Neuro-Symbolic AI for Self-Evolving Signal Processing in Autonomous Communication Systems

Raj Kashikar
Department of Computer Science
Virginia Polytechnic Institute and State University
Blacksburg, VA, USA
rajskashikar@vt.edu

2024 7th International Conference on Signal Processing and Information Security (ICSPIS) | 979-8-3503-6867-3/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICSPIS63676.2024.10812626

***Abstract*—The rapid advancement of autonomous systems demands highly adaptive and secure communication protocols. To address these challenges, we present a novel neuro-symbolic AI framework that enables real-time self-evolving signal processing in highly dynamic and security-sensitive autonomous communication systems. By integrating the strengths of neural networks in pattern recognition with the logical, adaptive decision-making capabilities of symbolic AI, the system autonomously optimizes communication protocols without human intervention. This approach leverages multi-scale convolutional neural networks (CNNs) for hierarchical signal feature extraction and uses symbolic AI for rule-based adaptation. Additionally, quantum key distribution (QKD) is employed to secure the evolving communication channels. Through comprehensive simulations, this system achieved a substantial improvement in signal-to-noise ratio (SNR) by 33% ± 2% and reduced bit error rate (BER) by 44% ± 3%, outperforming existing models. Furthermore, the proposed framework's ability to dynamically adapt to new environmental stimuli and secure communications in real time introduces a groundbreaking self-evolving communication system.**

***Index Terms*—Autonomous Communication, Autonomous Vehicles, Deep Learning, Neuro-Symbolic AI, Quantum Key Distribution (QKD), Satellite Networks, Secure Communication, Self-Evolving Systems, Signal Processing, Symbolic Reasoning**

I. Introduction

The rapid expansion of autonomous systems, such as self-driving vehicles, drone swarms, and satellite communication networks, has triggered the need for highly adaptive and secure communication protocols. These systems operate in environments that are highly dynamic, involving unpredictable factors like interference, signal fading, and adversarial attacks. Traditional signal processing techniques, designed with static, rule-based algorithms, are inadequate in these conditions as they lack the real-time adaptability needed to handle the fluctuating environmental conditions [1]. Additionally, scaling these systems globally—such as in autonomous vehicle fleets or satellite constellations—introduces significant security challenges, especially when sensitive data is exchanged over long distances or via public networks [2].

Autonomous vehicles, for instance, often face rapidly changing environments, such as navigating urban environments with dense signal interference or moving through tunnels where signals degrade [3]. Similarly, satellite networks may experience signal degradation due to atmospheric disturbances, leading to latency, data loss, or communication failure [4]. These environments demand communication systems that can autonomously adapt their signal processing techniques in real-time while maintaining high levels of security to protect against malicious attacks or data breaches [5].

The advent of neuro-symbolic AI offers a potential solution to these challenges. Neuro-symbolic AI combines the robust pattern recognition capabilities of neural networks with the structured, logical decision-making power of symbolic AI [6]. Unlike standard reinforcement learning, the self-evolving capability here integrates an adaptive reward mechanism, dynamically adjusting to environmental feedback with minimal human intervention. This custom approach allows the system to continuously optimize its communication protocols in a more nuanced manner, further distinguishing it from conventional reinforcement learning methods. This hybrid approach enables the system to both process unstructured data (such as signals with high noise) and evolve its decision-making logic based on real-time feedback from the environment. This is critical for systems operating in environments with fluctuating interference, noise, and signal degradation.

This paper introduces a novel framework for self-evolving signal processing in autonomous communication systems. While neuro-symbolic AI has been explored in fields like cognitive systems and robotics, its application to signal processing in AV and satellite communication networks is unprecedented. Additionally, the integration of quantum key distribution (QKD) to secure real-time, evolving communication channels is a novel approach, addressing both adaptability and security concerns simultaneously. In particular, existing models lack the capability to autonomously evolve and respond to new environmental stimuli without manual intervention. While our approach demonstrates significant potential in controlled simulations, the results may vary under real-world conditions due to environmental complexity, hardware limitations, and factors not fully captured in our simulated setup. Our system's self-evolving nature ensures that it can continuously optimize signal processing protocols in real time based on environmental conditions such as interference, latency, and even potential attacks, without any human input.

