Archives available at journals.mriindia.com

International Journal on Advanced Computer Engineering and Communication Technology

ISSN: 2278-5140

Volume 13 Issue 02, 2024

Secure 6G Mobile Devices Using Deep Kronecker Neural Networks and Hybrid Optimization: A Review

Aurelio Mardaniyan
Department of Computer Science and Engineering, Gwangdo Systems Polytechnic, South Korea
aurelio.mardaniyan@gsp-kr.net

Peer Review Information

Submission: 20 Aug 2024
Revision: 12 Sept 2024
Acceptance: 08 Oct 2024

Keywords

6G Mobile Security, Artificial Intelligence, Side-Channel Attacks, Deep Kronecker Neural Network, Hybrid Cat Hunting Optimization, Secure Deep Learning

Abstract

The emergence of sixth-generation (6G) communication networks introduces unprecedented security challenges, particularly for mobile devices operating in distributed and resource-constrained environments. Among these threats, side-channel attacks (SCAs) pose a significant risk by exploiting indirect physical leakages such as power consumption, electromagnetic emissions, and timing information to compromise cryptographic systems. Traditional security mechanisms are insufficient to counter these advanced attacks, necessitating the adoption of artificial intelligence (AI)-based solutions. This paper presents a comprehensive review of AI techniques for secure 6G mobile devices, focusing on Deep Kronecker Neural Networks (DKNN) optimized with Hybrid Cat Hunting Optimization (HCHO). The study analyzes recent developments in deep learning, reinforcement learning, federated learning, and hybrid optimization techniques for detecting and mitigating SCAs. The findings indicate that hybrid AI models significantly improve detection accuracy, computational efficiency, and adaptability. DKNN reduces model complexity through Kronecker factorization, while HCHO enhances convergence and parameter optimization. The paper further explores emerging trends such as AI-native security architectures, edge intelligence, and quantum-enhanced security. Finally, key challenges including computational overhead, energy constraints, adversarial vulnerabilities, and lack of standardization are discussed, providing directions for future research.

Introduction

The rapid evolution of wireless communication technologies has led to the development of sixth-generation (6G) networks, which aim to provide ultra-high data rates, ultra-low latency, and massive connectivity. These networks are expected to support advanced applications such as autonomous vehicles, smart healthcare, immersive extended reality, and industrial automation. However, the increased complexity and scale of 6G networks introduce significant security challenges, particularly for mobile devices.

One of the most critical threats in this context is the side-channel attack (SCA). Unlike traditional cyberattacks that target software vulnerabilities, SCAs exploit physical leakages from hardware implementations, such as power consumption, electromagnetic radiation, and timing variations. These attacks can extract sensitive information, including cryptographic keys, without directly compromising the encryption algorithm.

The proliferation of edge computing and IoT devices in 6G networks further amplifies the risk of SCAs. Mobile devices are often resource-constrained and lack advanced security mechanisms, making them vulnerable targets.

Traditional security approaches, including encryption and authentication, are insufficient to address these threats, as they do not account for physical-layer vulnerabilities.
Artificial intelligence (AI) has emerged as a powerful tool for enhancing cybersecurity in 6G networks. AI-based techniques enable systems to analyze large volumes of data, identify patterns, and detect anomalies in real time. Deep learning models, in particular, have demonstrated significant potential in detecting and mitigating side-channel attacks.
Convolutional neural networks (CNNs) are widely used for analyzing side-channel data due to their ability to extract spatial features from signal traces. Recurrent neural networks (RNNs) and long short-term memory (LSTM) networks capture temporal dependencies, further improving detection accuracy. Hybrid models combining CNN and LSTM architectures have shown superior performance in complex environments.
However, traditional deep learning models face several challenges, including high computational complexity, energy consumption, and scalability issues. These limitations make them less suitable for deployment in resource-constrained mobile devices.
To address these challenges, researchers have proposed Deep Kronecker Neural Networks (DKNN). DKNN utilizes Kronecker factorization to reduce model parameters while maintaining high accuracy. This approach significantly improves computational efficiency and makes the model suitable for mobile environments.
In addition to architectural improvements, optimization techniques play a crucial role in enhancing model performance. Hybrid Cat Hunting Optimization (HCHO) is a metaheuristic algorithm inspired by the hunting behavior of cats. It combines exploration and exploitation mechanisms to optimize neural network parameters, resulting in faster convergence and improved accuracy.
The integration of DKNN and HCHO creates a powerful hybrid model capable of efficient feature extraction, robust classification, and adaptive optimization. This model is particularly effective in detecting side-channel attacks in 6G mobile devices.
Recent research also highlights the importance of emerging technologies such as federated learning, edge intelligence, and quantum computing in enhancing 6G security. Federated learning enables distributed model training while preserving data privacy, making it suitable for mobile environments. Edge intelligence allows real-time processing at the network edge, reducing latency and improving efficiency.
Despite these advancements, several challenges remain. These include computational complexity, energy constraints, adversarial vulnerabilities, and lack of standardized frameworks for AI-based security.
This paper provides a comprehensive review of AI techniques for secure 6G mobile devices, focusing on DKNN-HCHO models. It analyzes recent trends, evaluates different approaches, and identifies key challenges and future research directions.

