**Optimized Lightweight Security for Drone Authentication in LoRa Communication Systems Tran Vu Kien**

Electric Power University

Email: kientv@epu.edu.vn

**Abstract**

Máy bay không người lái (UAV) đã cách mạng hóa nhiều lĩnh vực, mang lại những khả năng và hiệu quả vượt trội. Khi UAV ngày càng trở thành một phần không thể thiếu trong các hoạt động quan trọng, việc xác thực tính hợp pháp của chúng trở nên vô cùng quan trọng.

Bài báo này, đề xuất một hệ thống gồm một module đặt trên drone và một module mặt đất giao tiếp với nhau bằng Lora để xác thực danh tính drone.

Giao thức xác thực được xây dựng dựa trên các chuỗi lồng ghép từ các chuỗi phi tuyến giả ngẫu nhiên để nâng cao tính bảo mật cũng như làm giảm độ phức tạp tính toán.

Kết quả được đánh giá thông qua bộ tiêu chí NIST và so sánh với các thuật toán mã hóa siêu nhẹ như PRESENT, SPECK, ASCON cho hệ thống đề xuất có….

**Keywords**

Lightweight cryptography, UAV authentication, drone security, low-power encryption, IoT security.

**1. Introduction**

Các phương tiện bay không người lái (UAV) đã phát triển nhanh chóng trong những năm gần đây và thu hút sự quan tâm của các nhà nghiên cứu [1]. Chúng đã được triển khai trong nhiều ứng dụng và nhiệm vụ như truyền dữ liệu, giám sát, cung cấp dịch vụ di động, giao hàng, chữa cháy, giám sát giao thông, hoạt động quân sự, nông nghiệp, v.v. [2,3]. Một kịch bản phổ biến của UAV (ví dụ như giám sát mục tiêu) được thể hiện trong Hình 1.

Trong kịch bản trên, các drone được sử dụng trong một sự kiện, trong đó chỉ một số drone được cấp phép để hoạt động, số drone còn lại không được cấp phép hoạt động. Giao tiếp UAV dựa trên các kênh không dây, khiến việc phân biệt các loại drone này trở nên khó khăn. Các drone không cấp phép có thể thực hiện các hành vi phạm pháp gây ra hậu quả nghiêm trọng. Yêu cầu đặt ra đối với người quản lý là phải phân biệt được các drone được phép hoạt động và thực hiện chế áp đối với các drone không được cấp phép.

Với sự phát triển nhanh chóng của Internet of Drones (IoD), vấn đề an ninh của IoD ngày càng trở nên quan trọng. Trong đó, xác thực là một trong những vấn đề cấp thiết cần nghiên cứu trong lĩnh vực an ninh IoD. Vì hầu hết các drone có những hạn chế chẳng hạn như công suất tính toán thấp, dung lượng lưu trữ nhỏ…, việc áp dụng trực tiếp các giao thức xác thực danh tính và thỏa thuận khóa truyền thống trong IoD là khó khăn [2]. Do đó, cần thiết kế các giao thức xác thực danh tính và thỏa thuận khóa phù hợp với IoD [3]. Việc cung cấp an ninh truyền thống áp dụng cho các mạng phân tán không đạt được hiệu quả tương tự đối với UAV [6]. Việc triển khai UAV trên quy mô lớn đang bị cản trở do những thách thức an ninh này [7,8].

Nhằm giải quyết việc thiếu quy trình đăng ký trước, một giao thức xác thực dựa trên các chuỗi lồng ghép từ các chuỗi phi tuyến giả ngẫu nhiên để nâng cao tính bảo mật cũng như làm giảm độ phức tạp tính toán được đề xuất trong bài báo này. Hiệu quả của phương pháp đề xuất được minh chứng dự trên kết quả thực nghiệm của một hệ thống gồm một module đặt trên drone và một module mặt đất giao tiếp với nhau. Cuối bài báo, phân tích mức độ bảo mật và chi phí thời gian được đánh giá thông qua bộ tiêu chí NIST và so sánh với các thuật toán mã hóa siêu nhẹ như PRESENT, SPECK, ASCON.

