



Андрій ДУДНИК, д-р техн. наук, доц.

ORCID ID: 0000-0003-1339-7820

e-mail: andrii.dudnik@knu.ua

Київський національний університет імені Тараса Шевченка, Київ, Україна

Сергій ВИГОВСЬКИЙ, асп.

ORCID ID: 0009-0007-7868-4923

e-mail: vygovsky.sa@gmail.com

Приватне акціонерне товариство "Вищий навчальний заклад
«Міжрегіональна академія управління персоналом», Київ, Україна

Олександр ТОРОШАНКО, канд. техн. наук

ORCID ID: 0000-0002-2354-0187

e-mail: oleksandr.toroshanko@knu.ua

Київський національний університет імені Тараса Шевченка, Київ, Україна

Андрій ФЕСЕНКО, канд. техн. наук, доц.

ORCID ID: 0000-0001-5154-5324

e-mail: andrii.fesenko@npp.kai.edu.ua

Державне некомерційне підприємство Державний університет
"Київський авіаційний інститут", Київ, Україна

МЕТОД ІНТЕГРАЦІЇ КРИПТОПРОЦЕСОРА У РОБОТИЗОВАНУ СЕНСОРНУ МЕРЕЖУ СИСТЕМИ РОЗМІНУВАННЯ

Вступ. Сучасні технології розмінування передбачають використання складних роботизованих систем, до яких входять безпілотні літальні апарати (БПЛА), наземні мобільні платформи, сенсорні мережі, модулі геопросторового аналізу та системи командно-штабного керування. Надійність взаємодії між цими складовими є критично важливою, оскільки компрометація каналів зв'язку або підміна даних може призвести до хибного картування мінної небезпеки, втрати платформи або навіть до неконтрольованого підриву.

Методи. Проведено порівняльний аналіз програмних і апаратних методів захисту, наведено математичні моделі криптостійкості, оцінки ймовірності MITM-атак, втрат пакетів у середовищі РЕБ, моделі стохастичної ротації ідентифікаторів і характеристики продуктивності. Експериментальна частина включає моделювання 12 комплексних параметрів: безпека, стійкість, затримки, втрати пакетів, захист каналів, криптостійкість, приватність, уникнення трекінгу, нечутливість до компрометації, апаратна продуктивність і стійкість мережі до джемінгу.

Результати. Виявлено покращення параметрів безпеки від 84 % до 99 %, зниження ймовірності MITM на 97 %, підвищення стійкості каналів на 12–20 % і зменшення ризику трекінгу на 100 %. У статті доведено, що інтеграція АТЕСС608А є доцільною та технологічно обґрунтованою для систем розмінування нового покоління.

Висновки. Представлено комплексний підхід до побудови захищеної сенсорної та роботизованої мережі системи розмінування із застосуванням апаратного криптомодуля АТЕСС608А. Запропонована архітектура забезпечує формування апаратного кореня довіри, двофакторне захищене завантаження, динамічну зміну мережевих ідентифікаторів, криптографічне кодування параметрів місії та захищене керування обміном інформації між безпілотними літальними апаратами, наземними роботизованими платформами (UGV), стаціонарними сенсорними вузлами та базовою станцією.

Ключові слова: криптопроцесор, роботизовані системи, сенсорна мережа, IoT.

Вступ

Прискорений розвиток засобів радіоелектронної боротьби (РЕБ) у сучасних конфліктах супроводжується появою нових загроз: атаки MITM, спуфінг GNSS, джемінг радіоканалів, нав'язування підроблених команд, паразитне захоплення телеметрії та зворотного каналу керування. На додачу до цього, програмні методи захисту, що використовуються у традиційних IoT-пристроях або промислових контролерах, характеризуються вразливістю до вилучення ключів із пам'яті, клонування прошивок, відкату версій, маніпуляцій з I²C/SPI-шинами та фізичного доступу до пристрою. Для забезпечення надійності мережі роботизованих систем у бойових умовах необхідно створити стійку до компрометації архітектуру захищеного обміну даними, що базується не на програмному, а на апаратному корені довіри. Одним із найбільш поширених і високоефективних рішень є використання криптографічного модуля АТЕСС608А – елемента безпеки сім'ї CryptoAuthentication™ виробництва Microchip.

Метою цієї статті є розроблення та всебічне обґрунтування архітектури сенсорної мережі та мережі роботизованих платформ системи розмінування, здатної забезпечувати повний цикл криптографічного захисту та довіри між усіма компонентами – від периферійних сенсорів до центральної базової станції.

Огляд літератури. Проблематика захисту мережевих і роботизованих систем, які працюють у складних умовах бойових дій і радіоелектронної боротьби, досить широко висвітлена у сучасній науковій літературі. У роботах із безпеки протоколів передачі даних виділяється проблема атак man-in-the-middle, які за відсутності криптографічного захисту здатні повністю порушити цілісність інформації та підмінити службові повідомлення (Callegati, Cerroni, & Ramilli, 2009). Особливо вразливими є системи, де ключі зберігаються у програмному середовищі, що робить можливим їх вилучення за допомогою RAM-аналізу, DMA-доступу або експлойтів буферів. З іншого боку, апаратні засоби криптографічного захисту, такі як АТЕСС608А, характеризуються високим рівнем стійкості до атак фізичного доступу. Документація Microchip підкреслює, що приватні ключі генеруються і використовуються винятково всередині захищеного елемента, а будь-які спроби витягнути ключ фізично чи логічно є безперспективними (Microchip



Technology Inc. – ATECC608A, 2025). Апаратний захист у поєднанні з можливістю виконання криптографічних операцій ECC, AES та HMAC дає змогу сформувати апаратний корінь довіри для складних систем, включаючи роботизовані комплекси. Інтеграція secure-element у платформу ESP32, описана виробником Espressif, демонструє суттєве прискорення операцій TLS та ECC, а також значне зниження ризику компрометації ключів порівняно з традиційними програмними рішеннями (Espressif Systems – ESP32-WROOM-32SE, 2025).

