**М. І. Проценко**
**Р. В. Маслій**

# Комунікаційні протоколи для безпечного обміну даними між БПЛА у розподіленій системі

**Вінницький національний технічний університет**

**Анотація**

*З розвитком технологій безпілотних літальних апаратів (БПЛА) та збільшенням потреби у їх використанні для збору і обміну даними в реальному часі виникає важлива задача забезпечення надійної та безпечної комунікації між БПЛА у розподілених системах. В умовах зростаючих вимог до безпеки даних та швидкості обміну інформацією, безпечний обмін даними стає критично важливим для ефективного виконання різних операцій, таких як спільна розвідка, моніторинг або пошукові місії. Саме тому комунікаційні протоколи для таких мереж мають забезпечувати надійну передачу даних, стійкість до зломів та кібератак, а також оптимізацію ресурсів БПЛА для досягнення максимальної ефективності та економії енергії. Основними аспектами, що впливають на ефективність таких систем, є надійність передачі даних, захист від зломів та атак, а також забезпечення гнучкості у випадку динамічних змін в умовах експлуатації. У роботі досліджуються найсучасніші комунікаційні протоколи для безпечного обміну даними між БПЛА, такі як Ad-Hoc On-Demand Distance Vector (AODV), що дозволяє динамічну маршрутизацію в умовах змінюваної топології мережі, та Secure Routing Protocol (SRP), який забезпечує безпечну передачу даних через аутентифікацію учасників мережі. Крім того, розглядається протокол Datagram Transport Layer Security (DTLS), що забезпечує шифрування даних навіть у ненадійних мережах, та Optimized Link State Routing (OLSR), який оптимізує маршрутизацію в умовах великих мереж і забезпечує надійність передачі даних у складних середовищах. Окремо аналізуються механізми захисту, такі як аутентифікація вузлів, що дозволяє ідентифікувати кожен апарат у мережі, та шифрування даних, що перешкоджає доступу зловмисників до конфіденційної інформації. Захист від атак типу DoS забезпечує стійкість системи до перевантаження і втрати зв'язку. Такий підхід до побудови комунікаційної системи дозволяє ефективно і безпечно використовувати БПЛА для виконання місій у складних умовах, забезпечуючи їх надійність і довговічність навіть у випадку відмови окремих компонентів мережі. Впровадження нових технологій і підходів до організації передачі даних між безпілотниками дозволяє значно розширити можливості БПЛА, що є важливим кроком у розвитку цієї галузі.*

**Ключові слова:** *безпілотні літальні апарати, розподілені системи, безпечний обмін даними, комунікаційні протоколи, маршрутизація, шифрування, аутентифікація, Ad-Hoc мережі*

## Вступ

У сучасному світі безпілотних літальних апаратів виникає нагальна потреба у координації їхньої роботи в розподілених системах для збору, обробки та обміну даними в реальному часі. Різноманітні завдання, такі як розвідка, моніторинг, пошукові та рятувальні операції, вимагають тісної взаємодії між групами БПЛА. Оскільки ці апарати діють у динамічних середовищах і нерідко у віддалених або складних умовах, забезпечення надійної та безпечної передачі даних є критичним аспектом для успіху місії. Для успішної взаємодії між БПЛА необхідні спеціалізовані комунікаційні протоколи, які можуть забезпечити безпеку передачі даних, захист від зломів та кібератак, а також високу надійність у непередбачуваних умовах. Сучасні методи безпечної маршрутизації, шифрування даних та аутентифікації вузлів допомагають знизити ризики несанкціонованого доступу та атак на мережу.

Основними завданнями розподілених систем є стабільна маршрутизація даних навіть у змінних мережах, захист інформації від несанкціонованого доступу та атак за допомогою шифрування й аутентифікації, а також оптимізація використання ресурсів БПЛА для підвищення ефективності передачі інформації та зниження витрат енергії [1]. Крім того, такі системи повинні бути стійкими до відмов та забезпечувати безперебійну роботу навіть при втраті окремих вузлів мережі. Це дозволяє ефективно взаємодіяти, виконуючи складні завдання в розподілених умовах з мінімальними ризиками для безпеки передачі даних.

