series data, resulting in a model more effective in detecting attacks in the form of anomalies. In [54], Adiban et al. proposed anomaly detector using GAN inspired by OCAN and MAD-GAN. This GAN model is capable of learning the non-linear relationships in the SGS. Also, it makes use of multiple Generators instead of one to minimize mode collapse issue. In [55], Bashar et al. proposed TAnoGan to model the normal behaviour of the time series data and use an anomaly score to indicate how much the data points have deviated from the normal behaviour. Experiments show that TAnoGAN performs superior to traditional NN models. In [56], Alabugin et al. proposed a BiGAN-based anomaly detector in industrial control system (ICS). They implemented the proposed method on Secure Water Treatment Dataset (SWaT), which is a well known dataset for ICS. Current ANN models for CPS security are constraint by lack of big data processing capability and lack of comprehensive training data. In [57], Belenko et al. reviewed use of GAN for intrusion detection and lays out recommendations on how to incorporate GAN in the realm of connected CPS networks.

4.2.1 Other Applications of GAN in Cyber-physical Systems

Dimensionality Reduction In the era of Big Data, CPS is getting more dependent on decision making, as it provides faster and more accurate results. However, processing the high-dimensional CPS data is a big challenge, especially for the systems running in real-time. On the other hand, dimensionality reduction (DR) techniques can help reduce the dimension and give a lower-dimensional representation of the states of the system. In [58], Farajzadeh-Zanjani et al. studied the challenges of analyzing faults and cyberattacks on high-dimensional smart grid data. By utilizing GAN, they proposed two novel dimensionality reduction techniques called Generative Adversarial Supervised DR (GASDR) and Generative Adversarial Unsupervised DR (GAUDR). These techniques use GAN to provide the appropriate distribution of the states in the lower-dimensional space, where samples of specific states, such as normal, abnormal, faults, attacks, etc., can be isolated effectively. They showed the effectiveness of the proposed algorithms by comparing them with 20 state-of-the-art unsupervised and supervised DR techniques. Several forecasting and classification models has been proposed where no single model works for all given problems. Hence, determining the best model for the specific problem has become more of an art than a science. In [59], Zhou et al. proposed 3 approaches: LSTM with autoencoder, TCN-based NN & GAN-LSTM to improve the performance of the problem

at hand. It was found that these approaches outperformed classical algorithms such as random forest, gradient boosting and extra trees and bagging.

5 GAN in Networking Applications

In this section, we summarize applications of GAN in the networking domain.

5.1 GANs to Optimize Systems

GANs are also utilized in non-security application, rather to optimize the systems and create high dimensional flow-based dataset.

Network Packet Generation. Labeled flow-based data sets play a vital role in developing and testing networking-based research. The existing KDD CUP 99 or DAPRA 98 will be outdated soon, demanding newer and updated network datasets. Hence, in [60], Ring et al. proposed a synthetic flow-based network traffic generator that utilizes WGAN-GP and a two-scale update rule. GAN can only learn the distributions of continuous features, but the network traffic consists of heterogeneous discrete data. Hence, three different methods, named N-WGAN-GP, B-WGAN-GP, and E-WGAN-GP, are proposed. These methods pre-processed the heterogeneous data as numbers, binary, and embedded, respectively, to make them feedable to GANs. Their evaluation results on the CIDDS-001 dataset show E-WGAN-GP generates the best and most realistic dataset, which B-WGAN-WP follows. However, N-WGAN-GP fails to learn the distribution, and the generated dataset is less accurate.

Inferring Fine-grained Network Patterns. Large-scale mobile traffic analytics plays a crucial role in the dynamic allocation of the network resources and optimal parameter settings of the end-user devices in a particular area. However, exploiting the fine-grained traffic is challenging work due to complex and expensive computation. This needs costly equipment, massive storage, and extensive post-processing. To tackle these issues, in [61], Zhang et al. proposed Zip-NEt-GAN, a GAN-based model working with a deep Zipper Network which mimics the task of application of super-resolution problem in computer vision. The proposed framework can extract the localized traffic pattern, estimating the measurement granularity by around 100 times.