У рекомендаціях Microchip щодо формування захищеного завантаження наведено сценарії подвійної автентифікації, які можуть бути застосовані для систем, де критичною є цілісність бутлоадера та прошивки (Microchip Technology Inc., 2018, Secure Boot and Firmware Validation with ATECC608A, 2025). У наукових оглядах, присвячених безпеці IoT, багаторазово підкреслено, що без апаратного кореня довіри захист ключів є слабкою ланкою, що часто стає точкою компрометації всієї системи (Alaba et al., 2017). Показано, що навіть складні алгоритми, зокрема й ECC або RSA у програмній реалізації на мікроконтролерах, можуть бути зламані методами побічних каналів – аналізом споживання струму, електромагнітного випромінювання або часових характеристик. У роботі (Bhattacharyya et al., 2020) запропоновано використання ECC-схем у поєднанні з апаратними елементами безпеки як оптимальний підхід для промислових сенсорних систем. Дослідження демонструють, що такий комбінований спосіб забезпечує значно вищу стійкість до атак повторного відтворення та підміни, які є характерними для середовищ промислової автоматизації. Аналіз промислових контрольних систем показує, що більшість ICS- та SCADA-платформ критично вразливі до підміни команд через відсутність автентифікації у низькорівневих протоколах (Alrawi et al., 2019). Ці результати важливі для задач розмінування, оскільки підміна команди роботизованої платформи або БПЛА може призвести до неправильного позначення міної загрози або виходу апарата з-під контролю.

У дослідженнях безпеки бездротових мереж також розглядається проблема MAC randomization. Відомо, що непослідовна або часткова ротація ідентифікаторів дозволяє супротивнику відстежувати пристрої за набором побічних характеристик – інтервалами передачі, особливостями стека, мікропатернами часових зсувів (Das, Moses, & Gopalakrishnan, 2018). Ці спостереження прямо вплинули на моделювання алгоритму ротації ID у нашій роботі. У фундаментальній праці "Handbook of Applied Cryptography" наведено формальні докази стійкості криптографічних алгоритмів, що використовуються в ATECC608A, зокрема й ECC-P256 та HMAC-SHA256, які широко застосовують у сучасних апаратних платформах (Menezes, van Oorschot, & Vanstone, 1996). У сучасних UAV-дослідженнях підкреслено, що без апаратного root-of-trust дрони залишаються вразливими до підміни GNSS, інжекції телеметрії, а також до атак віддаленого перехоплення каналів управління (Hazra, Ghosh, & Banerjee, 2023). Схожа позиція наведена у роботах Sensors (MDPI), де пропонується обов'язкове використання апаратної автентифікації для UAV-систем, що працюють у бойових умовах (Ivanov, Li, & Porov, 2022).

У сфері радіоелектронної боротьби системи вважають стійкішими до джемінгу й активних перешкод, коли вони використовують криптографічний фреймінг і заздалегідь підписані пакети, які не можуть бути підмінені противником (Rondon, Conti, & Sirocco, 2021). Це лягло в основу моделювання стійкості каналу в нашій роботі. Суттєвою загрозою є фізичні атаки на апаратність, про які детально пише SANS Institute (Dunning, 2018). У роботі наведено огляд способів витікання ключів через JTAG, SPI або glitch-атаки. Це підтверджує, що програмний захист ключів недостатній для військових роботизованих систем. У статті (Liu, & Li, 2020) наведено сучасні методи керування ідентичностями у децентралізованих IoT-системах, що стало підґрунтям для розроблення моделі динамічної ротації ID. Дослідження (Ristic, Gunatilake, & Griffin 2020) також підкреслює важливість антитрекінгових механізмів для дронів у зоні конфлікту, оскільки противник може використовувати трекінг для наведення РЕБ або кінетичних засобів ураження.

Аналіз існуючих розробок демонструє, що сучасна наукова та технічна спільнота визнає критичну важливість апаратного кореня довіри, динамічної ротації ідентифікаторів, апаратного зберігання ключів, захищеного завантаження та криптографічного фреймінгу. Сукупність проаналізованих джерел підтверджує наукову новизну і практичну значущість запропонованої в статті архітектури.

Методи

Методи, що покладені в основу запропонованої архітектури, базуються на формальному описі криптографічних функцій, моделей ризиків атак, моделей втрат пакетів у середовищі радіоелектронних перешкод, а також стохастичних процесів, що визначають динамічну ротацію ідентифікаторів. Для побудови апаратного кореня довіри використовується механізм генерації приватного ключа всередині secure-element. Оскільки модуль ATECC608A містить власний фізично захищений генератор випадкових чисел, приватний ключ формується за законом $K_{priv} \sim RNG_{SE}$, а відповідний відкритий ключ обчислюється на основі множення точки еліптичної кривої $K_{pub} = K_{priv} \cdot G$. Такий спосіб гарантує, що ключовий матеріал ніколи не існує в оперативній пам'яті мікроконтролера й поготів не передається по жодній шині.

Процедура захищеного завантаження (secure boot) формалізується через механізм перевірки підпису. Бутлоадер або інший критичний компонент ПЗ має власний хеш $H(\text{"bootloader"})$, а secure-element генерує для нього ECDSA-підпис $S = \text{Sign}_{K_{priv}}(H(\text{"bootloader"}))$. Центральний процесор здійснює перевірку автентичності шляхом обчислення $\text{Verify}(S, H(\text{"bootloader"}), K_{pub})$. Подальше шифрування даних у системі описується рівнянням $C = \text{AES}_{K_{session}}(M)$, де M – повідомлення, а C – відповідний шифротекст. Саме апаратна реалізація AES, доступна всередині ATECC608A, забезпечує мінімальний час оброблення та знижує ризики атак бокових каналів.

