УДК 621.391.7

DOI: 10.20535/2523-4455.mea.237579

Огляд та порівняння цифрових алгоритмів захищеної передачі даних в автономних рухомих та стаціонарних системах

Якушкін Т. В., ORCID 0000-0003-3432-9237
Науково-виробнича фірма "РегМік"
Рівнопілля, Україна

Куц Є. В., ORCID 0000-0001-8062-0602
Єршов Р. Д., ORCID 0000-0002-0267-2906
Кафедра Електроніки, автоматики, робототехніки та мехатроніки
Національний університет «Чернігівська політехніка», ROR 048mcz794
Чернігів, Україна

Степенко[s] С. А., к.т.н. доц., ORCID 0000-0001-7702-6776
Кафедра Електричної інженерії та інформаційно-вимірювальних технологій
Національний університет «Чернігівська політехніка», ROR 048mcz794
Чернігів, Україна

***Анотація*—В роботі обґрунтовано перехід до криптографічно захищених каналів бездротового зв'язку в автономних системах керування як стаціонарного, так і рухомого виконання. Розглянуто можливі вектори атак в таких системах. Виконано аналітичний огляд та класифікацію сучасних алгоритмів криптографічного захисту (шифрування), що використовуються на представницькому, сеансовому та канальному рівнях комунікаційних інтерфейсів разом та наведені функціональні схеми для деяких з них. Виділені критерії для порівняння криптографічних алгоритмів, що дозволяє обирати оптимальний в залежності від виконуваних функцій та умов використання конкретної автономної системи.**

Ключові слова — бездротовий зв'язок; шифрування; криптографія; обчислювальна складність; безпілотний літальний апарат; БПЛА.

I. Вступ

Останнім часом багато робіт в галузі електротехнічних комплексів та систем спрямовані на підвищення автономності автоматичних систем керування. При цьому суттєво зростають вимоги до надійності таких систем. Надійність забезпечується в першу чергу резервуванням у найрізноманітніших його проявах та децентралізацією у прийнятті рішень. Останнє, в свою чергу, призводить до посилення обчислювальних можливостей окремого пристрою в системі та до появи спеціалізованих протоколів, що узгоджують роботу між пристроями в складі системи, об'єднуючи їх в мережу. За такими протоколами пристрої неперервно обмінюються короткими повідомленнями і ключовим питанням стає безпека під час взаємодії.

Формування стеку протоколів для об'єднання в мережу двох або більше пристроїв з метою узгодженої взаємодії залежить від ступеня охоплення мережі та вимог до захищеності її складових від потенційних зловмисників. Історично склалося так, що стаціонарні системи локалізувалися в межах одного або декількох приміщень з контрольованим доступом, тому за ступенем охоплення відносилися до персональних мереж (Personal Area Network), в яких переважно використовувались дротові інтерфейси. Рухомі системи, очевидно, не могли об'єднуватися в дротову мережу, до того ж їх складові розташовувались на відкритому незахищеному просторі, тому для них використовувались технології бездротових локальних обчислювальних мереж (Local Area Network).

Розповсюдження набули автономні системи, що базуються на парадигмі «пристроїв інтернету речей» (Internet of Things) [1]. Відповідно до неї окремі автономні обчислювальні пристрої утворюють бездротову розподілену мережу. Кожний такий пристрій реалізує логічно завершений алгоритм вимірювання, накопичення та обробки даних, їх перетворення та створення сигналів керування деяким технологічним

DOI: 10.20535/2523-4455.mea.237579

процесом, а також контролем за станом цього процесу. Для користувача окремий пристрій (або їх агрегована множина) виглядає як мережевий сервіс. Між собою обчислювальні пристрої також підтримують обмін повідомленнями невеликого розміру.

З автоматизацією до ступеня автономності таких процесів як доставка вантажів та перевезення людей парадигма «пристроїв інтернету речей» починає розповсюджуватись не лише на стаціонарні пристрої, а й на рухомі, в першу чергу, — на малі безпілотні літальні апарати (БПЛА). Це створює потенційні загрози з боку кваліфікованих зловмисників таких як терористи, контрабандисти та наркокур'єри. Постає актуальна проблема захищеної передачі даних та сигналів керування на відстанях до одиниць-десятків кілометрів без втрати зв'язку та можливості перехоплення керування.

Технології бездротового зв'язку (БЗ) знаходять широке використання в усіх сферах народного господарства: системах керування, моніторингу безпеки навколишнього середовища, промислової автоматизації, логістики, тощо.

Метою даної публікації є проведення аналітичного огляду і виділення критеріїв для порівняння можливостей цифрових алгоритмів забезпечення криптографічного захисту БЗ в автономних рухомих та стаціонарних системах на прикладі БПЛА.

II. Класифікація криптографічних алгоритмів

Забезпечення захищеності БЗ є вкрай важливим завданням, особливо в системах критичної інфраструктури та у військовому обладнанні.

Сучасні криптографічні алгоритми (КА) розрізняють за типом ключа (Рис. 1):

- безключові;
- одноключові;
- двоключові.

A. Безключові криптографічні алгоритми

Безключові КА не потребують наявності ключа для виконання перетворень. Представником таких алгоритмів є хешування.

Хешування — це процес перетворення вхідних даних довільної довжини у вихідну бітову стрічку фіксованої довжини [2]. Довжина результуючої стрічки визначається алгоритмом функції хешування. Вхідний масив даних називають «ключем» або «повідомленням, вихідні дані «хешем», «хеш-кодом», «хеш-сумою».