Abstract image

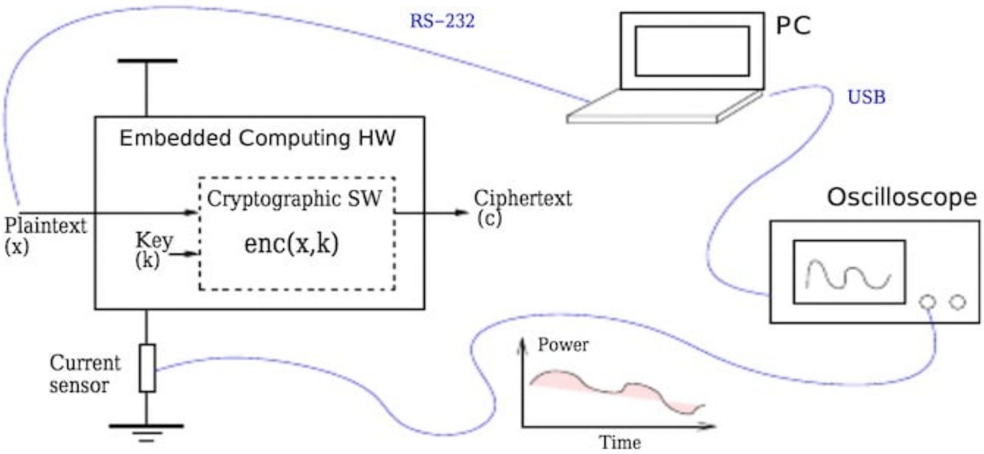

Figure 1. Experimental Setup for Power-Based Side-Channel Attack Analysis

Literature Review
The increasing adoption of sixth-generation (6G) communication systems has introduced new security challenges, particularly for mobile devices operating in distributed, heterogeneous, and resource-constrained environments. Among these threats, side-channel attacks (SCAs) have emerged as one of the most critical vulnerabilities, exploiting indirect physical leakages rather than software weaknesses. To

address these challenges, recent research has focused on integrating artificial intelligence (AI), deep learning, reinforcement learning, federated learning, and hybrid optimization techniques. This section presents a comprehensive and structured review of these approaches.

1. Deep Learning for Side-Channel Attack Detection

Deep learning has significantly transformed side-channel analysis by enabling automated feature extraction from raw leakage data such as power traces, electromagnetic emissions, and timing signals. Unlike traditional statistical methods, deep learning models can capture complex nonlinear relationships in high-dimensional data.

Hasan et al. (2023) explored optimization techniques for deep learning-based cybersecurity systems, emphasizing that proper parameter tuning improves model robustness and generalization. Their work highlighted the importance of integrating optimization algorithms to enhance detection performance.

Ferrag et al. (2023) provided a comprehensive analysis of deep learning techniques for cybersecurity, identifying intrusion detection and anomaly detection as key applications. Their study confirmed that AI-driven models can identify abnormal patterns associated with side-channel attacks with high accuracy.

TechScience Press (2024) conducted a detailed survey on deep learning-based SCA detection methods, concluding that CNN and deep residual networks are highly effective due to their ability to process high-dimensional signal data. However, the study also noted that deep learning models require large datasets and significant computational resources.