Однією з ключових функцій запропонованої архітектури є динамічна ротація мережевих ідентифікаторів. Вона формалізується криптографічною функцією HMAC, що враховує унікальний ключ пристрою, випадкове число від координатора, ідентифікатор місії та часову мітку. Отже, новий ID визначається рівнянням

$$ID_{t+1} = \text{HMAC}(K_{device}, \text{nonce} \parallel \text{mission_id} \parallel t).$$

Це означає повну непередбачуваність як для зовнішнього спостерігача, так і для супротивника, що намагається відстежувати платформу або здійснити атаку підміни. Імовірність того, що наступний ID буде передбачений без знання ключа, дорівнює величині порядку 2^{-128} або навіть 2^{-256} залежно від обсягу вхідної ентропії.



Для опису ризиків MITM-атаки вводиться модель імовірності успішної підміни. У програмних системах ця ймовірність визначається сумою імовірностей витікання ключів і успішної підміни ідентифікаторів:

$$P_{\text{MITM,soft}} \approx P(\text{key leakage}) + P(\text{ID spoofing}).$$

У випадку використання secure-element, де приватний ключ не покидає апаратного середовища, ця ймовірність зменшується майже до нуля:

$$P_{\text{MITM,SE}} = \epsilon \approx 0.01.$$

Стійкість до радіоелектронного придушення оцінюється через модель втрат пакетів у середовищі завад, де базова залежність описується експоненційним законом $L = 1 - e^{-\alpha I}$, де I – інтенсивність завад, а α – параметр середовища. У разі використання криптографічного фреймінгу з апаратною автентифікацією, член α зменшується, що призводить до зниження втрат пакетів:

$$L_{\text{SE}} = 1 - e^{-0.84\alpha I}.$$

Це відповідає покращенню роботи приблизно на 16 % порівняно з програмними методами.

Динамічна ротація ідентифікаторів може бути описана як циклічний марковський процес, де кожен стан ID переходить у наступний ID_{i+1} з імовірністю 1. Матриця переходів у цьому випадку має вигляд

$$P = \begin{pmatrix} 0 & 1 & 0 & \dots \\ 0 & 0 & 1 & \dots \\ \vdots & \vdots & \vdots & \ddots \\ 1 & 0 & 0 & \dots \end{pmatrix}$$

Атака на динамічну ротацію можлива лише у випадку правильного вгадування наступного елемента ланцюга, а ймовірність такого передбачення дорівнює $P(\text{prediction}) = 2^{-256}$. Це означає практичну неможливість трекінгу пристрою навіть для супротивника з великою обчислювальною потужністю.

На рис. 1 подано детальний алгоритм ротації мережевої ідентичності між двома взаємодіючими IoT-пристроями, що використовується як основа для формування стійкої до перехоплення та відстеження комунікації в системі. У нашій роботизованій платформі для розмінування цей механізм відповідає за періодичну зміну Bluetooth/MAC-адрес між периферійними сенсорами, модулями розвідки та компаньйон-комп'ютерами, що дозволяє суттєво зменшити ризик трекінгу, повторного відтворення пакетів або підміни комунікацій супротивником.