Для того, щоб хеш-функція вважалася криптографічно стійкою, визначають наступні критерії:

- Детермінованість. Однакові вхідні дані завжди дають однакові значення хеш-коду.
- Висока швидкість обчислення хеш-функції.
- Однонаправленість. Перетворене повідомлення неможливо отримати із результуючого хеш-коду, окрім як методом повного перебору "brute force".
- Лавинний ефект. Будь-яка зміна у вхідному повідомленні, повинна створювати кардинальні зміни у хеш-коді.
- Відсутність колізій. Неможливість обчислити однакове значення хеш-коду для двох різних повідомлень.

Прикладами широко використовуваних хеш-функцій є: MD5, SHA-1, сімейство SHA-2 (SHA-256, SHA-384, SHA-512 тощо), SHA-3 (KECCAK). Такі хеш-функції використовують для прискорення розрахунку цифрового підпису, для хешування паролів, хешування в транзакціях біткоїна [3].

B. Одноключеві криптографічні алгоритми

До одноключевих КА відносять симетричне шифрування та частковий випадок хешування.

Симетричне шифрування (СШ), або криптографічний алгоритм з закритим ключем — це алгоритм шифрування, в якому для процесів шифрування та дешифрування повідомлення використовується один і той же секретний ключ. Операція дешифрування є оберненою до операції шифрування. Ключ повинен зберігатися кожною стороною в таємниці, що викликає між сторонами такі проблеми, як необхідність попереднього узгодження ключа та алгоритму шифрування.

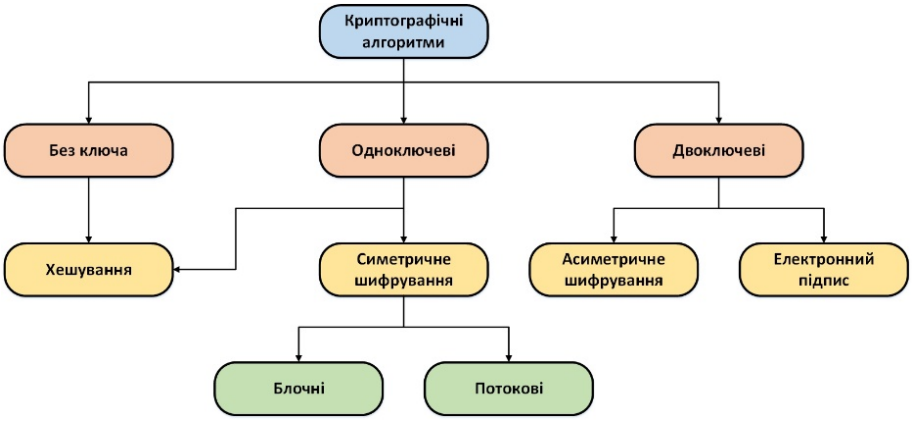

Рис.1 Класифікація криптографічних алгоритмів

DOI: 10.20535/2523-4455.mea.237579

Виходячи з даної проблеми, СШ використовують разом з асиметричним шифруванням (АШ), де за допомогою АШ сторони генерують спільний секретний ключ, який далі використовують для СШ. В свою чергу КА з закритим ключем поділяється на блочні та потокові.

В блочному СШ відкритий текст розбивається на блоки фіксованої довжини над якими здійснюються операції підстановки (S-бокси), перестановки (P-бокси), виключна диз'юнкція «XOR», циклічний зсув, заміна, розбиття і об'єднання блоку [4]. Розрізняють наступні способи втілення блочних СШ: Electronic Codebook, Cipher Block Chaining, Propagating Cipher Block Chaining, Cipher Feedback, Output Feedback, Counter Mode, Galois/Counter Mode.

В потокових СШ кожний елемент (біт/байт даних) шифрується окремо. Шифрування здійснюється операцією «XOR» між елементом відкритого тексту і т. зв. «гаммою». Гаммою в даному випадку називають псевдовипадкову послідовність отриману із секретного ключа. Потокові СШ відрізняються один від одного за методом створення гамми із секретного ключа [4].

До блочних СШ відносять наступні алгоритми: AES, DES, 3DES, RC5, Blowfish, IDEA тощо. До симетричних потокових шифрів відносять: RC4, SEAL, WAKE, A5/1.

У порівнянні з АШ, СШ має наступні переваги: висока швидкість шифрування, ключ меншої довжини та більш прості операції, що спрощують реалізацію. Серед недоліків одразу можна відмітити необхідність у наявності захищеного каналу зв'язку для попереднього обміну секретним ключем, що також викликає складності при передачі повідомлень між декількома учасниками.

C. Двоключові криптографічні алгоритми

Асиметричне шифрування та електронний підпис є представниками двоключових КА.

Асиметричне шифрування або криптографічний алгоритм з відкритим ключем — це алгоритм шифрування, в якому використовуються два ключі: відкритий ключ, який використовується для шифрування повідомлення, та закритий ключ, який використовується для розшифрування повідомлення.

В основі такого шифрування лежить поняття односторонніх функцій, котрі «легко» обчислюються, а задача обернення функції є «дуже складною» в тому сенсі, що потребує нереальних обчислювальних ресурсів та/або великої кількості часу.