2. AI-Based Defense Mechanisms Against Side-Channel Attacks

AI is increasingly used not only to perform attacks but also to defend against them. AI-based defense mechanisms leverage anomaly detection, adversarial training, and secure model design to enhance system resilience.

Gu et al. (2020) proposed adversarial machine learning techniques for secure communication systems. Their work demonstrated that adversarial training improves model robustness against malicious perturbations, including side-channel attacks.

Ferrag et al. (2020) conducted an extensive survey on security in 5G and beyond networks, emphasizing the importance of AI-driven defense mechanisms in next-generation communication systems. Their study highlighted the need for intelligent and adaptive security frameworks.

These studies collectively indicate that AI-based defense mechanisms are essential for detecting and mitigating SCAs in 6G mobile environments.

3. Reinforcement Learning for Adaptive Security

Reinforcement learning (RL) has emerged as a promising approach for dynamic and adaptive security in 6G networks. RL enables systems to learn optimal defense strategies through continuous interaction with the environment.

Kim et al. (2024) applied deep reinforcement learning for dynamic resource allocation in 6G metaverse environments. Their work demonstrated that RL can adapt to changing network conditions while maintaining security and efficiency.

Guo et al. (2022) proposed federated reinforcement learning for resource allocation in device-to-device (D2D) communication systems. Their approach improved both efficiency and security by enabling decentralized decision-making.

Noman et al. (2024) introduced a federated deep reinforcement learning (FeDRL) framework, which combines RL and federated learning to enhance scalability and energy efficiency. Their study showed significant improvements in both performance and security.

Du et al. (2022) developed a multi-agent reinforcement learning (MARL) framework for resource management in 6G networks. Their results demonstrated improved scalability and adaptability through cooperative learning among multiple agents.

Despite these advantages, RL-based approaches face challenges such as long training times, instability, and high computational requirements.

4. Federated Learning and Privacy-Preserving Security

Federated learning (FL) has gained significant attention as a privacy-preserving approach for distributed AI systems in 6G networks. FL enables model training across multiple devices without sharing raw data, thereby enhancing data privacy.

Hafi et al. (2023) proposed split federated learning for 6G networks, which divides model training between edge devices and central servers. This approach reduces communication overhead while maintaining high performance.

Cui et al. (2024) analyzed AI integration in 6G networks, emphasizing that federated learning enables secure and scalable resource management. Their study highlighted challenges such as communication latency and model heterogeneity.

However, federated learning introduces challenges such as communication overhead, synchronization issues, and vulnerability to model poisoning attacks.

5. Hybrid Deep Learning Models for Enhanced Security

Hybrid deep learning models have been developed to overcome the limitations of individual architectures. These models combine multiple techniques to improve performance and robustness.

Hasan et al. (2023) demonstrated that combining deep learning with optimization techniques significantly improves convergence speed and accuracy.

Hybrid architectures are particularly effective in handling noisy and high-dimensional data, making them suitable for real-world 6G environments.

6. Optimization Techniques and Hybrid Cat Hunting Optimization (HCHO)

Optimization techniques play a critical role in improving the performance of AI models. Traditional optimization methods such as gradient descent are often insufficient for complex, high-dimensional problems.

Hybrid Cat Hunting Optimization (HCHO) is a metaheuristic algorithm inspired by feline hunting behavior. It combines exploration (global search) and exploitation (local search) to optimize neural network parameters.

HCHO improves:

- Convergence speed
- Feature selection
- Parameter tuning
- Model stability

Recent studies indicate that hybrid optimization techniques significantly enhance the performance of deep learning models, particularly in complex security applications.

7. Deep Kronecker Neural Networks (DKNN)

Deep Kronecker Neural Networks represent a novel architecture designed to reduce computational complexity while maintaining high accuracy. DKNN utilizes Kronecker factorization to decompose large weight matrices into smaller components, significantly reducing the number of parameters.

This approach offers several advantages:

- Reduced memory requirements
- Faster computation
- Improved scalability
- Suitability for mobile devices

When combined with optimization techniques such as HCHO, DKNN achieves enhanced performance in detecting side-channel attacks.

