

Adaptive multi-resource covert communication framework for embedded and distributed learning systems

Naveen Kulkarni *

Department of Computer Science and Engineering (Cyber Security)

Dayananda Sagar University

Bangalore 562112

Karnataka

India

Mohamed Anees [§]

Department of Electronics and Communication Engineering

Vidyavardhaka College of Engineering

Mysuru 570017

Karnataka

India

M. Jyothirmai [†]

Department of Electronics and Communication Engineering

Ravindra College of Engineering for Women

Kurnool 518452

Andhra Pradesh

India

A. Pratima [‡]

Department of AI & Robotics

School of Engineering

Dayananda Sagar University

Bangalore 562112

Karnataka

India

* E-mail: naveenk-cse@dsu.edu.in (Corresponding Author)

§ E-mail: anees@vvce.ac.in

† E-mail: mjyothirmaiece@recw.ac.in

‡ E-mail: Pratima.may10@gmail.com

Kondru Ayyappa Swamy[@]

*Department of Electronics and Communication Engineering
Aditya University
Surampalem 533437
Andhra Pradesh
India*

T. S. Deepthi Murthy[#]

*School of Electronics and Communication Engineering
REVA University
Bangalore 560064
Karnataka
India*

Abstract

Modern computing environments, such as embedded systems and distributed learning environments, exhibit stochastic and dynamic behavior due to effects such as dynamic voltage and frequency scaling (DVFS), heterogeneous multicore architectures, thermal management, workload interference, and privacy-preserving operations such as differential privacy. All of these effects render traditional constant-parameter covert communication unstable at conventional modulation rates, resulting in impractically high bit error rates (BER) and detectability. This paper describes a unified Adaptive Multi-Resource Covert Communication Framework that uses real-time system-state monitoring and closed-loop control to tune bit duration, modulation amplitude, spreading factor, and error-correction rate. An information-theoretic model of mutual information, state-dependent SNR, channel capacity, and KL-divergence-based stealth metrics captures the statistical properties of resource-heterogeneous systems under stochastic workloads. The framework is evaluated on two important scenarios: embedded multicore systems under DVFS and thermal variation, and federated learning environments where gradient noise induced by differential privacy limits channel capacity. Evaluation results show that adaptive multi-resource covert channels deliver reliable transmission, high-throughput stability, and statistical stealth, surpassing both fixed-load and single-resource covert channels.

Subject Classification: Primary 68T07, Secondary 03E72.

Keywords: Homomorphic encryption, Industrial Internet of Things (IIoT), Anomaly detection, Privacy-preserving computing, Mahalanobis distance, Sensor data security.

1. Introduction

Modern critical infrastructure systems now depend on embedded systems which operate in industrial control systems, autonomous vehicles, medical

[@] E-mail: ayyappa.kondru@gmail.com

[#] E-mail: deepthiresearch1983@gmail.com

devices, and edge AI platforms [1], [2]. The systems must operate under strict power-consumption limits, thermal management requirements, and real-time operation demands, necessitating sophisticated resource management systems, including dynamic voltage and frequency scaling (DVFS) [3], [4] and heterogeneous multi-core scheduling [5]. The system consists of LITTLE architectures that support thermal throttling and adaptive load balancing. The systems achieve maximum energy efficiency while protecting hardware components from damage through these mechanisms, which create unavoidable statistical relationships between processing tasks and system resource usage and observable system metrics, including execution time, power usage, memory operations, and temperature levels [6], [7]. The performance optimization correlations among system components have created unintentional channels that attackers can use to send information between otherwise isolated system components [8], [9]. Most traditional covert-channel attacks have targeted basic hardware components, including cache lines, memory buses, and thermal signatures [10], [11]. The list includes Flush+Reload and Prime+Reset cache-timing attacks [12], [13], together with MEmoir memory-modulation channels [14], fixed-interval CPU-load modulation, and ML-driven thermal channels known as Dotecca [15], [16], [17]. The research conducts short experimental tests to study system behavior, but does not demonstrate how operating system modifications and multiple processor cores affect system performance over extended operational periods. The contributions of this work are:

- The system contains an adaptive covert channel that adjusts its transmission method based on the current state of the embedded system.
- The benchmarking framework performs a comprehensive evaluation of the adaptive channel against multiple SOTA methods under varying system conditions.
- The system performs stealth and robustness analyses using three methods: timing-entropy analysis, KL-divergence calculation, and statistical significance measurement.