До асиметричного шифрування відносять такі шифри: RSA, DSA, ECDSA, Elgamal, Diffie-Hellman, ECDH, тощо. АШ знаходять своє використання для шифрування повідомлень (RSA), як засіб розподілення ключів для симетричних криптографічних систем, автентифікації користувачів (DSA). На відміну від СШ, АШ не потребує захищеного каналу зв'язку, що є перевагою [5]. В той же час, АШ потребує значних обчислювальних ресурсів і великої довжини ключа для забезпечення криптостійкості порівняної з СШ, наприклад, при 56 біт СШ ключа, для АШ (RSA) потрібен ключ довжиною 384 біт.

Електронний підпис — це метод, який дозволяє ідентифікувати та підтвердити дійсність автора повідомлення. За допомогою криптографічних методів встановлюється зв'язок між автором та повідомленням, що робить неможливим підробку підпису.

Алгоритми отримання електронного підпису працюють за однією з наступних схем:

- Симетрична схема — в такій схемі підпис виконується до кожного біту повідомлення. Це призводить до того, що сам підпис може бути більшої довжини за саме повідомлення. Така схема майже не використовується.
- Асиметрична схема — в даній схемі підпис повідомлення виконується закритим ключем, перевірка підпису — відкритим. Дана схема є найбільш поширеною.
- За допомогою хеш-функції. В такій схемі із зашифрованого повідомлення отримується хеш-код, який в результаті підписується за допомогою асиметричної схеми. Такий спосіб є швидшим, тому що хеш-код за розміром може бути в рази менше, ніж повідомлення.

Прикладами алгоритмів цифрового підпису є RSA-PSS, DSA, ECDSA, DLR, BLS, GMR.

III. Методи шифрування в сучасних бездротових каналах зв'язку

Дані, які передаються бездротовим способом, можуть бути легко перехоплені зловмисником, тому виникає гостра необхідність в реалізації шифрування каналу зв'язку.

Основними представниками технології БЗ є — Wi-Fi, Bluetooth, ZigBee, LoRa. Перші три технології відносять до *Short Range* (1-200 метрів), а технологія LoRa – *Long Range* (до 2-3 км в місті, до 5-7 км в сільських місцевостях, робота на відстанях >10 км також можлива, але за особливих умов).

A. Шифрування в технології Wi-Fi

Першим криптографічним протоколом для мережі Wi-Fi був Wired Equivalent Privacy (WEP), який в основі мав алгоритм симетричного потокового шифру RC4 і контрольну суму CRC-32 для підтвердження цілісності даних. Над ключем довжиною 40 або 104 біт проводилася операція конкатенації з 24-х бітним вектором ініціалізації, результатом якої отримувався ключ довжиною 64 або 128 біт, який використовувався для шифрування алгоритмом RC4. Проблемою даного криптографічного протоколу була невелика довжина вектора ініціалізації, тому він міг повторюватися у великому обсязі трафіку, що є недопустимим для потокових шифрів.

На заміну WEP було створено наступні методи захисту: Wi-Fi Protected Access (WPA), WPA2, WPA3. У WPA на відміну від WEP було реалізовано

DOI: 10.20535/2523-4455.mea.237579

Temporary Key Integrity Protocol, суть якого полягала в динамічній генерації нового ключа довжиною 128 біт для кожного пакету. У даному протоколі було реалізовано алгоритм Message Integrity Check (MIC) на заміну CRC. Але у WPA були схожі проблеми з WEP, тому було розроблено протокол WPA2, в якому замість потокового RC4 шифру використовувався AES-128 в блочному режимі CCMP (комбінація CTR та CBC-MAC).

Структурна схема блоку шифрування в протоколі WPA2 зображена на Рис. 2, а саме процес створення MIC та шифрування даних. З часом WPA2 було вдосконалено до WPA3. Для обміну ключами під час автентифікації пристрою було реалізовано Simultaneous Authentication of Equals [6], який набагато безпечніший за попередній метод Pre-Shared Key.

Для державних установ, банків та підприємств створена версія WPA3-Enterprise, де для шифрування використовується GCMP-256, а для формування і підтвердження ключа − HMAC-SHA384, ECDH та ECDSA з використанням 384-біт еліптичної кривої для розподілення ключів і автентифікації [7].

B. Шифрування в технології Bluetooth

В технології Bluetooth доступно три режими захисту:

1) Security Mode 1. Режим без захисту.
2) Security Mode 2. Режим захисту сервісного рівня. Захист забезпечений для каналу L2CAP та для встановлення зв'язку (SDP, RFCOMM, TSC) [8]
3) Security Mode 3. Режим захисту рівня зв'язку. Процедура захисту розпочинається до налаштування зв'язку. У даному режимі можна завжди вимагати тільки автентифікацію або автентифікацію та шифрування разом [8].

Шифрування даних здійснюється за допомогою потокового шифру E0 [9]. Даний шифр повторно синхронізується для кожних нових даних. Спрощена структурна схема шифрування в каналі зв'язку Bluetooth зображена на Рис. 3.

Вхідними параметрами для генерації ключа Keystream (Key stream bits) є адреса майстру *BD_ADDR A*, 26-бітний таймер реального часу майстра *Clock A*, попередньо згенерований ключ *Encryption Key* (для генерації використовують RAND A, Link Key, значення отримане під час процедури автентифікації) [9].

Master передає значення *RAND A* до Slave, щоб він зміг згенерувати ключ *Encryption Key*. Між утвореним ключем *Keystream* та даними здійснюється операція XOR, далі зашифроване повідомлення можна передавати.

