

Federated learning assisted power control for covert and secure UAV-enabled IoT communications

G. Hemanth Kumar *

Dilip Kumar Jang Bahadur Saini [†]

Department of Computer Science and Engineering (Cyber Security)

School of Engineering

Dayananda Sagar University

Bangalore 562112

Karnataka

India

Vasu Namala [§]

Department of Electronics and Communication Engineering

Sree Rama Engineering College

Tirupati 517501

Andhra Pradesh

India

N. Gireesh [‡]

Department of Electronics and Communication Engineering

Mohan Babu University

Tirupati 517102

Andhra Pradesh

India

Kondru Ayyappa Swamy [@]

Department of Electronics and Communication Engineering

Aditya University

Surampalem 533437

Andhra Pradesh

India

* E-mail: hemanthtechi@gmail.com (Corresponding Author)

[†] E-mail: dilipsaini@gmail.com

[§] E-mail: vasu455@gmail.com

[‡] E-mail: naminenigireesh@gmail.com

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

G. Santhosh Kumar [#]

Department of Computer Science and Engineering (Data Science)
Dayananda Sagar University
Bangalore 562112
Karnataka
India

Abstract

UAVs enhance IoT communication in dynamic, infrastructure-limited settings but face risks of information leakage and eavesdropping. The majority of existing works on covert communication are based on deterministic models and assume a centralized optimization with global CSI, which is not suitable for dynamic UAV-IoT scenarios. To address these challenges, this paper presents a framework, FL-SCA (federated learning-assisted successive convex approximation), for joint secrecy-covertneess optimization in UAV-enabled IoT communications. In this context, the distributed IoT devices are trained using the developed FL model to estimate the warden's detection error probability, while keeping their data private to safeguard their collected data and reduce overused communication resources. The learned detection predictor is used to solve the power-control optimization problem of maximizing the achievable secrecy rate subject to covert communication and transmit-power constraints. Successive Convex Approximation (SCA) is used to solve the non-convex problem and Monte Carlo simulations verify the improvement in terms of secrecy-covertneess and resource efficiency. As a result, distributed learning-assisted optimization is applicable to the secure and covert UAV-assisted IoT communication in the dynamic wireless networks.

Subject Classification: Primary 93A30, Secondary 49K15.

Keywords: Cooperative jamming, Covert communications, Federated learning, Physical layer security, Privacy-preserving optimization, UAV-enabled IoT.

1. Introduction

The meteoric progress of the Internet of Things (IoT) enables large-scale connectivity across use cases from smart infrastructure monitoring to disaster relief scenarios, precision farming, and industrial settings [1], [2]. These use cases often operate in geographically dispersed, dynamic settings where traditional terrestrial communication infrastructures cannot keep pace. Unmanned aerial vehicles (UAVs), have emerged as flexible aerial relays that can provide project-specific temporary coverage, enable network topology reconfiguration, and even serve as relays for rapid deployment scenarios [3], [4]. The high altitude, agility, and line-of-sight capabilities of UAVs enable significantly increased connectivity and reliability for IoT networks. For instance, the effectiveness of the relay may not always be guaranteed in heterogeneous or third-party scenarios, as an untrustworthy relay may attempt to extract confidential information from forwarded packets, compromising secrecy

[#] E-mail: drsanthoshg1983@gmail.com

[5]. More critically, the wireless forwarding nature of the relay makes it vulnerable to a passive external warden that can sniff the medium for detection opportunities of the communication itself, which would pose a problem in scenarios where the mere existence of such a communication would compromise the operation in applications like civil or military surveillance, environmental monitoring, or health-critical sensing [6], [7]. Consequently, UAV-based IoT systems must ensure both secrecy and covertness. The techniques of cooperative jamming, artificial noise, relay power control, and trajectory optimization are well known to improve the secrecy performance of UAV networks [8]. Concurrently with the secrecy literature, the field of covert communication has explored techniques to maximize the warden's false-alarm probability through power allocation and coding strategies under energy-detection models. All of these approaches assume access to instantaneous or statistical CSI and model the adversary's detection performance using either time-instantaneous or tractable models. In addition, traditional optimization methods do not capture the time-varying nature of network behavior or consider the long-term consequences of their actions [9], [10]. Furthermore, most existing approaches assume a centralized architecture for data collection and processing, which leads to significant communication overhead, scalability limitations, and potential privacy breaches when using learning-based methods in scenarios such as covert channel detection [11], [12]. Despite these advances, most existing covert communication frameworks rely on deterministic channel models and centralized optimization schemes. This paper proposes a framework, FL-SCA, that combines federated learning with successive convex approximation to solve the joint secrecy/covertness problem for UAV-based IoT networks. In this system model, a UAV acts as both a relay and a cooperative jammer in decode-and-forward, while a passive warden performs energy detection. The major contributions of this paper are summarized as follows:

- A joint secrecy-covertness optimization framework is developed for UAV-assisted IoT communication under an untrusted relay and passive warden scenario, capturing the coupling between relay decoding capability and energy-based detection.
- A privacy-preserving federated learning model is designed to estimate the warden's detection error probability from distributed IoT observations without sharing raw data.
- To solve the non-convex problem, the SCA-based power control algorithm is proposed by linearizing the secrecy objective and the covertness constraint at each iteration.

The rest of this paper is organized as follows. Section II gives the system model. Section III proposes the FL-SCA algorithm. Section IV presents the simulation scenario. Section V provides the simulation results. Section VI concludes this paper.

2. System Model

The proposed UAV-aided IoT communication system is modeled in a consistent and unified manner. The system modeling begins with the network architecture, followed by the LoS/ NLoS channel model used to characterize the wireless propagation environment [13], [14]. Next, the two-phase relay transmission protocol is specified, which forms the basis of the secrecy model assumed the untrusted relay. Finally, the detection model and covertness model employed at the passive warden are derived, completing the analytical modeling of the system. A UAV-based IoT communication scenario is modeled to enable secure, covert information transmission in the presence of adversarial monitoring [15]. The model consists of a ground source node S, a legitimate destination node D, an unmanned aerial vehicle (UAV) relay U, and a passive external warden W. The UAV performs DF relaying between nodes S and D, and transmits artificial noise during the forward transmission phase to enhance covertness. Two types of security threats are modeled. First, the trustworthiness of the UAV is assumed to be potentially compromised; while the UAV is expected to forward the decoded message to D, it may also seek to extract confidential information from the received signal during relaying. Second, a passive warden continuously monitors the wireless channel and performs energy-based detection to determine whether communication is occurring.

3. Proposed FL-SCA Optimization Framework

The non-convex secrecy-rate maximization problem subject to secrecy and transmit power constraints as discussed in section 2. The non-convexity is due to the difference of logarithmic SNR terms, and cannot be solved by using any convex optimization method. As the detection-error probability is a function of non-linear energy detection statistics and stochastic fading statistics, it also cannot be solved in closed form. Therefore, a hybrid solution should be developed to solve this problem. To address these challenges, a successive convex approximation (SCA) framework using a federated learning approach is proposed. The SCA-based methodology enables a distributed, data-driven model of the detection-error probability and a convexification process that yields an iterative solution. In particular, the basic idea underlying this technique is to locally approximate the secrecy function by its first-order Taylor expansion around the current feasible point, where the local approximation is defined as

$$C_s(P) \approx C_s(P^{(r)}) + \nabla C_s(P^{(r)})^T (P - P^{(r)}) \quad (1)$$

This approximation maintains first-order accuracy at the expansion point and produces a convex surrogate objective whose gradient components are

$$\frac{\partial C_s}{\partial P_u} = \frac{|h_{UD}|^2}{2 \ln 2 (\sigma^2 + P_u |h_{UD}|^2)} \quad (2)$$

$$\frac{\partial C_s}{\partial P_s} = - \frac{|h_{SU}|^2}{2 \ln 2 (\sigma^2 + P_s |h_{SU}|^2)} \quad (3)$$

Because the covertness constraint is also expressed through the smooth surrogate $\hat{\zeta}(P)$ it can be similarly linearized:

$$\hat{\zeta}(P) \approx \hat{\zeta}(P^{(r)}) + \nabla \hat{\zeta}(P^{(r)})^T (P - P^{(r)}) \quad (4)$$

Substituting these first-order approximations yields a convex optimization subproblem at each iteration, subject to the original power bounds. The solution of this subproblem provides an updated transmit power vector $P^{(r+1)}$, which becomes the expansion point for the next iteration. The iterative process continues until the change between successive solutions satisfies. Since the first-order optimization in each iteration maintains feasibility and optimizes a tight local approximation, the objective value must monotonically increase, and the procedure terminates at a stationary point that satisfies the usual regularity conditions.