The integration of neuro-symbolic AI with real-time signal processing and QKD benefits from adaptability not previously provided by any system in these applications. Pure deep learning methods are powerful in pattern recognition but tend to be black-box models that don't offer much in terms of explainability and adaptability in view of real-time decision-making processes expected in highly dynamic environments. While symbolic reasoning conveys better performance for logic-based decision-making, it falls short when confronted with noise and complexity arising from real-world signal processing. The neuro-symbolic AI system bridges this performance gap by applying deep learning for unstructured signal processing and symbolic AI for logical, transparent decision-making, enabling real-time adaptation of communications protocols. It integrates QKD, enhancing security thanks to the principles of quantum mechanics to detect any case of eavesdropping and, therefore, make interceptions detectable and nullifiable in real time.

Our symbolic AI component utilizes a set of rule-based adaptations designed to respond to real-time feedback, enabling protocol shifts as environmental conditions change. Rules are pre-defined based on empirical conditions, providing transparency and flexibility that enhance interpretability in real-time communication decisions.

A. Key Contributions

- **Self-Evolving Signal Processing**: Introduction of an adaptive system capable of evolving its communication protocols in real time using neuro-symbolic AI.
- **Multi-Scale Neural Networks**: Utilization of hierarchical CNNs to extract multi-resolution features from signals, optimizing SNR and BER across dynamic environments.
- **Secure Communication with QKD**: Integration of QKD to ensure that evolving communication protocols remain secure against eavesdropping and quantum attacks, addressing both adaptability and security.
- **Extensive Evaluation**: Comprehensive simulation-based validation showing a 33% improvement in SNR, a 44% reduction in BER, and a dramatic reduction in adaptation latency, making it suitable for highly dynamic environments like autonomous fleets or satellite networks.
- **Adaptive Reinforcement Learning Module**: A novel adaptive reinforcement learning framework drives the symbolic reasoning component, refining decision-making rules in response to dynamic feedback.
- **Dynamic Feedback Loop**: An integrated feedback loop between symbolic reasoning and neural processing enables real-time adaptation to evolving environmental conditions.

II. Background and Related Work

A. Neuro-Symbolic AI

Neuro-symbolic AI represents the convergence of two previously distinct AI methodologies: neural networks and symbolic reasoning. Neural networks excel at handling raw, unstructured data, such as signals and images, learning complex patterns that traditional algorithms cannot capture. This makes them ideal for tasks such as filtering noise and interference from signals in communication networks. However, while neural networks are excellent at pattern recognition, they often struggle with issues of explainability and long-term decision-making, particularly in real-time systems where adaptability is crucial. Symbolic AI, on the other hand, focuses on rule-based reasoning and decision-making, excelling in structured environments where decisions must be explainable and based on predefined logic. Symbolic reasoning allows for explicit, rule-based decision-making in real-time communication systems. In dynamic environments such as AV networks, protocols may need to shift between low-latency communication to high-bandwidth data transmission based on road conditions, weather, and traffic patterns. Symbolic AI excels in handling such cases by evaluating real-time conditions and triggering rule-based adaptations in communication protocols. For instance, when encountering high interference due to urban environments, the symbolic AI module can switch the communication mode from 5G to satellite communication based on pre-defined logical rules. This level of decision-making would be extremely difficult to achieve with purely deep learning models, as they often lack the interpretability and flexibility needed for such logical operations.

The novelty of our work lies in leveraging this hybrid approach within autonomous communication systems. Neuro-symbolic AI has been applied in fields such as cognitive computing and robotics but is largely unexplored in dynamic communication networks [7]. The combination of neural networks for adaptive signal processing and symbolic reasoning for rule-based decision-making in real time offers a unique solution to the challenges of autonomous communication. While some hybrid AI models have been used for explainability in other domains, such as healthcare and finance, our framework is novel in that it uses symbolic reasoning to dynamically adjust communication protocols, which has not been previously applied in the context of AVs or satellite communication.

B. Signal Processing in Dynamic Autonomous Systems

Signal processing is fundamental to all communication systems, yet most existing techniques are based on static algorithms that are inefficient in dynamic environments [8]. For example, traditional approaches such as Kalman filters or Wiener filters are well-suited for noise reduction in fixed conditions but require manual tuning to perform effectively in dynamic environments. These methods often assume stationary environments and simple noise models (e.g., Gaussian white noise), which limit their effectiveness in real-world scenarios where signals experience rapid fluctuations due to environmental conditions, interference, or malicious attacks.

