МЕТОДИ ПОШУКУ ДУБЛІКАТІВ СКОМПАНОВАНИХ ТЕКСТІВ НАУКОВОЇ СТИЛІСТИКИ

Дана стаття присвячена такій темі, як пошук плагіату. У статті представлена модифікація алгоритму шинглів для пошуку нечітких дублікатів для скомпонованих документів. Виграш у продуктивності планується досягти за рахунок зменшення кількості порівнянь пар шинглів за рахунок розбиття скомпонованих тестів на розділи.

Ключові слова: хеш-функція, шингл, плагіат, скомпонований документ, дублікат, блок.

Квашина Юлия Андреевна, *кафедра программной инженерии, Харьковский национальный университет радиоэлектроники, Украина,* ***e-mail: julia.kvashina@gmail.com.***

Квашина Юлія Андріївна, *кафедра програмної інженерії, Харківський національний університет радіоелектроніки, Україна.*

Kvashina Julia, *Kharkiv National University of Radio Electronics, Ukraina,* ***e-mail: julia.kvashina@gmail.com***

УДК 621.391

Корчинский В. В.

МЕТОД ПОВЫШЕНИЯ СТРУКТУРНОЙ СКРЫТНОСТИ ПЕРЕДАЧИ ИНФОРМАЦИИ В СИСТЕМЕ СВЯЗИ МНОГОПОЛЬЗОВАТЕЛЬСКОГО ДОСТУПА

В статье предложен метод формирования группового сигнала для системы связи многопользовательского доступа. Для повышения структурной скрытности информационных двоичных сигналов индивидуальных каналов применена система кодирования на основе многоуровневых таймерных сигнальных конструкций. С целью снижения эффективности дешифрирования перехваченного группового сигнала используется метод разделения индивидуальных сигналов по уровню.

Ключевые слова: *таймерный, сигнал, уровень, конфиденциальный, сигнатура, несанкционированный доступ, скрытность, канал, защита.*

1. Введение

В настоящее время при проектировании конфиденциальных систем связи многопользовательского доступа особый интерес представляют методы передачи, которые обеспечивают не только увеличение пропускной способности канала связи, но и повышают скрытность передаваемой информации [1—6].

Скрытность передачи [4] является одним из важных показателей помехозащищенности и определяет способность системы противостоять действиям, направленным на обнаружение сигнала и измерение его параметров. Не менее важным показателем помехозащищенности является помехоустойчивость, которая характеризует способность системы работать с заданным качеством в условиях воздействия различного рода помех.

Очевидна связь этих двух показателей, так как при решении вопросов, направленных на повышение скрытности синтезируемых сигнальных конструкций, в первую очередь необходимо выполнить условие по обеспечению заданной верности передачи.

В зависимости от требований к показателю скрытности передачи различают следующие виды скрытностей сигнальных конструкций: энергетическая, структурная, информационная и т. д. [1]. Энергетическая скрытность определяет способность системы противостоять мерам, направленным на обнаружение сигнала средствами несанкционированного доступа (НСД). Структурная скрытность должна противостоять мерам НСД, которые направлены на раскрытие формы сигнала и измерение его параметров при условии, что сигнал уже обнаружен и перехвачен. Информационная скрытность [9—12] определяется способностью противостоять мерам, направленным на раскрытие смысла передаваемых сообщений с помощью сигналов информации. Данный вид скрытности реализуется в основном на верхних уровнях эталонной модели OSI [7, 8].

Потенциальная структурная скрытность определяется количеством двоичных измерений (д. из), которое необходимо выполнить для раскрытия структуры сигнала без учета алгоритмов обработки на станции НСД [4]. Общее выражение для потенциальной скрытности имеет вид

$$S = \log_2 A, \qquad (1)$$

где A — ансамбль реализаций, определяемый количеством всех возможных значений каких-либо параметров сигнала. Такими параметрами могут быть несущая частота, структура кода, время прихода сигнала и др. В общем случае скрытность зависит от способа построения конкретного вида сигнала.

В работе [5] рассмотрена возможность увеличения структурной скрытности сигналов в каждом индивидуальном канале системы за счет совместного использования таймерных сигнальных конструкций (ТСК) и псевдослучайных последовательностей. Представляет интерес дальнейшее развитие этого направления для задачи повышения структурной скрытности формируемых сигнальных конструкций группового сигнала.