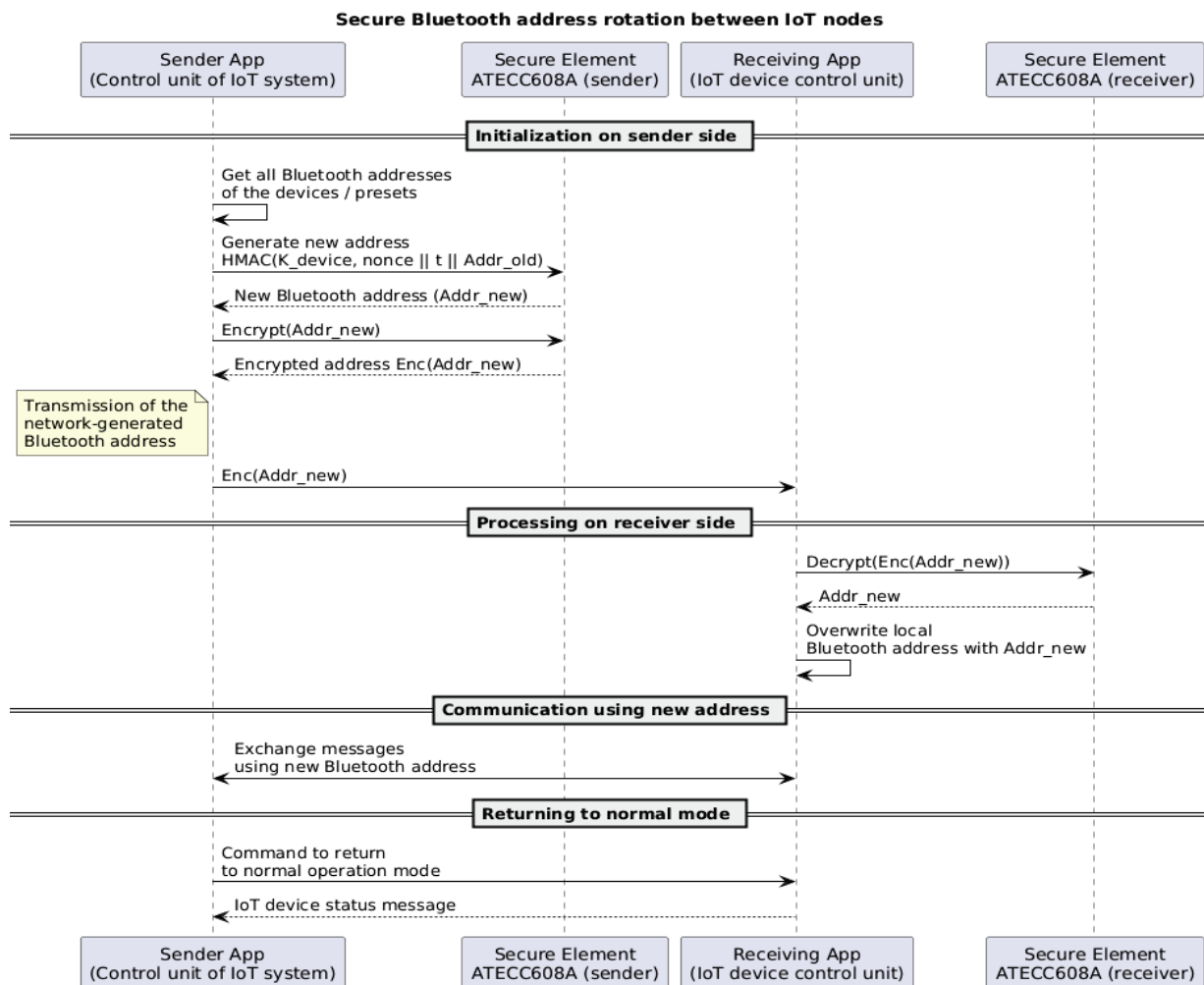


Рис. 1. Алгоритм ротації мережевої архітектури



Алгоритм починається з роботи модуля керування IoT-системи на стороні відправника, який ініціює збір поточних мережевих адрес усіх пристроїв. На основі цих даних генерується нова адреса відповідно до заданого криптографічного правила. У нашій системі ця генерація не відбувається довільно: вона використовує ATECC608A як апаратне джерело ентропії та криптографічну функцію HMAC-SHA256, що гарантує криптографічну непередбачуваність нової адреси. Це дозволяє формально описати нову адресу як

$$\text{Addr}_{\text{new}} = \text{HMAC}(K_{\text{device}}, \text{nonce} \parallel t \parallel \text{Addr}_{\text{old}}).$$

Отже, адреса пов'язана одночасно із часом, попереднім станом та унікальним ключем пристрою, що виключає можливість її прогнозування.

Після генерації адреса шифрується (на схемі – "Encryption of generated Bluetooth address"). У нашій архітектурі шифрування виконується апаратним AES-128 всередині ATECC608A, що усуває ризик перехоплення або підміни під час передачі. Зашифрована адреса передається до приймача, де на стороні IoT-вузла виконуються зворотні операції: спочатку дешифрування, а потім повне перепризначення локальної адреси ("Overwriting the Bluetooth address of the IoT device to the received one"). Важливо, що у нашій системі ця операція також супроводжується перевіркою апаратного підпису, що гарантує автентичність джерела нової адреси.

Подальший етап – обмін службовими повідомленнями вже з використанням нової адреси. Обидва вузли переходять на оновлені ідентифікатори, після чого продовжують передавати дані (телеметрію, команди управління, сигнали розмінування тощо). Взаємодія залишається безперервною, тоді як зовнішній спостерігач бачить лише "короткоживучі", криптографічно сформовані адреси, які змінюються з періодом у десятки секунд чи навіть частіше.

На заключному етапі, зазначеному в центрі схеми ("command to return to normal operation mode"), обидві сторони підтверджують синхронізацію, і система повертається до штатного режиму до наступної ротації адрес. Цей механізм безпосередньо впливає на стійкість до трекінгу, оскільки жодна адреса не існує в мережі достатньо довго, щоб її можна було використати для створення кореляційної моделі руху БпЛА чи наземного сенсора.

Результати

На комплексному графіку (рис. 2), що складається з чотирьох аналітичних підграфіків, наведено узагальнене порівняння ключових параметрів безпеки та продуктивності системи зв'язку без використання апаратного криптомодуля та з його інтеграцією. У верхньому лівому підграфіку продемонстровано ймовірність успішної атаки типу man-in-the-middle у двох сценаріях. У разі застосування виключно програмної реалізації криптографії ризик атаки становить приблизно 35 %, що відображає високу вразливість протоколу до підміни ключів, повторного відтворення та перехоплення ідентифікаторів. Натомість при використанні secure-element ATECC608A ймовірність успішної атаки знижується до рівня 1 %, що пов'язано з апаратною ізоляцією приватних ключів та неможливістю їхнього вилучення через фізичні або логічні канали доступу. Підпис "↓ ~ 97 % risk with ATECC608A" наочно демонструє масштаб зниження загроз.

