УДК 681.325.5.068

Сачанюк-Кавецька Н. В.
Бондаренко І. О.

Циклічне кодування даних в системах контролю доступу з використанням логіко-часових функцій у формі поліномів

Вінницький національний технічний університет

Анотація

В доповіді розглянуто можливість циклічного кодування ідентифікаційних логіко-часових функцій, що містять усі важливі характеристики переданих повідомлень. Для доступного формального опису такого кодування використано подання логіко-часових функцій у формі поліномів.

Ключові слова: логіко-часова функція, Δ-інтервал, поліном, циклічний код.

Abstract

The report considers the possibility of cyclic encoding of identification time-logic functions that contain all important characteristics of the transmitted messages. For an accessible formal description of such coding, representation of time-logic functions in the form of polynomials is used.

Keywords: time-logic functions, Δ- interval, polynomial, cyclic code.

Вступ

Розвиток інформаційних технологій вимагає стратегічної переорієнтації підприємств, організацій та установ. Використання комп'ютерних систем для вирішення різноманітних підприємницьких завдань, стратегічного розвитку, реалізації різноманітних зв'язків підприємств з їх партнерами, клієнтами, керуючими установами в On-line режимі дало можливість не обмежувати інформаційні потоки та інформаційні процеси межами окремого підприємства. Інформація та інформаційні системи, мережі, в яких функціонують підприємства, організації, установи, є їх надзвичайно важливими ресурсами [1]. Саме цілісність та конфіденційність інформації може мати особливе значення для конкурентоспроможності організації, руху коштів, рентабельності, відповідності правовим нормам законодавства України та міжнародним правовим вимогам, репутації установи. З іншого боку, через посилення залежності організацій від інформаційних, комунікаційних систем та послуг, вони стають більш вразливими до можливості несанкціонованого доступу до інформаційних ресурсів. Більше того, тенденція до переходу на розподілені обчислювальні системи значно зменшує можливості фахівців централізовано контролювати інформаційні системи та мережі. Тому актуальним є питання захисту інформаційних ресурсів від несанкціонованих управлінських дій та доступу сторонніх осіб або програм до комп'ютерних даних.

Результати дослідження

Система кодування інформації є одним із ключових моментів розробки політики інформаційної безпеки [2] та значно підвищує захист інформаційної інфраструктури від несанкціонованого доступу. Такий підхід легко можна реалізувати в логіко-часовому середовищі, перетворивши всі параметри необхідного для передачі повідомлення на логіко-часові функції (ЛЧФ) [3], яких є три функціонально повні класи. Наприклад, елементарна ЛЧФ першого класу, що між двома нулями приймає стале значення:

$$f(t,t_1,T_1)=\begin{cases} t-t_1, & \textit{якщо } t_1 < t \le t_1+T_1 \\ 0, & \textit{якщо } \ t_1+T_1 < t \le t_1 \end{cases}, \qquad (1)$$

де t – поточне значення параметра часу, t_1 – часова координата, T_1 – тривалість відрізку існування.

ЛЧФ розглядаються на часовому проміжку $[t_k, t_{k+1}]$, дискретизованому за допомогою Δ-інтервалу (Δ-дискретизації)– мінімального часового інтервалу, довжиною Δ_i ($\Delta_i = t_{i+1} - (t_i + T_i)$), між двома часовими координатами ЛЧФ. Потім за допомогою ЛЧФ-характеристик формують ідентифікаційну функцію сигналу (з ранжуванням характеристик, чи без), яка є унікальною для даного повідомлення і містить усю необхідну інформацію. Надалі ЛЧФ будемо позначати $f_i(t)$.

Для спрощення обрахунків в логіко-часовому середовищі пропонуємо використати циклічні коди, оскільки це є ціле сімейство завадостійких лінійних кодів, що забезпечують досить велику гнучкість з точки зору можливості реалізації коду із необхідною здатністю виявлення та виправлення помилок. Циклічний код відноситься до систематичних блочних (n, k) кодів, у яких k перших розрядів є комбінацією первинного коду, а наступні $(n-k)$ розрядів є перевірними.

В основі побудови циклічних кодів лежить операція ділення заданої ЛЧФ на породжуючий незвідний поліном ступеня r. Остача від ділення використовується при формуванні перевірних розрядів. При цьому операції ділення передує операція множення, яка здійснює зсув вліво k-розрядної інформаційної кодової комбінації на r розрядів.

