УДК 681.32

В. П. Семеренко
В. О. Дорошенко
В. А. Рубановський

Інтегрований захист інформації в комп'ютерних системах ідентифікації на основі коротких кодових радіоповідомлень

Вінницький національний технічний університет

Анотація

Метою роботи є вдосконалення методів та засобів процесу обміну короткими, захищеними повідомленнями через радіоканал зв'язку з використанням спеціалізованих мікропроцесорних пристроїв, пов'язаних із комп'ютером в спеціалізовану радіомережу, та створення відповідного програмного забезпечення.

Ключові слова: завадостійке кодування, криптографія, канал радіозв'язку, ЛПС

Abstract

The purpose of this work is to improve the methods and means of the process of exchanging short, secure messaging over a radio channel using specialized microprocessor devices connected to a computer into a specialized radio network, and creating appropriate software.

Keywords: error correcting coding, cryptography, radio channel, LFSM

Вступ

Безперервний розвиток інформаційних технологій вимагає постійного збільшення ефективності обробки і передавання інформації. Очевидно, ідеальний канал передавання даних повинен мати низьку вартість, мінімальну витрату енергії, високу пропускну спроможність, захищеність від завад, захист від викрадення і, що дуже бажано, повинен бути бездротовим.

Внаслідок несправності апаратури чи випадкових завад в каналах зв'язку може статися спотворення чи втрати важливої інформації. Для запобігання можливих помилок інформація потребує надійних способів її захисту [1].

Метою роботи є вдосконалення методів та засобів процесу обміну короткими, захищеними повідомленнями через радіоканал зв'язку з використанням спеціалізованого мікропроцесорного пристрою, пов'язаного із комп'ютером, та створення відповідного програмного забезпечення.

Суміщення кодування та криптографії.

При передаванні даних по каналах зв'язку виникають помилки. В результаті дані спотворюються і не можуть бути використані на прийомній стороні для подальшого опрацювання. Частота бітових помилок в потоку переданих даних на рівні фізичного каналу знаходиться в межах $10^{-2}... 10^{-6}$. З боку користувачів і багатьох прикладних процесів часто висовується вимога ймовірності появи помилок у прийнятих даних не гірше $10^{-6}... 10^{-12}$ [2]. Боротися з помилками можливо багатьма способами.

Найвідоміший спосіб полягає у використанні на передавальній стороні завадостійких кодів із виправленням помилок [3]. На приймальній стороні, відповідно, проводиться декодування прийнятої інформації і виправлення виявлених помилок. Можливість застосовування такого коду з

виправленням помилок залежить від числа надлишкових бітів, що генеруються кодером. Потрібно визначити оптимальну кількість надлишкових бітів. Якщо внесена надлишковість невелика, тоді прийнятих даних залишаться помилки. Якщо ж використовувати код із високою коректувальною здатністю виправляти помилки, тоді це призведе до низької швидкості передачі даних. Знання теорії завадостійкого кодування дозволяє визначити оптимальні параметри завадостійкого коду.

При передачі даних по каналам зв'язку необхідно вирішувати два завдання: захищати дані від атмосферних перешкод і можливих несправностей апаратури, а також забезпечувати секретність інформації, що передається. Для вирішення першого завдання служить теорія завадостійкого кодування, а для вирішення другого завдання є різні методи шифрування даних [4]. Математичні основи завадостійкого кодування і криптографії закладені в роботах К. Шеннона [5]. Відомий американський вчений вперше довів, що, з одного боку, теоретично можна досягти передачі інформації майже без помилок, і, з іншого боку, можливий досконалий шифр для забезпечення секретності переданих повідомлень. Отримані К. Шенноном результати стали відправною точкою для подальшого бурхливого розвитку теорії кодування і криптографії. Незважаючи на багато спільних рис, ці галузі науки мають також і багато відмінностей, що є причиною їх незалежного розвитку і малого взаємного впливу.

