УДК 004.934:681.391

Гуляницький Л.Ф., Огурцов М.І., Ходзінський О.М.
Інститут кібернетики ім. В.М. Глушкова НАН України

РОЗРОБКА АЛГОРИТМІВ ЗАХИСТУ ІНФОРМАЦІЇ ДЛЯ СПЕЦІАЛЬНИХ МЕРЕЖ

Створено і апробовано сімейство алгоритмів захисту передачі даних для мереж спеціального призначення з урахуванням особливостей дистанційного радіокерування рухом груп рухомих роботизованих систем, зокрема, у складних ситуаціях, що відповідають українським та міжнародним стандартам. Розроблено алгоритми криптографічного захисту інформації, яка циркулює в таких мережах. В результаті їх застосування жодні дані (команди керування, телеметрія, відеосигнали) не циркулюють у мережі у незашифрованому вигляді. Розроблене програмно-алгоритмічне забезпечення апробовано шляхом створення наземних дистанційно керованих модельних зразків рухомих роботизованих систем спеціального призначення та проведення тестування їх мережевої взаємодії.

Создано и апробировано семейство алгоритмов защиты данных для сетей специального назначения с учетом особенностей дистанционного управления двидением групп движущихся роботиззированных систем, я частности, в сложных ситуациях, которые соответствуют украинстким и международным стандартам. Разработано алгоритмы криптографической защиты иныормации, которая циркулирует в таких сетях. В результате их применения ни одни данные (команды управления, телеметрия, видеостгралы) не циркулируют в сети в незашифрованном виде. Разработанное программно-алгоритмическое обеспечение апробировано путем создания наземных дистанционно управляемых модельных образцовдвижущихся роботизированных систем специального назначения и проведения тестирования их сетевого взаимодействия.

Ключові слова: *рухомі роботизовано системи, спеціальні мережі, моделювання, маршрутизація, безпілотні літальні апарати, захист інформації.*

Вступ

Через стрімке зростання масштабу, складності задач і розширення сфер практичних застосувань мереж спеціального призначення необхідна розробка нових архітектур мереж, які б мали високу адаптивність до умов застосування, а також масштабованість та надійність. Зокрема, велику актуальність набувають питання розробки алгоритмів захищеної передачі даних та їх маршрутизації для спеціалізованих мереж, призначених для функціонування системи керування рухомими технічними об'єктами на основі синхронної і асинхронної передачі пакетів даних з мультимедійною інформацією і кодованих команд у зашифрованому виді. Існуючі стандарти для тимчасових безпровідних мереж і мобільні пристрої, які доступні на ринку, не передбачають роботу в умовах використання засобів радіоелектронної боротьби, високого рівня активних завад та хакерських атак [1–6], а також не відповідають ДСТУ.

Сучасними аналогами для мереж дистанційного управління за принципом побудови є безпровідні mesh і ad hoc мережі та за призначенням – GSM стільникові мережі для безпілотних літальних апаратів (БПЛА) і дистанційно керовані автопоїзди [7-8]. У відкритих закордонних джерелах розглядаються підходи до побудови систем керування групами роботів. Однак наразі комплексної системи подібного призначення не існує.

Якщо не використовувати технології захисту інформації, то потік даних, що циркулює в мережі, буде доступний будь-кому, хто має відповідні технічні засоби [9]. Тому функціонування засобів захисту даних є невід'ємною частиною інформаційних процесів у цих мережах. Зважаючи на обмеження обчислювальних потужностей,

необхідно досліджувати варіанти застосування стандартних симетричних та/або асиметричних схем шифрування для рухомих роботизованих систем (РРС) та схем розповсюдження ключів [10-14].

