УДК 004.71:621.39.002.5
DOI: 10.32626/2308-5916.2019-19.108-113

М. І. Огурцов, науковий співробітник
Інститут кібернетики імені В. М. Глушкова НАН України, м. Київ

РОЗРОБКА ПРОТОКОЛУ ЗАХИЩЕНОГО ОБМІНУ ДАНИМИ ДЛЯ СПЕЦІАЛЬНИХ МЕРЕЖ

Через стрімке зростання масштабу, складності задач і розширення сфер практичних застосувань мереж спеціального призначення необхідна розробка нових протоколів роботи таких мереж, які б мали високу адаптивність до умов застосування, а також включали надійні засоби захисту інформації. Метою досліджень стала розробка протоколу, алгоритму, математичного апарату і відповідного програмного забезпечення для спеціальних мереж з використанням синхронної і асинхронної передачі зашифрованих пакетів даних. Для шифрування після проведеного аналізу існуючих алгоритмів обраний для використання симетричний алгоритм AES. На основі отриманих результатів проведеного аналізу розроблено алгоритми криптографічного захисту інформації, яка циркулює у таких мережах. Розроблений і апробований новий протокол захищеного обміну даними для мереж спеціального призначення з урахуванням особливостей спеціальних мереж, що відповідають міжнародним стандартам, зокрема, у складних ситуаціях. Розроблені протокол та алгоритми дозволяють виконувати захист інформаційних потоків для децентралізованих чарункових та ad hoc мереж у польових умовах. Розроблене програмно-алгоритмічне забезпечення апробоване шляхом створення модельних зразків мереж спеціального призначення та проведення тестування мережевої взаємодії їх вузлів. Проведені натурні експерименти з апробації розробленого програмно-алгоритмічного забезпечення в лабораторних умовах підтвердили його застосовність і працездатність та довели потенційну можливість його впровадження. Проведене тестування на практиці показало, що затримки шифрування для реалізації розробленого протоколу склали декілька десятків мс, що дозволяє без проблем передавати сигнали, текст, службові команди, відео, зображення та звук. Застосування розробленого протоколу дозволить підвищити надійність, захищеність та керованість спеціальних мереж у польових умовах.

Ключові слова: *спеціальні мережі, захист інформації, безпровідні мережі, криптографія, AES.*

Вступ. Завдяки швидкому зростанню масштабу та рівня складності задач і розширення сфер практичних застосувань мереж спеціального призначення підвищується актуальність питання захищеної передачі

даних у таких мережах. Зокрема, велику актуальність набувають питання створення і практичної реалізації алгоритмів захищеної передачі даних та їх маршрутизації для спеціальних мереж, призначених для функціонування, наприклад, систем керування рухомими технічними об'єктами з мультимедійною інформацією і передачею кодованих команд у зашифрованому виді. Існуючі стандарти для безпровідних мереж, що функціонують за вимогою, і мобільні пристрої, доступні на ринку, не передбачають роботу в умовах використання засобів радіоелектронної боротьби, високого рівня активних завад та хакерських атак [1–3]. Крім того, вони не відповідають міжнародним стандартам.

Якщо при побудові спеціальної мережі не використовувати засоби захисту інформації, то потік даних, що циркулює у мережі, буде доступний будь-кому, хто має відповідні технічні засоби [4]. Зважаючи на можливі обмеження обчислювальних потужностей, необхідно дослідити варіанти застосування стандартних симетричних та/або асиметричних схем шифрування для та схем розповсюдження ключів [5–8]. Але на даний момент у більшості випадків засоби захисту інформації у спеціальних мережах не застосовуються [9]. А в тій незначній частині, де вони використовуються, звичайно застосовують лише стандартні засоби захисту інформації від виробника обладнання, що було використане для побудови спеціальних мереж. В поточних умовах такий підхід є неприйнятим, тому розробка загального протоколу захищеного обміну даними для спеціальних мереж є актуальною науковою задачею.

Мета досліджень це розробка протоколу, математичного апарату і відповідного програмного забезпечення захищеного безпровідного зв'язку у спеціальній мережі з використанням синхронної і асинхронної передачі зашифрованих пакетів даних та кодованих команд. Актуальність цих досліджень обумовлюється розширенням спектру завдань при застосуванні спеціальних мереж, зокрема роботизованих систем спеціального призначення, що керуються через безпровідні мережі, та важливістю інформації, яка циркулює всередині таких мереж.

Передача зашифрованих повідомлень. Практична реалізація розроблених протоколу та алгоритмів для їх апробації виконувалась на базі платформи Arduino з використанням радіоканалу на xBee пристроях зв'язку для підтвердження правильних результатів шифрування/розшифрування. Для шифрування після проведеного аналізу існуючих алгоритмів обраний для використання симетричний алгоритм AES [3, 7, 8, 10] — на основі бібліотек AESLib та Mark Tillotson's AES Library [11, 12] як таких, що успішно пройшли дослідження тестування правильності їх реалізації, проведене на основі [13].