C. Шифрування в технології ZigBee

В технології ZigBee реалізовані наступні режими захисту [10]:

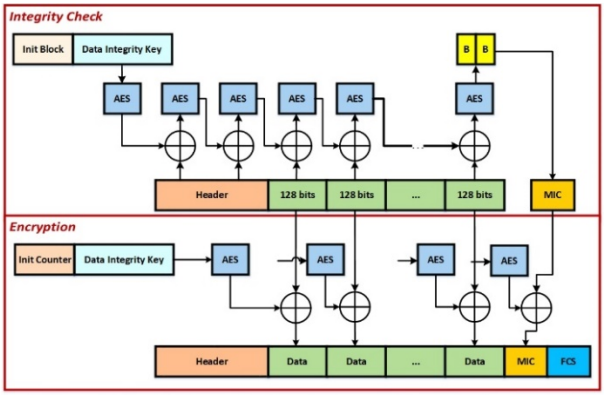

Рис. 2 Структурна схема блоку шифрування в протоколі WPA2

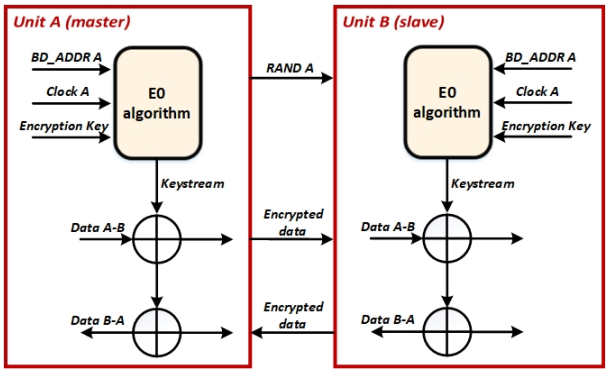

Рис. 3 Структурна схема блоку шифрування для Bluetooth

1) Контроль доступу.
2) Шифрування даних.
3) Цілісність даних.
4) Механізм протидії атаці повторного відтворення.

Механізм контролю доступу дозволяє отримувати повідомлення лише від конкретних пристроїв, попередньо записаних до таблиці Access Control Table. Для шифрування даних користувач може обирати між AES CTR і AES CCM* (32, 64, або 128 біт) [11]. Для цілісності даних використовується алгоритм MIC (32, 64, 128 біт). Також в ZigBee реалізовано Trust Center, який визначає та надає дозвіл для підключення нового пристрою в мережу, також він відповідає за розподілення ключів та їх оновлення [10].

В стандарті ZigBee використовується три типи ключів довжиною 128 біт: Network Key для широкомовного зв'язку між пристроями в мережі, Link Key для одноадресного спілкування, Master Key для підтримки захищеного обміну ключами Link Key між двома вузлами в протоколі обміну симетричними ключами SKKE [12].

Розподілення ключів здійснюється трьома способами: заздалегідь встановлені ключі, за допомогою протоколу SKKE або за допомогою Trust Centre.

DOI: 10.20535/2523-4455.mea.237579

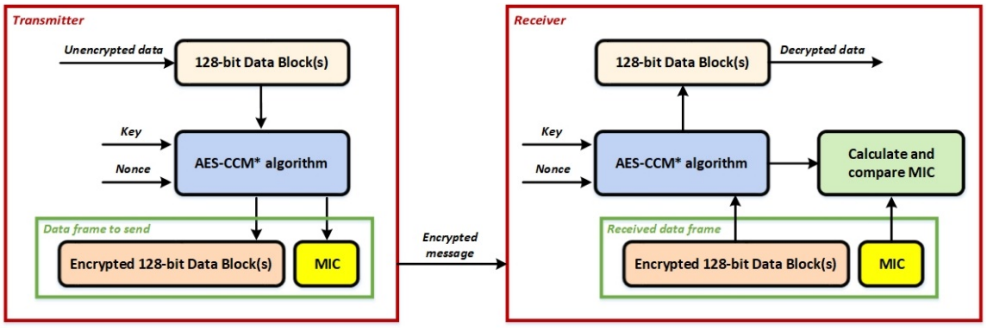

Рис. 4 Структурна схема блоку шифрування для ZigBee

На Рис. 4 можна побачити процес шифрування повідомлення ZigBee. Спершу, за допомогою AES-CCM* отримується MIC для перевірки цілісності даних та підтвердження автентифікації, далі дані шифруються, утворений фрейм у вигляді повідомлення може відправлятися до приймача. З боку приймача відбуваються зворотні дії: розшифровується повідомлення, розраховується на його основі MIC та порівнюється з отриманим. Якщо вони співпадають, то повідомлення можна вважати автентичним.

D. Шифрування в технології LoRa

Для LoRa створено мережевий протокол LoRaWAN. Даний протокол дозволяє побудувати мережу типу «зірка», де кінцеві пристрої (датчики) виконують свої функції та комунікують з базовими станціями (шлюзами) через канал зв'язку LoRa, захищений протоколом LoRaWAN. Захищений зв'язок реалізований алгоритмом AES-128 з різними блочними режимами: CMAC для захисту цілісності даних та CTR для шифрування [13].

Протоколом передбачено два варіанти активації кінцевих пристроїв: Over The Air Activation та Activation By Personalization. Перший потребує проходження процедури підключення до мережі, з подальшою генерацією сесійних ключів (мережі та додатку) і адреси DevAddr (локальна адреса кінцевого пристрою). Така процедура буде виконуватися завжди під час приєднання до нової мережі, або при втраті актуальної інформації про сесійні ключі. Варіант активації Activation By Personalization в свою чергу приєднується напряму, без процедури підключення. Сесійні ключі попередньо визначені та збережені в кінцевому пристрої. Вони не оновлюються, що робить даний тип активації потенційно небезпечним для мережі [14].