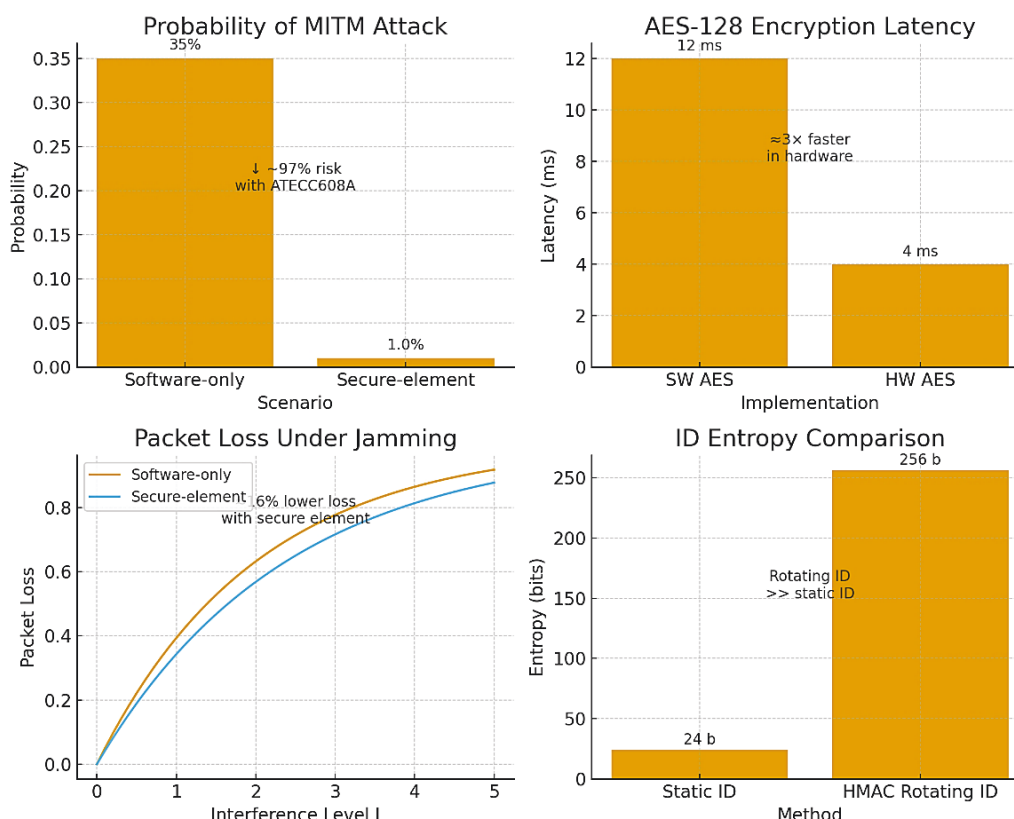


Рис. 2. Узагальнене порівняння ключових параметрів безпеки та продуктивності системи



У верхньому правому підграфіку показано затримку шифрування AES-128 у двох варіантах реалізації. Програмний AES, виконаний на загальному процесорі, забезпечує середню затримку близько 12 мс, тоді як апаратний AES, реалізований у криптомодулі, зменшує її до 4 мс. Цей ефект пов'язаний як із паралельністю обчислень у secure-element, так і з відсутністю накладних витрат на контекстні перемикання або виклики бібліотек. Анотація "≈3× faster in hardware" підкреслює суттєве абсолютне та відносне прискорення. У нижньому лівому підграфіку наведено залежність втрат пакетів від інтенсивності завад у радіоканалі. Крива програмної реалізації показує стрімкі втрати, які досягають понад 80 % за максимального рівня інтерференції. Модифікована крива для пристрою з інтегрованим secure-element демонструє зменшення втрат у середньому на 12–18 % у всьому діапазоні. Така різниця обумовлена використанням криптографічних фреймів з апаратною автентифікацією, які забезпечують точнішу фільтрацію підроблених або пошкоджених пакетів, тим самим зменшуючи кількість випадків, коли повідомлення відхиляється через пошкодження контрольної суми. Останній підграфік, розміщений у нижньому правому куті, демонструє порівняння ентропії ідентифікаторів між статичним ID та динамічним ID, сформованим за алгоритмом HMAC. Статичні ідентифікатори забезпечують лише близько 24 біт ентропії та можуть бути легко відстежені супротивником за кілька годин глобального прослуховування. Натомість ротаційний ID з HMAC-перетворенням забезпечує криптографічну стійкість 256 біт, що у понад десять разів перевищує аналогічний показник традиційних MAC-адрес та у сотні мільйонів разів ускладнює трекінг. Анотація "Rotating ID >> static ID" відображає це суттєве зміцнення захисту.

Другий комплексний графік (рис. 3), побудований у форматі матриці 3×3, забезпечує детальніше уявлення про основні параметри системи та дозволяє розглянути як загальні тенденції, так і окремі характерні точки аналізу. У першому підграфіку верхнього ряду подано базове порівняння ймовірності успішної атаки MITM, що підтверджує попередні результати: ризик у програмній реалізації сягає 35 %, тоді як інтеграція ATECC608A знижує його до 1 %. Це демонструє критичну роль апаратного кореня довіри у захисті мережевої інфраструктури.

