Enhancing Physical Layer Communication Security through Generative AI with Mixture of Experts

Changyuan Zhao, Hongyang Du, Dusit Niyato, Jiawen Kang, Zehui Xiong, Dong In Kim, Xuemin (Sherman) Shen, and Khaled B. Letaief

Abstract

AI technologies have become increasingly adopted in wireless communications. As an emerging type of AI technologies, generative artificial intelligence (GAI) is gaining attention in communication security. Due to its powerful learning ability, GAI models have demonstrated superiority over conventional AI methods. However, GAI still has several limitations, including high computational complexity and limited adaptability. Mixture of experts (MoE) technology, which uses multiple expert models for prediction through a gate mechanism, proposes possible solutions. In this article, we first review GAI model applications in physical layer communication security, discuss limitations, and explore how MoE can help GAI overcome these limitations. Furthermore, we propose an MoE-enabled GAI framework for network optimization problems for communication security. To demonstrate the framework's effectiveness, we provide a case study in a cooperative-friendly jamming scenario. The experimental results show that the MoE-enabled framework effectively assists the GAI algorithm, solves its limitations, and enhances communication security.

Introduction

As communication devices become a part of people's lives, carrying vast amounts of crucial information, the security and privacy of these communications face significant threats. Several threats exist in the physical layer of communication systems. The physical layer is a fundamental layer responsible for the raw transmission of bit streams across various transmission media. Attacks on this layer aim to disrupt data transmission or intercept data being transmitted. These vulnerabilities include attacks on communication signals, equipment, and sensors, highlighting the wide range of weaknesses that must be addressed for comprehensive communication network security. Due to the foundational level of wireless communication systems, ensuring the security of the physical layer is the first line of defense in wireless communications.

With the rise of AI technology, there has been a significant shift toward using advanced AI algorithms including machine learning and deep learning to solve security concerns at the physical layer. For example, Convolutional Neural Networks (CNNs) have been applied to facilitate multi-user authentication [1], and Recurrent Neural Networks (RNNs) have been utilized to design secure channel coding [2]. However, traditional AI methods fall short in addressing communication security challenges due to their inability to adapt to constantly changing wireless characteristics and sophisticated cyber threats. These methods are usually trained on specific datasets, which limits their effectiveness in unfamiliar conditions and unknown attacks. Additionally, collecting enough labeled data for physical layer attacks is difficult due to the complexity and variability of noise patterns, signal interference, and channel conditions [3]. Therefore, advanced AI models are needed to learn from and adapt to these environmental factors for robust security.

Generative Artificial Intelligence (GAI) is an essential AI technology that has proven to be remarkably effective in text, image, and audio generation. Unlike traditional AI models, GAI operates as an unsupervised learning, which can independently identify characteristics of data and generate new samples that closely resemble the original dataset. For example, Stable Diffusion, developed by Stability AI, is an advanced text-to-image generation model that can create highly detailed and accurate images based on textual descriptions (https://stability.ai/news/stable-diffusion-3). This ability of GAI to learn, replicate, and innovate is particularly useful in addressing crucial challenges in communication security, such as handling incomplete information and imbalanced data [4], which traditional AI models cannot effectively solve. Furthermore, the integration of GAI significantly strengthens the security framework, allowing for effective learning of both emerging and complex threats [5]. Despite its potential, GAI needs to be improved further due to its high computational complexity and limited adaptability. For

Changyuan Zhao is with Nanyang Technological University, Singapore, and CNRS@CREATE, Singapore; Hongyang Du is with University of Hong Kong, Hong Kong, China; Dusit Niyato is with Nanyang Technological University, Singapore; Jiawen Kang (corresponding author) is with Guangdong University of Technology, China; Zehui Xiong is with Singapore University of Technology and Design, Singapore; Dong In Kim is with Sungkyunkwan University, South Korea; Xuemin Shen is with University of Waterloo, Canada; Khaled B. Letaief is with Hong Kong University of Science and Technology, Hong Kong.

Digital Object Identifier: 10.1109/MWC.001.2400150

1536-1284/25/$25.00 © 2025 IEEE

instance, Stable Diffusion was trained using 256 Nvidia A100 GPUs on Amazon Web Services for a total of 150,000 GPU hours (https://www.gigantic.work/posts/stable-diffusion), which requires it to take relatively more computing resources and computing speed in the training and inference phases.

To address the aforementioned challenges effectively, the integration of the Mixture of Experts (MoE) approach into GAI-based models such as ChatGPT (https://medium.com/@seanbetts/peering-inside-gpt-4-understanding-its-mixture-of-experts-moe-architecture-2a42eb8bdcb3) presents a promising strategy. MoE is a machine learning ensemble technique that divides a complex task into several subtasks, which are then solved by specialized models, referred to as "experts." The MoE approach uses a gating mechanism to decide which experts to consult for a given input, effectively combining their strengths to improve overall performance on diverse or large-scale problems. In addition to language models, traditional AI models combined with MoE also have several applications in wireless communication security. For instance, ADMoE is an enhanced neural network-based anomaly detection algorithm by MoE [6], which demonstrates superior performance in noisy label detection.

Therefore, deploying MoE-enabled GAI models in wireless communication systems provide major advantages.

Flexibility and Specialization: By selecting different experts for different attack types, the MoE framework ensures that the GAI model can provide a more targeted and effective defense against complex attackers. For example, TB-CBR [7] selects different experts based on the feature of attacks to assign the most appropriate techniques for identifying the type of attack.