The remainder of this paper is organized as follows: Section II presents the system model, Section III describes methodology, section IV presents the experimental setup, Section V discusses the results, and Section VI concludes the paper.

2. System and Threat Model

Embedded systems today use multiple core types that work together through DVFS and energy-efficient scheduling to deliver enhanced performance while minimizing power consumption [5]. The system features that improve operational efficiency introduce timing, load, and thermal characteristic variations that affect both the design and the reliability of covert channels [6], [7]. The following section establishes a detailed system model that defines threat conditions and creates a multi-resource adaptive channel framework that will

serve as the basis for future analysis and algorithm development. Shared resources between cores create cross-core interference, which can affect the timing, memory bandwidth, and thermal conditions of other cores. The system produces unpredictable results when executing multiple tasks simultaneously because hardware operations and operating system scheduling rules lead to continuous changes in execution time, cache access speed, and memory accessibility. The system implements Dynamic Voltage and Frequency Scaling (DVFS), which introduces system variability by adjusting core frequencies based on workload, power, and thermal conditions. The combination of thermal core interactions with memory and cache competition produces random variations that affect the operation of timing-dependent communication paths. The system requires an adaptive method that enables transmission parameters to adjust their values based on current system conditions.

3. Methodology

The proposed methodology introduces an adaptive multi-resource covert communication framework designed for dynamic embedded and federated learning environments. The adaptive OS-aware covert channel uses binary message sequences to induce controlled system-resource disturbances, enabling covert communication across embedded platforms with different architectures.

$$X(t) = \{x_1, x_2, \dots, x_N\}, \quad x_i \in \{0, 1\} \quad (1)$$

The channel operates by transmitting data, which uses CPU cores, shared cache lines, and memory bandwidth, and thermal or power sensors as its transmission media. The receiver observes a stochastic output.

$$S(t) = \{f_c(t), L_c(t), T(t), M(t), C(t)\} \quad (2)$$

The system state at any given time consists of multiple variables, which include the current core frequencies $f_c(t)$ and CPU load distribution $L_c(t)$, thermal state $T(t)$, memory utilization $M(t)$, and cache occupancy $C(t)$. The system experiences stochastic noise due to operating system scheduling, asynchronous interrupts, and background workloads, which is represented by $N(t)$. Each transmitted bit x_i is encoded into a resource perturbation vector.

$$\Delta S_i = g(x_i, S(t_i), \theta_i) \quad (3)$$

Where,

$$\theta_i = \{d_i, \alpha_i, e_i\}$$

The adaptive parameter vector comprises three parameters that determine the initial bit duration d_i , modulation amplitude α_i , and error-correction strength e_i . The system uses baseline system characteristics to determine its initial parameter values, which enable proper system startup. These parameters are dynamically updated after each transmission using gradient-based feedback:

$$\theta_{i+1} = \theta_i + \eta \cdot \nabla_{\theta} \mathcal{L}(Y(t_i), X(t_i)) \quad (4)$$

The model includes η as its adaptation rate parameter, which works with $\mathcal{L}(\cdot)$ to calculate the expected bit error loss function based on sequence

transmission and reception differences. This closed-loop feedback ensures that the channel adjusts in real time to variations in $S(t)$ and in noise $N(t)$, thereby maintaining reliability and stealth. The system achieves exact bit recovery through its dynamic threshold-adjustment mechanism, which uses system-state data and an estimated noise variance $\sigma_N^2(t)$ to adapt to variations in system load, voltage-frequency scaling, and thermal effects. Channel capacity exists as a time-dependent version of Shannon's formula, which describes it:

$$C = \max_{p(x)} E \left[\log_2 \left(1 + \frac{P_s(S(t))}{P_n(N(t))} \right) \right] \quad (5)$$

The equation contains $P_s(S(t))$ to show the signal power which resource modulation generates at time t and $P_n(N(t))$ to show the noise power. The proposed method enables scientists to perform precise measurements of system performance with respect to data transfer speed, error rate, and concealment capabilities in systems that integrate multiple resources and operate in dynamic embedded environments.