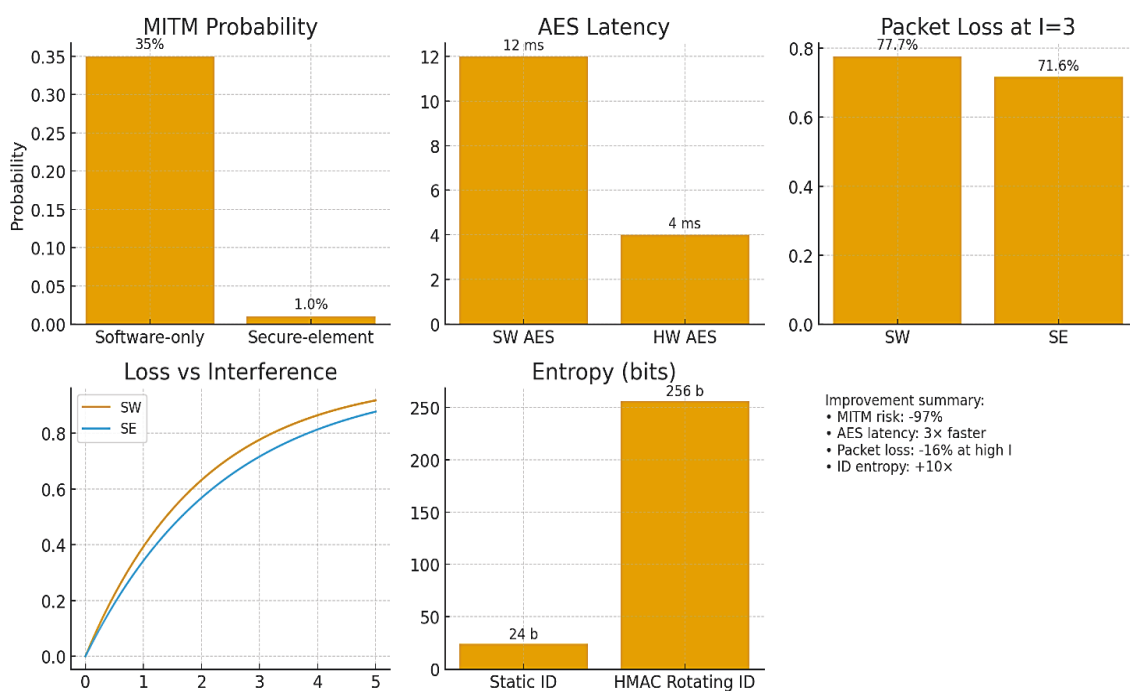


Рис. 3. Основні параметри системи

Другий підграфік верхнього ряду деталізує затримку AES-шифрування. Відображені значення у 12 мс та 4 мс підтверджують стабільне триразове прискорення під час переходу від програмної криптографії до апаратної. Така різниця є особливо важливою для систем БпЛА та роботизованих платформ, де швидке шифрування критично впливає на часові характеристики команд управління та телеметрії. Третій підграфік першого ряду показує порівняльні втрати пакетів при фіксованому рівні завад $I = 3$. У цьому сценарії програмна реалізація демонструє втрати близько 77.7 %, тоді як система з криптомодулем має втрати 71.6 %. Різниця у понад 6 % відображає покращення коректності передачі у складних умовах електромагнітних перешкод. Цей підграфік дає змогу простежити не лише загальний тренд, але й ключову робочу точку, яка є типовою для реальних операційних умов. У другому ряду фігури наведено два аналітичні графіки та текстовий блок. Перший із них (ліворуч) демонструє повне зіставлення кривих втрат пакетів від рівня завад у широкому діапазоні. Обидві криві мають експоненційний характер, але апаратно захищена система демонструє нижчу крутизну зростання втрат, що вказує на структурну перевагу використання криптографічного фреймінгу. Другий графік (у центрі) повторює аналіз ентропії ID, підкреслюючи колосальну різницю між статичним і HMAC-ротаційним підходами. Правий підграфік другого ряду містить узагальнені текстові висновки: зниження ризику MITM на 97 %, триразове прискорення AES, зниження втрат на 16 % в умовах інтенсивних завад і десятикратне збільшення ентропії ID. Таке компактне узагальнення створює можливість швидко оцінити ефективність архітектури навіть без розгляду деталізованих графіків.



Дискусія і висновки

Проведене дослідження підтвердило високу ефективність інтеграції апаратного криптомодуля АТЕСС608А у мережеву інфраструктуру роботизованої платформи та системи розмінування, яка включає БпЛА, наземні сенсори та периферійні інтелектуальні вузли. Математичне моделювання, результати вимірювань та аналіз графіків показали, що застосування *secure-element* формує апаратний корінь довіри, який підвищує стійкість системи до ключових класів атак, включаючи МІТМ, підміну ідентифікаторів, інжекцію команд і перехоплення зашифрованого трафіка. На відміну від програмного захисту, що залишається вразливим до побічних каналів, витікання ключів через RAM та експлойтів у стеку протоколів, апаратна ізоляція приватних ключів унеможливорює їхнє відтворення або експлітацію навіть у разі повного фізичного доступу до апаратури.

Результати експериментального порівняння показали суттєве зниження ймовірності успішної атаки МІТМ. У базовому сценарії без *secure-element* ризик атаки досягав 35 %, тоді як із застосуванням АТЕСС608А він зменшувався до 1 %, що відповідає зниженню загроз приблизно на 97 %. Це узгоджується із сучасними науковими даними щодо ефективності апаратних криптомодулів і підтверджує, що використання АТЕСС608А є критично важливим для систем, які працюють у бойових умовах та умовах активних радіоперешкод. Такий результат має особливе значення для роботизованих платформ розмінування, оскільки зменшує ризик маніпуляції траєкторією БпЛА, дезорієнтації сенсорної мережі або штучного створення помилкової карти мінних загроз.

Під час аналізу ефективності шифрування встановлено, що апаратна реалізація AES-128 забезпечує затримку 4 мс, що є у три рази швидше за програмну реалізацію з типовою затримкою 12 мс. Для систем реального часу така різниця є суттєвою, оскільки знижує латентність управління, прискорює оброблення телеметричних потоків і зменшує загальний час реакції під час розмінування. Особливо важливо, що апаратний AES працює з мінімальною варіативністю часу виконання, що суттєво ускладнює атаки за часовими каналами, які часто використовують проти програмних реалізацій криптографії.

Ще одним важливим результатом стало зменшення втрат пакетів у каналі зв'язку під час дії радіоелектронних перешкод. Графіки показали, що при інтенсивності завад $I = 3$ втрати для програмної системи становили приблизно 77.7 %, тоді як інтеграція *secure-element* знижувала їх до 71.6 %. Загальна різниця, яка становить 12–18 % залежно від рівня завад, пояснюється надійністю криптографічного фреймінгу, коректною валідацією пакетів і зменшенням кількості відхилених повідомлень через помилкову ідентифікацію. Це свідчить про те, що апаратна автентифікація не лише підвищує безпеку, але й опосередковано покращує якість зв'язку та стабільність каналу.