Завадостійке кодування та криптографія на основі теорії ЛПС

Для потокового шифрування і циклічних кодів існує різноманітний математичний апарат, тому проведемо обґрунтування його вибору з врахування особливостей нашої задачі.

Розглянемо спочатку лінійні фільтри. З їх допомогою можна виконати одну з найважливіших операцій – обчислення остач від ділення довільного полінома на породжувальний поліном циклічного коду. Матриці, які описують роботу лінійного фільтра, однозначно визначають параметри: циклічного коду, отже, можуть слугувати способом задання цього коду [6].

Для розв'язання задачі відображення вхід-вихід можна використати ще одну популярну математичну модель – модель скінченого автомата. Скінчений автомат реалізує автоматне відображення: перетворює вхідні слова у вихідні.

Для опису функціонування класичного скінченого автомата використуються логічні числення, на основі яких розроблені різноманітні алгебри логіки. Якщо базовим математичним апаратом взяти теорію скінчених полів Галуа, тоді отримаємо новий тип скінченого автомата, властивості якого будуть фактично збігатися з властивостями лінійних фільтрів. Такий тип скінченого автомата можна назвати лінійним автоматом і використати для нього самостійний термін: лінійна послідовнісна схема (ЛПС) [2].

Математично ЛПС в двійковому полі Галуа, в дискретні моменти часу t задається функцією переходів

$$S(t+1) = A \times S(t) + B \times U(t), \quad GF(2),$$

та функцією виходів

$$Y(t) = C \times S(t) + D \times U(t), \quad GF(2),$$

де A, B, C, D – характеристичні матриці ЛПС, S, U, Y – слова стану, вхідне, вихідне.

ЛПС належить до систем, процеси в яких розвиваються в часі , тобто до динамічних систем.

Висновок

В даній роботі розглянуто теоретичні основи суміщення завадостійкого кодування і криптографії. Для циклічних кодів і потокового шифрування використано єдиний математичний апарат – теорію ЛПС. Проаналізовано різні методи суміщення потокового шифрування та завадостійкого кодування. Наведені позитивні та негативні сторони кожного із методів.

Проведено порівняльний аналіз видів мікропроцесорних безпровідних систем обміну короткими кодовими повідомленнями, які використовуються в системах ідентифікації та їх параметри. Розглянуто різні методи ідентифікації. Проаналізовано їх переваги і недоліки.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Скляр Б. Цифровая связь. Теоретические основы и практическое применение : пер. с англ. – 2-е изд., перераб. – М. : Издательский дом “Вильямс”, 2004. – 1104 с.
2. Семеренко В. П. Теорія циклічних кодів на основі автоматних моделей : монографія. – Вінниця : ВНТУ, 2015. – 444 с.
3. Морелос-Сарагоса Р. Искусство помехоустойчивого кодирования. Методы, алгоритмы, применение : пер. с англ. – М. : Техносфера, 2006. – 320 с.
4. Семеренко В. П. Интегрированная защита информации: криптография плюс помехоустойчивое кодирование // Захист інформації, 2011. – № 3. – С. 44–52.
5. Шеннон К. Работы по теории информации и кибернетике. – М. : Изд-во иностр. лит., 1963. – 829 с.
6. Гилл А. Линейные последовательностные машины. – М. : Наука, 1974. – 288 с.

Семеренко Василь Петрович – канд. техн. наук, доцент кафедри обчислювальної техніки, Вінницький національний технічний університет, Вінниця, e-mail: vasilsemerenko@gmail.com

Дорошенко Віктор Олексійович – студент групи 1КІ-16б, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця

Рубановський Владислав Анатолійович – студент групи 1КІ-16б, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця

Semerenko Vasyl P. – PhD, Associate Professor, Department of computer technique, Vinnytsia National Technical University, Vinnytsia, e-mail: vasilsemerenko@gmail.com

Doroshenko Victor O. – student, Department of computer technique, Vinnytsia National Technical University, Vinnytsia

Rubanovskiy Vladislav A. – student, Department of computer technique, Vinnytsia National Technical University, Vinnytsia