На довільному Δ-інтервалі розбиття ЛЧФ може змінювати своє значення. В таких випадках доцільно коригувати значення відповідної функції. Це коригування ідентичне квантуванню, але для ЛЧФ таке коригування виконується за тією ж координатою, що й дискретизація. В цьому контексті краще використати термін «фільтрація». Тобто, для математичного опису повідомлення використовуються фільтровані функції.

Опис циклічних кодів та їх побудову зручно проводити за допомогою многочленів (або поліномів) [4]. Слід відмітити, що запис ЛЧФ у вигляді поліномів дозволяє відобразити формалізованим чином операцію циклічного зсуву вихідної ЛЧФ. Наприклад, для ЛЧФ другого класу, яка містить два відрізки існування, які не перетинаються між собою (рис. 1) відповідає поліном: $P_6(t) = t^2 + t^3 + t^6$,

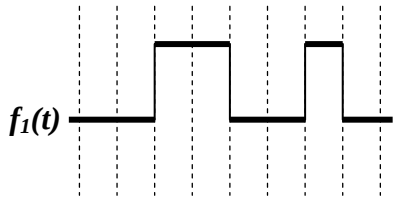

Рисунок 1 – Можливий варіант ЛЧФ з двома інтервалами травалості

а монотонно зростаючій ЛЧФ, зображеній на рисунку 2, відповідає поліном: $P_2(t) = t + 2t^2$.

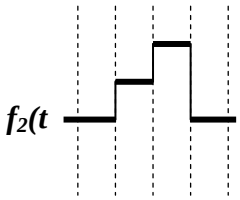

Рисунок 2 – Можливий варіант зростаючої ЛЧФ

Для представлення вихідного повідомлення, переданого у вигляді ЛЧФ, циклічним кодом, дотримуються такого алгоритму:

1. Подаємо вихідне повідомлення (ЛЧФ) у вигляді поліному $P_r(t)$.
2. Визначаємо контрольне число Δ-інтервалів (r – порядок поліному повідомлення). Визначаємо відповідно контрольному числу породжуючий поліном $P(t)$
3. Домножуємо $P_r(t)$ на t^r.
4. Ділимо $P_r(t) \cdot t^r$ на породжуючий поліном. Остачу такого ділення позначаємо через $R(t)$.

5. Формуємо поліном кодованого повідомлення $A(t) = P_r(t) \cdot t^r + R(t)$ та будуємо відповідну йому ЛЧФ.

Слід зауважити, що кодоване повідомлення немає помилок (інформація передана правильно), якщо остача від ділення цього повідомлення на породжуючий поліном дорівнює нулю. Операція ділення є звичайним діленням многочленів, однак замість віднімання використовуємо операцію нерівнозначного віднімання ($|k|$), яка базується на Δ - дискретизації:

$$f_1(t, t_{11}, T_{11}, a_1)|k|\, f_2(t, t_{21}, T_{21}, a_2) = \left\{(t - (t_1 + i\Delta_i)) \cdot |a_{i1} - a_{i2}|, t_1 = \min(t_{11}, t_{21})\right\}, \quad (2)$$

де t_{11}, t_{21} – часові координати змінних,

T_{11} та T_{21} - тривалості відрізків існування першої та другої функції,

a_1 та a_2 - відповідні амплітуди, i - кількість Δ - інтервалів в обраному часовому інтервалі,

Δ_i - тривалість Δ -інтервалу,

a_{i1}, a_{i2} - відповідні амплітуди на i -му Δ -інтервалі.

Результатом цієї операції буде знову ЛЧФ, яку можна назвати нерівнозначною різницею.

Знайдемо кодоване повідомлення для поліному $P_6(t) = t^2 + t^3 + t^6$. В даному випадку контрольне число Δ -інтервалів $r = 6$, тому $P(t) = t^6 + t + 1$ – породжуючий поліном. Помножимо поліном переданого повідомлення на t^6: $P_6(t) \cdot t^6 = t^8 + t^9 + t^{12}$. Остача від ділення одержаного поліному та породжуючий буде $R(t) = t^4 + 1$. Таким чином, поліном кодованого повідомлення $A(t) = P_r(t) \cdot t^r + R(t) = t^{12} + t^9 + t^8 + t^4 + 1$. ЛЧФ, що відповідає даному поліному подано на рисунку 3.