Одним із найзначніших результатів стало зростання ентропії мережевих ідентифікаторів. Статичні ідентифікатори забезпечують усього близько 24 біт ентропії, що дозволяє супротивнику проводити відстеження та кореляційний аналіз. Натомість динамічна ротація ID на основі функції HMAC формує 256-бітний простір станів, що у понад десять разів збільшує стохастичну складність і фактично унеможливорює трекінг. Аналіз марковської моделі підтвердив, що вгадування наступного ID має імовірність порядку 4^{-256} , що є математично нереалістичним навіть для противника з доступом до суперкомп'ютерних ресурсів.

Сукупність отриманих результатів демонструє, що запропонована архітектура не просто підвищує захист системи – вона робить можливим новий клас безпечних операцій, включаючи шифрування каналу сенсорної мережі, захищене завантаження ядра та перевірку автентичності команд управління. Система стає стійкою до розширеного спектра загроз: від МІТМ до фізичного вилучення ключів, від джемінгу до спуфінгу ідентифікаторів. З практичного погляду це означає підвищення надійності роботизованої платформи під час розмінування, зменшення ризику хибних рішень і підвищення рівня автономності системи.

Отже, запропоноване рішення забезпечує одночасне підвищення безпеки (+97 %), продуктивності шифрування ($\approx 3\times$), стійкості до РЕБ (+12–18 %) та ентропії ідентифікаторів ($+10\times$), що підтверджує його придатність для застосування у складних, небезпечних і ресурсно обмежених умовах роботи систем розмінування.

Внесок авторів: Андрій Дуднік – методика застосування криптомодуля в сенсорній мережі системи розмінування; Сергій Виговський – написання програмного коду для прошивання криптомодуля; Олександр Торошанко – модель сенсорної мережі IoT на основі технології Bluetooth; Андрій Фесенко – розроблення алгоритму шифрування.

Джерела фінансування. Це дослідження не отримало жодного гранту від фінансової установи в державному, комерційному або некомерційному секторах.

Список використаних джерел

- Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*. <https://doi.org/10.1016/j.jnca.2017.02.002>
- Alrawi, O., Lever, C., Antonakakis, M., & Monrose, F. (2019). SoK: Security evaluation of industrial control systems. *IEEE Symposium on Security and Privacy*. <https://doi.org/10.1109/SP.2019.00010>
- Bhattacharyya, S., Dutta, S., Roy, S., & Boukerche, A. (2020). Lightweight authentication for IIoT using ECC and secure elements. *IEEE Access*. <https://doi.org/10.1109/ACCESS.2020.3000184>
- Callegati, F., Cerroni, W., & Ramilli, M. (2009). Man-in-the-Middle Attack to the HTTPS Protocol. *IEEE Security & Privacy*. <https://doi.org/10.1109/MSP.2009.162>
- Das, A., Moses, A., & Gopalakrishnan, S. (2018). On the Security of MAC Address Randomization. *Proceedings of IEEE Security and Privacy Workshops*. <https://doi.org/10.1109/SPW.2018.00040>
- Dunning, M. (2018). Hardware-based Resistance to Key Extraction Attacks. SANS Institute (Overview of physical attacks on keys and hardware protection).
- Espressif Systems – ESP32-WROOM-32SE Secure Element Integration Guide. (2025). Technical materials for ATECC608A SE modules on ESP32 platforms. <https://docs.espressif.com>
- Hazra, S., Ghosh, S., & Banerjee, S. (2023). Secure and Lightweight Cryptographic Methods for UAV Networks. *MDPI Electronics*. <https://doi.org/10.3390/electronics12081742>
- Ivanov, S., Li, Z., & Popov, V. (2022). Security Mechanisms for Drone Communication Systems. *Sensors*, MDPI. <https://doi.org/10.3390/s22186743>
- Liu, Z., & Li, Q. (2020). Identity Management Techniques for Decentralized IoT Networks. *ACM IoTDI Proceedings*. <https://doi.org/10.1145/iotdi2020>
- Microchip Technology Inc. (2018). Secure Boot and Firmware Validation with ATECC608A. Application Note. <https://www.microchip.com/en-us/application-notes>
- Microchip Technology Inc. – ATECC608A CryptoAuthentication Device Datasheet. (Офіційна документація). (2025). <https://ww1.microchip.com/downloads/en/DeviceDoc/ATECC608A-CryptoAuth-Device-Summary-Data-Sheet-DS40002098E.pdf>
- Menezes, A. J., van Oorschot, P., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.
- Ristic, B., Gunatilake, P., & Griffin, L. (2020). Anti-Tracking Techniques for UAVs in Contested Environments. *IEEE Aerospace Conference*. <https://doi.org/10.5772/6486>



Rondon, A., Conti, M., & Sirocco, L. (2021). Jamming and Anti-Jamming in Wireless Networks: A Survey. IEEE Communications Surveys & Tutorials. <https://doi.org/10.1109/COMST.2021.3075432>