Scalability and Efficiency: By strategically allocating computational resources to the most pertinent experts for a specific task or learner, MoE-based systems can simultaneously manage a larger number of experts, thereby facilitating personalized learning at scale efficiently.

In conclusion, utilization of MoE in GAI models can enhance performance by dynamically allocating computational resources to specialized sub-models, thereby improving efficiency and adaptability in handling complex security tasks.

Based on these, we propose a framework to utilize the MoE structure in this article, enhancing the performance of GAI methods in communication security. The contributions of this article are summarized as follows.

We delve into the security considerations in the physical layer and provide a detailed analysis of GAI structure in communication security. Then, we discuss the benefits of implementing GAI models and explore the applications in physical layer communication security.

We present a general MoE-enabled GAI framework to solve optimization problems in communication security, which leverages the MoE's structural characteristics to enhance the protection performance of security protection algorithms in various scenarios.

We consider friendly jamming strategies in multi-user scenarios as a case study. We employ the MoE-enabled GAI reinforcement learning algorithm to solve the optimization problem and analyze the algorithm's efficacy improvement under various indicators.

Generative AI and Mixture of Experts in Physical Layer Communication Security

This section provides an overview of GAI models, and MoE concept, exploring how GAI and MoE can be effectively employed in physical layer communication security.

Generative AI for Physical Layer Communication Security

GAI models, which are based on unsupervised learning, have an ability to achieve self-learning from patterns and features in the data. They can emulate the dataset as closely as possible without needing label information. This capacity allows them to effectively address common data challenges in communication security, such as missing datasets and imbalanced data (Fig. 1). Currently, GAI models used in communication security include the following.

Autoencoder (AEs) and Variational Autoencoders (VAEs): AEs and VAEs compress the input into a lower-dimensional code and reconstruct the output from this representation as close as possible to the original input. Due to its encoding and decoding structure, it can be used to ensure Confidentiality, including wiretap code design, Joint Source Channel Coding (JSCC) [8]. Moreover, according to the reconstruction error, they can keep signal Integrity, aiding in anomaly detection.

Generative Adversarial Networks (GANs): GANs use adversarial learning to simultaneously improve the generation ability of the generator and the detection ability of the discriminator. Through adversarial learning, models can generate data similar to the dataset and enhance overall performance, ensuring data Availability and improving Resilience against various attacks, including spoofing attacks [5].

Diffusion Models (DMs): DM is a novel generative model that employs a unique technique for learning the underlying distribution of data. It first adds noise to the data and then removes it, effectively generating new data that follows the same distribution as the original. Due to its strong learning ability, DM is able to effectively learn and purify attacked data, preserving the Integrity of the data [9].

Even GAI models have different focuses and characteristics. It still faces some problems in dealing with today's more complex security issues.

High Complexity: GAI models are known for their sophisticated algorithms, complex training processes, and long inference times, contributing to their high complexity. When facing rapidly changing environments, they may struggle to infer and protect against cyber threats with limited resources.

Low Adaptability: Due to its dependence on predefined datasets, the inherent inflexibility can challenge maintaining effectiveness in diverse or novel contexts. As the model expands, retraining it from scratch becomes increasingly challenging, rendering it less adept at responding to unexpected events or data anomalies [10].

Limited Detection Performance: GAI models often focus on one or a few specific security threats, and when faced with complex real-world tasks, they typically demonstrate limited performance. This limitation is due to their high complex-

GAI models, which are based on unsupervised learning, have an ability to achieve self-learning from patterns and features in the data. They can emulate the dataset as closely as possible without needing label information.