*Метою роботи* є дослідження комунікаційних протоколів для забезпечення надійної, ефективної та безпечної передачі даних між БПЛА в умовах динамічної та розподіленої мережі.

## Основні комунікаційні протоколи

Для забезпечення надійної та безпечної комунікації між БПЛА у розподілених системах використовуються різні комунікаційні протоколи, кожен з яких має свої унікальні властивості та підходить для певних умов експлуатації. У цій роботі розглядаються чотири основні протоколи: Ad-Hoc On-Demand Distance Vector, Secure Routing Protocol, Datagram Transport Layer Security та Optimized Link State Routing. Кожен з цих протоколів має свої переваги та недоліки, що впливають на вибір відповідного рішення для конкретних задач, таких як забезпечення надійності маршрутизації, захисту даних та оптимізації ресурсів.

**Ad-Hoc On-Demand Distance Vector —** це один з найбільш вживаних протоколів маршрутизації для безпровідних Ad-Hoc мереж. AODV забезпечує динамічну маршрутизацію, що дозволяє БПЛА ефективно обмінюватися даними в умовах змінної топології мережі [2]. Основний принцип роботи цього протоколу полягає в тому, що маршрути створюються за запитом, лише тоді, коли це необхідно, що дозволяє зменшити витрати ресурсів. Алгоритм AODV працює за такою схемою:

1. Вузол хоче надіслати дані до іншого вузла, він створює запит на маршрутизацію (RREQ) і передає його через сусідні вузли. Запит містить ідентифікатор джерела, ідентифікатор цілі та інші параметри.
2. Кожен вузол, який отримує RREQ, перевіряє, чи має він вже маршрут до цільового вузла. Якщо маршруту немає, вузол повторно передає RREQ далі.
3. Запит досягає цільового вузла, він створює відповідь (RREP), яка повертається через той же шлях до джерела. Це дозволяє джерелу знати, через які вузли слід передавати дані.
4. Протокол постійно оновлює маршрути в міру зміни топології мережі, гарантуючи, що вузли мають актуальну інформацію про доступні маршрути.
5. Якщо вузол не отримує підтвердження про доставлення даних протягом певного часу, він може видалити застарілі маршрути, що допомагає зберегти ресурси [3].

Візуалізацію алгоритму AODV зображено на рисунку 1.

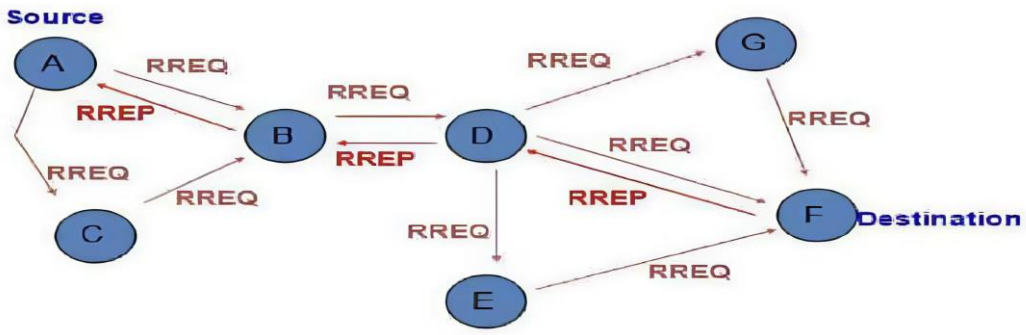


Рисунок 1 – Візуальна інтерпретація алгоритму AODV.

Однією з головних переваг AODV є його здатність динамічно створювати маршрути тільки за потреби, що значно зменшує навантаження на мережу та оптимізує використання ресурсів. Проте цей протокол має кілька суттєвих недоліків:

- AODV може створювати затримки при ініціалізації маршруту, оскільки він створюється на вимогу.
- Протокол є менш ефективним у мережах з великою кількістю вузлів через можливі збої у маршрутизації та широкомовні запити.

- Чутливий до частих змін у топології мережі, що може призводити до необхідності повторної маршрутизації та втрати даних під час зміни маршруту.