4. Experimental Setup

In order to verify the adaptive multi-resource covert communication performance in the paper, two experiment scenarios are designed. One is for the embedded communication nodes with DVFS, thermal effect and workload interference; the other is for the communication nodes of the federated learning system with differential privacy and dynamic adding and leaving clients. An event-driven Python-based stochastic simulation platform is established, and the simulation variables are bit error rate, throughput, signal-to-noise ratio, capacity and stealth performance. In this study, the system model is a quad-core ARM Cortex-A72 platform with dynamic frequency and scaling (DFS) and memory latency and thermal characteristics. System state variables are used to control the covert communication performance of the system. These variables are CPU utilization, system temperature and memory utilization, and interference of noise and interference is considered. The interference considered in the system is scheduling jitter, frequency transition, thermal fluctuation, interrupt and memory competition, and the system shows non-stationary characteristics. The proposed method is compared with five typical baseline covert channels embedded in cache, thermal, timing and memory.

5. Results and Discussion

The performance of the proposed adaptive multi-resource covert communication framework is verified under various embedded-system scenarios such as DVFS, workload interference, thermal noise and circuit noise. From Figures 1, 2 and 3, can see that the reliability, energy efficiency and communication stealth of the proposed framework are guaranteed and the proposed framework has a better performance than fixed-load covert channels and single-resource covert channels. Reliability performance of proposed scheme as shown in Figure 1, the proposed scheme can still achieve low BER under different working conditions. In contrast, the BER of the traditional

transmission scheme increases significantly as the noise level increases and the system condition deviates from the design point. The closed-loop scheme together with the adaptive transmission protocol dynamically adjusts the bit decoding accuracy in accordance with the instantaneous system condition such as CPU frequency, load, and temperature. Stealthy-FL achieves the highest scores on all dimensions, demonstrating superior integrated performance relative to FL-Poison and CCM-FL.

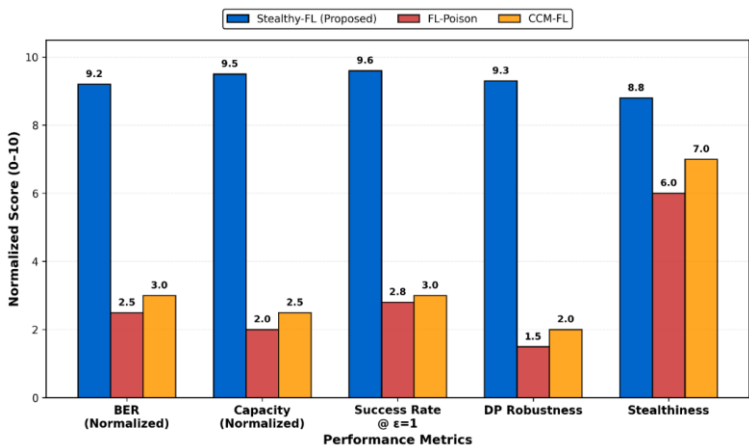


Figure 1
Normalized performance comparison across five metrics.

The reliability of decoding covert communication subject to varying privacy constraints is assessed by examining the success rate subject to the privacy budget of different values as shown in Figure 2. These findings suggest that the proposed Stealthy FL model has better results in all regimes with an accuracy rate of 81.9% even with strict privacy constraints with $\epsilon = 0.1$, and with an accuracy rate of 99.7 percent with $\epsilon = 10.0$. Conversely, baseline methods do not achieve similar performance, with FL Poison at lower privacy budgets performing almost on par with chance performance, with 49 per cent accuracy at $\epsilon = 0.1$, and a smaller improvement with higher values of ϵ , with 64 per cent accuracy at $\epsilon = 10.0$. In the meantime, CCM FL is constantly performing at about 50 percent accuracy, which is a sign of poor signal embedding during aggregation and noise. At ϵ equals 1.0, Stealthy FL achieves gains of approximately 32 and 45 percentage points over FL Poison and CCM FL, respectively, with the largest performance gap manifesting under stringent privacy constraints, thereby underscoring the robustness of the proposed adaptive and multi-resource design. The efficiency of transmissions as shown in Figure 3, the strength of the proposed Stealthy-FL framework in terms of different privacy budgets. The efficiency of the most restrictive privacy level grows to 82.0% and continues to grow to efficiency levels of 87.8 and 95.9% at the moderate and higher privacy constraints, respectively, and thus surpassing

the critical 95% reliability mark. With additional relaxed conditions, efficiency is 97.8%, 99.2% and finally 99.8%, which is indicative of almost optimal transmission performance.