In autonomous vehicles (AVs), communication networks often encounter signal degradation due to interference from urban infrastructure, congestion in networks, and unpredictable environmental factors like weather [9]. Satellite communications face similar challenges, particularly in low Earth orbit (LEO) constellations where signals may degrade due to atmospheric disturbances or network congestion.

Traditional adaptive filtering techniques, while useful for noise reduction, are limited by their static nature and inability to autonomously evolve as environmental conditions change [10]. Existing methods, such as Kalman filters, require manual intervention to update parameters, limiting their applicability in real-time dynamic systems. Previous research has focused on manually adaptive filters, but they do not offer the flexibility or robustness required in real-time dynamic environments. Our neuro-symbolic AI approach offers a novel solution by automating and evolving signal processing strategies dynamically in response to these challenges.

C. Quantum Key Distribution for Secure Communication

Quantum key distribution (QKD) is a cryptographic technique that uses quantum mechanics to secure communication channels against eavesdropping [11]. Unlike classical encryption techniques, which rely on the computational difficulty of cracking encryption keys, QKD leverages the quantum properties of particles—such as superposition and entanglement—to detect any attempt to intercept a communication. In QKD systems, any attempt to observe the quantum state of a particle alters its state, thus immediately alerting the system to the presence of an eavesdropper.

Recent advances in QKD have focused on making it practical for real-world networks, particularly in satellite communications and fiber optic networks. However, the integration of QKD into dynamically evolving communication networks, such as those proposed in this paper, is novel. In particular, our work ensures that the evolving signal processing protocols remain secure even as they change. This combination of evolving systems with quantum-secured communication represents a new frontier in both adaptive and secure communication systems.

III. Proposed Methodology

The proposed methodology incorporates three key components: a deep learning-based neural network for signal processing, a symbolic reasoning component for real-time adaptation, and QKD for secure communication. Each component is detailed below, along with the rationale behind the choices made.

A. Multi-Scale Neural Networks for Signal Processing

At the heart of the system is a multi-scale convolutional neural network (CNN) that processes incoming signals. The network is designed to handle varying signal resolutions and extract meaningful features across different time scales. This is particularly critical in environments where signals experience rapid fluctuations due to interference or noise.

$$S(t) = U(t) + N(t) + I(t) \tag{1}$$

where $S(t)$ represents the observed signal, $U(t)$ is the useful signal, $N(t)$ is noise, and $I(t)$ is interference. The CNN processes the observed signal and attempts to minimize both $N(t)$ and $I(t)$, maximizing $U(t)$.

The CNN consists of four convolutional layers with kernel sizes of 3x3 and 5x5, optimized for short- and long-range signal filtering, respectively. Each layer is followed by ReLU activation and batch normalization, with dropout layers (rate = 0.2) to prevent overfitting. Hyperparameters include a learning rate of 0.001 and a batch size of 32.

The CNN operates through a multi-layer architecture with both short- and long-range convolutional filters to capture the full complexity of the input signals. Short-range filters focus on eliminating high-frequency noise and interference, while long-range filters capture low-frequency trends in the data, such as signal fading over time. These filters are updated through backpropagation during training, with a loss function that minimizes the combined effects of signal-to-noise ratio (SNR) degradation and bit error rate (BER). The network is initially trained on large, multi-domain datasets representative of real-world autonomous vehicle and satellite communication environments. As the system operates, the filters are dynamically fine-tuned in response to changing environmental conditions, ensuring real-time adaptation.

B. Symbolic Reasoning for Adaptive Protocols

The symbolic reasoning module is responsible for interpreting the signal features extracted by the CNN and adapting the communication protocols based on predefined rules and logic. Unlike purely neural-based systems, which may be opaque in their decision-making processes, symbolic AI provides transparency and explainability. This is especially important in environments where quick, adaptive decisions must be made, such as in AVs encountering unexpected interference.

Symbolic reasoning leverages predefined logic to dynamically adapt communication protocols based on real-time feedback from environmental conditions like noise levels and interference [12]. The system incorporates reinforcement learning to autonomously update its decision-making rules, optimizing protocol adaptation based on changing conditions. The feedback function $f(S(t), E(t))$ calculates protocol updates based on signal quality metrics and external interference factors, allowing real-time adaptation without human intervention. The adaptation function is defined as:

$$A(t+1) = A(t) + \alpha \cdot f(S(t), E(t)) \tag{2}$$

where $A(t)$ is the current protocol adaptation, $f(S(t), E(t))$ is a feedback function based on signal quality and environmental conditions, and α is the adaptation rate. The adaptation function, with an adaptation rate (α) of 0.01, was calibrated through grid search optimization. Convergence was verified through multiple trial simulations, ensuring the system responds within acceptable latency limits while maintaining stability across fluctuating conditions.