IV. Шифрування даних та керуючих повідомлень в автономних рухомих системах

З поширенням безпілотних літальних апаратів виникають загрози несанкціонованого втручання в канал передачі даних для отримання конфіденційної інформації, яка передається від літального апарату, та несанкціоноване втручання в командну телеметрію, тобто, перехоплення керування БПЛА з метою виведення його з ладу або заволодіння їм. Виробники часто не приділяють належної уваги цьому аспекту.

A. Типові характеристики каналу керування БПЛА

Незважаючи на значну різноманітність типів, моделей і виробників БПЛА, можна виділити узагальнені параметри і характеристики, типові для виробів більшості виробників [15]:

- максимальна «легальна» потужність випромінюваного сигналу (в каналі керування) — 100 мВт;
- типові (пріоритетні) діапазони частот — 2.48 ГГц та/або 5.8 ГГц;
- вид модуляції (типово) — FSK2 (рідше — PSK2 (A/B) та/або OFDM);
- тривалість імпульсу (типова) — 500 мкс … 2.5 мс;
- символьна швидкість передачі даних (типова) — 1 000 … 2 000 кБод;

B. Підвищення завадостійкості каналу зв'язку

Для кращої завадостійкості (протидії постановці завад) у каналі зв'язку виробники промислових БПЛА використовують метод псевдовипадкової перебудови робочої частоти сигналу, особливістю якого є часта зміна несучої частоти. Частота змінюється відповідно до псевдовипадкової послідовності значень, відомої як відправнику, так і одержувачу.

C. Розповсюджені протоколи передачі даних по радіоканалу БПЛА

Протокол передачі визначає структуру пакетів даних, можливі схеми шифрування, які протокол буде використовувати та спосіб формування спектру на фізичному рівні каналу зв'язку. Виробники БПЛА масового вжитку застосовують однаковий протокол та схему шифрування в усіх реалізаціях своїх БПЛА через те, що використовують однакові інтегральні мікросхеми з налаштуваннями за умовчуванням. У документації до цих мікросхем можна знайти такі критичні вразливості, як паролі за замовчуванням та базова поведінка після відключення живлення (повторна ініціалізація).

Для комунікації між дистанційним пультом керування та БПЛА (Рис. 5) по радіоканалу існують такі закриті протоколи [16, 17]:

- D8, D16, LR12 (Frsky);

DOI: 10.20535/2523-4455.mea.237579

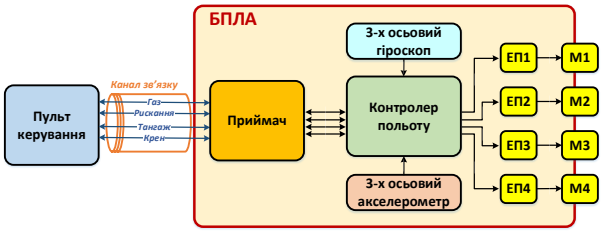

Рис.5 Схема зв'язку БПЛА з операторським пультом керування

- DSM, DSM2, DSMX (Spektrum);
- Flysky (Flysky);
- A-FHSS (Hitec);
- FASST (Futaba);
- Hi-Sky (Deviation).

Ці протоколи розроблені під конкретних виробників апаратного забезпечення.

Ще один протокол, широко підтримуваний БПЛА має назву MAVlink, найчастіше використовується для передачі телеметрії. MAVlink має відкритий вихідний код. Він реалізований у вигляді модуля мовою Python і розповсюджується під ліцензією LGPL. Цей протокол за умовчанням не застосовує шифрування при обміні даними і тому набагато вразливіший до атак у порівнянні з конкуруючими технологіями, де така функція є.

В опублікованому відео [18] дослідники демонструють процес відключення БПЛА після перехоплення його ідентифікатора для радіозв'язку, проте схожим способом можна перехопити керування БПЛА і викрасти його. Протокол MAVLink використовують в своїх БПЛА багато компаній, тому до уразливості схильні як відомі серійні моделі БПЛА (наприклад, AR.Drone), так і популярні системи керування (ArduPilot, PX4FMU), на базі яких ентузіасти збирають власні БПЛА.

D. Частота передачі даних

Більшість каналів керування БПЛА використовують частоту 2,4 ГГц, а для передачі відео 5,8 ГГц. Одночасно частота 2,4 ГГц є несучою для технології Wi-Fi, тому якщо використання БПЛА плануються в міських умовах, де є багато прийомо-передавачів Wi-Fi, це може створити велику кількість завад у каналі зв'язку та привести до багатократних тимчасових втрат контролю над БПЛА.

Передача сигналу на нижчих частотах, наприклад 900 МГц, потребує великих антен, що негативно позначається на масогабаритних показниках керуючого обладнання. Однак частота 900 МГц має хорошу огинаючу здатність, що дозволяє домогтися якісного керування за викривлень ландшафту [19].

БПЛА для військових застосувань використовують супутниковий зв'язок. Від моменту зльоту до покидання зони прямої видимості пункту керування, наземна станція здійснює пряму передачу даних. Після того, як літальний апарат зникає з поля зору, штучні супутники Землі служать точками доступу наземної станції до БПЛА [20].

E. Використання технології Wi-Fi

У разі використання технології Wi-Fi, як правило, на БПЛА створюється відкрита точка доступу або точка доступу з базовим рівнем захисту WEP. Пульт керування заздалегідь знає статичну IP-адресу та порт для проведення комунікацій.