Целью статьи является разработка метода формирования группового сигнала на основе множества многоуровневых таймерных сигнальных конструкций с разделением их по уровню.

2. Алгоритм кодирования сигнала индивидуального канала

Для увеличения структурной скрытности сигналов в каждом индивидуальном канале системы связи предлагается осуществлять кодирование информационных сигналов $x_1, x_2, ..., x_N$ многоуровневыми таймерными сигнальными конструкциями с последующим объединением их в групповой сигнал.

Рассмотрим принцип построения одноуровневой ТСК [3]. Множество ТСК формируется на задаваемом интервале времени $T_c = nt_0$ (n — количество элементарных посылок, t_0 — их длительность) при базовом элементе Δ ($\Delta = t_0/s$, $s \in 1, 2, 3, ..., l$ — целые числа).

В отличие от разрядно-цифрового кодирования, когда информация о передаваемом разряде определяется уровнем сигнала элементарной посылки, в ТСК информация заложена в нескольких отдельных временных интервалах сигнала $t_c = t_0 + k\Delta$ ($k \in 0, 1, 2, ..., s\cdot(n-2)$) и их взаимном положении на интервале формирования T_c. Пример формирования нескольких реализаций ТСК на интервале времени $T_c = 4t_0$ при базовом элементе Δ показан на рис. 1.

По своей структуре ТСК представляют собой вид разрядно-цифровых кодов (РЦК), в которых разрешенные для передачи сигнальные конструкции имеют не менее s подряд передаваемых элементов Δ одного знака («1» или «0»).

Такой метод формирования позволяет передавать в канал отрезки сигнала длительностью $t_A \geq \Delta\cdot(s+i)$, где $i = 0, 1, 2, 3 \ldots$, что исключает межсимвольные искажения. С другой стороны не кратность t_c величине t_0 уменьшает расстояния между сигнальными конструкциями до величины Δ. Это позволяет получить число реализаций ТСК $N_р$ на интервале nt_0 больше чем 2^n. При заданном s ($s = t_0/\Delta$) на интервале n единичных элементов число реализаций сигнального алфавита бинарных ТСК равно [3]

$$N_р = \frac{\left[\left(n\cdot s\right) - \left[\left(s-1\right)\cdot i\right]\right]!}{i!\cdot\left[\left[\left(n\cdot s\right) - \left[\left(s-1\right)\cdot i\right]\right] - i\right]!}, \quad (2)$$

где i — число информационных значащих моментов модуляции (ЗММ) в сигнале.

Для сигнальных конструкций с разным числом ЗММ формула (2) преобразуется к виду

$$N_р = \sum_{i=1}^{n} \frac{\left[\left(n\cdot s\right) - \left[\left(s-1\right)\cdot i\right]\right]!}{i!\cdot\left[\left[\left(n\cdot s\right) - \left[\left(s-1\right)\cdot i\right]\right] - i\right]!}. \quad (3)$$

Оценим изменение ансамбля реализаций ТСК $N_{рТСК}$ в зависимости от параметров n, s и i. На рис. 2 приведены зависимости $N_{рТСК}$ от n, s и $i = 1...n$, по которым видно, что количество реализаций ТСК существенно увеличивается с ростом n и s при $i = 1...n$ по сравнению с РЦК. Использование ТСК позволяет не только увеличить объем передаваемых данных на заданном интервале времени по сравнению с РЦК, но и обеспечить достаточно эффективный контроль целостности сигнальных конструкций на приемной стороне [5].