4. Experimental Setup

To evaluate the effectiveness of the FL–SCA framework, a thorough simulation is conducted. The following section describes the simulation scenario, the federated learning setup, the comparative benchmark schemes, and the chosen performance metrics. All evaluation techniques utilize Monte Carlo simulations in Python. Network geometry consists of a ground-source node, a legitimate receiver, a passive warden, and a UAV relay with decode-and-forward capability. Ground nodes are distributed randomly within a square area of $500 \times 500 \text{ m}^2$, and the UAV is positioned at a constant height of $H = 100\text{m}$ unless specified otherwise. The federated learning framework is used to construct a global surrogate model for the detection-error probability without centralizing any raw simulation data across the network. The federated learning setup uses $K = 10$ distributed IoT devices for collaborative learning. Each device generates 2000 training data points through local training. The training data are generated by randomly selecting transmit power settings and channel conditions from the simulation environment. Generating training data locally on each device ensures that geometry and fading conditions remain diverse while remaining localized to each device. The surrogate model is implemented using a multilayer perceptron (MLP) architecture with two hidden layers of 32 neurons and a linear output layer. The model is trained for $T_{\text{FL}} = 50$ communication rounds. In each round, devices train locally for 5 epochs before sending updates to the aggregation server.

5. Results and Discussion

The performance of the proposed FL–SCA framework is evaluated based on the assumptions made in the simulation setup. This includes verifying the convergence of the proposed method, the degree of improvement in the achieved secrecy performance, the level of secrecy preserved, and the system's reliability across various fading channels.

5.1 Convergence Behavior and Operating Point Validation

The convergence of the proposed FL–SCA is discussed in terms of numerical stability and modeling accuracy. As illustrated in Figure 1, the FL–SCA method eventually reaches the working point at which all secrecy and

covertness constraints are satisfied, with an optimal trade-off. As shown in Figure 1 (a) that the secrecy rate of the proposed FL-SCA increases with each SCA iteration, which verifies the applicability of the first-order convex surrogate functions for approximating the non-convex objective functions at their local optimum points. In addition, from Figure 1 (c), it is clear that the transmit power variables increase very rapidly at the initial iterations of the SCA method and converge rapidly to the optimal solution, which illustrates that the SCA method successfully improves the feasible region of the design variables while maintaining the constraints and, accordingly, achieving a better solution. In addition to the numerical convergence shown in Figure 1 (a) and 1 (b), the Monte Carlo realizations of the secrecy rate and the detection-error probability at the optimal operating point are provided. As expected, the analytical expressions fit into the high-resolution Monte Carlo results obtained by the proposed SL method with very small approximation errors, confirming that the obtained surrogate model by FL preserves the wireless channel and detection characteristics of the original non-linear system and keeps the approximation errors as small as possible, which has been demonstrated by the proposed approach. This represents the valid operating point geometrically as depicted in Figure 1 (d), along with the 2D network configuration and UAV position for optimal design. Intuitively, being closer to the legitimate drop-off point leads to stronger, more secure links, while being farther from the warden increases the UAV's stealth.

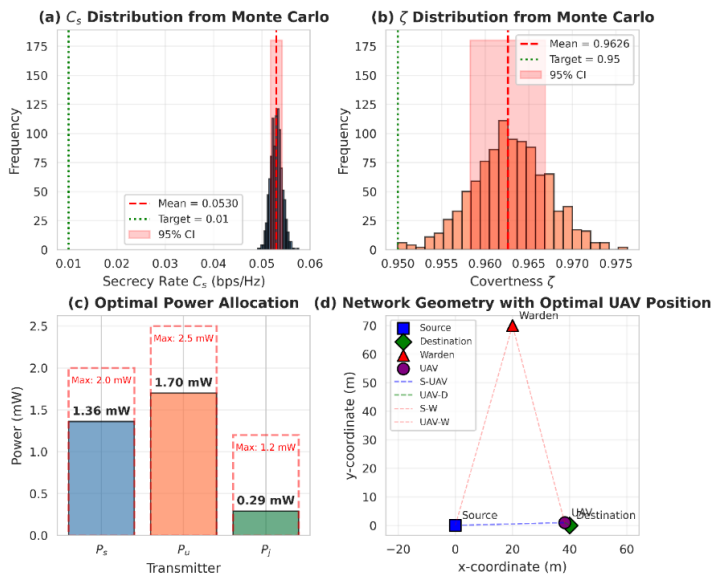


Figure 1

Monte Carlo validation of the optimal operating point: (a) Secrecy rate distribution, (b) Bovertness distribution, (c) Optimized transmit power allocation, and (d) Network geometry with the optimal UAV position.