6 Discussion

6.1 Literature Analysis

Figure 3a shows a brief overview of our survey work. Based on the review findings, we split the cyberspace into 3 domains: Cybersecurity, CPS security and networking. We find that more then 20 research papers belonged to the cybersecurity domain, constituting to the highest paper count compared to the total papers reviewed. After cybersecurity, we see that most of the other papers can be categorized to be in the CPS security domain. The review papers discussed covers about 13 different domain specific applications. Figure 3b shows that GAN is mainly used in attack synthesis, intrusion detection and anomaly detection applications followed by malware detection, botnet detection, cryptocurrency and defense system. Figure 3 also shows that most of papers appear to be published in the year 2020 as compared to the preceding two years. In fact, we see an increase in number of papers published per year. This suggests that GANs are getting more popular overtime and it is expected that this upward trend would continue in the coming years.

6.2 Limitations and Possibilities of GAN in Cyberspace

There are several challenges that hinders the GANs application in cybersecurity dataset.

The core challenges of cybersecurity data generation are mentioned below:

- Security records tend to be highly structured. There are several ordered fields in a firewall record, with each field having a certain type. The type of field usually limits record values. For example, a typical IPv4 address has four octets, each of which must be between $0 \lesssim 255$.
- There are not only numerical fields but categorical ones as well. During the generation process of data, every type will need to be dealt with differently.
- Features follows a temporal pattern that must be preserved to generate realistic samples. For example, requests and responses in any service are related through time. The communication patterns are repeated in the network because it captures the recurrence of the communication,