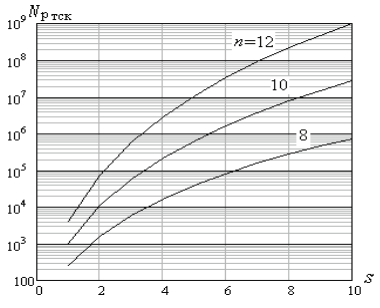

Рис. 2. Количество реализаций $N_{рТСК}$ в зависимости от s при значениях n = 8, 10, 12

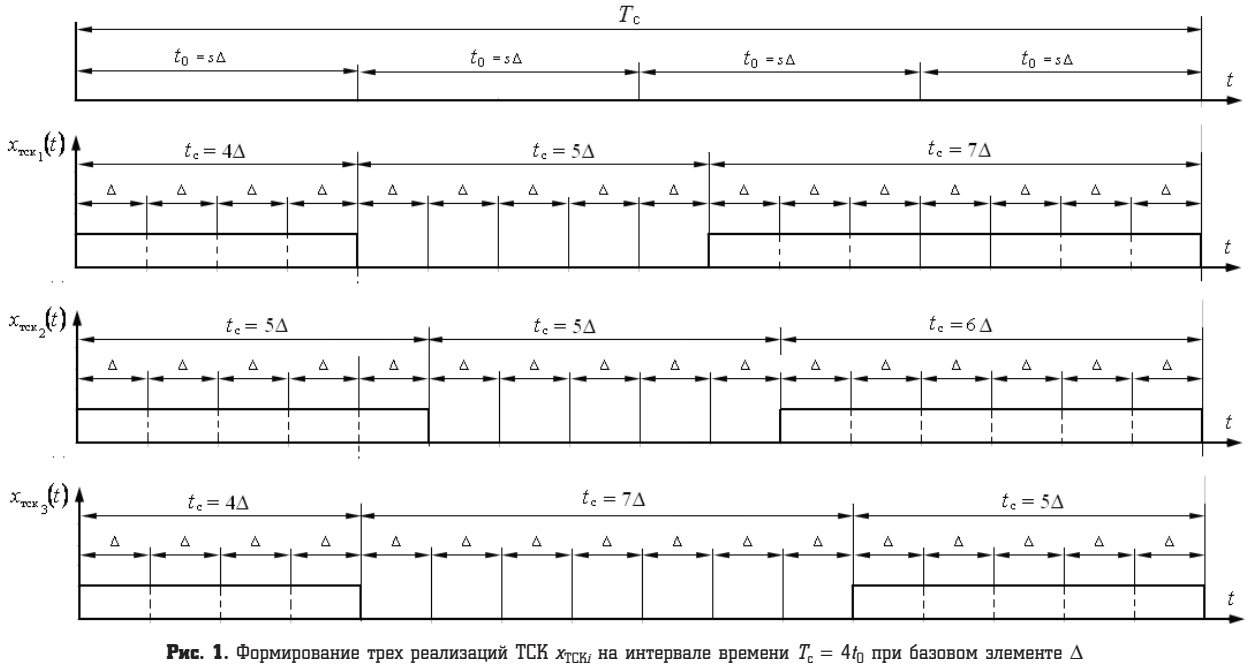

Рис. 1. Формирование трех реализаций ТСК $x_{ТСКi}$ на интервале времени $T_c = 4t_0$ при базовом элементе Δ

3. Оценка структурной скрытности ТСК

Требования по скрытности передачи формулируется, как правило, на сигнальном уровне, что предполагает выбор соответствующих характеристик и параметров сигнала. Оценим потенциальную структурную скрытность ТСК при изменении параметров n, s и i. Для этого определим минимальный ансамбль $A_{\text{ТСК}}$, который требуется проанализировать при несанкционированном доступе

$$A_{\text{ТСК}} = \sum_{n}\sum_{s}\sum_{i=1}^{n} \frac{\left[\left(n\cdot s\right)-\left[\left(s-1\right)\cdot i\right]\right]!}{i!\cdot\left[\left[\left(n\cdot s\right)-\left[\left(s-1\right)\cdot i\right]\right]-i\right]!}, \qquad (4)$$

где n, s и i — текущие значения параметров.

Тогда структурная скрытность ТСК

$$S_{\text{ТСК}} = \log_2 A_{\text{ТСК}}. \qquad (5)$$

На рис. 3 представлены зависимости структурной скрытности $S_{\text{ТСК}}$ от изменения параметров n, s и i. Как видно из рисунка $S_{\text{ТСК}}$ увеличивается с ростом n и s при $i=1\ldots n$. Таким образом, применение ТСК позволяет на заданном интервале времени увеличить структурную скрытность по сравнению с РЦК в 1,5...4 раза.