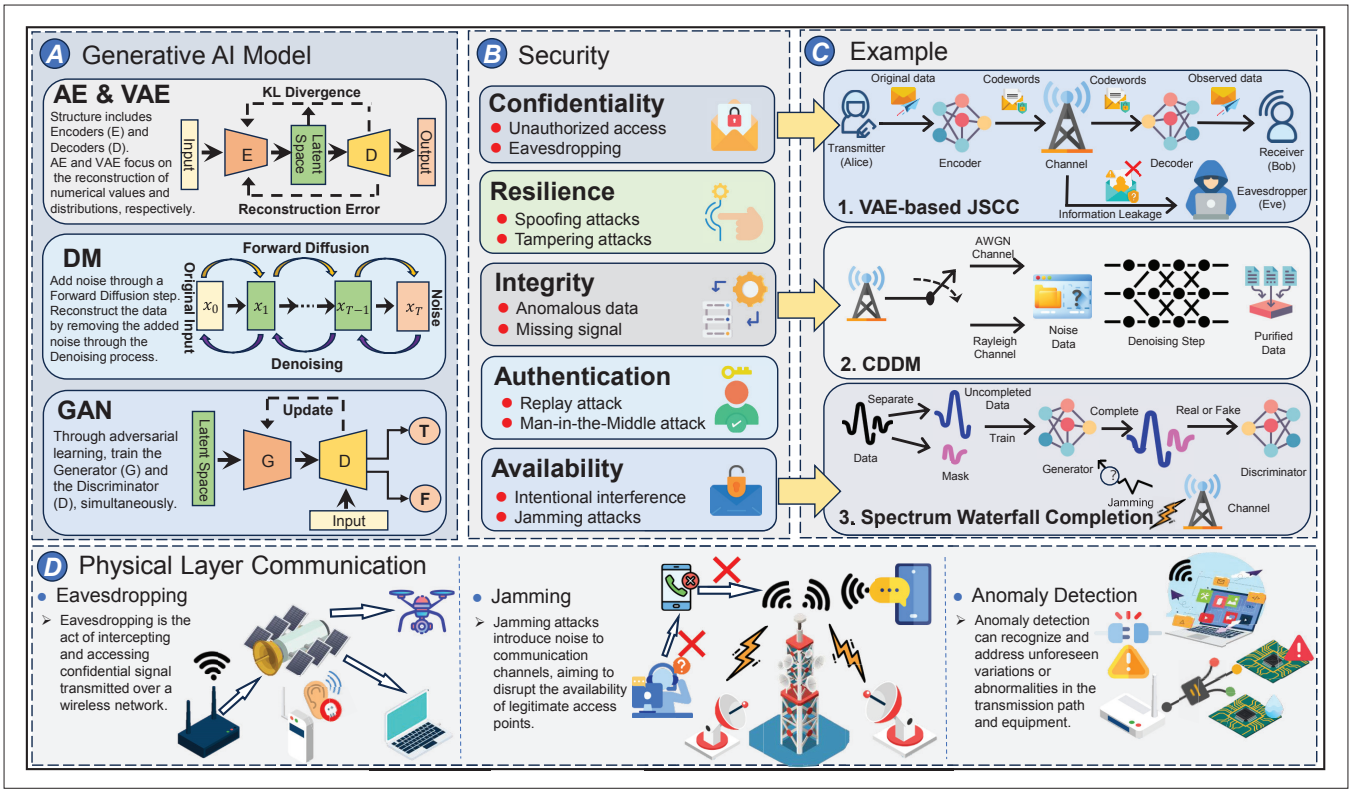

FIGURE 1. The overall of GAI for physical layer communication security. *Part A* illustrates the structure of GAI models. *Part B* presents security issues faced by physical layer communications. In *Part C*, we introduce three examples based on GAI for communication security. These three models are based on VAE [8], DM [9], and GAN [4], respectively. *Part D* demonstrates important physical layer communication attack scenarios, including eavesdropping, jamming, and anomaly detection

ity and low adaptability, which can hinder the AI's ability to accurately identify new, subtle, or sophisticated threats that differ from its training sets.

Given the challenges faced by existing GAI models, new architectures have been proposed to overcome these issues. MoE is an innovative approach aiming to enhance GAI's flexibility and effectiveness in dealing with a broader range of security threats by combining the strengths of multiple specialized models, that is, experts.

Mixture of Experts

MoE improves model performance, adaptability, and scalability by assigning tasks to specialized sub-models, or "experts," for a tailored approach to managing complex data [10]. By leveraging the unique strengths and expertise of multiple sub-models, each specialized in particular data types or tasks, MoE aims for higher accuracy and efficiency in computational problem-solving. An MoE model includes the following important components.

Gating Mechanism: A gating mechanism evaluates the input and decides which expert(s) should be activated for a given input, effectively routing the data to the most relevant expert models.

Expert Models: Each expert model, specialized in different tasks, processes the inputs that it receives. This specialization allows for tailored processing and improved handling of complex patterns within the data.

Combining Outputs: The outputs of the expert models are then aggregated. The method of aggregation can vary, including weighted sum, where the weights are often determined by the gating mechanism's output.

Figure 2 presents the main components of MoE and explains its working mechanism through two examples.

Due to its dynamic allocation capabilities and efficiency in tackling complex problems, the MoE framework has become widely used in Large Language Models (LLMs). MoE enables these models to manage diverse and complex linguistic tasks more effectively. Generally, using more expert models may increase the number of model parameters and training time. The gate mechanism of MoE chooses suitable expert models to ensure that only a set of selected model parameters are activated during the inference phase, guaranteeing inference speed without reducing the model's performance. For instance, Mixtral 8x7B (https://mistral.ai/news/mixtral-of-experts), a state-of-the-art transformer model developed on the MoE framework, has 46.7B total parameters but only uses 12.9B parameters per token. This efficient parameter use enables Mixtral to process inputs and generate outputs with the speed and cost efficiency of a 12.9 billion parameter model. Notably, Mixtral achieves competitive or superior performance compared to GPT-3.5 with 20.0B parameters across a range of benchmarks.

The above examples show that AI combined with MoE can bring a variety of improvements. Especially, in the field of communication security, combining MoE in GAI can bring many potential benefits.

Enhanced Detection: Learning the distribution of multiple hybrid attacks, including various spoofing attacks and jamming attacks, is usually a challenging task, which requires advanced structures for GAI models. By utilizing the MoE structure