Мета досліджень

Метою досліджень стала розробка математичного апарату і відповідного програмного забезпечення для керування групою рухомих роботизованих систем (РРС) з використанням синхронної і асинхронної передачі зашифрованих пакетів даних та кодованих команд в спеціалізованій безпровідній мережі. Актуальність тематики обумовлюється стрімким розширенням спектру завдань при застосуванні роботизованих систем спеціального призначення, що керуються через безпровідні мережі, та важливістю інформації, яка циркулює всередині таких мереж. Значущість тематики досліджень обумовлюється потребами підвищення якості і надійності управління роботизованими системами, наприклад, роботами розвідниками в умовах використання засобів радіоелектронної боротьби та радіорозвідки. Захищена від навмисних і природних завад система передачі даних дозволить здійснювати безперервне та децентралізоване стійке дистанційне керування технічними засобами в умовах бойових дій, чим підвищить живучість таких систем.

Передача зашифрованих повідомлень

Завдання пересилання зашифрованих повідомлень є актуальним як для передачі сигналів управління, так і для передачі фото- та відеоданих з РРС [15]. Першим кроком для виконання поставленої задачі стала передача зашифрованих повідомлень реалізована у вигляді двох програм (одна шифрує і посилає, друга приймає і розшифровує), їх роботу протестовано на Arduino платах з використанням радіоканалу на xBee пристроях зв'язку для підтвердження правильної роботи – рисунок 1. Для шифрування використано алгоритм AES – бібліотека AESLib [16]. Затримки шифрування склали декілька десятків мс.

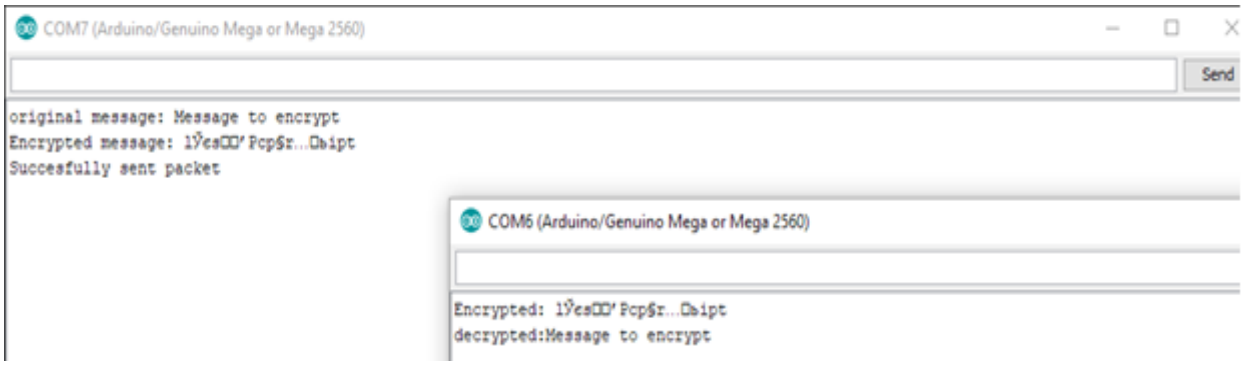


Рис. 1. Оригінальне, зашифроване та розшифроване повідомлення

Наступним кроком стала підтримка зчитування рядка символів, введеного в SerialMonitor з використанням під'єднаної клавіатури. Далі була реалізована двобічна передача зашифрованих даних. Було завершено роботу над програмою, що може одночасно приймати та передавати дані радіоканалом у захищеному вигляді. Дані вводяться з клавіатур, приєднаних до кожного з Arduino-пристроїв. Шифрування/дешифрування виконується за алгоритмом AES.

Результати двобічного прийому та передачі повідомлень подано на рис. 2.

Додатково була розроблена програма Bluetooth crypt для захищеного обміну даними між двома Arduino по bluetooth-радіоканалу на швидкості 57600-38400 біт/с. Як і в усіх попередніх версіях, дані шифруються відповідно до алгоритму AES.

Експерименти показали, що на високих швидкостях передачі даних (115200 біт/с та вище) зв'язок на використаних програмно-апаратних засобах є ненадійним, високий відсоток пакетів втрачається, що призводить до їх повторної передачі та загального зниження швидкості роботи. Тому рекомендованою швидкістю використання при

передачі по bluetooth-радіоканалу після 100 експериментів було визначено 57600 біт/с.