Table 2: Summary of GAN in Cyber Security

Author	Institute	Year	Domain	Application	Variant	Cite
Salem et al.	University of Central Florida, USA	2018	Cyber Security	Anomaly Detection	CycleGAN	[62]
Xia et al.	Nanjing University of Posts and Tel, China	2019	Cyber Security	Anomaly Detection	GAN-LSTM	[43]
Yan et al.	Shenzhen University, China	2019	Cyber Security	Attack Synthesis	WGAN-GP	[27]
AlEroud et al.	University of Maryland, Baltimore County, USA	2019	Cyber Security	Attack Synthesis	VGAN	[28]
Sweet et al.	Rochester Institute of Technology, USA	2019	Cyber Security	Attack Synthesis	WGAN	[26]
AlEroud et al.	Yarmouk University, Irbid, Jordan	2020	Cyber Security	Attack Synthesis	VGAN	[23]
Yilmaz et al.	Tennessee Tech University, USA	2020	Cyber Security	Attack Synthesis	VGAN	[63]
Shu et al.	Carnegie Mellon University, USA	2020	Cyber Security	Attack Synthesis	Modified VGAN	[22]
Yin et al.	Advanced Computing Zhengzhou, China	2018	Cyber Security	Botnet Detection	VGAN	[46]
Zola et al.	Basque Research and Technology Alliance, Spain	2020	Cyber Security	Cryptocurrency	GAN	[64]
Taheri et al.	University of Central Florida, USA.	2020	Cyber Security	Defense System	Pix2pix GAN	[45]
Ferdowsi et al.	Virginia Tech, USA	2019	Cyber Security	Intrusion Detection	VGAN	[47]
Sweet et al.	Rochester Institute of Technology, USA	2019	Cyber Security	Intrusion Detection	WGAN	[29]
Usama et al.	Information Technology University, Pakistan	2019	Cyber Security	Intrusion Detection	VGAN	[37]
Sedjelmaci et al.	Orange Labs, France	2020	Cyber Security	Intrusion Detection	VGAN	[38]
Huang et al.	Peking University China	2020	Cyber Security	Intrusion Detection	VGAN	[39]
Zhang et al.	University of Canterbury, New Zealand	2020	Cyber Security	Intrusion Detection	VGAN, BiGAN	[44]
Shahriar et al.	Florida International University, USA	2020	Cyber Security	Intrusion Detection	VGAN	[35]
Zhang et al.	Guizhou University, China	2020	Cyber Security	Malware Detection	VGAN	[24]
Liu et al.	Chinese Academy of Sciences, China	2020	Cyber Security	Malware Detection	GAN	[65]
Hitaj et al.	Stevens Institute of Technology, USA	2019	Cyber Security	Password Synthesis	WGAN	[48]
Khan et al.	Middle Tennesee State University, USA	2020	Cyber Security	Steganography	CycleGAN	[49]
Merino et al.	Towson University, USA	2019	Cyber Security	Traffic Generation	VGAN	[36]
Le et al.	Massachusetts Institute of Technology, USA	2020	Cyber Security	Traffic Generation	WGAN	[34]
Li et al.	National University of Singapore, Singapore	2018	CPS Security	Anomaly Detection	VGAN-LSTM	[53]
Li et al.	National University of Singapore, Singapore	2019	CPS Security	Anomaly Detection	VGAN-LSTM	[42]
Adiban et al.	Norwegian University of Science and Technology	2020	CPS Security	Anomaly Detection	VGAN	[54]
Bashar et al.	Queensland University of Technology, Australia	2020	CPS Security	Anomaly Detection	VGAN-LSTM	[55]
Alabugin et al.	South Ural State University, Russia	2020	CPS Security	Anomaly Detection	BiGAN	[56]
Ahmadian et al.	University of Houston, USA	2018	CPS Security	Attack Synthesis	VGAN	[50]
Ying et al.	China Electric Power Research Institute, China	2019	CPS Security	Attack Synthesis	VGAN	[41]
Mohammad et al.	Sahand University of Technology, Iran	2020	CPS Security	Attack Synthesis	CGAN	[51]
Shahriar et al.	Florida International University, USA	2021	CPS Security	Attack Synthesis	WGAN, CWGAN	[66]
Farajzadeh et al.	University of Windsor, Canada	2021	CPS Security	Dimensionality Reduction	Modified VGAN	[58]
Belenko et al.	Branch office of LG Electronics Inc, Russia	2018	CPS Security	Instrusion Detection	GAN	[57]
De et al.	University of Quebec, Montreal, Canada	2020	CPS Security	Intrusion Detection	VGAN-LSTM	[40]
Qu et al.	Deakin University, Australia	2020	Networking	Privacy Protection	VGAN	[33]
Ring et al.	Coburg University of ASA, Germany	2019	Networking	Traffic Generation	WGAN	[60]
Cheng et al.	Department of Defence, Australia	2019	Networking	Traffic Generation	VGAN	[25]

which increases the probability of mode collapse. The discriminator is fooled repeatedly by the success rate of only a few highly accurate samples.

From the evaluation, we find that the original GAN algorithm is used in most (90%) of the applications. However, such algorithm has several issues; thus, utilizing other stable version can be analyzed for different other applications. Future research can consider other applications/algorithms which are more common and promising in computer vision, such as pix-to-pix translation, video translation, etc. in cybersecurity domain and solve the problems in time-dependent dataset.

7 Conclusion

We have provided a comprehensive survey of GAN covering a wide range of applications in cybersecurity, CPS security and networks domain. First, we briefly introduced GAN, how its architecture is comprised of two neural network models: generator and discriminator and how they are successfully trained. Then we briefly touched on variants of GAN and their benefits. Then we presented current applications of GAN in the cyberspace by briefly discussing each reviewed paper. Then we discussed our findings by performing analysis on the reviewed papers. Finally, we ended with discussing the limitations of GAN in cyberspace and its potential. Considering the amount of traction GAN has gained in the year 2020, we expect the amount and diversity of GAN applications to increase as more papers will potentially be published overtime. Perhaps the applications appearing less frequently used could also be used more frequently as GAN limitations are further explored and better performing GAN variants emerge.

References

[1] Ian Goodfellow, Jean Pouget-Abadie, Mehdi Mirza, Bing Xu, David Warde-Farley, Sherjil Ozair, Aaron Courville, and Yoshua Bengio. Generative adversarial nets. *Advances in neural information processing systems*, 27, 2014.

