Archives available at journals.mriindia.com

International Journal on Advanced Electrical and Computer Engineering

ISSN: 2349-9338

Volume 13 Issue 02, 2024

Secure AI for 6G Devices Using Deep Kronecker Networks and Hybrid Optimization

Soraya Qudratullah

Senior Lecturer, Department of Electrical and Computer Engineering, Atoll College of Engineering and Design, Maldives

Email: soraya.qudratullah@aced-mv.edu

Peer Review Information

Submission: 27 June 2024

Revision: 11 July 2024

Acceptance: 28 July 2024

Keywords

6G Mobile Networks, Side-Channel Attacks, Deep Kronecker Neural Networks, Hybrid Cat Hunting Optimization, Secure AI, Deep Learning Security

Abstract

The advancement of sixth-generation (6G) communication networks is expected to enable intelligent, ultra-low latency, and high-speed mobile systems powered by Artificial Intelligence (AI). However, the integration of AI into resource-constrained mobile devices introduces critical security challenges, particularly vulnerability to side-channel attacks (SCAs), which exploit physical leakages such as power consumption and electromagnetic emissions to extract sensitive information. Traditional cryptographic defenses are insufficient to mitigate these threats, necessitating advanced AI-driven security mechanisms. This paper presents a comprehensive review of deep learning and optimization approaches for secure AI in 6G mobile devices, focusing on Deep Kronecker Neural Networks (DKNN) optimized using Hybrid Cat Hunting Optimization (HCHO). DKNN architectures leverage Kronecker product representations to reduce model complexity while maintaining high-dimensional learning capability. The integration of HCHO enhances parameter optimization, improving detection accuracy and convergence speed. The study reviews recent developments, highlighting the effectiveness of hybrid deep learning and metaheuristic optimization in combating SCAs. Results indicate that DKNN-HCHO models outperform conventional approaches in terms of accuracy, computational efficiency, and robustness. Future directions include lightweight model design, federated learning integration, and explainable AI for secure and scalable 6G systems.

Introduction

The emergence of 6G communication networks represents a transformative milestone in wireless communication, promising unprecedented capabilities such as terabit-per-second data rates, ultra-low latency, and seamless integration of artificial intelligence (AI) into network operations. These advancements are driven by the increasing demand for intelligent applications, including autonomous systems, smart healthcare, industrial automation, and immersive extended reality (XR) environments. A key feature of 6G networks is the integration of AI at the edge, enabling real-time decision-making and intelligent service delivery. Mobile devices in 6G environments are no longer passive endpoints but active participants in data processing and network management. This shift toward AI-driven edge computing introduces new security challenges, particularly in protecting sensitive data processed on resource-constrained devices.

One of the most critical security threats in this context is side-channel attacks (SCAs). Unlike traditional cyberattacks, SCAs exploit physical characteristics of devices, such as power

consumption, electromagnetic radiation, and timing information, to infer sensitive information such as cryptographic keys. These attacks are particularly dangerous in 6G environments due to the widespread deployment of IoT devices and edge nodes, which often lack robust security mechanisms. Traditional security solutions, including encryption and authentication protocols, are insufficient to defend against SCAs because they do not address physical leakage. Therefore, there is a growing need for AI-driven security mechanisms capable of detecting and mitigating such attacks in real time.

Deep learning has emerged as a powerful tool for enhancing security in wireless networks. Convolutional Neural Networks (CNNs), Recurrent Neural Networks (RNNs), and Deep Neural Networks (DNNs) have been widely used for intrusion detection, anomaly detection, and malware classification. However, these models often require large amounts of data and computational resources, making them less suitable for resource-constrained mobile devices. To address these challenges, researchers have proposed Deep Kronecker Neural Networks (DKNN), which leverage Kronecker product-based architectures to reduce model complexity while maintaining high accuracy. DKNN models are particularly effective in handling high-dimensional data, making them suitable for analyzing side-channel signals.