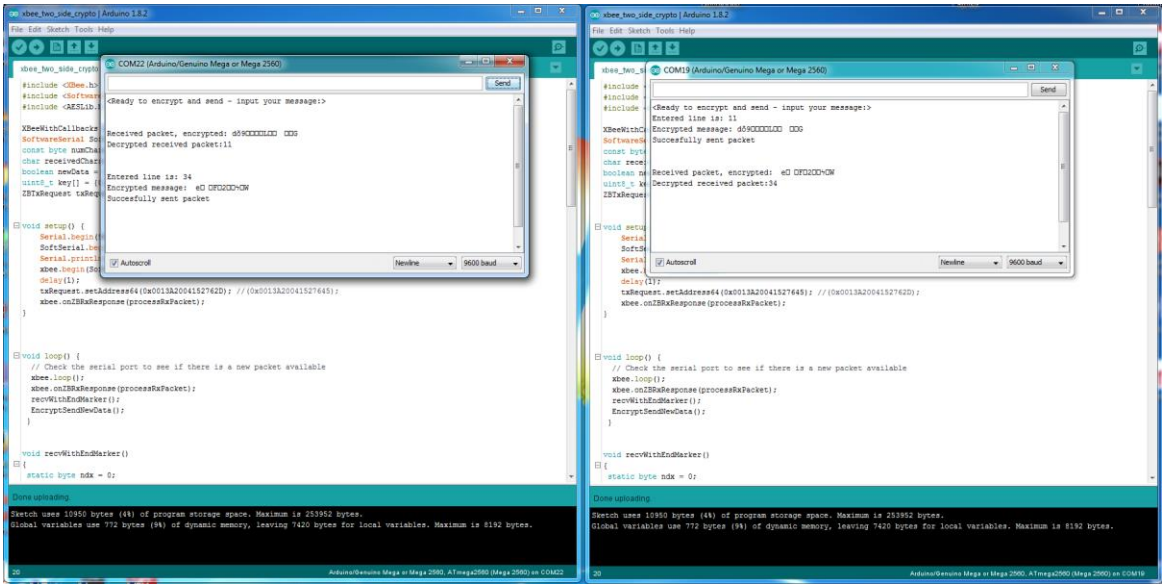


Рис. 2. Двобічний прийом та передача зашифрованих повідомлень

Алгоритм та програмна реалізація шифрування в chain-mode

Розглянемо тепер шифрування даних алгоритмом AES в режимі chain-mode при якому однакові пакети, шифруючись один за одним, будуть на виході видавати різний шифртекст. Використання цього режиму дозволить значно підвищити рівень захисту даних, особливо, команд керування РРС.

Для надійного захисту даних, що шифруються алгоритмом AES в режимі chain-mode, слід використовувати випадковим чином згенерований вектор ініціалізації (IV). Проведений аналіз показав, що найнадійнішим буде використання такого розробленого алгоритму:

- генерація частково-випадкового вектора IV на першому вузлі мережі, а для випадку керування РРС – на робочому місці оператора;
- шифрування вектора IV довготерміновим ключем;
- передача зашифрованого вектора IV іншим членам мережі (іншим РРС);
- розшифрування вектора IV та використання AES на його основі в режимі chain-mode.

У випадку слідування цій схемі навіть дізнавшись ключ шифрування, без знання початкового вектора зловмиснику неможливо буде розшифрувати отримані повідомлення.

Розроблена програма генерації частково випадкового вектора IV працює таким чином. Вона зчитує шумові сигнали з непідключених контактів плати та використовує ці випадкові фізичні значення для ініціалізації вектора IV.

Наступним етапом роботи стала розробка практичного варіанта двобічного застосування шифрування у поточному режимі через канал bluetooth, що реалізував описаний вище алгоритм.

Такий підхід значно підвищує рівень захищеності даних, що передаються, особливо у випадку, коли є необхідність декілька разів поспіль передати однакові пакети даних.