**Secure Routing Protocol** – це протокол, призначений для забезпечення безпечної маршрутизації в ad-hoc мережах, таких як мережі безпілотних літальних апаратів (БПЛА) [4]. Його головна мета – захист від атак та забезпечення надійної передачі даних між вузлами мережі. Алгоритм працює за таким принципом:

1. Генерує запит маршруту (Route Request або RREQ), який містить ідентифікатори джерела, призначення, а також криптографічний підпис для аутентифікації запиту, щоб інші вузли могли переконатися, що запит справжній.
2. Кожен вузол, що отримує цей запит, перевіряє підпис, щоб переконатися, що він походить від авторизованого вузла і що запит не було підроблено. Це допомагає захистити мережу від атаки, де зловмисник може спробувати створити фальшивий маршрут.
3. Запит поширюється мережею, доки не досягає вузла призначення або вузла, що знає шлях до призначення. Вузол, що отримав запит, також може бути проміжним вузлом, який має знання про шлях до кінцевого призначення.
4. Коли вузол призначення або вузол із відомим шляхом отримує запит маршруту, він генерує відповідь (Route Reply або RREP), яка відправляється назад до джерела. Відповідь також підписується криптографічно для забезпечення її достовірності. Це дозволяє джерелу впевнитися, що відповідь дійсно надійшла від призначеного вузла і що маршрут не був скомпрометований.
5. Після встановлення маршруту дані, які передаються між вузлами, шифруються, забезпечуючи їхню конфіденційність під час транспортування. Це унеможливлює перехоплення даних третіми сторонами.

На рисунку 2 зображено принцип роботи алгоритму.

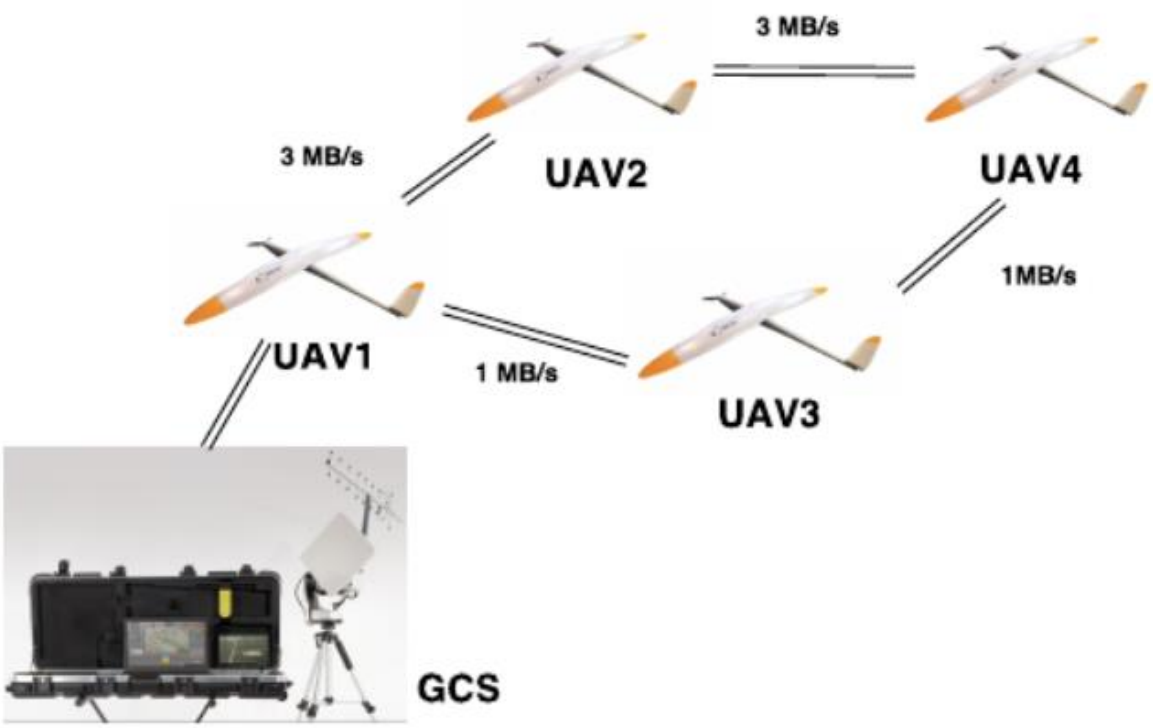


Рисунок 2 – Візуальна інтерпретація Secure Routing Protocol

Переваги Secure Routing Protocol:

- Забезпечує надійний захист маршрутизаційних повідомлень шляхом використання криптографічних методів, що знижує ризик несанкціонованого втручання або атаки на дані.
- Активно протидіє атакам, де зловмисники намагаються перехопити або змінити маршрутизаційну інформацію між вузлами.
- Завдяки механізму аутентифікації вузлів, SRP знижує ризики, пов'язані з проникненням зловмисних елементів у мережу.