[2] Jie Gui, Zhenan Sun, Yonggang Wen, Dacheng Tao, and Jieping Ye. A review on generative adversarial networks: Algorithms, theory, and applications. *IEEE Transactions on Knowledge and Data Engineering*, 2021.

[3] Mikael Sabuhi, Ming Zhou, Cor-Paul Bezemer, and Petr Musilek. Applications of generative adversarial networks in anomaly detection: A systematic literature review. *IEEE Access*, 2021.

[4] Hojjat Navidan, Parisa Fard Moshiri, Mohammad Nabati, Reza Shahbazian, Seyed Ali Ghorashi, Vahid Shah-Mansouri, and David Windridge. Generative adversarial networks (gans) in networking: A comprehensive survey & evaluation. *Computer Networks*, 194:108149, 2021.

[5] Nan Gao, Hao Xue, Wei Shao, Sichen Zhao, Kyle Kai Qin, Arian Prabowo, Mohammad Saiedur Rahaman, and Flora D Salim. Generative adversarial networks for spatio-temporal data: A survey. *ACM Transactions on Intelligent Systems and Technology (TIST)*, 13(2):1–25, 2022.

[6] Sung-Wook Park, Jae-Sub Ko, Jun-Ho Huh, and Jong-Chan Kim. Review on generative adversarial networks: Focusing on computer vision and its applications. *Electronics*, 10(10):1216, 2021.

[7] Alec Radford, Luke Metz, and Soumith Chintala. Unsupervised representation learning with deep convolutional generative adversarial networks. *arXiv preprint arXiv:1511.06434*, 2015.

[8] Mehdi Mirza and Simon Osindero. Conditional generative adversarial nets. *arXiv preprint arXiv:1411.1784*, 2014.

[9] Xi Chen, Yan Duan, Rein Houthooft, John Schulman, Ilya Sutskever, and Pieter Abbeel. Infogan: Interpretable representation learning by information maximizing generative adversarial nets. *Advances in neural information processing systems*, 29, 2016.

[10] Augustus Odena, Christopher Olah, and Jonathon Shlens. Conditional image synthesis with auxiliary classifier gans. In *International conference on machine learning*, pages 2642–2651. PMLR, 2017.

[11] Han Zhang, Tao Xu, Hongsheng Li, Shaoting Zhang, Xiaogang Wang, Xiaolei Huang, and Dimitris N Metaxas. Stackgan: Text to photo-realistic image synthesis with stacked generative adversarial networks. In *Proceedings of the IEEE international conference on computer vision*, pages 5907–5915, 2017.

[12] Jun-Yan Zhu, Taesung Park, Phillip Isola, and Alexei A. Efros. Unpaired image-to-image translation using cycle-consistent adversarial networks. In *Proceedings of the IEEE International Conference on Computer Vision (ICCV)*, Oct 2017.

[13] Martin Arjovsky, Soumith Chintala, and Léon Bottou. Wasserstein generative adversarial networks. In *International conference on machine learning*, pages 214–223. PMLR, 2017.

[14] Abhishek Kumar, Prasanna Sattigeri, and Tom Fletcher. Semi-supervised learning with gans: Manifold invariance with improved inference. *Advances in neural information processing systems*, 30, 2017.

[15] Tero Karras, Timo Aila, Samuli Laine, and Jaakko Lehtinen. Progressive growing of gans for improved quality, stability, and variation. *arXiv preprint arXiv:1710.10196*, 2017.

[16] Tero Karras, Samuli Laine, and Timo Aila. A style-based generator architecture for generative adversarial networks. In *Proceedings of the IEEE/CVF conference on computer vision and pattern recognition*, pages 4401–4410, 2019.

[17] Ayush Jaiswal, Wael AbdAlmageed, Yue Wu, and Premkumar Natarajan. Bidirectional conditional generative adversarial networks. In *Asian Conference on Computer Vision*, pages 216–232. Springer, 2018.

[18] Yunus Saatci and Andrew G Wilson. Bayesian gan. *Advances in neural information processing systems*, 30, 2017.