Верифікація імплементації розробленого алгоритму

Для оцінки якості рівня криптографічного захисту, що забезпечується з використанням розроблених та імплементованих алгоритмів та бібліотек шифрування, виконано верифікацію та тестування цих алгоритмів захисту інформації.

Першим етапом роботи по верифікації та тестуванню реалізації алгоритму AES шифрування на основі бібліотеки AESLib [16] стало використання відомої реалізації алгоритму в якості еталону. І перші результати отримано шляхом порівняння блоків після зашифровування з еталонними результатами шифрування [17]. Це вимагало переводити результати в формат Base64 – еталонна реалізація алгоритму видає результати шифрування саме у цьому форматі. Результати шифрування розробленої реалізації алгоритму

AES з тими ж вхідними даними та ключем, що були використані в еталонній реалізації: результат – блоки зашифрованих даних, отримані імплементованою на Arduino версією і еталонною реалізацією алгоритму [17], збігаються.

Наступним етапом стало тестування імплементованої реалізації бібліотеки AESLib для FIPS 197 [18] відповідно до американського стандарту валідації алгоритму AES – AESAVS [19]. Розглянемо отримані результати валідації для варіантів з ключем 128 і 256 біт.

Першою було виконано валідацію для тестів VarKey Mode 128 (варіант зі змінним ключом). Зашифрований та розшифрований тексти для усіх взятих зі стандарту тестових прикладів відповідали еталонним.

Наступним кроком реалізація бібліотеки AESLib була окремо протестована в CBC режимі шифрування для визначення її відповідності стандарту. Результати зашифрування та розшифрування з використанням еталонних блока даних та ключа розміром 128 біт також відповідають еталонним даним. Таким чином, виходячи з отриманих результатів тестування бібліотеки AESLib в chain mode (CBC) – тест підтвердив правильну роботу в цьому режимі.

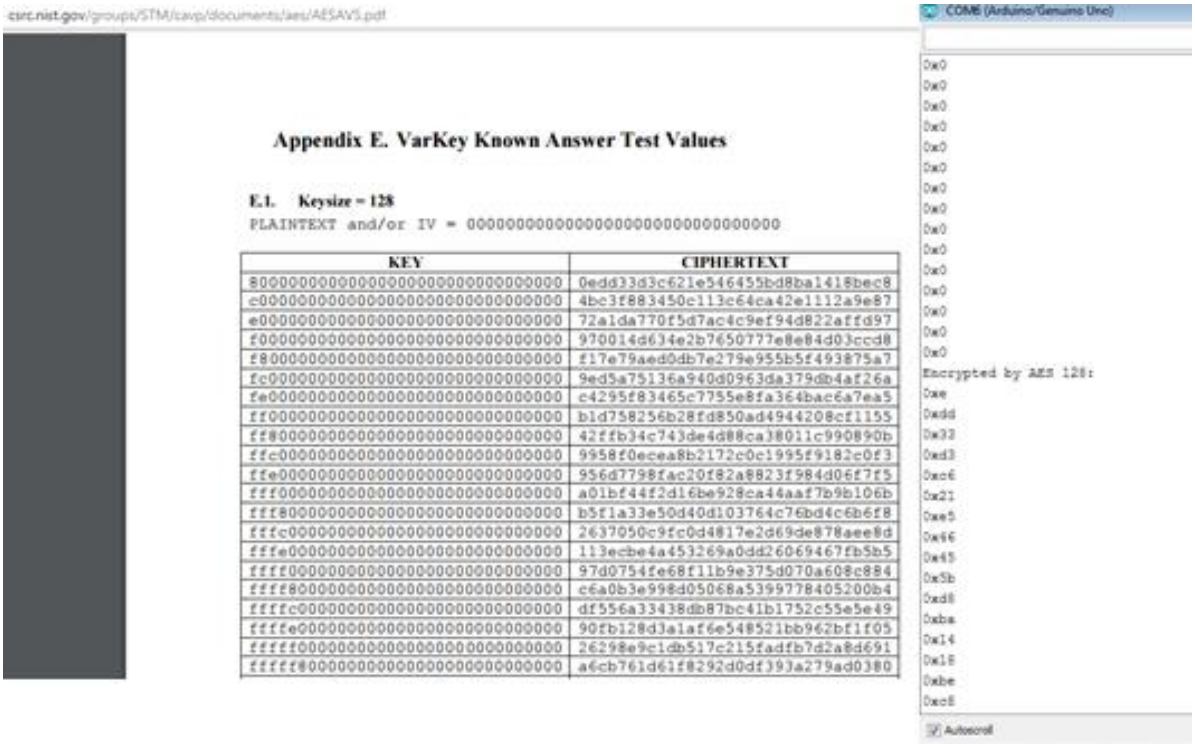
В процесі використання та дослідження бібліотеки AESLib виявлено, що ця бібліотека базується на бібліотеках Atmel. Плати Arduino Due, Arduino Uno, Arduino Mega побудовані на базі процесора Atmel AVR, тому бібліотека AESLib може на них працювати.