Проте, SRP має певні обмеження:

- У великих мережах, з численними вузлами, може виникнути складність у підтримці високого рівня безпеки без зниження продуктивності.
- Складність управління ключами може ускладнювати підтримку протоколу в умовах динамічних або швидкозмінних мереж.

**Datagram Transport Layer Security –** це протокол, що забезпечує захист даних при їх передачі в ненадійних мережах, таких як UDP. На відміну від стандартного TLS, який працює поверх протоколу TCP, DTLS дозволяє шифрувати й автентифікувати пакети в мережах, де не гарантується послідовна доставка або контроль помилок. Алгоритм працює за наступною схемою:

1. На початковому етапі встановлюється захищене з'єднання між клієнтом і сервером, подібне до TLS.
2. Пакети передаються з використанням шифрування для забезпечення конфіденційності та захисту від модифікацій.
3. У разі втрати пакетів або їх дублювання протокол DTLS коригує передачу даних, не порушуючи основного з'єднання.

Особливістю DTLS є те, що він зберігає високий рівень безпеки, властивий TLS, але дозволяє працювати у мережах з меншою надійністю передачі даних, таких як UDP [5].

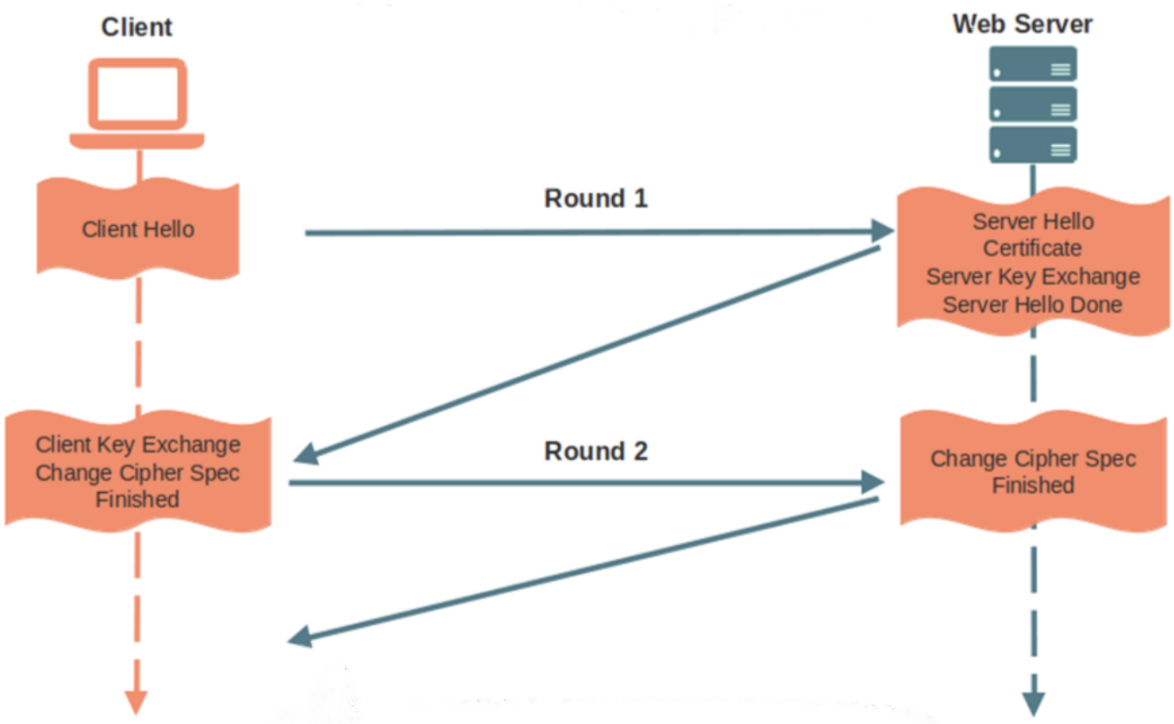


Рисунок 3 – Візуальна інтерпретація Datagram Transport Layer Security

Переваги Datagram Transport Layer Security:

- Забезпечує конфіденційність і цілісність даних у ненадійних мережах, таких як UDP, де не гарантується доставка або правильна послідовність пакетів.
- Підтримує шифрування даних і автентифікацію, що значно знижує ризик перехоплення або модифікації переданих пакетів.
- Працює в реальному часі, завдяки чому DTLS підходить для застосувань, де важлива мінімальна затримка, як у мультимедіа-стримінгу або в системах управління БПЛА.

Проте, DTLS має певні обмеження:

- Обробка втрат пакетів може спричиняти затримки, особливо у високонавантажених мережах, де часті втрати пакетів можуть вимагати додаткового відновлення зв'язку.
- Потребує налаштування параметрів тайм-аутів і повторних передач для уникнення проблем з продуктивністю в умовах нестабільних мереж.

**Optimized Link State Routing** — це протокол для маршрутизації в бездротових mesh-мережах, який особливо ефективний для великих та динамічних мереж. OLSR використовує проактивний підхід, що означає, що маршрути між вузлами завжди підтримуються актуальними, незалежно від того, чи необхідні вони цієї миті [6]. Основні принципи роботи OLSR включають:

1. OLSR періодично передає інформацію про стан зв'язків між вузлами через всю мережу, що дозволяє кожному вузлу мати повну картину топології мережі.
2. Один із ключових механізмів оптимізації в OLSR — це використання MPR. Кожен вузол вибирає підмножину сусідніх вузлів, через які він передає свої контрольні повідомлення. Це знижує обсяг контрольного трафіку і дозволяє зменшити затримки у великій мережі.
3. OLSR постійно оновлює таблиці маршрутизації, щоб всі вузли мали актуальну інформацію про оптимальні маршрути для передачі даних. Цей підхід забезпечує швидку реакцію на зміни в топології мережі, такі як зміни у розташуванні або втрати вузлів.

