Протокол криптозащиты канала БПЛА

УДК 004.056

П.Р. МАТВЕЕВ, преподаватель кафедры "Инфокоммуникационные технологии и системы связи" ГБОУ ВО "Нижегородский государственный инженерно-экономический университет", С.В. ШАХТАНОВ, доцент кафедры "Инфокоммуникационные технологии и системы связи" кандидат технических наук, Р.В. КЛИМОВ, доцент кафедры "Инфокоммуникационные технологии и системы связи" кандидат технических наук

Введение

Беспилотные летательные аппараты (БПЛА) широко применяются в мониторинге, картографировании, логистике, охране объектов и поисково-спасательных операциях. При этом устойчивость их работы определяется не только качеством навигации и алгоритмов управления, но и защищенностью канала связи между наземной станцией управления (НСУ) и бортовым оборудованием. Канал управления функционирует в открытой радиосреде, что делает возможным пассивный перехват сообщений, повторную передачу ранее записанных пакетов и подмену управляющих воздействий. На практике эти угрозы особенно опасны для систем, использующих открытые и широко документированные протоколы обмена [1], [13].

Одним из наиболее распространенных протоколов взаимодействия в системах на базе ArduPilot и PX4 является MAVLink. Его достоинства — открытость спецификации, простота реализации и широкая поддержка в существующих программно-аппаратных комплексах. Вместе с тем базовая конфигурация MAVLink не обеспечивает конфиденциальности передаваемых сообщений, а встроенные средства защиты не закрывают задачу комплексной криптографической защиты канала управления. Систематический анализ уязвимостей протокола, выполненный в работах [5], [6], показал, что MAVLink подвержен атакам подмены команд, перехвата телеметрии и повторного воспроизведения пакетов.

Целью работы является разработка протокола криптографической защиты канала управления БПЛА, обеспечивающего конфиденциальность, подлинность и защиту от повторного воспроизведения сообщений при ограниченных вычислительных ресурсах бортового контроллера.

Таблица 1

Сравнение каналов управления и передачи данных БПЛА

Характеристика	Канал управления	Канал передачи данных
Типичный размер пакета, байт	20 – 100	200 – 1500
Частота обмена	1 – 50 Гц	Непрерывный поток
Допустимая задержка, мс	50 – 200	200 – 500
Критичность потери пакета	Высокая	Низкая – средняя
Требования к аутентификации	Критически высокие	Средние

Таблица 2

Структура пакета MAVLink v2

Поле	Размер, байт	Назначение
Маркер начала (0xFD)	1	Идентификация формата
Длина полезной нагрузки	1	Определение размера данных
Флаги	2	Управляющие признаки
Номер пакета	1	Последовательный номер (0 – 255, циклический)
Идентификатор системы	1	Номер системы отправителя
Идентификатор компонента	1	Номер компонента отправителя
Идентификатор сообщения	3	Тип передаваемого сообщения
Полезная нагрузка	0 – 255	Данные сообщения
Контрольная сумма	2	Проверка целостности при передаче
Подпись (опционально)	13	Аутентификация (при включенном Signing)

Объект исследования

Объектом исследования является канал управления БПЛА, построенный на двустороннем обмене между НСУ и полетным контроллером. По восходящей линии передаются команды управления: задание режима полета, целевые координаты, высота, скорость. По нисходящей — телеметрия: текущие координаты, ориентация в пространстве, состояние бортовых систем. В большинстве систем оба направления обслуживаются одной радиолинией, работающей в диапазонах 433, 868, 915 МГц или 2,4 ГГц.

Канал управления предъявляет существенно более жесткие требования, чем канал передачи данных. Сравнение их характеристик приведено в табл. 1.

Протокол MAVLink v2 добавил механизм подписи пакетов, однако, как показано в работах [5], [6], он имеет два существенных ограничения: подпись обеспечивает только аутентификацию, не шифрует полезную нагрузку и усечена до 48 бит, что при скорости перебора порядка 10^9 вариантов в секунду допускает полный перебор за несколько суток.

Структура пакета MAVLink v2 приведена в табл. 2.

Статью целиком читайте в бумажной версии журнала

ПРОТОКОЛ КРИПТОЗАЩИТЫ КАНАЛА БПЛА

UAV CHANNEL CRYPTOGRAPHIC PROTECTION PROTOCOL

УДК 004.056

МАТВЕЕВ Павел Романович, **ШАХТАНОВ Сергей Валентинович** (кандидат технических наук),
КЛИМОВ Роман Владимирович (кандидат технических наук)
(ГБОУ ВО "Нижегородский государственный инженерно-экономический университет")

Рассматривается задача защиты канала управления беспилотного летательного аппарата от подмены команд и несанкционированного считывания передаваемой информации. Показано, что открытые протоколы обмена, в частности MAVLink, в базовой конфигурации не обеспечивают достаточной конфиденциальности и аутентификации.