Але для деяких задач, повязаних з криптографією, необхідно застосовувати плати Arduino Due, побудовані на 32-bit процесорі ARM. І на Arduino Due бібліотека AESLib не може бути імплементована в принципі, як вона працювала б на базі багатопроцесорних обчислювальних комплексів (БОК). Тому постала задача обрати з існуючих бібліотек або створити нове рішення, що забезпечить роботу алгоритму AES на Arduino Due.

Проведений аналіз показав, що для цієї мети найкращим рішенням серед розглянутих (включаючи [20-21]) є застосування більш універсальної криптографічної бібліотеки AES, створеної Mark Tillotson [22]. Вона є не прив'язаною до бібліотек Atmel і працює на Arduino Due.

Розглянемо отримані результати проведеної верифікації створеної імплементації цієї бібліотеки на Arduino Due. Тести та порядок верифікації повторювали аналогічні тести та порядок для бібліотеки AESLib.

Еталонні значення для шифрування 128 біт в режимі VarKey співпали з відповідними отриманими результатами тестування бібліотеки AES для ключа розміром 128 біт (рис. 3).



csrc.nist.gov/groups/STM/cavp/documents/aes/AESAVS.pdf

Appendix E. VarKey Known Answer Test Values

E.1. Keysize = 128

PLAINTEXT and/or IV = 00000000000000000000000000000000

KEY	CIPHERTEXT
80000000000000000000000000000000	0edd33d3c621e546455bd8ba1418bec8
c0000000000000000000000000000000	4bc3f883450c113c64ca42e1112a9e87
e0000000000000000000000000000000	72a1da770f5d7ac4c9ef94d822affd97
f0000000000000000000000000000000	970014d634e2b7650777e8e84d03ccd8
f8000000000000000000000000000000	f17e79aed0db7e279e955b5f493875a7
fc000000000000000000000000000000	9ed5a75136a940d0963da379db4af26a
fe000000000000000000000000000000	c4295f83465c7755e8fa364bac6a7ea5
ff000000000000000000000000000000	b1d758256b28fd850ad4944208cf1155
ff800000000000000000000000000000	42ffb34c743de4d88ca38011c990890b
ffc00000000000000000000000000000	9958f0ecea8b2172c0c1995f9182c0f3
ffe00000000000000000000000000000	956d7798fac20f82a8823f984d06f7f5
fff00000000000000000000000000000	a01bf44f2d16be928ca44aaf7b9b106b
fff80000000000000000000000000000	b5f1a33e50d40d103764c76bd4c6b6f8
fffc0000000000000000000000000000	2637050c9fc0d4817e2d69de878aee8d
fffe0000000000000000000000000000	113ecbe4a45326 9a0dd26069467fb5b5
ffff0000000000000000000000000000	97d0754fe68f11b9e375d070a608c884
ffff8000000000000000000000000000	c6a0b3e998d05068a5399778405200b4
ffffc000000000000000000000000000	df556a33438db87bc41b1752c55e5e49
ffffe000000000000000000000000000	90fb128d3a1af6e548521bb962bf1f05
fffff000000000000000000000000000	26298e9c1db517c215fadfb7d2a8d691
fffff800000000000000000000000000	a6cb761d61f8292d0df393a279ad0380