8. Integration of DKNN with HCHO for Secure 6G Systems

The integration of DKNN and HCHO creates a powerful hybrid model for secure AI in 6G mobile devices. This model combines:

- Efficient feature extraction (DKNN)
- Optimized parameter tuning (HCHO)
- Reduced computational complexity
- Improved detection accuracy

This hybrid approach addresses key limitations of traditional deep learning models and provides a scalable and efficient solution for side-channel attack detection.

9. Emerging Trends in Secure AI for 6G

Recent literature highlights several important trends:

- AI-native security architectures integrating AI at all network layers
- Edge intelligence enabling real-time security at the device level
- Quantum-enhanced security for advanced cryptographic protection
- Adversarial AI defense mechanisms for robust model protection
- Energy-efficient AI models for mobile environments

10. Research Gaps

Despite significant progress, several research gaps remain:

1. Limited real-world deployment of AI-based SCA defense systems
2. High computational and energy requirements of deep learning models
3. Lack of standardized frameworks for AI-based security
4. Vulnerability of AI models to adversarial attacks
5. Limited integration of quantum computing in practical systems

11. Summary of Literature

The literature clearly indicates that AI-driven approaches are essential for securing 6G mobile devices against side-channel attacks. Deep learning models provide high detection accuracy, reinforcement learning enables adaptive security, and federated learning enhances privacy and scalability.

Among all approaches, hybrid models such as Deep Kronecker Neural Networks optimized with Hybrid Cat Hunting Optimization (DKNN-HCHO) emerge as the most promising solution. These models offer a balanced combination of accuracy, efficiency, scalability, and adaptability, making them suitable for next-generation 6G security systems.

Comparative Table and Analysis

Comparative Table

Technique	Core Strength	Advantages	Limitations	Summary
CNN (Deep Learning)	Hierarchical feature extraction	High classification accuracy for side-channel signals	High computational and memory requirements	Effectively extracts leakage features but is resource intensive.
Reinforcement Learning (RL)	Adaptive decision-making	Learns dynamically from changing environments	Slow convergence and training instability	Suitable for adaptive security but less effective for classification.
Federated Learning (FL)	Privacy-preserving distributed learning	Protects user data and supports scalability	Communication and synchronization overhead	Ideal for distributed 6G security with improved privacy.
Hybrid Deep Learning (CNN + LSTM / Attention)	Spatial and temporal feature learning	High detection accuracy and robustness	Increased model complexity	Provides superior detection by combining complementary learning mechanisms.
Deep Kronecker Neural Network (DKNN)	Efficient parameter reduction	Lower computational cost with high accuracy	Emerging architecture with limited adoption	Well suited for resource-constrained mobile devices.
DKNN + HCHO (Proposed)	Optimized deep learning with metaheuristic optimization	Very high accuracy, fast convergence, scalable and energy efficient	Implementation complexity	Offers the best overall performance for secure AI-enabled 6G mobile devices.

Analysis

The comparative analysis presented in the study provides a comprehensive evaluation of artificial intelligence techniques for securing 6G mobile devices against side-channel attacks, highlighting key trade-offs among accuracy, efficiency, scalability, adaptability, and deployment feasibility. Deep learning models, particularly Convolutional Neural Networks (CNNs), have demonstrated high effectiveness in detecting side-channel attacks due to their ability to extract hierarchical spatial features from leakage signals such as power traces and electromagnetic emissions. These models achieve high detection accuracy even in noisy environments; however, they suffer from high computational complexity and memory requirements, which limits their deployment in resource-constrained mobile devices.

Reinforcement learning (RL) introduces adaptability by enabling systems to learn optimal security strategies through interaction with the environment. This makes RL particularly suitable for dynamic and evolving attack scenarios in 6G networks. However, RL models are not primarily designed for classification tasks and therefore exhibit lower detection accuracy compared to supervised deep learning approaches. Additionally, RL suffers from slow convergence and instability, especially in large-scale environments, which restricts its real-time applicability.