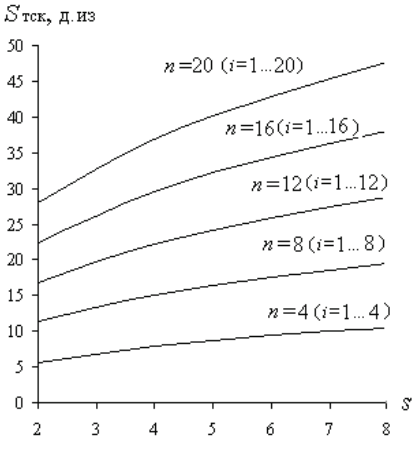

Рис. 3. Зависимости структурной скрытности $S_{\text{ТСК}}$ от параметров *n, s* и *i*

4. Алгоритм формирования группового сигнала

Пусть в системе связи многопользовательского доступа имеется некоторое количество источников цифрового сигнала $x_1, x_2, ..., x_N$, использующих избыточные коды, и соответствующее им количество двоичных каналов с ограниченной полосой пропускания ΔF и минимальной базой сигнала $B=\Delta F t_0=1$. В результате кодирования цифрового сигнала $x_1, x_2, ..., x_N$ получаем соответствующее множество ТСК $x_{\text{ТСК1}}, x_{\text{ТСК2}}, ..., x_{\text{ТСКN}}$, поступающее на вход устройства формирования уровней канала (УФУК).

В системе с разделением по уровню [6] параметром разделения является амплитуда сигналов, принимающая ряд дискретных значений $h_1, h_2, \ldots, h_N$, а полезная информация содержится в длительности сигналов. Сигналы первого уровня канала имеют амплитуду $h_1=U_0$, сигналы второго канала — $h_2=U_0/2$, третьего — $h_3=U_0/2^2$, n-го — $h_N=U_0/2^{n-1}$. Таким образом, с выхода УФУК формируется множество многоуровневых ТСК $x^1_{\text{ТСК1}}, x^2_{\text{ТСК2}}, ..., x^N_{\text{ТСКN}}$. Групповой сигнал $X_{\text{ГР}}(t_0)$ будет получен в результате суммирования многоуровневых последовательностей всех индивидуальных каналов

$$X_{\text{ГР}} = \sum_{i=1}^{n} x^i_{\text{ТСК}i}. \qquad (6)$$

Многопозиционный сигнал с выхода сумматора поступает на модем, а затем в канал. На приемной стороне с выхода дискретного канала групповой сигнал $X'_{\text{ГР}}$ поступает на многоуровневый компаратор напряжения для выделения разностного сигнала Δh_i с длительностями импульсов, соответствующих сигналам $x_{\text{ТСК}i}$. Для упрощения предположим, что изменение формы сигнала в ДК были незначительными, т. е. $x'^1_{\text{ТСК1}} \approx x^1_{\text{ТСК1}}$, $x'^2_{\text{ТСК2}} \approx x^2_{\text{ТСК2}}$, ..., $x'^n_{\text{ТСК}n} \approx x^n_{\text{ТСК}n}$. Чтобы произвести разделение сигналов необходима следующая последовательность действий:

1. Для выделения длительностей импульсов сигналов $x_{\text{ТСК1}}$ первого канала сигнал $X'_{\text{ГР}}$ ограничивается сверху на уровне h_1, а снизу на уровне $\sum_{i=2}^{n} h_i$. Выделенный сигнал Δh_1 следует увеличить в $h_1 \Big/ \left(h_1 - \sum_{i=2}^{n} h_i\right)$ раз и вычесть его из $X'_{\text{ГР}}$. В результате будет получен сигнал Σ_1.

2. Ограничиваем результирующий сигнал $\Sigma_1 = X'_{\text{ГР}} - x^1_{\text{ТСК1}}$ сверху на уровне h_2, а снизу на уровне $\sum_{i=3}^{n} h_i$. В результате будут выделены длительности таймерных сигналов $x_{\text{ТСК2}}$ второго канала. Увеличиваем выделенный сигнал Δh_2 с учетом отношения $h_2 \Big/ \left(h_2 - \sum_{i=3}^{n} h_i\right)$ и вычитаем его из Σ_1. Получаем смесь сигналов $\Sigma_2 = X'_{\text{ГР}} - (x^1_{\text{ТСК1}} + x^1_{\text{ТСК2}})$.

