УДК 004.056

В. І. Малюшицький[1]
О. П. Войтович[2]

МЕТОД КОДУВАННЯ У СЕНСОРНИХ МЕРЕЖАХ

1 Вінницький національний технічний університет.

Анотація

Розглянуто новий метод захисту передачі даних в сенсорних мережах, шляхом кодування інформації з використанням М-послідовності.

Ключові слова: WSN, проблеми безпеки, кодування, М-послідовність, регістр зсуву з лінійним зворотнім зв'язком.

Abstract

The new method of protecting data in sensor networks by encoding information using M-sequence is considered.

Keywords: WSN, security issues, encoding, the M-sequence, linear feedback shift register,.

Вступ

Бездротові сенсорні мережі (БСМ) щороку все активніше проникають у всі галузі промисловості та сфери діяльності людини. На даний час вони широко використовуються не тільки для збору і обробки даних та керування промисловими об'єктами, але і у звичайному побуті у вигляді Інтернету речей (Internet of Things).

Основним завданням БСМ є збір даних з розподілених на значній території сенсорів фізичних параметрів. БСМ ефективно використовують у системах екологічного, технічного та медичного моніторингу. Однак останнім часом все частіше як джерела інформації в БСМ виступають аудіосенсори та відеосенсори, що ставить підвищені вимоги до характеристик цих мереж. На сьогоднішній день системи захисту сенсорних мереж не використовують всі необхідні послуги безпеки, і необхідно розробляти нові методи, що враховують всі сучасні вимоги.

Результати дослідження

При передачі даних в сенсорних мережах від сенсора до сенсора, інформація може бути легко перехоплена і використана зловмисником в своїх цілях. Оскільки, БСМ є мережею, яка передає конфіденційні дані, необхідно захищати інформацію. Даний метод пропонує використовувати кодування інформації.

Кодування відбувається на основі регістра зсуву із лінійним зворотнім зв'язком, який потрібен для створення М-послідовності, яка має такі властивості:

- М-послідовності є періодичними з періодом $N = 2^n - 1$;
- протягом одного періоду М-послідовності кількість символів, які приймають значення одиниця, на одиницю більша, ніж кількість символів, які приймають значення нуль;
- будь-які комбінації символів довжини n, протягом одного періоду М-послідовності за винятком комбінації з нулів зустрічаються не більше одного разу. Комбінація з нулів заборонена, оскільки на її основі може генеруватися лише послідовність з одних нулів;
- сума по модулю 2 будь якої М-послідовності з її довільним циклічним зсувом також є М-послідовністю;
- періодична АКФ будь-якої М-послідовності має постійний рівень бічних пелюсток, що дорівнює $1/N$.

Регістр зсуву з лінійним зворотним зв'язком (англ. linear feedback shift register, LFSR) – поширений спосіб отримання псевдовипадкових послідовностей.

У регістрі зсуву з лінійної зворотним зв'язком виділяють дві частини (модуля): власне регістра зсуву і схеми (або підпрограми) обчислення значення зсуву біта. Регістр складається з функціональ-

них осередків (або бітів машинного слова або кількох слів), в кожному з яких зберігається поточний стан одного біта. Кількість осередків, називають довжиною регістра. Біти (комірки) зазвичай нумеруються числами, в даному випадку *0, 1, 2,…255*, кожна з яких здатна зберігати *1* біт, причому в комірку *0* відбувається зсув обчисленого біта, а з комірки *255* витягується черговий згенерований біт (рис. 1). Обчислення зсуву біта зазвичай виробляється до зсуву регістра, і тільки після зсуву значення обчисленого біта поміщається в комірку *0*.

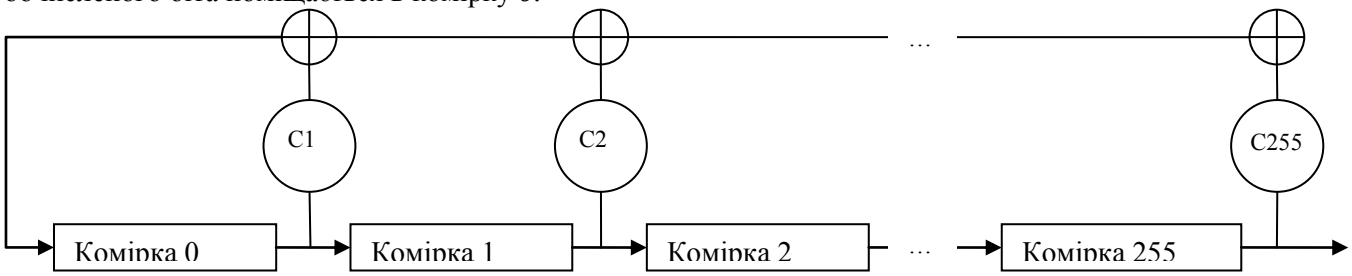

Рисунок 1 - Схема регістру зсуву зі зворотнім зв’язком

Оскільки, сенсори підключаються хаотично один до одного є велика необхідність захищати дані, тому наведено новий метод кодування.

Сторона А відправляє стороні В дані довжиною 256 біт. В момент передачі біт, що виходить з LFSR та біт з пакету даних об’єднуються операцією XOR і формується закодована інформація. Значення регістра зсуву із лінійним зворотнім зв’язком попередньо узгоджується між сторонами.

Для даних, що передаються, обчислюється автокореляційна функція (АФК). Для комбінації з 256 символів АФК дорівнює 128 [1].

Сторона В прийнявши закодоване повідомлення порівнює його побітово із М-послідовністю, отриманою на стороні В. Створюється лічильник, який підраховує кількість одиниць, які співпали. Для комбінації, що передається обчислюється автокореляційна функція (АФК). Для комбінації з 256 символів АФК дорівнює 128. Якщо ця кількість більша за 128, тобто більша за половину, значить сторона В отримала правильну послідовність [2].

Для збільшення надійності сторона А надсилає одну й ту саму отриману 256-бітну послідовність 256 разів, а сторона В кожного разу надсилає стороні А відповідь, щодо кількості одиниць, якщо кількість одиниць більша за половину (128 біт), то сторона А може довіряти стороні В і передавати закодовані дані в подальшому.

Отже, можна отримати метод захищеної передачі даних на основі кодування повідомлення та самосинхронізації сторін А та В.

Висновки

Описано спосіб кодування, який дозволяє створити безпечний канал передачі даних, застосувавши кодування на основі М-послідовності, яка має ряд властивостей і утворюється за допомогою регістра зсуву з лінійним зворотнім зв’язком, що забезпечує безпеку передачі від сторони А до сторони В.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Кулик А. Я. Аналіз ортогональних кодових послідовностей, використовуваних для організації широкосмугової модуляції / А. Я. Кулик, А. Є. Шакула // Вісник ВПІ. – Вінниця: ВНТУ, 2005 – 76-81 с.
2. Harmuth H. F. Nonsinusoidal waves for radar and radio communication. / H. F. Harmuth. – Washington: The Catholic University of America, 1981.

Віктор Іванович Малюшицький - студент групи БС-13 б, факультет інформаційних технологій та комп’ютерної інженерії, Вінницький національний технічний університет, Вінниця, e-mail: 18viktor01@gmail.com.

Олеся Петрівна Войтович – к. т. н. доцент каф. захисту інформації, Вінницький національний технічний університет, м. Вінниця.

Viktor I. Malyushitskiy - student of BS-13 b, Faculty of Information Technology and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: 18viktor01@gmail.com .

Olesya P. Voytovych - Cand. Sc. (Eng), Associate Professor Department information security, Vinnytsia National Technical University, Vinnytsia.