Дані всередині бездротової мережі передаються у відкритому вигляді. При використанні Wi-Fi з будь-яким типовим шифруванням (WEP, WPA, WPA2) у атакуючого є можливість у відкритому ефірі переглянути MAC-адреси клієнтів, які підключені до точки доступу. Створюється вразливість, яка полягає у можливості атакуючої сторони відправити спеціально сформований пакет deAUTH. Це призводить до розриву каналу між пультом дистанційного керування та БПЛА і його зависанням в повітрі за кілька секунд [21].

Раніше фахівець з комп'ютерної безпеки Самі Камкар створив літальний апарат SkyJack, здатний перехоплювати сигнал керування БПЛА Parrot, після чого захоплений БПЛА переходив під контроль оператора SkyJack [22].

F. Можливі вектори атак на БПЛА

- Придушення сигналів навігаційних систем і систем зв'язку та керування, якими користуються БПЛА.
- Генерація підроблених вхідних команд атакуючою стороною і випромінювання їх в ефір.
- Атака переповнення буфера, помилки кодування або декодування. Підмішування до оригінального сигналу з пульта керування шуму для ускладнення правильного розпізнавання повідомлення.
- GPS-спуфінг. Використовують для придушення сигналу від навігаційних супутників та передачі в ефір власного сигналу, що транслює на приймаючий пристрій помилкові координати. Через це блок керування БПЛА вважає, ніби він знаходиться в районі найближчого аеропорту. Розрахунок робиться на те, що в програмному забезпеченні більшості БПЛА закладена заборона на польоти над цивільними повітряними просторами — при наближенні до аеропорту БПЛА автоматично приземляється або буде намагатись облетіти його.

V. Критерії і методи оцінювання надійності шифрування в каналах зв'язку

Кожний алгоритм шифрування має свої сильні та слабкі сторони за набором критеріїв, сформованим для розглянутої предметної області. Виділимо наступні критерії:

Обчислювальна складність — залежність кількості елементарних обчислювальних операцій, що

DOI: 10.20535/2523-4455.mea.237579

витрачається на шифрування/дешифрування повідомлення в залежності від його розміру. За допомогою апроксимації знаходять, до якої ступеневої залежності наближається графік залежності (лінійна, квадратична, кубічна, і т.д.). У Табл. 1 наведено обчислювальну складність під час різних атак на КА.

Час шифрування/дешифрування — визначає скільки часу витрачається на перетворення відкритого тексту в шифротекст та перетворення шифротексту в відкритий текст. Дана величина залежить від режиму блочного шифрування, довжини ключа, довжини блоку і впливає на швидкодію системи [23]. Чим менше часу КА потребує для шифрування/дешифрування тим це краще для систем, в яких вони використовуються.

Довжина ключа, довжина блоку, кількість раундів — дані параметри опосередковано визначають захищеність КА від різноманітних атак. Збільшення довжини ключа робить КА надійним завдяки більшій варіації різноманітних ключів, що зменшує шанси на підбір ключа методом повного перебору [24]. Надійність зростає також при використанні КА, в яких довжина блоку та кількість раундів шифрування є значними.

Затрати пам'яті для шифрування/дешифрування — даний критерій визначає кількість пам'яті, необхідної для виконання шифрування та/або дешифрування. Він також залежить від обчислювальної складності, довжини ключа, вектору ініціалізації і режиму блочного шифрування [25]. Чим менше пам'яті використовується, тим КА більше підходить для вбудованих застосувань.

Ентропія — цей критерій визначає міру випадковості зашифрованого повідомлення. Чим більше значення ентропії, тим складніше стає взаємозв'язок між ключем та шифротекстом, що в результаті ускладнить атаку зловмисникам [25].

У роботах [23-25] проведено порівняльний аналіз між різними КА за критеріями, зазначеними вище. Два найкращих і один найгірший КА по кожному з критеріїв зведено до Табл. 2.

З отриманих результатів наведених в Табл. 2 можна зробити висновок, що кращими КА, за обраними критеріями, є Blowfish та AES.

ТАБЛИЦЯ 1. ОБЧИСЛЮВАЛЬНА СКЛАДНІСТЬ АТАК НА КА

КА	Тип атаки	Розрядність ключа, біт	Показник ОС
AES	Biclique attack	128	$2^{126.1}$
		192	$2^{189.7}$
		256	$2^{254.4}$
	Related-key attack	192	2^{176}
		256	$2^{99.5}$
DES	Brute-force attack	56	2^{55}
	Linear cryptanalysis		2^{43}
3DES	Plain text attack	112	2^{113}

ТАБЛИЦЯ 2 НАЙКРАЩІ КА ЗА ОБРАНИМИ КРИТЕРІЯМИ

Критерій	Найкращі КА	Гірший КА
Час шифрування	Blowfish, AES	RSA
Час дешифрування	Blowfish, AES	RSA
Довжина ключа	RSA(4096bit), Blowfish(448bit)	DES(56bit)
Довжина блоку	AES(128bit), RC6(128bit)	DES, 3DES, Blowfish(64 bit)
Кількість раундів	3DES(48bit), RC6(20)	AES (10-14 bit)
Затрати пам'яті	Blowfish, AES	RSA
Ентропія	Blowfish, AES	DES, 3DES

ВИСНОВКИ

В роботі розглянуто проблеми інформаційної безпеки БПЛА та методи запобігання перехопленню даних та захопленню керування потенційним зловмисником. Проаналізовано використання алгоритмів криптографічного захисту даних: симетричні та асиметричні алгоритми, їх відмінності між собою. Виділено критерії порівняння КА. З порівняльного аналізу існуючих КА встановлено, що найбільш ефективними для БПЛА-застосувань є Blowfish та AES.