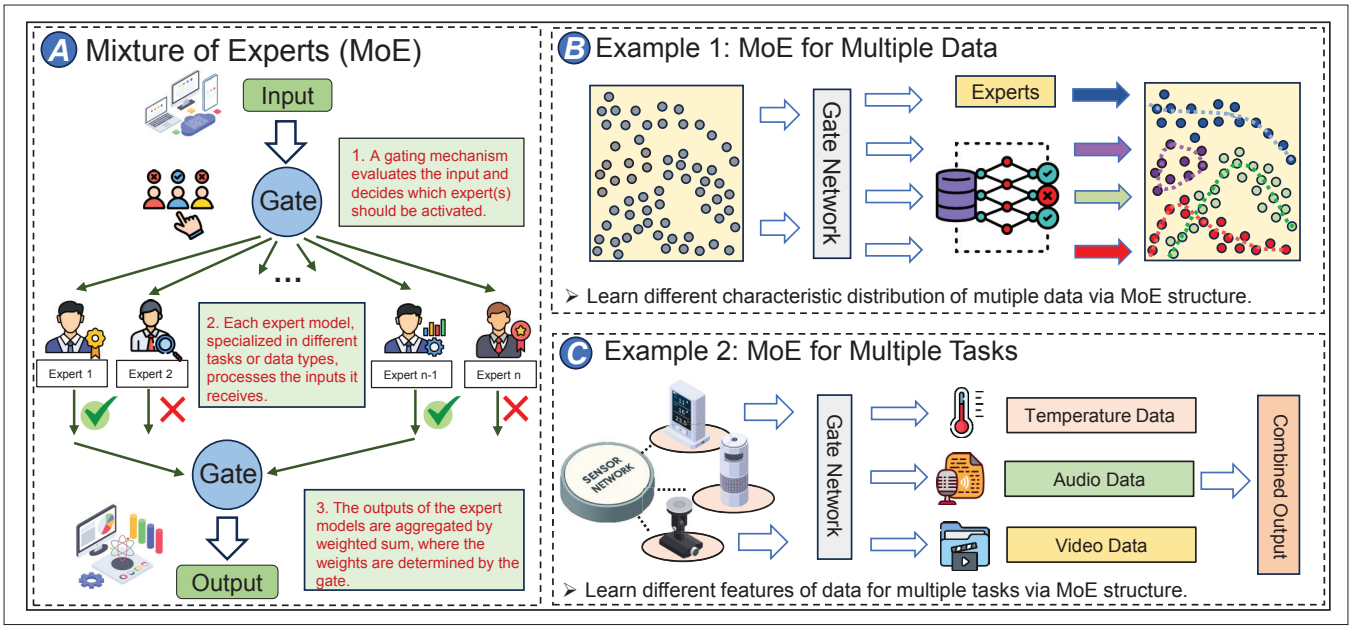

FIGURE 2. The structure of MoE. In Part A, we illustrate the main components and working mechanism of the MoE framework. Part B presents an example of using the MoE framework to learn the different characteristic distributions of multiple data. Part C demonstrates how to learn different features of data for multiple tasks via MoE structure.

that combines multiple expert models, a single sub-model can focus on learning the distribution of certain attacks, thus improving the fitting capability for the attacks with a relatively simple model.

Resource Efficiency: In the inference phase, the GAI model needs to use all parameters under its complex network structure, making it difficult to deploy and perform real-time calculations on edge devices with limited resources. The gate mechanism enables the MoE model to activate only the most suitable sub-model for the specific task at hand, optimizing the use of available resources and ensures a more effective response to cyber threats.

Adaptive Learning: In wireless communications, whenever the GAI model needs to learn the distribution of a new attack, such as jamming attacks from a new source, all parameters of the model need to be trained. The MoE uses a gate mechanism to train the key parameters of GAI model, reducing the training cost of the overall model, and improving the overall adaptability.

These features can address issues encountered by GAI models mentioned above, providing a foundation for using the MoE structure to improve the performance of GAI models in communication security.

Applications of Generative AI and Mixture of Experts for Physical Layer Security

GAI technology has numerous applications for wireless communications. In this section, we present several GAI applications in physical layer communication security and provide examples of combining GAI with MoE (Table 1).

GAI for Confidentiality

JSCC optimizes both source coding (compression) and channel coding (error correction) in a unified approach to enhance efficiency and reliability of data transmission while safeguarding data confidentiality against eavesdroppers over a wiretap channel. GAI models, particularly AEs and VAEs, are able to encode data into a latent space and then decode it back to the original space through distribution decoding in the feature space, effectively serving as a JSCC mechanism. For example, a VAE-based JSCC approach proposed in [8] was designed to minimize information leakage and protect sensitive information from being deciphered by unauthorized parties. Specifically, this approach involves a transmitter (Alice) encoding source data and a receiver (Bob) aiming to reconstruct the encoded data with high fidelity, while ensuring that the sensitive information remains undetectable by any potential eavesdroppers (Eves). This is achieved by maximizing the mutual information between the user's data and the noisy codewords observed by Bob, while minimizing the distortion to improve the pixel-wise data reconstruction quality. According to the experiments, the proposed method can achieve good performance in both single channel and parallel channels scenarios. Especially in the parallel Channels scenario, Eve's classification accuracy is only 20% on average [8].

GAI for Integrity

During the transmission of data, it will be affected by factors such as noise and attacks, which will affect the integrity and accuracy of the data received by receivers, even with the presence of attacks to alter the data maliciously. Due to its inherent ability to progressively remove noise, DMs have the potential to aid the receivers in mitigating channel noise and purifying received data. A representative example is Channel Denoising Diffusion Models (CDDM) [9] designed to leverage the noise reduction properties of DMs. The proposed model consists of three stages, where the first and last stages are the JSCC encoder and decoder trained to minimize the reconstruction error, respectively. The second stage utilizes a noise schedule that closely simulates the distri-

Security Consideration	Reference	Algorithm	Pros & Cons
Confidentiality	[8]	VAE-based JSCC	● A data-driven approach using VAE-based JSCC ✓ Conceal the confidential data different from the original signal × Assume worse eavesdropping channel quality
Integrity	[9]	CDDM	● A channel denoising diffusion models to remove noise in communications channels ✓ Remove the channel nosie under multiple fading channels × Require relatively long sampling time
	[11]	MEx-CVAEC	● An anomaly detection method combined with MoE framework ✓ Learn multiple latent space features instead of a single feature space × Lack experiments on complex data sets
Availability	[4]	GAN	● A GAN-based algorithm designed to uncover the data relationships and fill in the gaps in the data ✓ Recover spectrum data in multiple jamming conditions × Lack real-world experiments

TABLE 1. Summary of GAI and MoE for communication security. Blue circles describe the methods; Green correct markers and Red cross markers represent pros and cons respectively.

bution of channel noise, rendering the CDDM adaptable to a variety of channel conditions. The efficacy of integrating CDDM into communication systems is evident from the results, which show a consistent performance improvement across all signal-to-noise ratio (SNR) levels. Specifically, the inclusion of CDDM under an Additive White Gaussian Noise (AWGN) channel and a Rayleigh fading channel at 20 dB SNR results in gains of 0.49 dB and 1.06 dB [9], respectively.