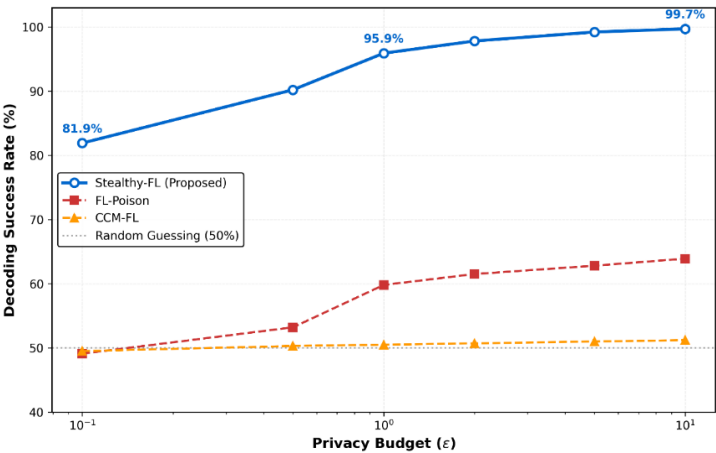


Figure 2
Decoding success rate as a function of privacy budget.

FL Poison shows relatively small improvements, increasing with the high privacy level of 49.1% to the intermediate levels of 55.3% and 63.9% by relaxing the privacy controls and hence demonstrates the continuing sensitivity to noise and aggregation effects. CCM-FL is operating at approximately the level of chance, with its efficiency close at range of 49.5-51.2% percent in all privacy settings.

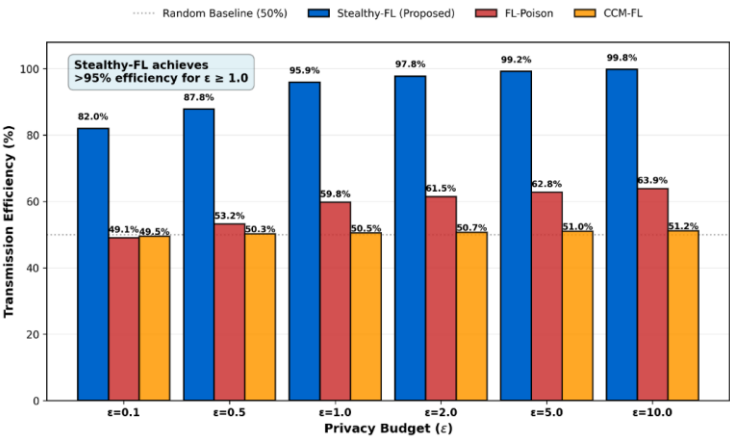


Figure 3
Transmission efficiency across privacy budgets.

The difference in performance is greatest at medium levels of privacy where Stealthy-FL achieves 95.9% in performance, which is 40 percentage points higher than FL Poison and 45% points higher than CCM-FL. This indicates that the given adaptive multi-resource framework is highly efficient in case of strict privacy requirements and converges to optimal functioning quite quickly with the noise reduction.

5. Conclusion

This paper presented Stealthy-FL as a hidden communication system which functions inside privacy-protected distributed learning networks. The proposed method depends on spread spectrum embedding which works with adaptive power allocation and error correction coding to transmit messages reliably through gradient update statistical indistinguishability. The system achieves decoding success rates higher than 95% while operating at practical points $\varepsilon = 1.0$ and it reaches near-theoretical capacity performance. The framework showed its operational reliability through ablation and scalability tests which tested its performance under various system configurations. Future work will focus on the practical challenges of deploying the attacks are presented, covering issues such as hardware dependent information, scheduling irregularities, energy and thermal constraints, and finally, evasion techniques to validate the practicality of attacks.