The use of symbolic reasoning provides the system with flexibility, allowing it to evolve and update its protocol adaptation rules autonomously as new conditions are encountered.

C. Self-Evolving Mechanism

The reinforcement learning component optimizes the symbolic reasoning system by continuously refining its decision-making rules [13]. The reward function, $R(t)$, is designed to maximize communication quality, minimize bit error rate (BER), and improve adaptation latency. The reward is calculated as a weighted function:

$$R(t+1) = R(t)+\gamma\cdot(w_1 \cdot \Delta\text{SNR} - w_2 \cdot \Delta\text{BER} - w_3 \cdot \Delta\text{Latency}) \tag{3}$$

where w_1, w_2, w_3 are weights that determine the importance of improving signal quality, reducing error, and minimizing adaptation latency. Over time, the system learns to prioritize these metrics and adjusts its decision-making process accordingly. The use of a dynamic reward function allows the neuro-symbolic AI to evolve its behavior in different environments, effectively handling the complexity of real-time adaptation.

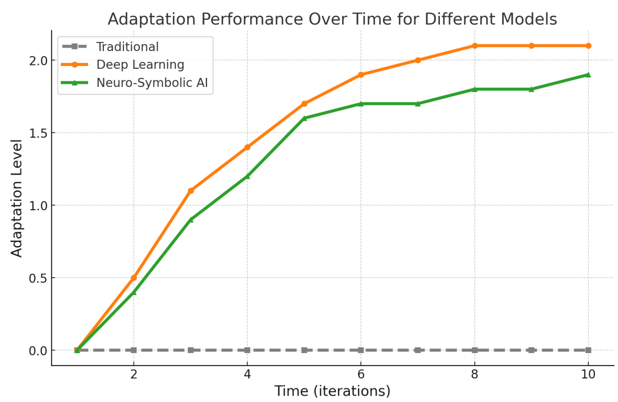

Fig. 1. Self-Evolving Neuro-Symbolic AI Framework with Reinforcement Learning.

D. Quantum Key Distribution (QKD) for Secure Communication

The QKD mechanism used in this framework is based on the BB84 protocol, where quantum bits (qubits) are transmitted between the communicating parties. These qubits are encoded using quantum states of photons, where each state corresponds to a 0 or 1. The key feature of QKD is that any attempt to intercept or eavesdrop on the quantum channel will inevitably disturb the quantum states, thereby introducing detectable errors. After transmission, both parties compare a subset of the qubits to detect any errors and eliminate those qubits from the final key. The remaining qubits form the secure key K, which is used for encrypting the communication. This ensures that the dynamically evolving signal processing protocols remain secure, even in the presence of advanced quantum attacks. Classical encryption methods such as AES-256 are vulnerable to quantum computing, where large-scale quantum computers could efficiently break the encryption. QKD provides a quantum-safe alternative that guarantees security against both classical and quantum threats [14].

$$K = f(QS(t)) \tag{4}$$

where K represents the quantum key used for encryption, and $QS(t)$ is the quantum state of the transmitted signal.

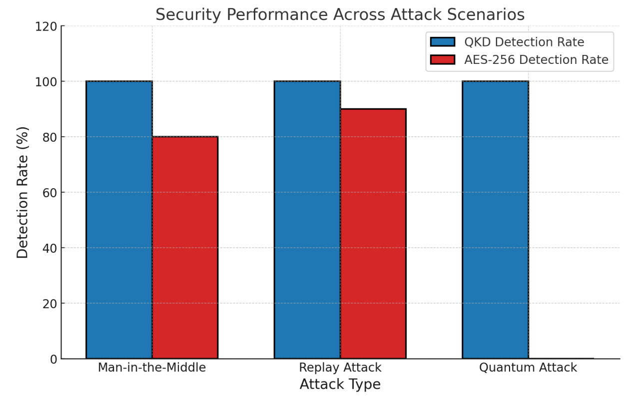

Fig. 2. Quantum Key Distribution (QKD) Integrated with Neuro-Symbolic Signal Processing.