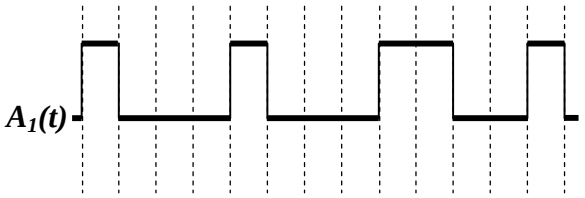

Рисунок 3 – Кодоване повідомлення інформації, переданої ЛЧФ $f_1(t)$

Оскільки частка від ділення кодованого повідомлення на породжуючий поліном дорівнює нулю, то дане повідомлення не містить помилок.

Знайдемо кодоване повідомлення для зростаючої ЛЧФ $f_2(t)$, зображеної на рисунку 2. Даній функції відповідає поліном $P_2(t) = t + 2t^2$, з контрольним числом $r = 2$. Таким чином, породжуючий поліном набуває вигляду $P(t) = t^2 + t + 1$ і $P_2(t) \cdot t^6 = 2t^4 + t^3$. Виконавши ділення одержаного поліному на породжуючий одержуємо $R(t) = 2t + 2$. Отже, $A(t) = P_r(t) \cdot t^r + R(t) = 2t^4 + t^3 + 2t + 2$ і ЛЧФ, що відповідає даному поліному зображена на рисунку 4.

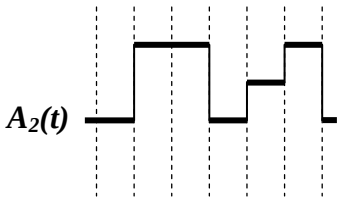

Рисунок 4 – Кодоване повідомлення інформації, переданої зростаючою ЛЧФ $f_2(t)$

Так як $\frac{2t^4 + t^3 + 2t + 2}{t^2 + t + 1} = 2t^2 + 2$ і залишок дорівнює нулю, то дане повідомлення не містить помилок.

Висновки

Спосіб циклічного кодування ідентифікаційних ЛЧФ, що містять усі важливі характеристики переданого повідомлення, значно підвищує захист інформаційної інфраструктури від несанкціонованого доступу. Використання логіко-часового середовища дозволяє передати велику кількість інформації з мінімальною кількістю помилок. Запропонований спосіб циклічного кодування досить легко апаратно реалізувати на базі регістрів зсуву з прямими та зворотними зв'язками.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Смит С. Цифровая обработка сигналов. Практическое руководство для инженеров и научных работников / Смит Стивен; пер. с англ. А. Ю. Линовича, С. В. Витязева, И. С. Гусинского. – М. : Додэка XXI, 2-12. – 720 с
2. Панасенко С. П. Алгоритмы шифрования : специальный справочник / Панасенко С. П. – СПб. : 2009. – 230 с.
3. Сачанюк-Кавецька Н. В. Елементи око-процесорної обробки зображень у логіко-часовому середовищі. Монографія / Сачанюк-Кавецька Н. В., Кожем'яко В. П. – Універсум-Вінниця, – 2004. – 135 с.
4. N. Sachaniuk-Kavets'ka, V. Kozhemiako, W. Wojcik, D. Kassymkhanova, A. Kalizhnova The use polynomials as a possible variant analytical processing on logic-time functions// Optical Fibers and Their Applications 2015 Proceedings of SPIE.– Volume 9816. –Lublin, Poland, 98161S-1 to 98161S-2.

Сачанюк-Кавецька Наталія Василівна – канд.техн. наук, доцент, доцент каф. ВМ, Вінницький національний технічний університет, e-mail: skn1901@gmail.com

Бондаренко Ірина Олексіївна – студентка групи УБ-15б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет

Sachaniuk-Kavets'ka Natalia – Candidate of Technical Sciences, Associate Professor, Associate Professor the department of Higher mathematics, Vinnysia National Technical University, e-mail: skn1901@gmail.com

Iryna Bondarenko – student of UB-15b group, faculty of management and informational security, Vinnytsia National Technical University