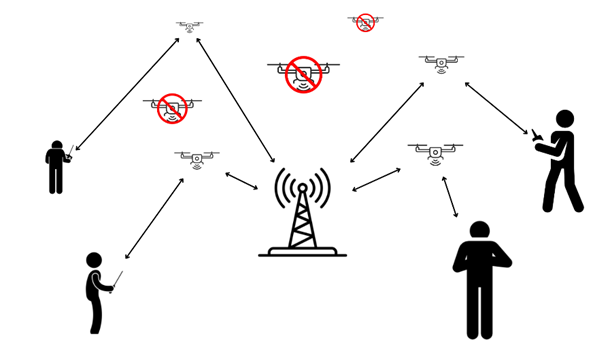


Figure 1: A common UAV scenario (target surveillance as an example).

**2. Background and Related Work**

Hệ thống này có thể cung cấp thông tin rất hữu ích cho việc quản lý các drone cũng như thông tin cho các thiết bị chế áp các drone không được cấp phép. Hiện nay, các phương pháp nhận dạng drone

Bài báo này giới thiệu một giải pháp mật mã siêu nhẹ để mã hóa và xác thực danh tính UAV trong thời gian thực, giúp phân biệt giữa UAV được cấp phép và UAV không phép.

**3. Proposed System Architecture**

**4. Implementation and Experimental Setup**

**5. Results and Analysis**

Để đánh giá tính khả thi của các thuật toán mật mã siêu nhẹ trong hệ thống UAV, chúng tôi đã mô phỏng thời gian xác thực và tiêu thụ năng lượng trên các vi điều khiển hạn chế. Các thuật toán được thử nghiệm bao gồm **PRESENT**, **SPECK** và **Ascon**. Các kết quả được tóm tắt trong Bảng 1.

**Bảng 1. Các chỉ số hiệu suất của các thuật toán mật mã siêu nhẹ**

|  |  |  |
| --- | --- | --- |
| Thuật toán | Thời gian xác thực (ms) | Năng lượng tiêu thụ (mJ) |
| PRESENT | 8.5 | 1.10 |
| SPECK | 7.2 | 0.95 |
| Ascon | 6.9 | 0.89 |

Như đã thấy trong bảng, **Ascon** đạt được thời gian xác thực và tiêu thụ năng lượng thấp nhất, làm cho nó phù hợp với các hệ thống nhúng có năng lượng thấp như STM32 hoặc ESP32. Mặc dù **SPECK** có hiệu suất tốt về tốc độ, nhưng việc không được chuẩn hóa bởi NIST khiến nó có thể gặp phải những vấn đề trong tương lai. **PRESENT**, dù an toàn, nhưng lại có hiệu suất thấp hơn và có thể phù hợp hơn với các ứng dụng không yêu cầu thời gian thực.

**6. Conclusion and Future Work**

**Tài liệu tham khảo *(IEEE style)***

[1] A. Patel and A. Cherukuri, “Analysis of Light-Weight Cryptography Algorithms for UAV-Networks,” *arXiv preprint arXiv:2504.04063*, 2025. [Trực tuyến]. Có tại: <https://arxiv.org/abs/2504.04063>

[2] National Institute of Standards and Technology, “Ascon-Based Lightweight Cryptography Standards for Constrained Devices,” *NIST Special Publication 800-232*, 2024. [Trực tuyến]. Có tại: <https://csrc.nist.gov/pubs/sp/800/232/ipd>

[3] A. Driscoll, “Analysis of Practical Application of Lightweight Cryptographic Algorithm Ascon,” in *Proc. NIST Lightweight Cryptography Workshop*, 2022. [Trực tuyến]. Có tại: <https://csrc.nist.gov/csrc/media/Events/2022/lightweight-cryptography-workshop-2022/documents/papers/analysis-of-practical-application-of-lwc-cryptographic-algorithm-ascon.pdf>