[19] Okwudili M Ezeme, Qusay H Mahmoud, and Akramul Azim. Design and development of ad-cgan: Conditional generative adversarial networks for anomaly detection. *IEEE Access*, 8:177667–177681, 2020.

[20] Youngnam Kim and Seungjin Choi. Forward-backward generative adversarial networks for anomaly detection. In *Asian Conference on Machine Learning*, pages 1142–1155. PMLR, 2019.

[21] Hanling Wang, Mingyang Li, Fei Ma, Shao-Lun Huang, and Lin Zhang. Unsupervised anomaly detection via generative adversarial networks. In *2019 18th ACM/IEEE International Conference on Information Processing in Sensor Networks (IPSN)*, pages 313–314. IEEE, 2019.

[22] Dule Shu, Nandi O Leslie, Charles A Kamhoua, and Conrad S Tucker. Generative adversarial attacks against intrusion detection systems using active learning. In *Proceedings of the 2nd ACM Workshop on Wireless Security and Machine Learning*, pages 1–6, 2020.

[23] Ahmed AlEroud and George Karabatis. Bypassing detection of url-based phishing attacks using generative adversarial deep neural networks. In *Proceedings of the Sixth International Workshop on Security and Privacy Analytics*, pages 53–60, 2020.

[24] Sicong Zhang, Xiaoyao Xie, and Yang Xu. A brute-force black-box method to attack machine learning-based systems in cybersecurity. *IEEE Access*, 8:128250–128263, 2020.

[25] Adriel Cheng. Pac-gan: Packet generation of network traffic using generative adversarial networks. In *2019 IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, pages 0728–0734. IEEE, 2019.

[26] Christopher Sweet, Stephen Moskal, and Shanchieh Jay Yang. On the veracity of cyber intrusion alerts synthesized by generative adversarial networks. *arXiv preprint arXiv:1908.01219*, 2019.

[27] Qiao Yan, Mingde Wang, Wenyao Huang, Xupeng Luo, and F Richard Yu. Automatically synthesizing dos attack traces using generative adversarial networks. *International Journal of Machine Learning and Cybernetics*, 10(12):3387–3396, 2019.

[28] Ahmed AlEroud and George Karabatis. Sdn-gan: generative adversarial deep nns for synthesizing cyber attacks on software defined networks. In *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*, pages 211–220. Springer, 2019.

[29] Christopher R Sweet. Synthesizing cyber intrusion alerts using generative adversarial networks. 2019.

[30] Weiwei Hu and Ying Tan. Generating adversarial malware examples for black-box attacks based on gan. *arXiv preprint arXiv:1702.05983*, 2017.

[31] Maria Rigaki and Sebastian Garcia. Bringing a gan to a knife-fight: Adapting malware communication to avoid detection. In *2018 IEEE Security and Privacy Workshops (SPW)*, pages 70–75. IEEE, 2018.

[32] Thomas Schlegl, Philipp Seeböck, Sebastian M Waldstein, Ursula Schmidt-Erfurth, and Georg Langs. Unsupervised anomaly detection with generative adversarial networks to guide marker discovery. In *International conference on information processing in medical imaging*, pages 146–157. Springer, 2017.

[33] Youyang Qu, Jingwen Zhang, Ruidong Li, Xiaoning Zhang, Xuemeng Zhai, and Shui Yu. Generative adversarial networks enhanced location privacy in 5g networks. *Science China Information Sciences*, 63(12):1–12, 2020.

[34] Joie Le, Arun Viswanathan, and Yuening Zhang. Generating high-fidelity cybersecurity data with generative adversarial networks. In *ASCEND 2020*, page 4117. 2020.

[35] Md Hasan Shahriar, Nur Imtiazul Haque, Mohammad Ashiqur Rahman, and Miguel Alonso. G-ids: Generative adversarial networks assisted intrusion detection system. In *2020 IEEE 44th Annual Computers, Software, and Applications Conference (COMPSAC)*, pages 376–385. IEEE, 2020.