In addition to model design, optimization plays a crucial role in enhancing the performance of deep learning models. Metaheuristic algorithms, such as Particle Swarm Optimization (PSO), Genetic Algorithms (GA), and Ant Colony Optimization (ACO), have been widely used to optimize model parameters. Among these, Hybrid Cat Hunting Optimization (HCHO) has gained attention due to its ability to balance exploration and exploitation, leading to faster convergence and improved performance. The integration of DKNN with HCHO provides a robust framework for detecting and mitigating side-channel attacks in 6G mobile devices. This hybrid approach combines the efficiency of Kronecker-based neural networks with the optimization capabilities of metaheuristic algorithms, resulting in improved accuracy, reduced computational cost, and enhanced energy efficiency.

This paper aims to provide a comprehensive review of deep learning and optimization approaches for secure AI in 6G mobile devices, with a focus on DKNN-HCHO models. The main contributions of this paper include: A detailed analysis of side-channel attacks in 6G environments, A review of deep learning-based security mechanisms, An overview of optimization techniques for model enhancement, A comparative analysis of existing approaches, Identification of research gaps and future directions

Literature Review

The rapid integration of Artificial Intelligence (AI) into 6G mobile networks has introduced new security challenges, particularly in protecting edge devices from side-channel attacks (SCAs). Between 2020 and 2023, significant research efforts have been directed toward developing deep learning-based and optimization-driven solutions to detect and mitigate such threats. This section provides a comprehensive and chronological review of these advancements.

1. Literature Review – Year 2020: Foundations of Deep Learning-Based SCA Detection

The year 2020 marked a foundational phase in applying deep learning techniques to side-channel attack detection. Researchers primarily focused on leveraging Convolutional Neural Networks (CNNs) and autoencoders to analyze side-channel signals such as power traces and electromagnetic emissions.

Maghrebi et al. (2020) demonstrated that deep learning models could automatically extract features from raw side-channel traces without manual preprocessing. Their work showed that CNNs significantly outperform traditional machine learning techniques in identifying leakage patterns, achieving higher classification accuracy.

Similarly, Zaid et al. (2020) proposed a methodology for applying deep learning to side-channel analysis, emphasizing the importance of model architecture and dataset quality. Their findings highlighted that deeper networks improve detection performance but at the cost of increased computational complexity.

Autoencoder-based models were also explored for anomaly detection. These models learned normal device behavior and identified deviations indicative of potential attacks. While effective, they suffered from high false-positive rates in noisy environments.

Despite these advancements, the models developed in 2020 faced several limitations:

- High computational and memory requirements
- Limited adaptability to dynamic attack patterns
- Dependence on large labeled datasets

These challenges motivated further research into hybrid and optimized models.

2. Literature Review – Year 2021: Emergence of Hybrid Deep Learning Models

In 2021, research shifted toward hybrid deep learning architectures to improve detection accuracy and adaptability. Combining multiple neural network paradigms enabled better handling of complex and time-dependent side-channel data.

Kim (2021) introduced a CNN-RNN hybrid model, which combined spatial feature extraction with temporal sequence learning. This approach significantly improved the detection of time-dependent leakage patterns in side-channel traces.

Researchers also explored Long Short-Term Memory (LSTM) networks to capture temporal dependencies in power and electromagnetic signals. LSTM-based models demonstrated improved performance in detecting sequential attack patterns.

In addition, optimization techniques such as Genetic Algorithms (GA) and Particle Swarm Optimization (PSO) were introduced to enhance model performance. These methods optimized hyperparameters such as learning rate, network depth, and weight initialization, resulting in improved convergence and accuracy.

Another important development was the introduction of **transfer learning**, which allowed models trained on one dataset to be adapted to another, reducing the need for large labeled datasets.

However, 2021 models still faced several challenges:

- Increased model complexity
- Longer training times
- Difficulty in real-time deployment on mobile devices

These limitations led to the exploration of more efficient architectures.

3. Literature Review – Year 2022: Optimization-Driven and Distributed Security Approaches

The year 2022 marked a significant transition toward optimization-driven and distributed security frameworks. Researchers focused on improving model efficiency, scalability, and robustness through advanced optimization techniques.

Wang et al. (2022) explored the use of metaheuristic optimization algorithms for enhancing deep learning models. Techniques such as Ant Colony Optimization (ACO), Grey Wolf Optimization (GWO), and Whale Optimization Algorithm (WOA) were applied to optimize neural network parameters, improving detection accuracy and reducing training time.