При розгляді проблем інформаційної небезпеки БПЛА іншим важливим параметром є несуча частота для передачі сигналу керування. При роботі на частоті 900 МГц створюються умови для передачі сигналу на значні відстані. Використання сигналу з частотою 5.8 ГГц дозволяє передавати зображення високої якості, з антеною мінімальних розмірів, але не дозволяє працювати за горизонтом. Виходячи з цього, оптимальною частотою для передачі даних між пультом керування та БПЛА є 2.4 ГГц, але не в умовах міста. На інші ж частоти потрібен спеціальний дозвіл.

ПОДЯКА

Поточні дослідження виконуються в межах держбюджетної науково-дослідної роботи молодих вчених № 0120U101554 «Автономні електроенергетичні системи з високою ефективністю, покращеними масогабаритними характеристиками та підвищеною надійністю для спеціальних застосувань»

ВНЕСОК АВТОРІВ

Головна ідея та концепція, Єршов Р. Д., Якушкін Т. В.; аналіз джерел, Якушкін Т. В., Куц Є. В.; підготовка письмового оригіналу, Якушкін Т. В., Куц Є. В.; перевірка та редагування оригіналу тексту, Єршов Р. Д., Степенко С. А.; візуалізація та рисунки, Якушкін Т. В., Куц Є. В.; супервізори роботи, Єршов Р. Д., Степенко С. А..

ПОСИЛАННЯ

[1] L. Globa, J. Yamnenko, V. Kurdecha, and D. Trokhymenko, "Securing internet of things data," Information and Telecommunication Sciences, pp. 40-46, 2019. **DOI:** 10.20535/2411-2976.22019.40-46.

DOI: 10.20535/2523-4455.mea.237579

[2] D. Knuth, "The Art of Computer Programming vol. 3, Sorting and Searching," Addison-Wesley, Reading, MA., United States, p. 527, 1973.

[3] Daniel Augot, Matthieu Finiasz, Nicolas Sendrier, "A Fast Provably Secure Cryptographic Hash Function," no. 230, pp. 3-4, 2003.

[4] Baigneres, Thomas & Finiasz, Matthieu, "Selected areas in cryptography," 13th international workshop, Montreal, Canada, p. 77, August 17-18, 2006. **ISBN:** 9783540744610.

[5] T. Radivilova, L. Kirichenko, D. Ageyev, M. Tawalbeh and V. Bulakh, "Decrypting SSL/TLS traffic for hidden threats detection," 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT), pp. 143-146, 2018. **DOI:** 10.1109/DESSERT.2018.8409116.

[6] D. Harkins, "Simultaneous Authentication of Equals: A Secure, Password-Based Key Exchange for Mesh Networks," 2008 Second International Conference on Sensor Technologies and Applications (sensorcomm 2008), pp. 839-844, 2008. **DOI:** 10.1109/SENSORCOMM.2008.131.

[7] A. Bartoli, "Understanding Server Authentication in WPA3 Enterprise," Applied Sciences, no 21, pp. 78-79, 2020. **DOI:** 10.3390/app10217879.

[8] C. Gehrmann, J. Persson, B. Smeets, "Bluetooth Security. Artech House computer security series," 2004, **ISBN:** 1580538851, 9781580538855.

[9] C. De Canniere, T. Johansson, B. Preneel, "Cryptanalysis of the Bluetooth stream cipher," COSIC Internal Report, 2001.

[10] P. V. Halkyn, and D. V. Karlovskyi, "Osobennosty realyzatsyy besprovodnykh sensornykh setei na osnove tekhnolohyy ZigBee [Features of the implementation of wireless sensory networks based on ZigBee technology]," Aktualne problemy nowoczesnych nauk, no. 31, pp. 7-11, 2010.

[11] M. Sun and Y. Qian, "Study and Application of Security Based on ZigBee Standard," 2011 Third International Conference on Multimedia Information Networking and Security, pp. 508-511, 2011. **DOI:** 10.1109/MINES.2011.79.

[12] E. Yuksel, "Analysing zigbee key establishment protocols," arXiv preprint **arXiv:** 1205.6678, 2012.

[13] M. Eldefrawy et al., "Formal security analysis of LoRaWAN," Computer Networks, pp. 328-339, 2019. **DOI:** 10.1016/j.comnet.2018.11.017.

[14] E. Aras, G. S. Ramachandran, P. Lawrence and D. Hughes, "Exploring the Security Vulnerabilities of LoRa," 2017 3rd IEEE International Conference on Cybernetics (CYBCONF), pp. 1-6, 2017. **DOI:** 10.1109/CYBConf.2017.7985777.

[15] N. M. Boev, P. V. Sharshavyn, Y. V. Nyhrutsa, "Postroenye system sviazy bespylotnykh letatelnykh apparatov dlia peredachy ynformatsyy na bolshye rasstoianyia [Construction of communication systems of unmanned aircraft for transmitting information over long distances]," Yzvestyia Yuzhnoho federalnoho unyversyteta. Tekhnycheskye nauky, no. 3(152), 2014.