[36] Tim Merino, Matt Stillwell, Mark Steele, Max Coplan, Jon Patton, Alexander Stoyanov, and Lin Deng. Expansion of cyber attack data from unbalanced datasets using generative adversarial networks. In *International Conference on Software Engineering Research, Management and Applications*, pages 131–145. Springer, 2019.

[37] Muhammad Usama, Muhammad Asim, Siddique Latif, Junaid Qadir, et al. Generative adversarial networks for launching and thwarting adversarial attacks on network intrusion detection systems. In *2019 15th international wireless communications & mobile computing conference (IWCMC)*, pages 78–83. IEEE, 2019.

[38] Hichem Sedjelmaci. Attacks detection and decision framework based on generative adversarial network approach: Case of vehicular edge computing network. *Transactions on Emerging Telecommunications Technologies*, page e4073, 2020.

[39] Shuokang Huang and Kai Lei. Igan-ids: An imbalanced generative adversarial network towards intrusion detection system in ad-hoc networks. *Ad Hoc Networks*, 105:102177, 2020.

[40] Paulo Freitas de Araujo-Filho, Georges Kaddoum, Divanilson R Campelo, Aline Gondim Santos, David Macêdo, and Cleber Zanchettin. Intrusion detection for cyber-physical systems using generative adversarial networks in fog environment. *IEEE Internet of Things Journal*, 2020.

[41] Huan Ying, Xuan Ouyang, Siwei Miao, and Yushi Cheng. Power message generation in smart grid via generative adversarial network. In *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, pages 790–793. IEEE, 2019.

[42] Dan Li, Dacheng Chen, Baihong Jin, Lei Shi, Jonathan Goh, and See-Kiong Ng. Mad-gan: Multivariate anomaly detection for time series data with generative adversarial networks. In *International Conference on Artificial Neural Networks*, pages 703–716. Springer, 2019.

[43] Bin Xia, Junjie Yin, Jian Xu, and Yun Li. Loggan: a sequence-based generative adversarial network for anomaly detection based on system logs. In *International Conference on Science of Cyber Security*, pages 61–76. Springer, 2019.

[44] Xiran Zhang. Network intrusion detection using generative adversarial networks. 2020.

[45] Shayan Taheri, Aminollah Khormali, Milad Salem, and Jiann-Shiun Yuan. Developing a robust defensive system against adversarial examples using generative adversarial networks. *Big Data and Cognitive Computing*, 4(2):11, 2020.

[46] Chuanlong Yin, Yuefei Zhu, Shengli Liu, Jinlong Fei, and Hetong Zhang. An enhancing framework for botnet detection using generative adversarial networks. In *2018 International Conference on Artificial Intelligence and Big Data (ICAIBD)*, pages 228–234. IEEE, 2018.

[47] Aidin Ferdowsi and Walid Saad. Generative adversarial networks for distributed intrusion detection in the internet of things. In *2019 IEEE Global Communications Conference (GLOBECOM)*, pages 1–6. IEEE, 2019.

[48] Briland Hitaj, Paolo Gasti, Giuseppe Ateniese, and Fernando Perez-Cruz. Passgan: A deep learning approach for password guessing. In *International Conference on Applied Cryptography and Network Security*, pages 217–237. Springer, 2019.

[49] Nibraas Khan, Ruj Haan, George Boktor, Michael McComas, and Ramin Daneshi. Steganography gan: Cracking steganography with cycle generative adversarial networks. *arXiv preprint arXiv:2006.04008*, 2020.

[50] Saeed Ahmadian, Heidar Malki, and Zhu Han. Cyber attacks on smart energy grids using generative adverserial networks. In *2018 IEEE Global Conference on Signal and Information Processing (GlobalSIP)*, pages 942–946. IEEE, 2018.

[51] Mostafa Mohammadpourfard, Fateme Ghanaatpishe, Marziyeh Mohammadi, Subhash Lakshminarayana, and Mykola Pechenizkiy. Generation of false data injection attacks using conditional generative adversarial networks. In *2020 IEEE PES Innovative Smart Grid Technologies Europe (ISGT-Europe)*, pages 41–45. IEEE, 2020.