Предложен протокол защищенного взаимодействия между наземной станцией и бортовым вычислительным модулем, основанный на установлении сеансового ключа, разделении ключевого материала по направлениям передачи и применении аутентифицированного шифрования. Для реализации используются механизмы X25519, HKDF — SHA-256, HMAC — SHA-256 и ChaCha20 — Poly1305. Показано, что предложенный подход обеспечивает конфиденциальность, целостность и подлинность командно-телеметрического обмена при сохранении совместимости с системами на базе MAVLink и ограничениями типовых бортовых контроллеров.

This article examines the problem of protecting an unmanned aerial vehicle's control channel from command spoofing and unauthorized reading of transmitted information. It is shown that open communication protocols, in particular MAVLink, in their basic configurations do not provide sufficient confidentiality and authentication.

A protocol for secure interaction between a ground station and an onboard computing module is proposed. This protocol is based on establishing a session key, separating the key material by transmission direction, and using authenticated encryption. The implementation utilizes X25519, HKDF-SHA-256, HMAC-SHA-256, and ChaCha20-Poly1305 mechanisms. It is demonstrated that the proposed approach ensures the confidentiality, integrity, and authenticity of command and telemetry exchange while maintaining compatibility with MAVLink-based systems and the limitations of typical onboard controllers.

Ключевые слова: БПЛА, канал управления, криптографическая защита, MAVLink, аутентифицированное шифрование, подмена команд, повторное воспроизведение пакетов, защита информации.

Keywords: *UAV, control channel, cryptographic protection, MAVLink, authenticated encryption, command spoofing, packet replay, information security.*

Литература

1. Долгий Е.Ю., Шошина К.В., Алешко Р.А. Разработка схемы защищенного канала дальнего радиуса действия для наземной станции управления беспилотного летательного аппарата// Молодой ученый. 2015. № 13.1 (93.1). С. 10 — 12.
2. Сорокин И.А., Романов П.Н., Шибаева М.Ю. Применение метода перестановочного декодирования в системе управления беспилотных летательных аппаратов малого класса (дроны, мультикоптеры)// Молодой ученый. 2017. № 6. С. 34 — 37.
3. Allouch A., Cheikhrouhou O., Koubaa A., et al. MAVSec: Securing the MAVLink Protocol for Ardupilot/PX4 Unmanned Aerial Systems./ Proceedings of the International Wireless Communications and Mobile Computing Conference (IWCMC). IEEE. Tangier, 2019. P. 621 — 628.
4. Dixit B., Ananthapadmanabhan A., Thahsin A., et al. A Novel Cipher for Enhancing MAVLink Security: Design, Security Analysis, and Performance Evaluation Using a Drone Testbed (MAVShield)./ arXiv.org. 2025: [Электронный ресурс]. Дата обращения: 06.05.2025.
5. Enhancing UAV Security Against GPS Spoofing Attacks Through a Genetic Algorithm-Driven Deep Learning Framework// Information. 2025. Vol. 16. № 2. Article 115.
6. Hadi H.-J., et al. A Comprehensive Survey on Security, Privacy Issues and Emerging Defence Technologies for UAVs// Journal of Network and Computer Applications. 2023. Vol. 213. Article 103607.
7. Huang K.-W., Chen J.-H., Chen Y.-F. Combating the Control Signal Spoofing Attack in UAV Systems// IEEE Transactions on Vehicular Technology. 2018. Vol. 67. № 11. Pp. 11192 — 11202.
8. Kim A., et al. Empirical Analysis of MAVLink Protocol Vulnerability for Unmanned Aerial Vehicles// IEEE Access. 2018. Vol. 6. Pp. 43203 — 43212.
9. Krawczyk H., Eronen P. HMAC-based Extract-and-Expand Key Derivation Function (HKDF)./ rfc-editor.org. Internet Engineering Task Force. 2010. [Электронный ресурс]. Дата обращения: 06.05.2025.
10. Kumar N., Chaudhary A. Surveying cybersecurity vulnerabilities and countermeasures for enhancing UAV security// Computer Networks. 2024. Vol. 253. Article 110714.
11. Kwon Y.-M., et al. Vulnerability Analysis of the MAVLink Protocol for Command and Control of Unmanned Aircraft. — Monterey: Naval Postgraduate School. 2014.
12. Langley A., Hamburg M., Turner S. Elliptic Curves for Security./ rfc-editor.org. Internet Engineering Task Force. 2016. [Электронный ресурс]. Дата обращения: 06.05.2025.
13. Lee J., et al. Drone Security Module for UAV Data Encryption./ Proceedings of the Conference on Electronics, Information and Communication (ICEIC). IEEE. Barcelona, 2020. Pp. 1 — 4.
14. Nir Y., Langley A. ChaCha20 and Poly1305 for IETF Protocols./ rfc-editor.org. Internet Engineering Task Force. 2018. [Электронный ресурс]. Дата обращения: 06.05.2025.
15. Nir Y. ChaCha20, Poly1305, and Their Use in the Internet Key Exchange Protocol (IKE) and IPsec./ rfc-editor.org. Internet Engineering Task Force. 2015. [Электронный ресурс]. Дата обращения: 06.05.2025.