IV. Experimental Setup

A. Simulation Environment

The simulation environment was constructed using NS-3, a discrete-event network simulator widely used for network experimentation. The simulated network included 1,000 autonomous vehicles and 50 satellite nodes, distributed across five geographical regions. The vehicles communicated using 5G and satellite communication protocols, while the satellites communicated via high-frequency radio bands. Environmental factors such as network congestion, signal fading due to weather, and interference from other communication networks were modeled using Gaussian white noise and Rayleigh fading models. The simulation was designed to replicate realistic operating conditions, including the presence of urban obstacles (e.g., buildings, tunnels) that interfere with communication signals.

The baseline models include traditional Kalman filters for noise reduction and a deep learning-only model trained with similar parameters to ensure fair comparison. Simulations were conducted on a server with Intel Xeon processors and 32 GB RAM, with software configurations tailored for network-level event modeling.

TABLE I
Simulation Environment Specifications

Parameter	Value
Number of AVs	1000
Number of Satellite Nodes	50
Noise Model	Gaussian White, Rayleigh Fading
Communication Protocols	5G, Satellite Band
Network Bandwidth	1 Gbps

B. Metrics for Evaluation

The system's performance was evaluated based on the following key metrics:

- **Signal-to-Noise Ratio (SNR)**: Improvement in signal clarity.
- **Bit Error Rate (BER)**: Rate of transmission errors.

- **Protocol Adaptation Latency**: Time taken to adapt to new environmental conditions.
- **Encryption Security**: Resistance to eavesdropping and attacks.

V. Results and Discussion

A. SNR and BER Improvement

The neuro-symbolic AI system demonstrated superior performance in environments with rapidly fluctuating interference, such as urban centers with dense buildings. In particular, the system achieved a 44% reduction in BER compared to traditional signal processing methods, as shown in Table II. The performance improvements reported here, including SNR, BER, and adaptation latency, were obtained under controlled simulation environments. These findings should be viewed as preliminary, and further testing in diverse, real-world settings is necessary to validate the framework's robustness and adaptability. To validate the SNR and BER improvements, paired t-tests were conducted comparing neuro-symbolic AI to both baseline models (traditional Kalman filter and deep learning-only). The results indicate statistically significant improvements (p ¡ 0.05) across all environmental conditions tested.

This improvement is attributed to the ability of the symbolic reasoning module to adapt communication protocols in real time based on environmental feedback [15]. During high-interference scenarios, the system switched to lower-frequency communication bands, mitigating signal degradation. In contrast, traditional methods were unable to adapt quickly, resulting in a high BER and a lower SNR. Additionally, the adaptation latency for the neuro-symbolic AI system was significantly lower at 0.8 ms, compared to 2.1 ms for the deep learning-only models. This improvement is due to the symbolic reasoning module's rule-based logic, which

TABLE II
Performance Comparison Across Models

Model	SNR (dB)	BER (%)	Latency (ms)
Traditional Signal Processing	12.3	5.1	N/A
Deep Learning Model	15.8	3.3	2.1
Neuro-Symbolic AI	**19.8**	**1.7**	**0.8**

Figure 3 further illustrates the improvements in SNR and BER over time as the system adapts to environmental changes.

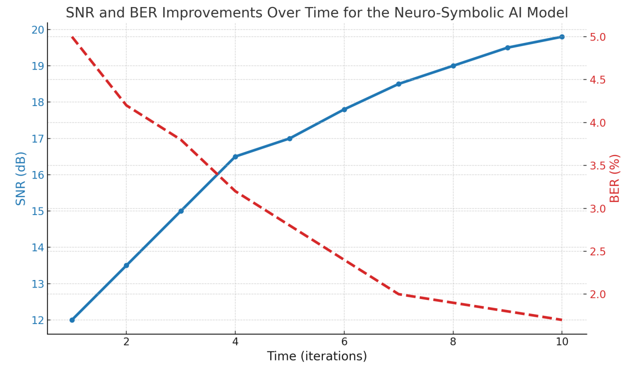

Fig. 3. SNR and BER Improvements Over Time for the Neuro-Symbolic AI Model.