GAI for Availability

The jamming attack aims to cause interference by introducing noise, thereby disrupting legitimate communications at the physical layer. Jamming attacks often result in incomplete data due to their attack characteristics, which hinders the ability of anti-jamming strategies to accurately identify jamming attacks. The authors in [4] have proposed an efficient algorithm that makes use of a GAN to complete missing information in a spectrum waterfall. A spectrum waterfall is a thermodynamic block diagram that defines the environmental state. By automatically mining relationships within the data, the algorithm can accurately complete any missing data. Unlike an original GAN, where noise inputs were used, the authors utilized the spectrum waterfall with the missing data as the generator input, consequently limiting the generator's artistry. According to the corresponding complement results, the proposed algorithm outperforms the method without pre-classification since the generator adding auxiliary information to the data is more targeted. The accuracy of the proposed algorithm is over 95%, compared to the nearly 80% accuracy of the method that does not use pre-classification [4].

MoE-Based GAI for Security

Typically, reconstruction-based GAI models for anomaly detection only consider a single latent space. However, multiple latent spaces contain various correlation discriminative features, each contributing differently to efficient anomaly detection. MEx-CVAEC [11] is an MoE-based model, comprising two convolutional VAEs and CNNs. Each component operates as an expert with an identical procedural framework to efficiently process highly relevant information. According to the latent space visualization comparison, a model with multiple expert structures can better cluster normal and abnormal data than a single expert. Compared with other unsupervised learning or GAI baselines, the mean Area Under the Curve (AUC) of this model based on three different datasets can achieve the best performance [11]. In conclusion, by leveraging the potential of several latent spaces via the MoE structure, the overall detection performance can be enhanced.

Lessons Learned

From above applications, we can draw the following key observations:

- GAI models are able to learn the distribution of the dataset and then reconstruct the data from the distribution, which is suitable for secure communications. For instance, VAE models can be utilized to improve the encoding of physical layer data transmission [8].
- Different from traditional AI models, GAI models can purify data by learning the characteristics of attacks or noise. In the above example, if the data is not purified, the accuracy of the received information will be seriously affected and the integrity cannot be ensured.
- By practicing adversarial learning, GAI has the ability to learn data features more precisely, and also enhance the accuracy of the discriminator. This approach resolves the issue of data incompleteness and imbalance caused by intricate scenes such as jamming attacks.
- The MoE structure allows AI detection models to utilize more complex data including multi-label, multi-category, and multi-latent distributions, improving detection accuracy compared to a single model.

However, most existing works only consider certain scenarios and lack real-world testing since they have difficulty inferring and adapting to additional fast, time-varying information in real-time [4]. Therefore, using the MoE structure has become one of the feasible solutions to solve GAI's issues in communication security.

MoE-Enabled Generative AI for Physical Layer Communication Security

In this section, we discuss research challenges in communication security optimizations. Then, we propose an MoE-enabled GAI framework focusing on optimization problems in communication security.

Research Challenges

Communication security emphasizes the design of secure, safe, and reliable information transmission methods [12]. From the perspective of system optimization and design, ensuring communication security mainly includes the following aspects.

Resource Allocation: Secure resource allocation aims to optimize limited communication resources, such as bandwidth and energy, to maximize the requirement of various performance metrics, including Secrecy Rate, Secrecy Outage Probability (SOP), power consumption, and Energy Efficiency (EE) [12].

Signal Processing: Secure beamforming and precoding are advanced signal processing techniques designed to enhance the confidentiality of wireless communications. By intelligently shaping and directing transmitted signal beams, these methods minimize potential eavesdropping and jamming, thus optimizing the network's Secrecy Rate and EE.

Antenna Selection and Cooperation: In multi-antenna wireless networks, selection and cooperation of antennas can improve performance metrics such as secrecy rate and outage probability [13]. These strategies can reduce power consumption while boosting EE.

Reinforcement Learning (RL) algorithms based on DMs have recently achieved success in solving such communication optimization problems, including UAV path planning and resource allocation [13]. However, it usually focuses only on a single optimization goal and cannot address joint considerations of communication security [12]:

- The transmission effectiveness is evaluated through the achievable Secrecy Rate.
- Reliability is measured in terms of SOP.
- Power cost refers to the minimum power consumption required to ensure secure Quality of Service (QoS).
- EE is concerned the quantity of secret bits transferred per unit of energy.

Framework Design

Based on the characteristics of MoE and GAI framework, in this part, we propose the MoE-enabled GAI framework to solve communication security optimization problems.

Architecture: Our framework follows the GAI-based RL model, GDM [13]. Incorporating the denoising module into the RL framework, GDM leverages the reward function to assess the current denoising outcome. This enables GDM to generate an action strategy that aims for the highest, that is, the optimal resource allocation strategy. With the introduction of noise and the denoising process, GDM significantly improves exploration and learning capabilities compared to traditional RL algorithms. Consequently, GDM is better suited for addressing complex optimization problems in wireless communications [13].