[52] Apostolos P Fournaris, Aris S Lalos, and Dimitrios Serpanos. Generative adversarial networks in ai-enabled safety-critical systems: friend or foe? *Computer*, 52(9):78–81, 2019.

[53] Dan Li, Dacheng Chen, Jonathan Goh, and See-kiong Ng. Anomaly detection with generative adversarial networks for multivariate time series. *arXiv preprint arXiv:1809.04758*, 2018.

[54] Mohammad Adiban, Arash Safari, and Giampiero Salvi. Step-gan: A step-by-step training for multi generator gans with application to cyber security in power systems. *arXiv preprint arXiv:2009.05184*, 2020.

[55] Md Abul Bashar and Richi Nayak. Tanogan: Time series anomaly detection with generative adversarial networks. In *2020 IEEE Symposium Series on Computational Intelligence (SSCI)*, pages 1778–1785. IEEE, 2020.

[56] Sergei K Alabugin and Alexander N Sokolov. Applying of generative adversarial networks for anomaly detection in industrial control systems. In *2020 Global Smart Industry Conference (GloSIC)*, pages 199–203. IEEE, 2020.

[57] Viacheslav Belenko, Valery Chernenko, Maxim Kalinin, and Vasiliy Krundyshev. Evaluation of gan applicability for intrusion detection in self-organizing networks of cyber physical systems. In *2018 International Russian Automation Conference (RusAutoCon)*, pages 1–7. IEEE, 2018.

[58] Maryam Farajzadeh-Zanjani, Ehsan Hallaji, Roozbeh Razavi-Far, and Mehrdad Saif. Generative adversarial dimensionality reduction for diagnosing faults and attacks in cyber-physical systems. *Neurocomputing*, 2021.

[59] Kun Zhou, Wenyong Wang, Teng Hu, and Kai Deng. Time series forecasting and classification models based on recurrent with attention mechanism and generative adversarial networks. *Sensors*, 20(24):7211, 2020.

[60] Markus Ring, Daniel Schlör, Dieter Landes, and Andreas Hotho. Flow-based network traffic generation using generative adversarial networks. *Computers & Security*, 82:156–172, 2019.

[61] Chaoyun Zhang, Xi Ouyang, and Paul Patras. Zipnet-gan: Inferring fine-grained mobile traffic patterns via a generative adversarial neural network. In *Proceedings of the 13th International Conference on emerging Networking EXperiments and Technologies*, pages 363–375, 2017.

[62] Milad Salem, Shayan Taheri, and Jiann Shiun Yuan. Anomaly generation using generative adversarial networks in host-based intrusion detection. In *2018 9th IEEE Annual Ubiquitous Computing, Electronics & Mobile Communication Conference (UEMCON)*, pages 683–687. IEEE, 2018.

[63] Ibrahim Yilmaz, Rahat Masum, and Ambareen Siraj. Addressing imbalanced data problem with generative adversarial network for intrusion detection. In *2020 IEEE 21st International Conference on Information Reuse and Integration for Data Science (IRI)*, pages 25–30. IEEE, 2020.

[64] Francesco Zola, Jan Lukas Bruse, Xabier Etxeberria Barrio, Mikel Galar, and Raul Orduna Urrutia. Generative adversarial networks for bitcoin data augmentation. In *2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pages 136–143. IEEE, 2020.

[65] Zhicheng Liu, Shuhao Li, Yongzheng Zhang, Xiaochun Yun, and Zhenyu Cheng. Efficient malware originated traffic classification by using generative adversarial networks. In *2020 IEEE Symposium on Computers and Communications (ISCC)*, pages 1–7. IEEE, 2020.

[66] Md Hasan Shahriar, Alvi Ataur Khalil, Mohammad Ashiqur Rahman, Mohammad Hossein Manshaei, and Dong Chen. iattackgen: Generative synthesis of false data injection attacks in cyber-physical systems. In *2021 IEEE Conference on Communications and Network Security (CNS)*, pages 200–208. IEEE, 2021.