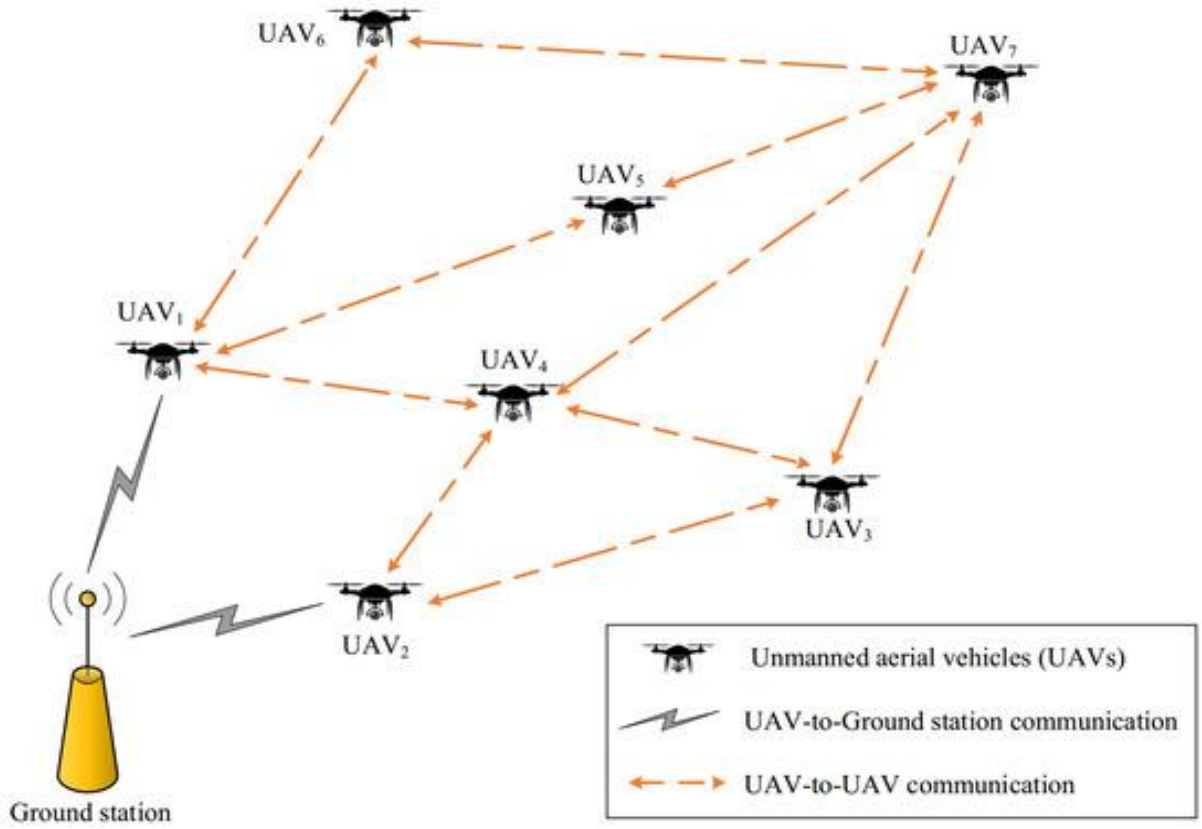


Рисунок 4 – Візуальна інтерпретація Optimized Link State Routing

Переваги OLSR:

- Завдяки постійному оновленню таблиць маршрутизації, вузли завжди мають актуальні маршрути, що мінімізує затримки при передачі даних.
- Використання MPR значно зменшує кількість контрольних повідомлень, що покращує масштабованість протоколу в великих мережах.
- OLSR добре підходить для мереж з великою кількістю вузлів, зокрема для динамічних мереж БПЛА, де топологія постійно змінюється.

Недоліки OLSR:

- У невеликих мережах або мережах зі статичною топологією обсяг контрольного трафіку може бути занадто великим відносно обсягу корисного трафіку.
- OLSR не має вбудованих механізмів безпеки, тому в реальних умовах застосування може потребувати додаткових методів захисту, таких як шифрування або аутентифікація вузлів.

## Висновки

Було розглянуто кілька ключових протоколів для забезпечення безпечної комунікації в мережах, таких як AODV, SRP, DTLS та OLSR. У процесі роботи було детально проаналізовано їхні особливості, переваги та обмеження, а також потенційні сфери застосування.

AODV є надійним рішенням для динамічних мереж, забезпечуючи ефективну маршрутизацію з мінімальним обміном повідомленнями, що робить його оптимальним вибором для великих та мінливих мереж. Однак, його схильність до перевантаження внаслідок частих оновлень маршрутів є значним обмеженням.

SRP продемонстрував свою здатність забезпечувати безпечну маршрутизацію за допомогою криптографічних методів і механізмів аутентифікації вузлів, що робить його ідеальним для мереж із високими вимогами до безпеки. Проте, складність управління ключами та підтримання безпеки в великих мережах може знижувати його продуктивність.

DTLS, у свою чергу, пропонує надійний механізм для забезпечення безпеки даних у ненадійних мережах, таких як UDP. Його здатність працювати в реальному часі та підтримувати шифрування робить його важливим інструментом для застосувань із мінімальними затримками. Однак, необхідність налаштування параметрів для уникнення затримок в умовах високих навантажень може бути викликом для впровадження.

OLSR, на відміну від інших протоколів, оптимізує маршрутизацію в великих мережах, знижуючи кількість обміну контрольними повідомленнями завдяки використанню оптимізованих алгоритмів. Цей протокол дозволяє забезпечити стабільну та ефективну маршрутизацію в умовах швидкої зміни топології, що є важливим для великих та динамічних мереж, таких як БПЛА. Проте, високі вимоги до обчислювальних ресурсів можуть стати обмеженням при впровадженні в мережах з низькою пропускною здатністю.