COM6 (Arduino/Genuino Uno)

0x0
0x0
0x0
0x0
0x0
0x0
0x0
0x0
0x0
0x0
0x0
0x0
0x0
0x0
0x0
0x0
Encrypted by AES 128:
0xe
0xdd
0x33
0xd3
0xc6
0x21
0xe5
0x46
0x45
0x5b
0xd8
0xba
0x14
0x18
0xbe
0xc8

Autoscroll

Рис. 3. Приклад порівняння еталонних та реальних даних в режимі VarKey

Для розміру ключа 256 біт був додатково проведений тест Монте-Карло [23]. Отримані результати також співпали з еталонними. Наступним тестом для розміру ключа 256 біт був тест зі змінним текстом – VarText.

Всі тести пройдені успішно, таким чином, бібліотека може вважатись такою, що відповідає стандарту шифрування FIPS 197 [18].

В процесі тестування імплементації другої бібліотеки AES виявилось, що ця бібліотека має інакше організований chain-режим – CBC. Відповідно до застосованої при розробці бібліотеки AES ідеології, в режимі, запропонованому автором бібліотеки Mark Tillotson, вона є для нас непридатною, оскільки вимагає наявності усіх даних, що будуть передані в цьому режимі, перед початком передачі. Для випадків передачі потокового відео, або передачі команд керування, що мають виконуватись в поточному режимі, нові дані будуть надходити вже після того, як наявна частина даних має бути вже передана та отримана.

У зв'язку з цим виникла потреба розробити імплементацію CBC режиму шифрування даних для другої бібліотеки AES з нуля для забезпечення роботи у цьому режимі у прийнятному для виконання поставлених задач вигляді. Розглянемо результати роботи розробленого CBC режиму для бібліотеки AES.

Виконане тестування розробленої реалізації показало, що режим працює правильно, при послідовному пересиланні однакових блоків за рахунок зміни IV отримуємо різні блоки шифрованих даних, які відповідають еталонним значенням.

Виконане тестування результатів шифрування в цьому режимі на відповідність до стандарту AES підтвердило правильну роботу реалізації CBC-режиму.

Таким чином, після тестування відповідно до усіх необхідних для валідації програмної реалізації алгоритму AES тестів визначено, що реалізація розробленої імплементації бібліотек AESLib та AES алгоритму AES повністю відповідають стандарту FIPS 197.

Протокол захищеного обміну даними з РРС

Після завершення робіт над програмною реалізацією cipher-block chaining режиму бібліотеки AES, був виконаний аналіз шляхів застосування цього режиму. На основі результатів проведеного аналізу існуючих методів та алгоритмів захисту інформації в подібних системах передачі даних та результатів генерації випадкового вектору IV був розроблений новий протокол захищеного обміну даними з РРС.

Наведемо алгоритм його роботи.

1. Для випадку зв'язку типу точка-точка (наприклад, для керування оператором лише одним РРС) алгоритм роботи CBC-режиму за цим протоколом є очевидним і описаний вище. Дані передаються з підтвердженням отримання задля збереження синхронизації. Цей алгоритм повторюється для кожного нового сеансу зв'язку.

2. Алгоритм роботи протоколу захищеного обміну даними з РРС для випадку однорангової mesh-мережі, що містить більше одного учасника:

а) На першому етапі роботи, виконується ініціалізація мережі, на кожному її елементі незалежно будується таблиця маршрутизації. Таблицю маршрутизації кожен РРС будує незалежно – це зручніше, ніж її весь час розсилати, та й це б суперечило логіці однорангової mesh-мережі на вимогу. Визначається, з якими з елементів мережі є прямий зв'язок, з якими – зв’язок лише через ретрансляцію. Далі, коли є необхідність передати дані за якоюсь адресою, визначається, чи є прямий зв'язок з отримувачем, чи потрібна ретрансляція. В будь-якому випадку визначається, кому потрібно передати пакет даних.