Аналогичным образом осуществляется выделение сигнальных конструкций остальных каналов. На рис. 4 показан процесс формирования группового сигнала и выделения длительностей ТСК для трех каналов с амплитудами сигналов $h_1=8$, $h_2=4$, $h_3=2$.

5. Выводы

В заключение можно сделать следующие выводы.

В данной статье предложен метод формирования группового сигнала на основе множества многоуровневых таймерных сигнальных конструкций с разделением их по уровню. Для увеличения структурной скрытности информационных сигналов индивидуальных каналов в системе используются многоуровневые ТСК с последующим объединением их в групповой сигнал. С целью снижения эффективности средств НСД на процедуру дешифрирования перехваченного группового сигнал используется метод разделения ТСК по уровню. Представ-

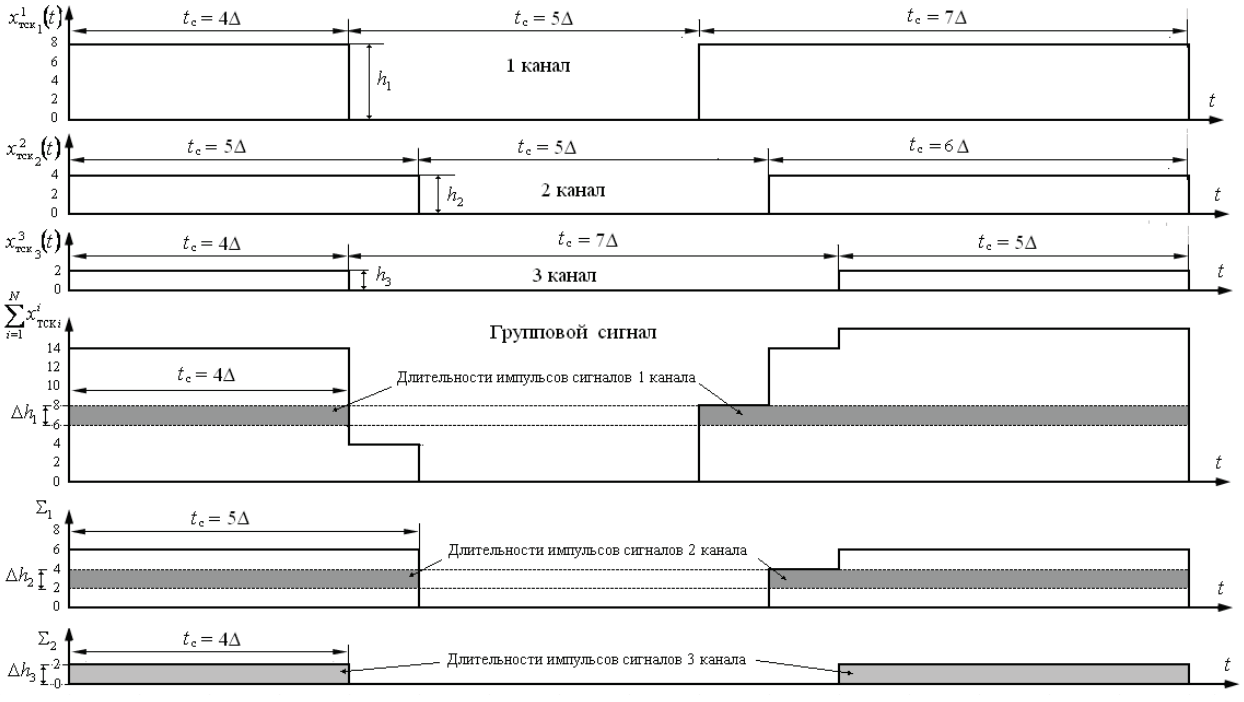

Рис. 4. Формирование группового сигнала и выделение длительностей ТСК для трех индивидуальных каналов

ляет интерес разработка методики расчета структурной скрытности группового сигнала на основе ТСК.