5.2 Baseline Comparison and Efficiency Analysis

After defining the trade-off between structural secrecy and covertness, the suggested FL-SCA framework is compared with benchmark strategies to assess relative performance benefits. Figure 2 (a) shows the combined secrecy-covertness success rate. As illustrated in Figure 2 (b), the performance gap between the secrecy-only optimization and the proposed FL-SCA in terms of secrecy-covertness metric is shown. Although secrecy-only optimization can achieve a higher peak secrecy rate in a certain region, it always violates the detection constraint, which explains why the proposed FL-SCA offers a better trade-off between secrecy gain and covert transmission. Figure 2 (c) further demonstrates that the proposed distributed learning approach enjoys better resource efficiency than the centralized designs. This is because centralized designs inevitably suffer from heavy computation concentrated at the center node, as the center node must utilize global CSI for optimization, which must be communicated from all transmitter nodes. Combined, Figures 2 (a)-(d) prove that the suggested FLSCA framework reaches a positive balance between performance, communication efficiency, and scalability. Even though centralized optimization defines a hypothetical maximum, the distributed design achieves nearly optimal secrecy with significantly lower overhead and is therefore especially suitable for enabling large-scale IoT applications.

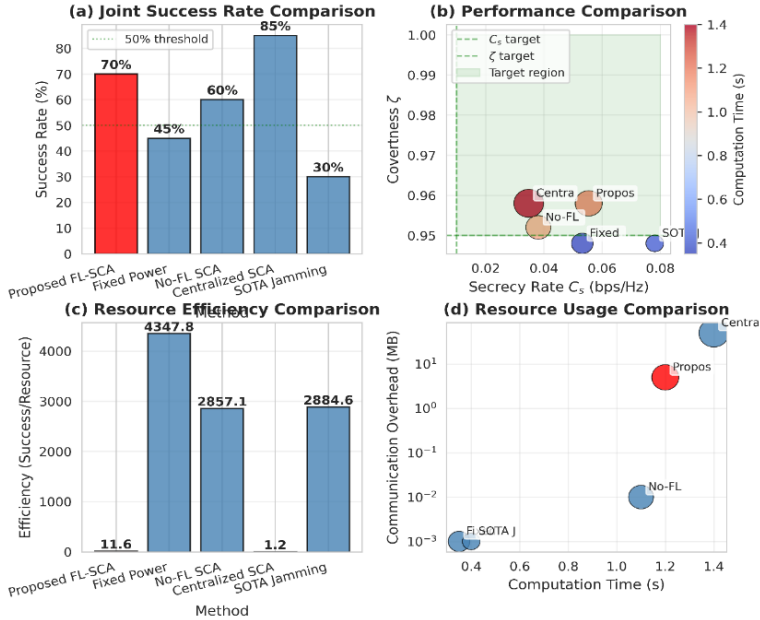


Figure 2
Comparison with baseline methods: (a) Joint success rate, (b) Secrecy covertness performance comparison, (c) Resource efficiency comparison, and (d) Computation and communication overhead comparison.

6. Conclusion

This paper outlines a federated learning-supported power management system that has been developed to achieve collective secrecy and covertness of UAV-based Internet of Things communications. The suggested FL-SCA algorithm integrates distributed federated learning with successive convex approximation to approximate the probability of detection error by the warden, and to optimize transmit-power assignment, consequently meeting secrecy and covertness. Simulation results obtained empirically bear witness to the idea that the proposed framework improves secrecy-covertness performance, and at the same time reduces communication overhead compared to traditional centralized and fixed-power schemes. Future work will focus on extending the framework to dynamic UAV trajectory optimization and multi-warden detection scenarios. In addition, online learning mechanisms can be incorporated to support channel conditions that vary with time. The validity of the developed framework has been supported by massive Monte Carlo simulations; however, the hardware implementation and experimentation in the real world are key directions of future studies.