б) Пакет даних це: 128 біт зашифровані дані + 4 біта адреса + (за необхідності) додаткові службові дані. За умовами постановки задачі маємо невелику групу РРС (зазвичай до 4 РРС), тому логічно зробити маленький адресний пул з прив'язкою адрес – для 8 РРС це буде 2 в 3 ступені – 3 біта. Отже, 4 біта нададуть необхідний рівень надлишковості.

Якщо з цим вузлом мережі обмін даними попередньо не виконувався, відбуваються ті ж дії, що і у випадку 1 – на основі фізичних випадкових даних генерується початковий вектор IV. Він шифрується довготерміновим ключем, передається цьому вузлу і далі зберігається обома вузлами у таблиці маршрутизації для відповідного вузла.

в) В подальшому цей вектор (що відповідно до принципу роботи CBC режиму, змінюється після кожного переданого пакета)

починає використовуватись для передачі даних між ними з підтвердженням отримання кожного пакету.

Таким чином, для кожної пари вузлів буде використовуватись індивідуальний вектор IV. Це призведе до зростання обсягу пам'яті, що потрібно мати на кожному вузлі зв'язку (додаткові 128 біт на кожен вузол мережі), але ці вимоги не є значними, а при цьому надається високий рівень захисту даних, що циркулюватимуть цією мережею.

г) Алгоритм передачі пакету по поточній таблиці маршрутизації: РРС визначає, чи безпосередньо він має посилати пакет до отримувача, чи через ретранслятор. Адреса отримувача передається в незашифрованому вигляді, тому одержувач отримує цю адресу без необхідності розшифрування пакету. Якщо адреса не його – він визначає по власній таблиці маршрутизації, як і відправник, куди слати цей пакет – і повторює процедуру з пункту а).

Висновки

В результаті досліджень створено і апробовано сімейство алгоритмів захисту передачі даних для мереж спеціального призначення з урахуванням особливостей дистанційного радіокерування рухом груп РРС (БПЛА та БНР), зокрема, у складних ситуаціях, що відповідають українським та міжнародним стандартам (ДСТУ ISO/IEC 15946-3, ДСТУ ISO/IEC 11770-3, ДСТУ ISO/IEC 18033-3:2015 та ін.). Розроблено алгоритми криптографічного захисту інформації, яка циркулює в таких мережах. В результаті їх застосування жодні дані (команди керування, телеметрія, відеосигнал) не циркулюють у мережі у незашифрованому вигляді. Розроблені алгоритми дозволяють виконувати захист інформаційних потоків для децентралізованих чарункових та ad hoc мереж у польових умовах без розгортання криптографічних серверів ключів навіть на базі низькопродуктивних серійних обчислювальних пристроїв.

Розроблене програмно-алгоритмічне забезпечення апробовано шляхом створення наземних дистанційно керованих модельних зразків РРС спеціального призначення та проведення тестування їх мережевої взаємодії. Проведені натурні експерименти з апробації розробленого програмно-алгоритмічного забезпечення у лабораторних умовах на базі макетів наземних дистанційно керованих РРС розвідувального призначення підтвердили його застосовність і працездатність та довели потенційну можливості його впровадження.

Досягнуті результати дозволяють, при збільшенні розмірів, потужності, вологозахищеності та інших параметрів розроблених дослідних зразків РРС, необхідних для ефективного їх використання, застосовувати їх (та розроблене відповідне програмне забезпечення) у незмінному вигляду у спеціальних застосуваннях. Це дозволить: підвищити надійність, захищеність та керованість РРС у польових умовах та протидіяти підміні GPS-позиціонування.

Перспектива продовження розробок в напрямі створення засобів захищеного керування групами РРС – це створення прототипу захищеної системи дистанційного радіокерування з резервними каналами: Wi-Max базова станція і бортовий Wi-Max/WiFi модем та резервні захищені мережі GPRS/GSM.