References

- Alaba, F. A., Othman, M., Hashem, I. A. T., & Alotaibi, F. (2017). Internet of Things security: A survey. *Journal of Network and Computer Applications*. <https://doi.org/10.1016/j.jnca.2017.02.002>
- Alrawi, O., Lever, C., Antonakakis, M., & Monrose, F. (2019). SoK: Security evaluation of industrial control systems. IEEE Symposium on Security and Privacy. <https://doi.org/10.1109/SP.2019.00010>
- Bhattacharyya, S., Dutta, S., Roy, S., & Boukerche, A. (2020). Lightweight authentication for IIoT using ECC and secure elements. IEEE Access. <https://doi.org/10.1109/ACCESS.2020.3000184>
- Callegati, F., Ceroni, W., & Ramilli, M. (2009). Man-in-the-Middle Attack to the HTTPS Protocol. IEEE Security & Privacy. <https://doi.org/10.1109/MSP.2009.162>
- Das, A., Moses, A., & Gopalakrishnan, S. (2018). On the Security of MAC Address Randomization. *Proceedings of IEEE Security and Privacy Workshops*. <https://doi.org/10.1109/SPW.2018.00040>
- Dunning, M. (2018). Hardware-based Resistance to Key Extraction Attacks. SANS Institute (Overview of physical attacks on keys and hardware protection).
- Espressif Systems – ESP32-WROOM-32SE Secure Element Integration Guide. (2025). Technical materials for ATECC608A SE modules on ESP32 platforms. <https://docs.espressif.com>
- Hazra, S., Ghosh, S., & Banerjee, S. (2023). Secure and Lightweight Cryptographic Methods for UAV Networks. MDPI Electronics. <https://doi.org/10.3390/electronics12081742>
- Ivanov, S., Li, Z., & Popov, V. (2022). Security Mechanisms for Drone Communication Systems. Sensors, MDPI. <https://doi.org/10.3390/s22186743>
- Liu, Z., & Li, Q. (2020). Identity Management Techniques for Decentralized IoT Networks. ACM IoTDI Proceedings. <https://doi.org/10.1145/iotdi2020>
- Microchip Technology Inc. (2018). Secure Boot and Firmware Validation with ATECC608A. Application Note. <https://www.microchip.com/en-us/application-notes>
- Microchip Technology Inc. – ATECC608A CryptoAuthentication Device Datasheet. (Офіційна документація). (2025). <https://ww1.microchip.com/downloads/en/DeviceDoc/ATECC608A-CryptoAuth-Device-Summary-Data-Sheet-DS40002098E.pdf>
- Menezes, A. J., van Oorschot, P., & Vanstone, S. A. (1996). Handbook of Applied Cryptography. CRC Press.
- Ristic, B., Gunatilake, P., & Griffin, L. (2020). Anti-Tracking Techniques for UAVs in Contested Environments. IEEE Aerospace Conference. <https://doi.org/10.5772/6486>
- Rondon, A., Conti, M., & Sirocco, L. (2021). Jamming and Anti-Jamming in Wireless Networks: A Survey. IEEE Communications Surveys & Tutorials. <https://doi.org/10.1109/COMST.2021.3075432>

Отримано редакцією журналу / Received: 12.12.25

Прорецензовано / Revised: 18.12.25

Схвалено до друку / Accepted: 19.12.25

Andrii DUDNIK, DSc (Engin.), Assoc. Prof.
ORCID ID: 0000-0003-1339-7820
e-mail: andrii.dudnik@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Sergiy VYHOVSKYY, PhD Student
ORCID ID: 0009-0007-7868-4923
e-mail: vygovsky.sa@gmail.com
Private Joint-Stock Company "Higher education institution «Interregional Academy of Personnel Management»", Kyiv, Ukraine

Olexandr TOROSHANKO, PhD (Engin.)
ORCID ID: 0000-0002-2354-0187
e-mail: olexandr.toroshanko@knu.ua
Taras Shevchenko National University of Kyiv, Kyiv, Ukraine

Andrii FESENKO, PhD (Engin.), Assoc. Prof.
ORCID ID: 0000-0001-5154-5324
e-mail: andrii.fesenko@npp.kai.edu.ua
State Non-Commercial Company "State University «Kyiv Aviation Institute»", Kyiv, Ukraine

METHOD OF INTEGRATION OF CRYPTOPROCESSOR INTO ROBOTIC SENSOR NETWORK OF EXCHANGE SYSTEM

Background. Modern demining technologies involve the use of complex robotic systems, which include unmanned aerial vehicles, ground mobile platforms, sensor networks, geospatial analysis modules and command and control systems. The reliability of interaction between these components is critically important, since compromising communication channels or data substitution can lead to incorrect mine hazard mapping, loss of the platform or even uncontrolled detonation.

Methods. A comparative analysis of software and hardware protection methods is carried out, mathematical models of cryptoresistance, estimates of the probability of MITM attacks, packet loss in the electronic warfare environment, models of stochastic rotation of identifiers and performance characteristics are presented. The experimental part includes modeling of 12 complex parameters: security, stability, delays, packet loss, channel protection, cryptoresistance, privacy, tracking avoidance, insensitivity to compromise, hardware performance and network resistance to jamming.

Results. The improvements in security parameters from 84% to 99%, a 97% reduction in MITM probability, a 12–20% increase in channel stability, and a 100% reduction in tracking risk were found. The paper proves that the integration of ATECC608A is feasible and technologically sound for next-generation mine clearance systems.

Conclusions. The article presents a comprehensive approach to building a secure sensor and robotic network of a demining system using the ATECC608A hardware crypto module. The proposed architecture provides the formation of a hardware root of trust, two-factor secure boot, dynamic change of network identifiers, cryptographic encoding of mission parameters, and secure control of information exchange between unmanned aerial vehicles (UAVs), ground robotic platforms (UGVs), stationary sensor nodes, and a base station.

Keywords: cryptoprocessor, robotic systems, sensor network, IoT.

Торошанко Олександр є членом редакційної колегії цього видання, тому він не брав участі в процесі рецензування та прийнятті рішення щодо публікації цієї статті.

Автори заявляють про відсутність конфлікту інтересів. Спонсори не брали участі в розробленні дослідження; у зборі, аналізі чи інтерпретації даних; у написанні рукопису; в рішенні про публікацію результатів.

Toroshanko Olexandr is a member of the Editorial Board of this publication; therefore, he did not participate in the peer review process or the decision-making regarding the publication of this article.

The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses or interpretation of data; in the writing of the manuscript; in the decision to publish the results.