[16] Yu. S. Peterheria, A. H. Kyseleva, "Osobennosty postroenyia vychyslytelno-upravliaiushchei sety lokalnoho obъekta [Features of building a computationally controlling network of a local object]," Elektronyka y sviaz, pp. 208-213, 2008.

[17] V. Chamola, P. Kotesh, A. Agarwal, Naren, N. Gupta, M. Guizani, "A comprehensive review of unmanned aerial vehicle attacks and neutralization techniques," Ad Hoc Networks, pp. 102-324, 2020. **DOI:** 10.1016/j.adhoc.2020.102324.

[18] Anti-drone device demo, YouTube - shellntel, 2021; **URL:** https://www.youtube.com/watch?v=sycgvpIxvPU.

[19] A. N. Bondarev, R. V. Kyrychek, "Obzor bespylotnykh letatelnykh apparatov obshcheho polzovanyia y rehulyrovanyia vozdushnoho dvyzhenyia BPLA v raznykh stranakh [Review of unmanned aerial vehicles and regulating the air traffic control of the UAV in different countries]," Ynformatsyonnye tekhnolohyy y telekommunykatsyy, no. 4, p. 13, 2016.

[20] Han, Maojie, "Authentication and encryption of aerial robotics communication," Diss. San Jose State University, 2018. **DOI:** 10.31979/etd.un7n-43r8

[21] E. V. Dmytryeva, A. V. Krasov, O. B. Fylyppov, "Razrabotka kompleksa prohrammno-apparatnoho obespechenyia dlia perekhvata bespylotnoho letatelnoho apparata [Development of a software and hardware complex for intercepting unmanned aircraft]," Aktualnye problemy ynfotelekommunykatsyi v nauke y obrazovanyy (APYNO 2017), pp. 266-270, 2017.

[22] A drone engineered to autonomously seek out, hack, and wirelessly take full control over any other Parrot or 3DR drones within wireless or flying distance, creating an army of zombie drones under your control, GitHub - samyk/skyjack, 2021; **URL:** https://github.com/samyk/skyjack.

[23] Nazeh Abdul Wahid MD, Ali A, Esparham B, Marwan MD, "A Comparison of Cryptographic Algorithms: DES, 3DES, AES, RSA and Blowfish for Guessing Attacks Prevention," J Comp Sci Appl Inform Technol, vol. 3, no. 2. pp. 1-7, 2018. **DOI:** 10.15226/2474-9257/3/2/00132.

[24] Z. Hercigonja, "Comparative analysis of cryptographic algorithms," International Journal of Digital Technology & Economy, vol. 1, no. 2, pp. 127-134, 2016. **URL:** http://www.ijdte.com/index.php/ijdte/article/view/14/12

[25] T. Egerton, V. Emmah, "Comparative Analysis of Cryptographic Algorithms in Securing Data," International Journal of Engineering Trends and Technology (IJETT), vol. 58, no. 3, pp. 118-122, April 2018. **DOI:** 10.14445/22315381/IJETT-V58P223

Надійшла до редакції 20 липня 2021 р.
Прийнята до друку 09 серпня 2021 р.

UDC 621.391.7

DOI: 10.20535/2523-4455.mea.237579

Review and Comparison of Digital Algorithms for Secure Data Transmission in Autonomous Mobile and Stationary Systems

T. V. Yakushkin, ORCID 0000-0003-3432-9237
Research and production firm "REGMIK"
Rivnopillia, Ukraine

Ie. V. Kuts, ORCID 0000-0001-8062-0602
R. D. Iershov, ORCID 0000-0002-0267-2906
Department of Electronics, Automation, Robotics and Mechatronics
Chernihiv Polytechnic National University, ROR 048mcz794
Chernihiv, Ukraine

S. A. Stepenko[s], PhD Assoc.Prof., ORCID 0000-0001-7702-6776
Department of Electrical Engineering and Information and Measurement Technologies
Chernihiv Polytechnic National University, ROR 048mcz794
Chernihiv, Ukraine

Abstract—Autonomous systems based on the "Internet of Things" paradigm have become widespread. The Internet of Things devices are used for collecting and analyzing data, control electrical systems. The Internet of Things the most common fields of use are smart houses, smart cities, smart traffic, environment monitoring, healthcare etc. With the automation to the degree of autonomy of such processes as cargo delivery and human transportation, the Internet of Things paradigm begins to extend not only to stationary devices, but also to mobile, primarily small unmanned aerial vehicles. UAV can be used not only for civil use but for police or military operations too. This poses a potential threat to skilled criminals such as terrorists, smugglers and drug couriers. There is an urgent problem of secure transmission of data and control signals at distances up to tens of kilometers without loss of communication and the possibility of interception of control.

Wireless communication technologies are widely used in all areas of the economy: control systems, environmental safety monitoring, industrial automation, logistics, etc. Wireless networks have many characteristics in common with wireline networks, and therefore, many security issues of wireline networks apply to the wireless environment. Wireless data is easy to intercept by potential eavesdroppers. Issue of security and privacy become more notable with wireless networks.

The paper substantiates the transition to cryptographically protected wireless communication channels in autonomous control systems for both fixed and mobile performance. Possible attack vectors in such systems are considered. An analytical review and classification of modern cryptographic protection (encryption) algorithms used at the representative, session and channel levels of communication interfaces together and functional diagrams for some of them are performed. Selected criteria for comparing cryptographic algorithms, which allows you to choose the best depending on the functions performed and the conditions of use of a particular autonomous system.

Keywords — wireless communication; encryption; cryptography; computational complexity; unmanned aerial vehicle; UAV.