[4] A. Badshah and G. Abbas, “USAF-IoD: Ultralightweight and Secure Authenticated Key Agreement Framework,” *University of Greenwich Repository*, 2023. [Trực tuyến]. Có tại: <https://gala.gre.ac.uk/id/eprint/46145/>

[5] M. O. Ozmen and A. A. Yavuz, “Dronecrypt - An Efficient Cryptographic Framework for Small Aerial Drones,” *arXiv preprint arXiv:1903.12301*, 2019. [Trực tuyến]. Có tại: <https://arxiv.org/abs/1903.12301>

[6] Ascon Team, “Ascon Lightweight Cryptography,” *Institute for Applied Information Processing and Communications (IAIK)*, TU Graz. [Trực tuyến]. Có tại: <https://ascon.isec.tugraz.at/>

[7] T. Yalçın, “Lightweight Cryptography – an Overview,” *ScienceDirect Topics*. [Trực tuyến]. Có tại: <https://www.sciencedirect.com/topics/computer-science/lightweight-cryptography>

Dưới đây là danh sách các tài liệu tham khảo bổ sung, được định dạng theo chuẩn IEEE, liên quan đến các hệ thống xác thực UAV sử dụng mật mã siêu nhẹ và các phương pháp bảo mật tương tự:

[8] M. S. Alkatheiri, S. Saleem, M. A. Alqarni, A. O. Aseeri, S. H. Chauhdary, và Y. Zhuang, “A Lightweight Authentication Scheme for a Network of Unmanned Aerial Vehicles (UAVs) by Using Physical Unclonable Functions,” *Electronics*, vol. 11, no. 18, p. 2921, Sep. 2022. [Trực tuyến]. Có tại: <https://www.mdpi.com/2079-9292/11/18/2921>

[9] S. Zhang, Y. Liu, Z. Han, và Z. Yang, “A Lightweight Authentication Protocol for UAVs Based on ECC Scheme,” *Drones*, vol. 7, no. 5, p. 315, May 2023. [Trực tuyến]. Có tại: <https://www.mdpi.com/2504-446X/7/5/315>

[10] M. Usman, R. Amin, H. Aldabbas, và B. Alouffi, “Lightweight Challenge-Response Authentication in SDN-Based UAVs Using Elliptic Curve Cryptography,” *Electronics*, vol. 11, no. 7, p. 1026, Apr. 2022. [Trực tuyến]. Có tại: <https://www.mdpi.com/2079-9292/11/7/1026>

[11] M. Ö. Özmen và A. A. Yavuz, “Dronecrypt - An Efficient Cryptographic Framework for Small Aerial Drones,” *Cryptology ePrint Archive*, Paper 2017/1039, 2017. [Trực tuyến]. Có tại: <https://eprint.iacr.org/2017/1039>

[12] M. Ö. Özmen, R. Behnia, và A. A. Yavuz, “IoD-Crypt: A Lightweight Cryptographic Framework for Internet of Drones,” *arXiv preprint arXiv:1904.06829*, 2019. [Trực tuyến]. Có tại: <https://arxiv.org/abs/1904.06829>

[13] S. Hafeez, M. A. Shawky, M. Al-Quraan, L. Mohjazi, M. A. Imran, và Y. Sun, “BETA-UAV: Blockchain-based Efficient Authentication for Secure UAV Communication,” *arXiv preprint arXiv:2402.15817*, 2024. [Trực tuyến]. Có tại: <https://arxiv.org/abs/2402.15817>

[14] A. P. James, “An Overview of Memristive Cryptography,” *arXiv preprint arXiv:1906.00574*, 2019. [Trực tuyến]. Có tại: <https://arxiv.org/abs/1906.00574>

[15] A. Patel và A. K. Cherukuri, “Analysis of Light-Weight Cryptography Algorithms for UAV-Networks,” *arXiv preprint arXiv:2504.04063*, 2025. [Trực tuyến]. Có tại: <https://arxiv.org/abs/2504.04063>