References

- [1] P. Joshi, A. Kalita, and M. Gurusamy, "Reliable and efficient data collection in UAV-based IoT networks," arXiv preprint arXiv:2311.05303 (2023).
- [2] C. Gao, L. Tian, Q. Zhao, D. Zheng, and X. Jiang, "Covert and secure communication in untrusted UAV-assisted wireless systems," *IEEE Internet Things J.*, vol. 12, no. 17, pp. 35329–35339 (2025).
- [3] W. Wang, S. Fu, L. Yang, C. Li, and Y. Ren, "Age of information optimization for UAV deployment with covert communication: A deep reinforcement learning approach," *IEEE Trans. Veh. Technol.*, vol. 74, no. 12, pp. 19772–19776 (2025).
- [4] Y. Wu, C. Xing, J. Tang, N. Zhao, X. Y. Zhang, K.-K. Wong, and G. K. Karagiannidis, "Covert ISAC against collusive wardens," *IEEE Trans. Wireless Commun.*, vol. 24, no. 11, pp. 9763–9776 (2025).
- [5] I. Ud Din, I. Taj, A. Almogren, and M. Guizani, "Federated learning for trust enhancement in UAV-enabled IoT networks: A unified approach," *IEEE Internet Things J.*, vol. 12, no. 8, pp. 9596–9603 (2025).
- [6] A. S. S. Al Farsi, A. Khan, M. R. Mughal, and M. M. Bait-Suwailam, "Privacy and security challenges in federated learning for UAV systems: A systematic review," *IEEE Access*, vol. 13, pp. 86599–86615 (2025).

- [7] X. Chen, J. An, Z. Xiong, C. Xing, N. Zhao, F. R. Yu, and A. Nallanathan, "Covert communications: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, vol. 25, no. 2, pp. 1173–1198 (2023).
- [8] R. He, G. Li, J. Chen, H. Wang, R. Ma, W. Yang, W. He, and Y. Xu, "When the warden does not know transmit power: Detection performance analysis and covertness strategy design," *IEEE Trans. Commun.*, vol. 72, no. 6, pp. 3184–3198 (2024).
- [9] P. Wu, X. Yuan, Y. Hu, and A. Schmeink, "Joint power allocation and trajectory design for UAV-enabled covert communication," *IEEE Trans. Wireless Commun.*, vol. 23, no. 1, pp. 683–698 (2024).
- [10] M. T. Mamaghani and Y. Hong, "Secure short-packet communications via UAV-enabled mobile relaying: Joint resource optimization and 3D trajectory design," *IEEE Trans. Wireless Commun.*, vol. 23, no. 4, pp. 3157–3173 (2024).
- [11] D. D. Wang, X. Zhao, W. Shen, Z. Li, N. Cheng, H. Qin, and L. Cao, "Optimal transmit power and hovering location for UAV covert communication in IoT systems," *IEEE Internet Things J.*, vol. 11, no. 15, pp. 26118–26130 (2024).
- [12] F. Yang, C. Wang, J. Xiong, and N. Deng, "UAV-enabled robust covert communication against active wardens," *IEEE Trans. Veh. Technol.*, vol. 73, no. 6, pp. 9159–9164 (2024).
- [13] L. Chen, W. Zhang, M. A. Kishk, and M.-S. Alouini, "Correlation of line-of-sight probabilities in aerial-terrestrial communications: Modeling, analysis, and application," *IEEE Trans. Veh. Technol.*, vol. 73, no. 5, pp. 7049–7065 (2024).
- [14] C. Sun, G. Fontanesi, B. Canberk, A. Mohajerzadeh, S. Chatzinotas, D. Grace, and H. Ahmadi, "Advancing UAV communications: A comprehensive survey of cutting-edge machine learning techniques," *IEEE Open J. Veh. Technol.*, vol. 5, pp. 825–854 (2024).
- [15] Y. Xiao, Z. Ye, M. Wu, H. Li, M. Xiao, M.-S. Alouini, and S. Cioni, "Space-air-ground integrated wireless networks for 6G: Basics, key technologies, and future trends," *IEEE J. Sel. Areas Commun.*, vol. 42, no. 12, pp. 3327–3354 (2024).

Received March, 2026