To consider multiple performance metrics at the same time, we incorporate the MoE structure after the state input layer. By adopting the MoE structure, different experts can focus on some most suitable performance metrics with a shared-bottom model [14] rather than optimizing all metrics at the same time. In addition, the trainable gate network can explore more prediction results for different inputs to meet multiple indicators during the training process. For instance, suppose two performance metrics need to be optimized in a wireless communication system, including secrecy rate and energy efficiency. In such a case, the GAI framework with MoE can be trained by combining two experts. Each expert can be automatically assigned to capture either shared performance metrics information or a specific one, which is more conducive than one network to finding the theoretically optimal solution for two metrics.

Specifically, regarding secure communication, the definitions of the state space, action space, and reward are as follows:

- *State Space:* The state space consists of the current information and previously selected actions. The state is the channel information, which includes characteristics such as channel quality, current interference levels, signal fading, and other relevant environmental conditions affecting signal transmission.
- *Action Space:* The action space encompasses a range of adjustable parameters that can significantly influence its performance and security. Examples of these parameters include frequency, bandwidth, transmission power, and devices distance.
- *Reward:* The reward based on each action taken at the current state is determined by security performance metrics [12]. The performance metrics are different security metrics including Secrecy Rate, SOP, and EE, and so on.

User Workflow: In the proposed framework, to solve an optimization problem about communication security, one may follow these steps (Fig. 3 Part A):

- *Task Setting:* To optimize a secure transmission, users must first confirm reasonable performance metrics that consider security performance. This is usually achieved through a variety of metrics, which are then divided into individual tasks. For example, when designing a system to prevent eavesdropping, users can consider the hybrid metrics.
- *MoE Learning:* By using the gate mechanism in MoE, the input states can be divided into individual independent expert models. Then different experts can automatically capture either shared and task-oriented information, allowing them to obtain higher action reward. For instance, users can assign three or more experts to optimize different performance metrics, through the learning of gate network.
- *Denosing Diffusion:* Based on the GDM structure [13], users predict actions in the current state by using a conditional denoising process to filter out noise. The conditions used in this process can correspond to various subtasks, such as current state, previously selected action, or a combination of both. For instance, when focusing on improving security performance, the users can choose the current channel state and the previous transmission power as conditions in the subtask of transmission power.
- *Action Evaluation:* Instead of denoising toward the maximum value of the probability distribution, the actor network is learned by denoising toward the direction that maximizes reward, and then combined with the gate network to obtain the finial decision.

Combining the powerful generation capability of GAI with learning for an optimal action denois-

Secure beamforming and precoding are advanced signal processing techniques designed to enhance the confidentiality of wireless communications. By intelligently shaping and directing transmitted signal beams, these methods minimize potential eavesdropping and jamming, thus optimizing the network's Secrecy Rate and EE.

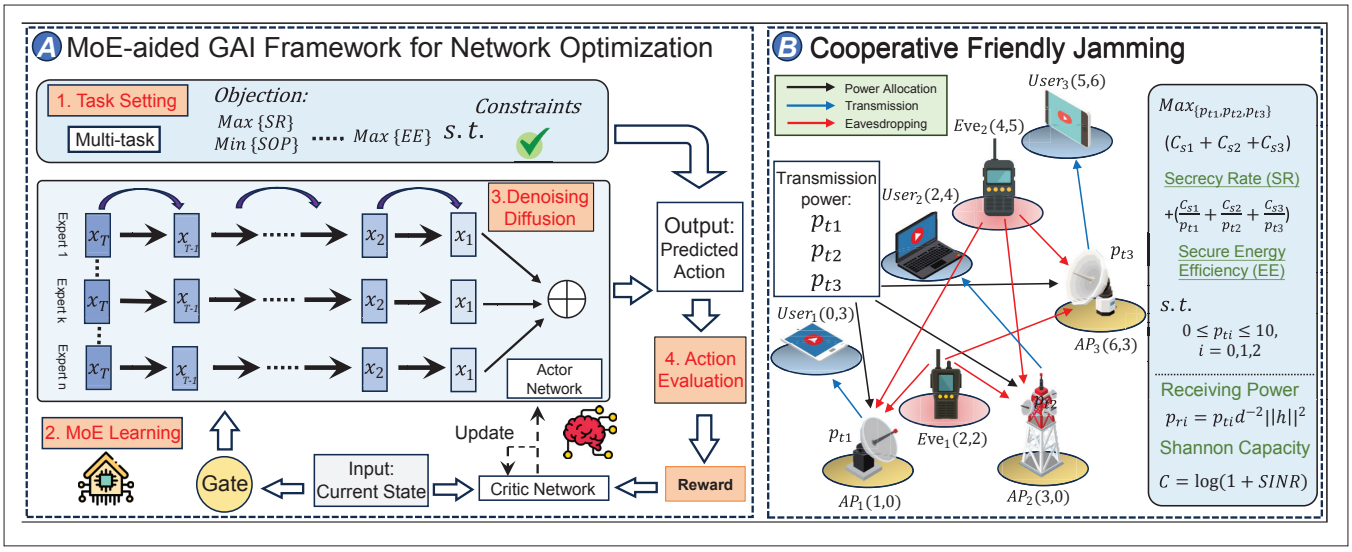

FIGURE 3. The workflow of the proposed framework. In Part A, the proposed framework solves optimization problems through reinforcement learning following 4 steps: 1). Task Setting; 2). MoE Learning; 3). Denoising Diffusion; 4). Action Evaluation. Part B illustrates the cooperative friendly jamming optimization problem considered below. The figure introduces the detail scenario and optimization problem settings including optimization objectives, constraints, and so on.

ing can help to explore the optimal solution more effectively [13]. By incorporating the MoE structure, the framework can focus on multiple performance metrics simultaneously, achieving better results in multi-objective optimization problems.