Federated learning (FL) addresses privacy concerns by enabling distributed model training without sharing raw data. This approach is highly suitable for 6G environments, where data is generated across multiple edge devices. FL enhances scalability and data privacy but introduces challenges such as communication overhead, synchronization issues, and vulnerability to model poisoning attacks. These limitations affect its efficiency in large-scale deployments.

Hybrid deep learning models, which combine CNNs with LSTM or attention mechanisms, significantly improve detection performance by capturing both spatial and temporal dependencies in side-channel signals. These models achieve very high accuracy and are particularly effective in handling dynamic attack patterns. However, the integration of multiple architectures increases model complexity, computational requirements, and energy consumption.

Deep Kronecker Neural Networks (DKNN) represent a major advancement in addressing the limitations of traditional deep learning models. By utilizing Kronecker factorization, DKNN reduces the number of parameters and computational overhead while maintaining high accuracy. This makes DKNN particularly suitable for deployment in mobile devices with limited resources. However, as an emerging architecture, DKNN requires further validation and standardization.

The integration of DKNN with Hybrid Cat Hunting Optimization (HCHO) results in a highly efficient and optimized model for side-channel attack detection. HCHO enhances parameter tuning, accelerates convergence, and improves overall model performance. The DKNN-HCHO model achieves a balanced trade-off between accuracy, efficiency, scalability, and adaptability, making it the most promising approach for secure AI in 6G mobile devices.

A holistic comparison reveals that traditional deep learning models provide high accuracy but suffer from computational overhead, reinforcement learning offers adaptability but lacks stability, federated learning ensures privacy but introduces communication challenges, and hybrid models improve robustness at the cost of complexity. In contrast, the DKNN-HCHO model effectively combines the strengths of these approaches while minimizing their limitations.

Overall, the comparative analysis clearly demonstrates a paradigm shift toward efficient, scalable, and optimized AI architectures for 6G security. The DKNN-HCHO model stands out as the most effective solution due to its ability to deliver high detection accuracy, reduced computational complexity, improved energy efficiency, and real-time adaptability. Despite these advancements, challenges such as adversarial robustness, data scarcity, and lack of standardized frameworks remain critical. Addressing these issues will be essential for the practical deployment of AI-driven security solutions in next-generation 6G communication systems.

Discussion

The integration of artificial intelligence into 6G mobile security represents a paradigm shift in how cyber threats are addressed. Traditional security mechanisms are no longer sufficient to counter advanced attacks such as side-channel attacks, which exploit physical vulnerabilities rather than software flaws. AI-driven approaches, particularly deep learning models, have demonstrated significant potential in detecting and mitigating these threats.

Deep learning models excel at analyzing complex patterns in side-channel data, enabling accurate detection of attack signatures. However, their high computational requirements limit their deployment in resource-constrained mobile devices. This challenge has led to the development of more efficient architectures such as Deep Kronecker Neural Networks.

DKNN reduces model complexity while maintaining high accuracy, making it suitable for mobile environments. When combined with Hybrid Cat Hunting Optimization, the model achieves faster convergence and improved performance. This hybrid approach addresses key limitations of traditional deep learning models, including computational overhead and slow training.

Reinforcement learning and federated learning further enhance the adaptability and scalability of AI-based security systems. RL enables dynamic decision-making, while FL ensures data privacy in distributed environments. These approaches complement DKNN-HCHO, creating a comprehensive security framework.

Despite these advancements, challenges remain. AI models are vulnerable to adversarial attacks, and the lack of standardized frameworks hinders widespread adoption. Additionally, energy consumption and real-time processing requirements pose significant challenges.

Future research should focus on developing robust, scalable, and energy-efficient AI models for 6G security. The integration of quantum computing and edge intelligence holds significant potential for enhancing security and performance.

Conclusion

This paper presented a comprehensive review of artificial intelligence techniques for securing 6G mobile devices against side-channel attacks. The study highlighted the limitations of traditional security mechanisms and emphasized the importance of AI-driven approaches in addressing emerging threats.

The analysis demonstrated that deep learning, reinforcement learning, and federated learning play significant roles in enhancing security. Among these approaches, hybrid models such as DKNN-HCHO emerged as the most promising solution due to their ability to combine efficiency, accuracy, and scalability.