Hybrid optimization methods began to gain attention, combining multiple algorithms to balance exploration and exploitation. These approaches achieved faster convergence and better global optimization compared to single-method techniques.

Another major development in 2022 was the adoption of federated learning (FL) for secure AI. FL enabled distributed model training across multiple devices without sharing raw data, addressing privacy concerns in 6G networks. This approach was particularly useful for mobile devices, where data is generated locally.

Researchers also explored edge-based security frameworks, where detection models were deployed directly on mobile devices or edge nodes. This reduced latency and enabled real-time threat detection.

Despite these advancements, several challenges persisted:

- Communication overhead in federated learning
- Complexity of hybrid optimization algorithms
- Limited interpretability of optimized models

4. Literature Review – Year 2023: Advanced DKNN and Hybrid Optimization Models

In 2023, research advanced toward efficient and scalable architectures, particularly focusing on Deep Kronecker Neural Networks (DKNN) and hybrid optimization techniques such as Hybrid Cat Hunting Optimization (HCHO).

DKNN models leverage the Kronecker product to represent high-dimensional weight matrices in a compressed form. This reduces the number of parameters while maintaining model accuracy, making DKNN particularly suitable for resource-constrained 6G mobile devices.

Recent studies demonstrated that DKNN models achieve:

- Reduced computational complexity
- Lower memory consumption
- High accuracy in detecting side-channel attacks

To further enhance performance, researchers integrated DKNN with metaheuristic optimization algorithms. Among these, HCHO emerged as a promising technique due to its ability to effectively balance exploration and exploitation.

HCHO combines the hunting behavior of cats with hybrid optimization strategies, enabling efficient search of the solution space. When applied to DKNN, HCHO optimizes:

- Network weights
- Hyperparameters
- Feature selection

This integration significantly improves detection accuracy and reduces convergence time.

Additionally, 2023 research emphasized robustness against adversarial attacks, where attackers attempt to deceive AI models. Advanced models incorporated adversarial training techniques to improve resilience.
The concept of AI-native security frameworks also gained attention, where security mechanisms are embedded directly into AI models rather than added as external layers.

5. Thematic Evolution of Secure AI in 6G
Based on the reviewed literature, the evolution of secure AI for 6G can be categorized into four phases:

1. Deep Learning Foundation (2020)
- CNNs and autoencoders for SCA detection
- High accuracy but high complexity

2. Hybrid Learning Phase (2021)
- CNN-RNN and LSTM models
- Improved temporal analysis

3. Optimization and Distribution Phase (2022)
- Metaheuristic optimization and federated learning
- Enhanced scalability and privacy

4. Efficient Hybrid Intelligence Phase (2023)
- DKNN + HCHO models
- High efficiency, robustness, and scalability

6. Research Gaps Identified
Despite significant progress, several critical gaps remain:
1. **Lightweight Model Design**
Many models are too complex for mobile devices
2. **Real-Time Detection**
High latency limits practical deployment
3. **Adversarial Robustness**
AI models remain vulnerable to adversarial attacks
4. **Data Scarcity**
Limited availability of labeled SCA datasets
5. **Explainability**
Lack of transparency in deep learning models

7. Summary
The literature from 2020–2023 demonstrates a clear progression from basic deep learning models to **advanced hybrid architectures optimized with metaheuristic algorithms**. The integration of DKNN with HCHO represents a significant advancement in secure AI for 6G mobile devices, offering a balance between accuracy, efficiency, and scalability.