Case Study: Cooperative Friendly Jamming for Physical Layer Communication Security

In this section, we present a case study that demonstrates the optimization for cooperative friendly jamming and utilizes the proposed framework to demonstrate how MoE can improve the performance of GAI models.

System Model

We consider a cooperative friendly jamming scenario, where Access Points (APs) produce friendly jamming signals to further degrade eavesdropping [15]. This scenario involves multiple APs, multiple users, and potential eavesdroppers. When a user downloads data from a certain AP, the other APs will act as jammers to prevent any eavesdroppers from intercepting the user's traffic. In this case study, we consider 3 APs, 3 users, and 2 eavesdroppers, where each user communicates with one AP with limited transmission power p_t (Fig. 3 Part B). For the received power p_r of the system, we consider large-scale fading based on distance d and small-scale fading *h* based on the Rayleigh fading model. For a given user or eavesdropper, the Shannon capacity is determined by the Signal to Interference plus Noise Ratio (SINR), where SINR is calculated from the received APs power and noise.

Optimization Problem Formulation

We aim to jointly maximize Secrecy Rate and secure EE [12] to find the optimal transmission power allocation pt to the APs. The effectiveness of physical layer communication security strategies can be measured using Secrecy Rate. Our assessment of Secrecy Rate involves comparing the data rate of the legitimate channel to that of the wiretap channel with the Gaussian codebook. For a given user, the Secrecy Rate C_s is calculated via the Shannon capacity minus the largest Shannon capacity of eavesdroppers.

Our goal for EE is to ensure that the transmission strategy operates in a confidential and eco-friendly manner. To achieve this, we utilize secure EE, which is the amount of secret bits transmitted with the consumption of one unit of energy. For a given AP, its secure EE S_e is determined by the ratio of Secrecy Rate of the corresponding user to AP's transmission power p_t.

Numerical Results

Experimental Setup: Our experiment is based on Python along with the PyTorch package, conducted on a V100 Linux server. The main program is based on the GDM framework [13]. The proposed MoE method includes 3 experts and selects the best expert each time.

Performance Analysis: Figure 4 illustrates the comparison of various performance metrics between the proposed MoE-enabled GAI method, GDM without MoE, and Deep Deterministic Policy Gradient (DDPG) algorithm [13] in a given scenario. Among them, the blue curve represents the MoE method, the orange curve represents GDM, the green curve represents DDPG, and the reward represents the specific numerical value of metrics. Based on the transmission power derived from two approaches, Fig. 4a illustrates the learning curve for the sum of Secrecy Rate and secure EE. Clearly, the proposed method demonstrates the ability to converge to a reward of approximately 40.56 and has the potential to explore and achieve a reward as high as 47.19. In comparison, the reward obtained through GDM tends to converge around 27.99, with the maximum reward during training reaching only 34.63. The DDPG method performs even worse, achieving only around 23.17 and the maximum reward capped at 34.52. Figure 4b shows the numerical relationship between the two indicators among the three methods. From the scatter plot, we can observe that the two security metrics are not strongly correlated, indicating the challenge of simultaneously optimizing two indicators. Based on the linear

trend lines, as Secure EE increases, the Secrecy Rate metrics of all three methods show a downward trend. Notably, the proposed method (blue curve) decreases slowly, and higher Secure EE values can be explored compared to the other two methods with the same Secrecy Rate value.

Discussion

The experimental results above demonstrate that in a cooperative friendly jamming scenario, the MoE-enabled GAI optimization algorithm can achieve better exploration performance and convergence results in optimizing mixed metrics, including Secrecy Rate and secure EE. Through the comparison results (Fig. 4), the proposed MoE-enabled approach can achieve performance similar to, or better than, other methods, especially for Secure EE, when dealing with a single task. Moreover, the MoE can explore more suitable resource allocation strategies to improve the performance of one task (Secure EE) without significantly compromising the performance of another task (Secrecy Rate). In summary, the proposed MoE-enabled method can ensure single solution capabilities and simultaneously explore high-performance resource allocation strategies for the multi-task target. Since the MoE only activates one expert through the gate network for training and inference each time, the overall computational complexity is similar to that of the original GDM and does not increase significantly.

Future Directions

Zero-Trust Physical Layer Communication

Zero-trust communication refers to a security strategy where every communication attempt must be verified. The MoE-based GAI algorithm allows for the simultaneous maximization of various security performance metrics during the network design process, such as MoE-based DMs for graph generation. Therefore, all network entities can be verified and trusted, minimizing the risk of tampering or interception.

Real-time Anomaly Detection

The high communication speed has put forward requirements for real-time anomaly detection. By leveraging MoE structure, only important network levels will be activated according to the gate mechanism, reducing the inference speed of GAI models. This approach could also significantly improve the detection of sophisticated cyber-attacks that conventional systems might overlook.

Enhanced Privacy Preservation

Data privacy protection is also an important part of physical layer security. During transmission, MoE-enabled GAI model can process signals in a way that maximizes data privacy. For instance, experts within the MoE model could specialize in different privacy-preserving techniques such as data anonymization, encryption, and differential privacy.