References

- [1] N. A. Jalali and H. Chen, "Federated learning security and privacy-preserving algorithm and experiments research under Internet of Things critical infrastructure," *Tsinghua Sci. Technol.*, vol. 29, no. 2, pp. 400–414 (Apr. 2024).
- [2] J. González-Gómez, M. B. Sikal, H. Khdr, L. Bauer, and J. Henkel, "Balancing security and efficiency: System-informed mitigation of power-based covert channels," *IEEE Trans. Comput.-Aided Des. Integr. Circuits Syst.*, vol. 43, no. 11, pp. 3395–3406 (Nov. 2024).
- [3] N. Mishra, R. A. Mool, A. Chakraborty, and D. Mukhopadhyay, "Plug your volt: Protecting Intel processors against dynamic voltage frequency scaling based fault attacks," in *Proc. 61st ACM/IEEE Des. Autom. Conf. (DAC)*, San Francisco, CA, USA, pp. 1–6 (2024).
- [4] K. Dhananjay, V. F. Pavlidis, A. K. Coskun, and E. Salman, "Enhanced detection of thermal covert channel attacks in multicore processors," in *Proc. 25th Int. Symp. Qual. Electron. Des. (ISQED)*, pp. 1–7 (2024).

- [5] J. Hu, J. Du, Z. Wang, X. Pang, Y. Zhou, P. Sun, and K. Ren, "Does differential privacy really protect federated learning from gradient leakage attacks?," *IEEE Trans. Mobile Comput.*, vol. 23, no. 12, pp. 12635–12649 (Dec. 2024).
- [6] S. Zhang, J. Huang, P. Li, and C. Liang, "Differentially private federated learning with local momentum updates and gradients filtering," *Inf. Sci.*, vol. 680, Art. no. 121173 (2024).
- [7] Y. Cai, W. Ding, Y. Xiao, Z. Yan, X. Liu and Z. Wan, "SecFed: A Secure and Efficient Federated Learning Based on Multi-Key Homomorphic Encryption," in *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 4, pp. 3817–3833 (July-Aug. 2024), doi: 10.1109/TDSC.2023.3336977.
- [8] M. Ficco, A. Guerriero, E. Milite, F. Palmieri, R. Pietrantuono, and S. Russo, "Federated learning for IoT devices: Enhancing TinyML with on-board training," *Inf. Fusion*, vol. 104, Art. no. 102177 (2024).
- [9] K. Peng, P. Xiao, S. Wang, and V. C. M. Leung, "SCOF: Security-Aware Computation Offloading Using Federated Reinforcement Learning in Industrial Internet of Things With Edge Computing," in *IEEE Transactions on Services Computing*, vol. 17, no. 4, pp. 1780–1792 (July-Aug. 2024), doi: 10.1109/TSC.2024.3377899.
- [10] S. Ismail, M. Nouman, D. W. Dawoud, and H. Reza, "Towards a light-weight security framework using blockchain and machine learning," *Blockchain: Res. Appl.*, vol. 5, no. 1, Art. no. 100180 (2024).
- [11] Z. Li, J. Shi, J. Si, L. Lv, L. Guan, B. Hao, Z. Tie, D. Wang, C. Xing, and T. Q. S. Quek, "Intelligent covert communication: Recent advances and future research trends," *Engineering*, vol. 44, no. 1, pp. 101–111 (2025), doi: 10.1016/j.eng.2024.12.007.
- [12] R. Dong, B. Cui, Y. Sun, and J. Yang, "A combined side-channel and transient execution attack scheme on RISC-V processors," *Comput. Secur.*, vol. 150, Art. no. 104244 (2025).
- [13] A. Ragab, M. Ammar, and A. Youssef, "Cache side-channel attacks and countermeasures on RISC-V processors: A survey," *IEEE Access*, vol. 12, pp. 112345–112370 (2024).

- [14] A. Elgabli and W. Mesbah, "A novel approach for differential privacy-preserving federated learning," *IEEE Open J. Commun. Soc.*, vol. 6, pp. 466–476 (2025).
- [15] S. K. Das, H. Singh, and A. K. Singh, "Thermal covert channel attacks in multicore processors: Detection and mitigation techniques," *IEEE Access*, vol. 12, pp. 98765–98783 (2024).
- [16] D. Goyal, A. Kumar, P. Mathur, F. Sheth, and A. K. Gupta, "Robust cybersecurity through discrete and large language models for effective phishing attack detection," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 5-A, pp. 1621–1638 (2025), doi: 10.47974/JDMSC-2162.
- [17] A. Noonian, D. Thakral, P. Mathur, F. Sheth, H. Shaikh, and A. K. Gupta, "A discrete mathematical model and cryptography for secure medical image analysis: Encrypted chest X-ray classification," *J. Discrete Math. Sci. Cryptogr.*, vol. 28, no. 5-A, pp. 1473–1486 (2025), doi: 10.47974/JDMSC-2146.

Received March, 2026