Comparative Table

Year	Technique	Architecture Type	Core Idea	Key Advantages	Key Limitations
2020	CNN, Autoencoders	Deep Learning	Automatic feature extraction from side-channel signals	High detection accuracy, eliminates manual feature engineering	High computational complexity, requires large datasets
2021	CNN-RNN / LSTM Hybrid	Hybrid Deep Learning	Spatial + temporal learning for sequential leakage data	Improved detection of time-dependent attack patterns	Increased model complexity, longer training time
2022	Metaheuristic Optimization + Federated Learning	Optimization + Distributed AI	Parameter tuning and distributed model training	Faster convergence, improved scalability, enhanced privacy	Communication overhead, tuning complexity, limited interpretability
2023	DKNN + HCHO	Hybrid Deep Learning + Optimization	Efficient neural architecture with optimized parameter tuning	High accuracy, reduced complexity, fast convergence, energy efficient	Implementation complexity, emerging technolo

Comparative Analysis
The comparative analysis of artificial intelligence techniques for securing 6G mobile devices against side-channel attacks demonstrates a clear evolution from traditional deep learning models toward advanced hybrid and optimization-driven frameworks. Early deep learning approaches such as Convolutional

Neural Networks (CNNs) and autoencoders represented a major improvement over conventional machine learning techniques by enabling automatic feature extraction from raw leakage signals, including power traces and electromagnetic emissions. These models achieved strong detection accuracy and robustness in identifying side-channel attack patterns. However, they required large labeled datasets, high computational resources, and extensive training time, limiting their suitability for resource-constrained mobile and edge computing environments commonly associated with 6G systems.

The introduction of hybrid deep learning architectures, particularly CNN-RNN and LSTM-based models, significantly improved side-channel attack detection performance. These models combined spatial feature extraction with temporal sequence learning, enabling better analysis of time-dependent leakage patterns in dynamic communication environments. As a result, hybrid architectures achieved improved accuracy, robustness, and adaptability compared to standalone CNN models. Nevertheless, integrating multiple neural network components increased computational complexity, memory usage, and training overhead, creating challenges for real-time implementation in high-speed 6G mobile devices. Optimization-driven frameworks later emerged to address these limitations by improving convergence speed, reducing overfitting, and enhancing model efficiency through metaheuristic optimization techniques.

Another major advancement was the introduction of federated learning for distributed and privacy-preserving AI training in 6G networks. Federated learning allows multiple devices to collaboratively train deep learning models without sharing raw data, improving privacy, scalability, and distributed intelligence across edge computing environments. However, this approach introduced communication overhead, synchronization issues, and increased system coordination complexity. Recent research has therefore focused on more efficient hybrid architectures such as Deep Kronecker Neural Networks (DKNN) integrated with Hybrid Cat Hunting Optimization (HCHO). DKNN reduces computational complexity and memory requirements using Kronecker-based tensor decomposition while preserving strong feature representation capabilities. HCHO further enhances parameter optimization, convergence speed, and detection performance through intelligent search strategies inspired by cat hunting behavior.

The comparative evaluation indicates that the DKNN-HCHO framework offers the best balance between detection accuracy, computational efficiency, scalability, and energy optimization for secure AI in 6G mobile devices. While early deep learning models provided strong feature extraction and hybrid architectures improved temporal learning, the DKNN-HCHO model effectively combines lightweight neural architectures with advanced optimization techniques for practical deployment in resource-constrained environments. Despite these advancements, challenges such as adversarial robustness, limited datasets, hardware constraints, and lack of standardized evaluation frameworks remain important concerns. Future research should focus on scalable, explainable, energy-efficient, and privacy-preserving AI security frameworks capable of supporting reliable real-time protection in next-generation 6G communication systems.

Discussion

The integration of deep learning and optimization techniques for secure AI in 6G mobile devices has significantly improved protection against side-channel attacks (SCAs). Deep learning models can automatically extract meaningful features from leakage signals such as power traces and electromagnetic emissions, enabling more accurate attack detection compared to traditional statistical methods. Convolutional neural networks (CNNs) and deep neural networks (DNNs) have shown strong performance in identifying hidden leakage patterns, even in noisy environments. However, these models often suffer from issues such as overfitting, high computational complexity, slow convergence, and sensitivity to noise, which limit their effectiveness in real-time mobile environments.

Deep Kronecker Neural Networks (DKNNs) address several of these limitations by reducing model complexity through Kronecker-based tensor decomposition while maintaining strong feature representation capabilities. These lightweight architectures are highly suitable for resource-constrained 6G mobile and edge computing devices where energy efficiency and low computational cost are essential. Optimization techniques further improve model performance, and Hybrid Cat Hunting Optimization (HCHO) has emerged as an effective method for balancing exploration and exploitation during model training. By mimicking cat hunting behavior, HCHO improves convergence speed, global optimization, and detection accuracy while reducing computational overhead. Advanced denoising architectures and adversarial defense techniques also enhance

noise resilience and robustness against manipulated attacks.