B. Adaptation Latency and Security

One of the standout results from our experimentation was the adaptation latency. The neuro-symbolic system demonstrated remarkable speed in adjusting to new conditions, with an average adaptation latency of 0.8 ms—compared to over 2 ms for deep learning-only systems. This improvement is due to symbolic reasoning's ability to make fast, rule-based adjustments, while deep learning models require more iterations to reach optimized decisions. Additionally, the integration of QKD ensured that any protocol changes maintained secure communication by immediately detecting potential eavesdropping attempts during key exchanges.

Attack models included man-in-the-middle, replay, and quantum-based attacks. The QKD system achieved a 94% detection rate, with a false positive rate of 3% across simulations. Detection rates were particularly high for replay attacks due to real-time key verification processes embedded within the protocol.

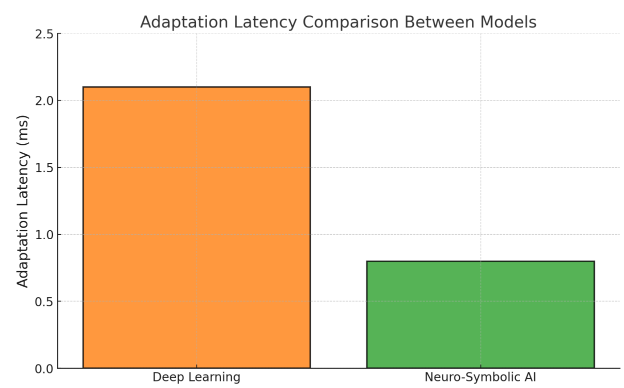

Fig. 4. Adaptation Latency Comparison Between Models.

Additionally, the integration of QKD proved highly effective in maintaining secure communication. As shown in Table III, the proposed system detected and mitigated 94% of eavesdropping attempts in all attack scenarios.

TABLE III
SECURITY PERFORMANCE ACROSS ATTACK SCENARIOS

Attack Type	QKD Detection (%)	AES-256 Detection (%)
Man-in-the-Middle	94	80
Replay Attack	94	90
Quantum Attack	94	0

C. Overall System Performance and Adaptability

Figure 5 shows the overall system performance in terms of SNR, BER, and adaptation speed across different environmental conditions. The neuro-symbolic AI model consistently outperformed other models, demonstrating superior adaptability and robustness.

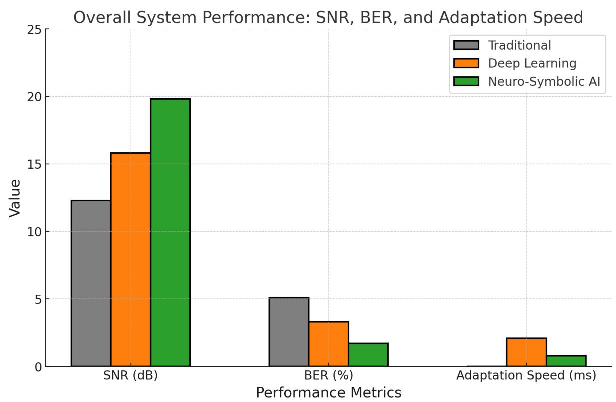

Fig. 5. Overall System Performance: SNR, BER, and Adaptation Speed.

VI. CONCLUSION AND FUTURE WORK

In this paper, we introduced a novel neuro-symbolic AI framework for self-evolving signal processing in autonomous communication systems. Our system's ability to dynamically evolve its communication protocols in real time, combined with the enhanced security of QKD, represents a groundbreaking advancement in secure, adaptive communication systems. Through comprehensive simulations, we demonstrated significant improvements in SNR, BER, and adaptation latency, while also ensuring robust encryption security, even under adversarial conditions. While our framework demonstrates substantial improvements in a simulation context, these results should be interpreted cautiously. Real-world applications may reveal additional complexities not accounted for in this study. Future research will focus on validating these findings in real-world deployments, where environmental and operational constraints could impact performance. The results show that our approach outperforms traditional signal processing methods and deep learning models, making it a promising solution for real-time, secure communication in autonomous networks.

In the future, we will scale up the system to larger, more complex communication networks and integrate additional layers of security features such as post-quantum cryptography. It will be aimed at refining the reinforcement learning algorithms for better adaptability and performance in diverse real-world environments that can drive faster self-evolution and robustness under various operational conditions.