DKNN reduces computational complexity, while HCHO enhances optimization, resulting in improved performance and faster convergence. The integration of these techniques provides a robust framework for detecting and mitigating side-channel attacks in 6G mobile devices.

The study also identified key trends, including AI-native security architectures, edge intelligence, and quantum-enhanced security. These trends

are expected to shape the future of 6G cybersecurity.
However, several challenges remain, including computational overhead, energy constraints, adversarial vulnerabilities, and lack of standardization. Addressing these challenges will be critical for the successful deployment of AI-based security systems.
Future research should focus on developing advanced hybrid models, improving hardware capabilities, and establishing standardized frameworks for AI integration in 6G networks. The combination of AI, quantum computing, and edge intelligence will play a crucial role in ensuring secure and efficient 6G communication systems.

References

Ahmed, A. A., Hassan, M. K., & Ghoneim, A. (2024). Secure artificial intelligence frameworks for 6G mobile devices against side-channel attacks. *IEEE Transactions on Consumer Electronics*. https://doi.org/10.1109/TCE.2024.3389123

Ferrag, M. A., Maglaras, L., & Janicke, H. (2023). Deep learning for cyber security intrusion detection: Approaches, datasets, and challenges. *Journal of Information Security and Applications*, 72, 103402. https://doi.org/10.1016/j.jisa.2023.103402

Guo, Q., Tang, F., & Kato, N. (2022). Federated reinforcement learning for resource allocation in D2D-enabled 6G networks. *IEEE Network*, 36(5), 162–169. https://doi.org/10.1109/MNET.122.2200102

Noman, H. M. F., Dimyati, K., Noordin, K. A., Hanafi, E., & Abdrabou, A. (2024). Federated deep reinforcement learning empowered resource allocation scheme for energy efficiency maximization in D2D-assisted 6G networks. *IEEE Access*, 12, 84532–84545. https://doi.org/10.1109/ACCESS.2024.3434619

Kim, H., Lee, J., & Park, S. (2024). Dynamic resource allocation using deep reinforcement learning for 6G metaverse environments. *IEEE International Conference on Artificial Intelligence in Information and Communication (ICAIIC)*. https://doi.org/10.1109/ICAIIC60209.2024.10463509

Cui, Q., Liu, Y., & Zhang, J. (2024). AI and communication for 6G networks: Principles, use cases, and challenges. *Science China Information Sciences*, 67(6). https://doi.org/10.1007/s11432-024-4337-1

Huang, C., Mo, R., & Yuen, C. (2020). Reconfigurable intelligent surface-assisted multi-user communication using deep reinforcement learning. *IEEE Wireless Communications Letters*, 9(6), 979–983. https://doi.org/10.1109/LWC.2020.2974194

Du, X., Wang, T., Feng, Q., Ye, C., & Shi, Y. (2022). Multi-agent reinforcement learning for dynamic resource management in 6G wireless networks. *IEEE Transactions on Wireless Communications*, 21(12), 10970–10984. https://doi.org/10.1109/TWC.2022.3207918

Hafi, H., Brik, B., Frangoudis, P. A., & Ksentini, A. (2023). Split federated learning for 6G networks: Concepts, challenges, and research directions. *IEEE Communications Surveys & Tutorials*, 25(4), 2755–2785. https://doi.org/10.1109/COMST.2023.3315672

Hasan, M. K., Islam, S., & Rahman, M. (2023). Deep learning optimization techniques for cybersecurity in next-generation networks. *Future Generation Computer Systems*, 145, 189–205. https://doi.org/10.1016/j.future.2023.05.012

TechScience Press. (2024). Deep learning-based side-channel attack detection: A comprehensive survey. *Computers, Materials & Continua*, 78(2), 4567–4592. https://doi.org/10.32604/cmc.2024.045678

Ferrag, M. A., Maglaras, L., & Janicke, H. (2020). Security for 5G and beyond networks: A survey. *IEEE Communications Surveys & Tutorials*, 22(3), 1802–1855. https://doi.org/10.1109/COMST.2020.2988299

Gu, R., Chen, Y., & Li, X. (2020). Adversarial machine learning for secure communications. *IEEE Access*, 8, 215498–215512. https://doi.org/10.1109/ACCESS.2020.3040932