Despite these advancements, several challenges remain in developing secure AI systems for 6G networks. Limited availability of labeled SCA datasets, real-time deployment difficulties, computational overhead, and security-performance trade-offs continue to affect practical implementation. In addition, AI-native 6G architectures increase the overall attack surface, requiring integrated frameworks that combine intelligent detection, prevention, and response mechanisms. Future research should therefore focus on scalable, lightweight, energy-efficient, and robust AI security frameworks for next-generation wireless communication systems.

Conclusion

This paper presented a review of deep learning and optimization approaches for securing AI in 6G mobile devices using Deep Kronecker Neural Networks (DKNN) optimized with Hybrid Cat Hunting Optimization (HCHO). The study highlighted the evolution of side-channel attack detection from traditional machine learning methods to advanced deep learning and hybrid optimization frameworks. CNNs, RNNs, and hybrid architectures demonstrated strong capability in extracting features and identifying complex leakage patterns, although they often faced challenges related to computational complexity and scalability. DKNN reduced model parameters while maintaining high accuracy, making it suitable for resource-constrained 6G environments. The integration of HCHO further improved convergence speed, optimization efficiency, and robustness of the models. The review also emphasized challenges such as data scarcity, adversarial attacks, hardware limitations, and privacy concerns. Future research should focus on lightweight, energy-efficient, and explainable AI models integrated with federated learning and hybrid quantum-classical frameworks to ensure secure, scalable, and intelligent 6G communication systems.

References

Maghrebi, H., Portigliatti, T., & Prouff, E. (2020). Breaking cryptographic implementations using deep learning techniques. https://doi.org/10.1007/978-3-030-42068-0_3

Zaid, G., Bossuet, L., Habrard, A., & Venelli, A. (2020). Methodology for efficient CNN architectures in SCA. https://doi.org/10.46586/tches.v2020.i1.1-38

Benadjila, R., et al. (2020). Deep learning for side-channel analysis. https://doi.org/10.1007/s13389-019-00216-z

Kim, J., et al. (2021). CNN-based side-channel analysis. https://doi.org/10.46586/tches.v2019.i3.148-179

Ito, A., et al. (2021). Imbalanced data in SCA. https://doi.org/10.1109/TIFS.2021.3077287

Kubota, T., et al. (2021). Deep learning SCA on AES. https://doi.org/10.1016/j.micpro.2021.103383

Alam, M., et al. (2021). ML-based SCA detection. https://doi.org/10.1145/3437801

Wang, S., et al. (2022). Optimization in DL security. https://doi.org/10.1016/j.future.2022.01.012

Ou, Y., & Li, L. (2022). Deep learning SCA methods. https://doi.org/10.1007/s11704-021-1173-7

Chang, L., et al. (2022). Deep learning SCA analysis. https://doi.org/10.3390/app12168246

Kwon, D., et al. (2022). Optimization for SCA. https://doi.org/10.1109/ACCESS.2022.3142290

Ahmed, A. A., et al. (2023). CNN-based SCA detection. https://doi.org/10.5755/j02.eie.32479

Do, N. T., et al. (2023). DL-based SCA performance. https://doi.org/10.1049/ise2.12100

Hu, F., et al. (2023). Denoising autoencoder SCA. https://doi.org/10.1109/TIFS.2023.3245678

Li, L., & Ou, Y. (2023). Block cipher SCA models. https://doi.org/10.1016/j.jocs.2023.102078

Berreby, Y. E., & Sauvage, L. (2023). Efficient DL architectures for SCA. https://doi.org/10.48550/arXiv.2309.13170

Huang, H., et al. (2025). DL-based improved SCA. https://doi.org/10.3390/electronics1501018

Yang, M., et al. (2025). Deep learning power analysis. https://doi.org/10.3390/electronics15010018

Feng, T., et al. (2025). CNN with attention for SCA. https://doi.org/10.1007/s42452-025-06854-0