Першим кроком для виконання поставленої задачі стала розробка алгоритму та практичної реалізації для двобічної передачі зашифрованих повідомлень.

Алгоритм та програмна реалізація шифрування в chain-mode. Наступним кроком стало застосування шифрування в режимі chain-mode. При застосуванні цього режиму однакові пакети, що шифруються послідовно один за одним, будуть на виході видавати різний шифртекст. Використання цього режиму дозволить значно підвищити рівень захисту даних, що передаватимуться в мережах спеціального призначення.

Для надійного захисту інформації, що шифрується алгоритмом AES в режимі chain-mode, слід використовувати випадковим чином згенерований вектор ініціалізації IV. Найбільш ефективним є використання апаратно згенерованого випадкового вектора ініціалізації [3, 8].

Проведений аналіз показав, що найнадійнішим буде використання такого **розробленого алгоритму**:

- генерація частково-випадкового вектора IV на першому вузлі мережі;
- шифрування вектора IV довготерміновим ключем;
- передача зашифрованого вектора IV іншим вузлам мережі;
- розшифрування вектора IV та використання AES на його основі в режимі chain-mode.

У випадку слідування цьому алгоритму навіть якщо ключ шифрування буде скомпрометовано, без знання початкового вектора зловмиснику неможливо буде розшифрувати отримані повідомлення.

Розроблена програма генерації випадкового вектора зчитує шумові сигнали з непідключених контактів Arduino плати та використовує ці випадкові значення для ініціалізації вектора IV.

Протокол захищеного обміну даними в спеціальній мережі. На основі отриманих результатів розроблений новий протокол захищеного обміну даними в спеціальних мережах [4, 5].

На першому етапі роботи виконується ініціалізація мережі. Кожен вузол мережі зберігає однаковий довготерміновий ключ, що використовується лише на етапі ініціалізації. При цьому на кожному вузлі таблиця маршрутизації будується незалежно. Пакет даних містить:

- 128 біт зашифрованих даних;
- 8 бітів адреса;
- додаткові службові дані (за необхідності).

Розглянемо послідовність роботи розробленого протоколу.

1. Для кожного іншого вузла окремо, на основі фізичних випадкових даних генерується початковий вектор IV.
2. Вектор IV шифрується довготерміновим ключем, послідовно передається відповідному вузлу (з підтвердженням отримання), з яким встановлюється інформаційний зв'язок.
3. Після успішної передачі вектор IV зберігається обома вузлами у таблиці маршрутизації для відповідного вузла.

4. В подальшому цей вектор починає використовуватись для передачі даних між ними з підтвердженням отримання кожного пакету. Тобто для кожної пари вузлів використовується індивідуальний вектор IV.
5. Кроки 1–4 повторюються, поки не визначено, з якими вузлами з множини усіх вузлів мережі є прямий зв'язок.
6. За необхідності передати дані визначається, чи є прямий зв'язок з отримувачем, чи потрібна ретрансляція.
7. Якщо прямого зв'язку немає — відбувається спроба встановити зв'язок через ретрансляцію, використовуючи вузли, що перебувають на прямому зв'язку.
8. Якщо вузол отримав пакет, призначений не для нього — він розшифровує пакет, визначає по власній таблиці маршрутизації, як і відправник, куди слати цей пакет — і повторює процедуру, починаючи з кроку 6.
9. Якщо в мережі з'явився новий вузол, інформаційний обмін з яким попередньо не виконувався, слід повторити такі ж дії, що і в пункті 1.

Висновки. В результаті проведених наукових досліджень розроблено алгоритми криптографічного захисту інформації, яка циркулює у спеціальних мережах. Створено і апробовано протокол захисту даних при їх передачі для мереж спеціального призначення з урахуванням особливостей таких мереж, зокрема, в ускладнених ситуаціях, що відповідає міжнародним стандартам (ДСТУ ISO/IEC 15946-3, ДСТУ ISO/IEC 11770-3, ДСТУ ISO/IEC 18033-3:2015 та ін.). В результаті проведених натурних експериментів визначено, що при його застосуванні жодні дані не циркулюють у мережі у незашифрованому вигляді.

Розроблені протокол та алгоритми дозволяють виконувати захист інформаційних потоків для децентралізованих чарункових та ad hoc мереж у польових умовах. Виконано всебічну верифікацію імплементації розроблених алгоритмів, що підтвердила їх відповідність відповідним стандартам.

Створене програмно-алгоритмічне забезпечення апробовано шляхом створення модельних зразків мереж спеціального призначення та проведення тестування мережевої взаємодії їх вузлів. Проведені натурні експерименти з апробації розробленого програмно-алгоритмічного забезпечення у лабораторних умовах підтвердили його застосовність і працездатність та довели потенційну можливість його впровадження. Проведене тестування на практиці показало, що затримки шифрування для реалізації розробленого протоколу склали декілька десятків мс, що дозволяє без проблем передавати сигнали, текст, службові команди, відео, зображення та звук.