Таким чином, вибір відповідного протоколу має ґрунтуватися на специфіці завдання та вимогах до безпеки та продуктивності мережі. Кожен із протоколів пропонує унікальні рішення для різних викликів, і розуміння їхніх переваг та обмежень є важливим для досягнення оптимальних результатів у побудові сучасних безпечних мереж.

## СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ


1. Gupta, S., & Kumar, P. Secure Routing Techniques for UAV Networks: A Survey. In Proceedings of the 2021 International Conference on Signal Processing and Communication (ICSPC), 2021.
2. Perkins, C. E., & Royer, E. M. Ad-hoc On-Demand Distance Vector Routing. In Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications. IEEE, 1999.
3. Perkins, C. E., Belding-Royer, E., & Das, S. R. Ad hoc On-Demand Distance Vector (AODV) Routing. RFC 3561, 2003.
4. Papadimitratos, P., & Haas, Z. Secure Routing for Mobile Ad hoc Networks. In Proceedings of the SCS Communication Networks and Distributed Systems Modeling and Simulation Conference, 2002.
5. Rescorla, E., & Modadugu, N. Datagram Transport Layer Security (DTLS) Protocol Version 1.2. RFC 6347. Internet Engineering Task Force (IETF), 2012.
6. Alsalami, O. M., Yousefpoor, E., Hosseinzadeh, M., & Lansky, J. (2024). A Novel Optimized Link-State Routing Scheme with Greedy and Perimeter Forwarding Capability in Flying Ad Hoc Networks. *Mathematics*, 12(7), 1016. https://doi.org/10.3390/math12071016



***Проценко Михайло Ігорович*** — аспірант кафедри АІІТ, факультет інтелектуальних інформаційних технологій та автоматизації, Вінницький національний технічний університет, Вінниця, e-mail: mishagg45@gmail.com

***Маслій Роман Васильович*** – доцент кафедри АІІТ, Вінницький національний технічний університет, Вінниця, e-mail: maslij.r.v@vntu.edu.ua

**M. I. Protsenko**
**R. V. Maslii**

# Communication protocols for secure data exchange between UAVs in a distributed system

**Vinnytsia National Technical University**

***Abstract.***

*With the development of unmanned aerial vehicle (UAV) technologies and the increasing need to use them to collect and share data in real time, an important challenge arises to ensure reliable and secure communication between UAVs in distributed systems. With increasing demands on data security and the speed of information exchange, secure data exchange is becoming critical to the effective execution of various operations, such as joint reconnaissance, monitoring, or search missions. That is why communication protocols for such networks must ensure reliable data transmission, resistance to hacking and cyberattacks, and optimization of UAV resources to maximize efficiency and energy savings. The main aspects affecting the effectiveness of such systems are the reliability of data transmission, protection against hacking and attacks, and flexibility in the event of dynamic changes in operating conditions. This paper investigates the most advanced communication protocols for secure data exchange between UAVs, such as Ad-Hoc On-Demand Distance Vector (AODV), which allows dynamic routing in a changing network topology, and Secure Routing Protocol (SRP), which provides secure data transmission through authentication of network participants. In addition, the author discusses the Datagram Transport Layer Security (DTLS) protocol, which provides data encryption even in unreliable networks, and Optimized Link State Routing (OLSR), which optimizes routing in large networks and ensures reliable data transmission in complex environments. Security mechanisms, such as node authentication, which identifies each device in the network, and data encryption, which prevents intruders from accessing confidential information, are analyzed separately. Protection against DoS attacks ensures that the system is resistant to overload and loss of communication. This approach to building a communication system allows UAVs to be used efficiently and safely to carry out missions in difficult conditions, ensuring their reliability and durability even in the event of a failure of individual network components. The introduction of new technologies and approaches to organizing data transmission between drones can significantly expand the capabilities of UAVs, which is an important step in the development of this industry.*

***Keywords:*** *unmanned aerial vehicles, distributed systems, secure data exchange, communication protocols, routing, encryption, authentication, Ad-Hoc networks.*

***Protsenko Mykhailo I.*** — Department of Intelligent Information Technologies and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: mishagg45@gmail.com

***Maslii Roman V.*** – associate professor at the Department of AIIT, Vinnytsia National Technical University, Vinnytsia, email: maslij.r.v@vntu.edu.ua