Список використаних джерел

1. Хорошко В. А., Чекатков А. А. Методы и средства защиты информации. – К.: “Юниор”, 2003. – 504 с.

2. Домарев В.В. Безопасность информационных технологий. Методология создания систем защиты. –К.:ООО «ТИД ДС», 2001. – 688 с.

3. Петраков А. В. Основы практической защиты информации. –М.: Радио и связь, 2005. – 384 с.

4. Корольов В.Ю. Персоналізація віртуальних обчислювальних ресурсів і інформаційних джерел в сервісно-орієнтованих архітектурах // Вісті академії інженерних наук України. – № 4 (34). – 2007. – С. 13–20.

5. Степанов Е.А. Корнеев И.К. Информационная безопасность и защита информации. – М.: ИНФРА-М, 2001. – 304 с.

6. Олейников Е. Экономическая и национальная безопасность. – М.: Экзамен, 2005. – 768 с.

7. Скляр Б. Цифровая связь. Теоретические основы и практическое применение. 2-е изд. – М.: Издательский дом "Вильямс", 2003. – 1104 с.

8. One A. Быстро и легко. Сеть для дома и офиса. – М.: Лучшие книги, 2004. – 400 с.

9. Bhaiji Yu. Network Security Technologies and Solutions. – Cisco Press, 2008. – 840 p.

10. Фергюсон Н., Шнайер Б. Практическая криптография.: Пер. с англ. – М.: Издательский дом "Вильямс", 2005. – 424 с.

11. Kahn D. The Codebreakers. The Story of Secret Writing. – New York: Charles Scribner's Sons, 1967. – 473 с.

12. Schneier B. Applied cryptography: protocols, algorithms, and source code in C. – John Wiley&Sons, 2007. – 816 p.

13. Баричев С.Г., Гончаров В.В., Серов Р.Е. Основы современной криптографии. – М.: Горячая линия–Телеком, 2002. – 175 с.

14. Венбо Мао Современная криптография. Теория и практика. – М.: Вильямс, 2005. – 768 с.

15. Кос С. Cryptographic Engineering. – Springer, 2009. – 528 p.

16. Arduino Library for AES Encryption (source based on avr-crypto-lib) [Електронний ресурс]. – Режим доступу: https://github.com/DavyLandman/AESLib

17. AES encryption. Encrypt and decrypt text with AES algorithm [Електронний ресурс]. – Режим доступу: http://aesencryption.net/

18. FIPS, PUB. "197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, US Department of Commerce, November 2001." [Електронний ресурс]. – Режим доступу: http://csrc. nist. gov/publications/fips/fips197/fips-197. pdf.

19. Lawrence E. Bassham III The Advanced Encryption Standard Algorithm Validation Suite (AESAVS) [Електронний ресурс]. – Режим доступу: http://csrc.nist.gov/groups/STM/cavp/documents/aes/AESAVS.pdf

20. New AES library [Електронний ресурс]. – Режим доступу: http://forum.arduino.cc/index.php?topic=88890.0

21. AES for microcontrollers (Arduino & Raspberry pi) [Електронний ресурс]. – Режим доступу: https://github.com/spaniakos/AES

22. Mark Tillotson's AES Library [Електронний ресурс]. – Режим доступу: http://utter.chaos.org.uk:/~markt/AES-library.zip

23. Соболь И.М. Метод Монте-Карло. – М.: Наука, 1978. – 64 с.

Інфомація про авторів:

Гуляницький Леонід Федорович – доктор технічних наук, старший науковий співробітник, завідувач відділу, Інститут кібернетики імені В.М. Глушкова НАН України. Наукові інтереси:

E-mail: leonhul.icyb@gmail.com

Огурцов Максим Ігорович – науковий співробітник, Інститут кібернетики імені В.М. Глушкова НАН України.

E-mail: romantic84@gmail.com

Ходзінський Олександр Миколайович – кандидат фізико-математичних наук, старший науковий співробітник, Інститут кібернетики ім. В.М. Глушкова НАН України.

E-mail: okhodz@gmail.com