УДК 519.6 + 004.942

В. Є. Опанасюк
І. Ю. Іванов
Ю. Ю. Іванов

МЕТОД ЗАХИСТУ ТЕЛЕМЕТРИЧНОЇ ІНФОРМАЦІЇ

Вінницький національний технічний університет

Анотація

У роботі проаналізовано метод захисту інформації на основі турбо-кодів у телеметричній системі діагностики.

Ключові слова: захист інформації, шифрування, завадостійке кодування, турбо-код, інтерлівер, телеметрична система.

Abstract

In this paper has been analyzed the method of information protection based on turbo-codes in the telemetry diagnostic system.

Keywords: information protection, encryption, error correcting coding, turbo-code, interleaver, telemetry system.

Вступ

Ефективна робота системи охорони здоров'я неможлива без впровадження новітніх технологій підготовки, передавання, зберігання та оброблення інформації, що дозволить прискорити аналіз стану здоров'я пацієнтів, заощадить час та людські ресурси [1, 2]. *Метою роботи* є розробка програмного комплексу для телеметричної діагностики з двонаправленим обміном цифровою інформацією між лікарем та пацієнтом зі збереженням конфіденціальності.

Результати дослідження

Програмний комплекс складається з системи реєстрації, оброблення та передавання інформації. Дані отримуються на місці та передаються на відстань до спеціаліста-лікаря, який зворотним каналом зв'язку може повідомити подальші дії [3]. Для прямої корекції помилок в об'ємних інформаційних повідомленнях на високих швидкостях передавання даних запропоновано використання турбо-коду з секретним ключем, який здатний не тільки протидіяти шуму у каналі зв'язку, а й захищати дані від несанкціонованого доступу. Відомі схеми об'єднаного захисту інформації застосовують додатковий модуль перед процесом кодування [4]. Запропонований метод дозволяє шифрувати дані прямо під час турбо-кодування, що зменшує часові затримки на обмін даними та складність системи.

Принцип роботи. Турбо-кодування базується на використанні двох паралельно працюючих елементарних кодерів. Інформаційний блок кодується двічі, причому другий раз – після попереднього випадкового перемішування бітів інтерлівером. Декодована інформація з виходу першого (другого) декодера використовується в якості апріорної інформації для входу другого (першого) декодера з метою уточнення результату декодування. Подібну операцію можна проводити багаторазово. Математично інтерлівер – це алгебраїчна система, яка виконує бієкцію $f : Z(q) \to Z(q)$, тобто дозволяє відобразити набір елементів $Z(q)$ на $Z(q)$, де q є довжиною блока інтерлівера. Задача деінтерлівера – виконати зворотні перетворення і відновити вихідну структуру інформації на етапі приймання [5]. Запропоновано, крім заданого інтерлівера, включити в процес турбо-кодування додатковий перемішувач та контролювати їх роботу секретним ключем. Обидва деінтерлівери теж контролюються даним ключем. Тільки санкціоновані користувачі мають доступ до ключів і можуть генерувати правильні перестановки індексів, що дозволяє декодувати дані та правильно дешифрувати їх. Зловмисники, які використовують неправильні ключі, отримають спотворений результат, оскільки інтерлівери та деінтерлівери чутливі до секретних ключів. Знайти секретну перестановку можна за виразом

$$X_{key} = (k \cdot X_0)(\mathrm{mod}\, q), \quad (1)$$

де $k = \{1,...,q-1\}$ – секретний ключ; X_0 – випадкова перестановка індексів від 0 до q-1 без повторень; q – розмір інтерлівера, просте число.

Оцінювання ефективності. Для оцінки криптостійкості системи можна використати коефіцієнт кореляції R між стартовими та дешифрованими даними. Значення $R = 1$ можна отримати у випадку співпадіння ключів, а це відбувається в одному із q-1 випадків. Простір ключів розширюється зі збільшенням розміру інтерлівера q. Для оцінювання завадостійкості системи необхідно знайти експериментальні залежності $BER = f(E_b/N_o)$, тобто частоти виникнення помилок залежно від нормованого відношення сигнал/шум. Оскільки інтерлівери, керовані секретними ключами, не збільшують кореляцію бітів в послідовності, то показник BER_{mod} для даної схеми не буде статистично відрізнятися від значення BER звичайного турбо-коду.

Висновки

Розглянутий метод захисту інформації на основі турбо-кодів можна використовувати для розв'язання задач передавання даних у телеметричній системі, завдяки простоті та гнучкості.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Akyildiz I.F. Wireless Multimedia Sensor Networks: A Survey / I.F. Akyildiz, T. Melodia, K.R. Chowdhury // IEEE Wireless Communications. – 2007. – Vol. 14. – P. 32-39.

2. Security and Privacy for Distributed Multimedia Sensor Networks / D. Kundur, W. Luh, U.N. Okorafor, T. Zourntos // Proceedings of the IEEE. – 2008. – Vol. 96. – P. 112-130.

3. Пономарчук Ю.В. Сравнительный анализ методов выборочного шифрования в беспроводных мультимедиа-сенсорных сетях / Ю.В. Пономарчук // Вестник ТОГУ. Информатика, вычислительная техника и управление. – 2013. – № 4(31). – С. 65-74.

4. Gligoroski D. Cryptocoding-Encryption and Error Correction Coding in a Single Step / D. Gligoroski, S. Knapskog, S. Andova // International Conference on Security and Management. – 2006. – P. 1-7.

5. Варгаузин В.А. Турбо-коды и итеративное декодирование: принципы, свойства, применение / В.А. Варгаузин, Л.Н. Протопопов // ТелеМультиМедиа. – 2000. – № 4. – С. 33-38.

Опанасюк Владислав Євгенович — студент групи 1АКІТ-20м, Факультет комп'ютерних систем і автоматики, Вінницький національний технічний університет, м. Вінниця.

Іванов Ігор Юрійович — лікар вищої категорії, медична мережа "Світ здоров'я", м. Вінниця.

Іванов Юрій Юрійович — канд. техн. наук, доцент кафедри автоматизації та інтелектуальних інформаційних технологій, Вінницький національний технічний університет, м. Вінниця, e-mail: Yura881990@i.ua.

Opanasyuk Vladislav Ye. — student, Faculty of Computer Systems and Automation, Vinnytsia National Technical University, Vinnytsia.

Ivanov Igor Yu. — doctor of the highest category, medical network "Svit Zdorovya", Vinnytsia.

Ivanov Yurii Yu. — Cand. Sc. (Eng), Docent, Faculty of Computer Systems and Automation, Vinnytsia National Technical University, Vinnytsia, e-mail: Yura881990@i.ua.