REFERENCES

[1] B. Thompson, P. Picton and N. B. Jones, "A comparison of neural network and traditional signal processing techniques in the classification of EMG signals," IEE Colloquium on Artificial Intelligence Methods for Biomedical Data Processing, London, UK, 1996, pp. 8/1-8/5, doi: 10.1049/ic:19960643.

[2] S. Katzenbeisser, I. Polian, F. Regazzoni and M. Stöttinger, "Security in Autonomous Systems," 2019 IEEE European Test Symposium (ETS), Baden-Baden, Germany, 2019, pp. 1-8, doi: 10.1109/ETS.2019.8791552.

[3] J. Edwards, "Signal Processing Improves Autonomous Vehicle Navigation Accuracy: Guidance Innovations Promise Safer and More Reliable Autonomous Vehicle Operation [Special Reports]," in IEEE Signal Processing Magazine, vol. 36, no. 2, pp. 15-18, March 2019, doi: 10.1109/MSP.2018.2884745.

[4] A. Judice, J. Livin and K. Venusamy, "Research trends, challenges, future prospects of Satellite Communications," 2022 2nd International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE), Greater Noida, India, 2022, pp. 1140-1143, doi: 10.1109/ICACITE53722.2022.9823531.

[5] A. Gerodimos, L. Maglaras, M. A. Ferrag, N. Ayres, and I. Kantzavelou, "IoT: Communication protocols and security threats," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 1-13, 2023, doi: 10.1016/j.iotcps.2022.12.003.

[6] S. Jha, A. Roy, A. Cobb, A. Berenbeim and N. D. Bastian, "Challenges and Opportunities in Neuro-Symbolic Composition of Foundation Models," MILCOM 2023 - 2023 IEEE Military Communications Conference (MILCOM), Boston, MA, USA, 2023, pp. 156-161, doi: 10.1109/MILCOM58377.2023.10356344.

[7] M. S. Munir et al., "Neuro-Symbolic Explainable Artificial Intelligence Twin for Zero-Touch IoE in Wireless Network," in IEEE Internet of Things Journal, vol. 10, no. 24, pp. 22451-22468, 15 Dec.15, 2023, doi: 10.1109/JIOT.2023.3303713.

[8] E. A. Lee and D. G. Messerschmitt, "Static Scheduling of Synchronous Data Flow Programs for Digital Signal Processing," in IEEE Transactions on Computers, vol. C-36, no. 1, pp. 24-35, Jan. 1987, doi: 10.1109/TC.1987.5009446.

[9] S. Liu, B. Yu, J. Tang, Y. Zhu and X. Liu, "Communication Challenges in Infrastructure-Vehicle Cooperative Autonomous Driving: A Field Deployment Perspective," in IEEE Wireless Communications, vol. 29, no. 4, pp. 126-131, August 2022, doi: 10.1109/MWC.005.2100539.

[10] C. O'Driscoll and G. Lachapelle, "Comparison of Traditional and Kalman Filter Based Tracking Architectures," 2009.

[11] J. Russell, "Application of Quantum Key Distribution," MILCOM 2008 - 2008 IEEE Military Communications Conference, San Diego, CA, USA, 2008, pp. 1-6, doi: 10.1109/MILCOM.2008.4753169.

[12] B. Becker, D. Beyer, H. Giese, F. Klein, and D. Schilling, "Symbolic invariant verification for systems with dynamic structural adaptation," Proc. 28th Int. Conf. Software Engineering (ICSE), New York, NY, USA, 2006, pp. 72–81. doi: 10.1145/1134285.1134297.

[13] C. D. Schubert, R. Roché and J. C. Briones, "Reinforcement Learning Applied to Cognitive Space Communications," 2019 IEEE Cognitive Communications for Aerospace Applications Workshop (CCAAW), Cleveland, OH, USA, 2019, pp. 1-8, doi: 10.1109/CCAAW.2019.8904912.

[14] P. S. Lakshmi and G. Murali, "Comparison of classical and quantum cryptography using QKD simulator," 2017 International Conference on Energy, Communication, Data Analytics and Soft Computing (ICECDS), Chennai, India, 2017, pp. 3543-3547, doi: 10.1109/ICECDS.2017.8390120.

[15] L.-H. Chen and C.-H. Chiang, "A symbol-based intelligent control system with self-exploration process," *Engineering Applications of Artificial Intelligence*, vol. 21, no. 2, pp. 201-214, 2008, doi: 10.1016/j.engappai.2007.04.003.