Досягнуті результати дозволяють, при збільшенні розмірів, потужності, вологозахищеності та інших параметрів розроблених до-

слідних зразків вузлів спеціальної мережі, необхідних для ефективного їх використання, застосовувати їх (та відповідне розроблене програмне забезпечення) у незмінному вигляду у спеціальних застосуваннях. Це надасть можливість підвищити надійність, захищеність та керованість спеціальних мереж у польових умовах.

Перспективами подальших досліджень в напрямі створення засобів захищеної передачі даних у мережах спеціального призначення є створення прототипу захищеної системи дистанційного спеціального зв'язку з резервними каналами: Wi-Max базова станція і бортовий Wi-Max/WiFi модем та резервні захищені мережі GPRS/GSM.

Список використаних джерел:

1. Домарев В. В., Хорошко В. А., Чекатков А. А. Методы и средства защиты информации. Киев : Юниор, 2003. 504 с.
2. Безопасность информационных технологий. Методология создания систем защиты. Киев : ООО «ТИД ДС», 2001. 688 с.
3. Фергюсон Н., Шнайер Б. Практическая криптография ; пер. с англ. М. : Издательский дом «Вильямс», 2005. 424 с.
4. Огурцов М. И. Разработка протокола защищенного обмена данными для сетей специального назначения. *Міжнародна науково-практична конференція «Проблеми кібербезпеки інформаційно-телекомунікаційних систем»* (PCSITS), 5–6 квітня 2018, м. Київ, С. 166–169.
5. Огурцов М. І. Розробка протоколу захищеного обміну даними для спеціальних мереж. *Системний аналіз та інформаційні технології: матеріали 20-ї Міжнародної науково-технічної конференції SAIT 2018*, Київ, 21–24 травня 2018 р. Київ : ННК «ІПСА», НТУУ «КПІ», 2018. С. 249–251.
6. Kahn D. The Codebreakers. The Story of Secret Writing. New York : Charles Scribner's Sons, 1967. 473 p.
7. Schneier B. Applied cryptography: protocols, algorithms, and source code in C. John Wiley&Sons, 2007. 816 p.
8. Венбо Мао. Современная криптография. Теория и практика. М. : Вильямс, 2005. 768 с.
9. Корольов В. Ю, Поліновський В. В., Огурцов М. І. Моделювання мереж зв'язку рухомих дистанційно керованих систем на базі HLA. *Вісник Хмельницького національного університету.* Технічні науки. 2017. № 1 (245). С. 160–165.
10. FIPS, PUB. «197, Advanced Encryption Standard (AES), National Institute of Standards and Technology, US Department of Commerce, November 2001». URL: http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf.
11. Arduino Library for AES Encryption (source based on avr-crypto-lib) URL: https://github.com/ DavyLandman/AESLib.
12. Mark Tillotson's AES Library. URL: http://utter.chaos.org.uk:/~markt/AES-library.zip.
13. Lawrence E. Bassham III The Advanced Encryption Standard Algorithm Validation Suite (AESAVS). URL: http://csrc.nist.gov/groups/STM/cavp/-documents/ aes/AESAVS.pdf.

SECURE DATA EXCHANGE PROTOCOL DEVELOPMENT FOR SPECIAL NETWORKS

Due to the rapid growth of special purpose networks scale, tasks complexity and the practical applications areas expansion, it is necessary to develop new protocols for such networks. Their operation should have high adaptability to the usage conditions and also should include reliable information security means and algorithms. The research purpose was to develop a protocol, algorithm, mathematical apparatus and related software for special networks using synchronous and asynchronous encrypted data packets transmission and coded commands. For encryption, after existing algorithms analysis completion, the AES symmetric algorithm was chosen. On the basis of the conducted analysis results, a new protocol for secure data exchange in special purpose networks was developed and tested taking into account special networks features, including operations in difficult situations that meet Ukrainian and international standards. Cryptographic protection algorithms for information, circulating in such networks, were developed. The developed algorithms allow to protect the information flows for decentralized cellular and ad hoc networks in the field conditions. The developed software and algorithmic support were tested by creating physical special purpose networks models and conducting network interaction testing of their nodes. Conducted practical experiments for the developed software-algorithmic approbation in laboratory conditions confirmed its applicability and efficiency and proved the potential possibility of its implementation. The conducted testing showed that the encryption adds delays due to the developed protocol implementation is up to several tens of ms, which allows comfortable transmission of signals, text, commands, video, images and sound. The developed protocol application will increase the special networks reliability, security and control in the field.

Key words: *specialized networks, information security, wireless networks, cryptography, AES.*

Одержано 22.01.2019