Conclusions

The article demonstrated how GAI models can improve communication security and explores their capabilities when combined with the MoE framework. Specifically, we started by introducing the GAI technology and its application in physical layer communication security. We emphasized superior capabilities of GAI and compared them to conventional AI models in communication security by providing examples. Subsequently, we highlighted the limitations of the GAI model. By introducing the structure and characteristics of MoE, we explored the possibility of the MoE framework to overcome limitations of GAI models. Finally, we proposed an MoE-enabled GAI framework focusing on network optimization problems in communication security. Through a case study in a cooperative friendly jamming scenario, it illustrated how the MoE structure improves GAI algorithms to ensure safety in wireless communication systems.

FIGURE 4. Performance comparison of three methods in the cooperative friendly jamming scenario: a) Comparisons of sum of Secrecy Rate and secure EE for three methods; b) Comparison of metrics relationship for three methods.

Acknowledgment

This research is supported by the National Research Foundation, Singapore, and Infocomm Media Development Authority under its Future Communications Research & Development Programme, Defence Science Organisation (DSO) National Laboratories under the AI Singapore Programme (FCP-NTU-RG-2022-010 and FCP-ASTAR-TG-2022-003), Singapore Ministry of Education (MOE) Tier 1 (RG87/22), the NTU Centre for Computational Technologies in Finance (NTU-CCTF), and Seitee Pte Ltd; in part by the National Natural Science Foundation of China under Grants No. 62102099, and Guangdong Basic and Applied Basic Research Foundation under Grant 2023A151514 0137; in part by the National Research Foundation of Korea

(NRF) Grant funded by the Korean Government (MSIT) under Grant 2021R1A2C2007638 and the MSIT under the ITRC support program (IITP-2023-RS-2023-00258639) supervised by the IITP (Institute for ICT Planning & Evaluation); in part by the Hong Kong Research Grants Council under the Areas of Excellence scheme grant AoE/E-601/22-R.

References

[1] R. Liao *et al.*, "A Novel Physical Layer Authentication Method With Convolutional Neural Network," *Proc. IEEE Int'l. Conf. Artificial Intelligence and Computer Applications*, IEEE, 2019, pp. 231–35.
[2] X. Xiao *et al.*, "Designing Finite Alphabet Iterative Decoders of Ldpc Codes via Recurrent Quantized Neural Networks," *IEEE Trans. Commun.*, vol. 68, no. 7, 2020, pp. 3963–74.
[11] Q. Yu, M. S. Kavitha, and T. Kurita, "Mixture of Experts With Convolutional and Variational Autoencoders for Anomaly Detection," *Applied Intelligence*, vol. 51, 2021, pp. 3241–54.
[12] D. Wang *et al.*, "A Survey of Optimization Approaches for Wireless Physical Layer Security," *IEEE Commun. Surveys & Tutorials*, vol. 21, no. 2, 2018, pp. 1878–1911.
[13] H. Du *et al.*, "Beyond Deep Reinforcement Learning: A Tutorial on Generative Diffusion Models in Network Optimization," arXiv preprint arXiv:2308.05384, 2023.
[3] J. Wang *et al.*, "Generative AI for Integrated Sensing and Communication: Insights From the Physical Layer Perspective," arXiv preprint arXiv:2310.01036, 2023.
[4] Y. Cai *et al.*, "Spectrum Waterfall Completion in Jamming Enviroment: A General Adversarial Networks Method," *Proc. IEEE 9th Joint Int'l Information Technology and Artificial Intelligence Conf.*, IEEE, vol. 9, 2020, pp. 1661–65.
[5] Y. Shi, K. Davaslioglu, and Y. E. Sagduyu, "Generative Adversarial Network in the Air: Deep Adversarial Learning for Wireless Signal Spoofing," *IEEE Trans. Cognitive Commun. Networking*, vol. 7, no. 1, 2020, pp. 294–303.
[6] Y. Zhao *et al.*, "Admoe: Anomaly Detection With Mixture-of-Experts From Noisy Labels," *Proc. Association Advancement of Artificial Intelligence Conf. Artificial Intelligence*, vol. 37, no. 4, 2023, pp. 4937–45.
[7] C. I. Pinzón *et al.*, "Real-Time CBR-Agent With a Mixture of Experts in the Reuse Stage to Classify and Detect DoS Attacks," *Applied Soft Computing*, vol. 11, no. 7, 2011, pp. 4384–98.
[8] E. Erdemir, P. L. Dragotti, and D. Gündüz, "Privacy-Aware Communication Over a Wiretap Channel With Generative Networks," *Proc. IEEE Int'l. Conf. Acoustics, Speech and Signal Processing*, IEEE, 2022, pp. 2989–93.
[9] T. Wu *et al.*, "CDDM: Channel Denoising Diffusion Models for Wireless Communications," *Proc. IEEE Global Commun. Conf.*, IEEE, 2023, pp. 7429–34.
[10] J. Wang *et al.*, "Toward Scalable Generative Ai via Mixture of Experts in Mobile Edge Networks," arXiv preprint arXiv:2402.06942, 2024.
[14] J. Ma *et al.*, "Modeling Task Relationships in Multi-Task Learning With Multi-Gate Mixture-of-Experts," *Proc. 24th ACM SIGKDD Int'l. Conf. Knowledge Discovery & Data Mining*, 2018, pp. 1930–39.
[15] S. A. Hoseini *et al.*, "Cooperative Jamming for Physical Layer Security Enhancement Using Deep Reinforcement Learning," arXiv preprint arXiv:2403.10342, 2024.

Biographies

Author biographies were unavailable at the time of publication.