Литература

1. Куприянов, А. И. Теоретические основы радиоэлектронной борьбы [Текст] / А. И. Куприянов, А. В. Сахаров. — М. : Вузовская книга, 2007. — 356 с.
2. Шаньгин, А. И. Информационная безопасность компьютерных систем и сетей [Текст] / А. И. Шаньгин. — М. : ИД «Форум»: ИФРА-М, 2008. — 416 с.
3. Гуляев, Ю. В. Информационные технологии на основе динамического хаоса для передачи, обработки, хранения и защиты информации [Текст] / Ю. В. Гуляев, Р. В. Беляев, Г. М. Воронцов и др. // Радиотехника и электроника. — 2003. — Т. 48. — № 10. — С. 1157—1185.
4. Корчинский, В. В. Повышение структурной скрытности передачи систем с хаотическими сигналами [Текст] / В. В. Корчинский // Восточно-Европейский журнал передовых технологий. — 2013. — Т. 1, № 9(61). — С. 53—57.
5. Захарченко, Н. В. Эффективность использования таймерных сигнальных конструкций в системах передачи с кодовым разделением каналов [Текст] / Н. В. Захарченко, В. В. Корчинский, Б. К. Радзимовский // Наукові праці ДонНТУ. — 2011. — Випуск № 20(182). — С. 145—151.
6. Темников, Ф. Е. Теоретические основы информационной техники [Текст] / Ф. Е. Темников, В. А. Афонин, В. И. Дмитриев. — М. : Энергия, 1979. —512 с.
7. Richard, K. Recommendations of the National Institute of Standards and Technology [Text] / K. Richard, T. Walsh, W. Fries. — NIST SP 800-58. —2005. — P. 93.
8. Базова модель ВВС. — Geneva [Text] / Recomendation CCITT X. 200. Reference Model of open systems interconnection for CCITT applications // Стандарт ISO 7498-1:1984. — 1991. — P. 31.
9. Carvalho, M. Using Mobile Agents as Roaming Security Guards to Test and Improve Security of Hosts and Networks Proceedings of the 2004 ACM Symposium on Applied Computing (SAC'04) [Text] / M. Carvalho, T. Cowin, N. Suri, M. Breedy, K. Ford. — 2004. — ACM.
10. Pedireddy, T. Prototype Multi Agent Network Security System. Proceedings of the AAMAS'03 [Text] / T. Pedireddy, J. Vidal. — 2003. — ACM.
11. Menezes, R. Self-Organization and Computer Security Proceedings of the 2005 ACM Symposium on Applied Computing (SAC'05) [Text] / R. Menezes. — 2005. — ACM.
12. Valeyev, S. Multiagent Technology and Information System Security Proceedings of the 7-th International Workshop on Computer Science and Information Technologies CSIT'2005 [Text] / S. Valeyev, T. Bakirov, D. Pogorelov, I. Starodumov. — Vol. 1. — Ufa, Russia. — 2005. — Pp. 195—200.

МЕТОД ПІДВИЩЕННЯ СТРУКТУРНОЇ СКРИТНОСТІ ПЕРЕДАЧІ ІНФОРМАЦІЇ В СИСТЕМІ ЗВ'ЯЗКУ БАГАТОКОРИСТУВАЦЬКОГО ДОСТУПУ

У статті запропоновано метод формування групового сигналу для системи зв'язку багатокористувацького доступу. Для підвищення структурної скритності інформаційних двійкових сигналів індивідуальних каналів застосована система кодування на основі багаторівневих таймерних сигнальних конструкцій. З метою зниження ефективності дешифрування перехопленого групового сигналу використовується метод розділення індивідуальних сигналів по рівню.

Ключові слова: таймерний, сигнал, рівень, конфіденційний, сигнатура, несанкціонований доступ, скритність, канал, захист.

Корчинский Владимир Викторович, *кандидат технических наук, доцент, кафедра информационной безопасности и передачи данных, Одесская национальная академия связи им. А. С. Попова, Украина.*

Корчинський Володимир Вікторович, *кандидат технічних наук, доцент, кафедра інформаційної безпеки та передачі даних, Одеська національна академія зв'язку ім. О. С. Попова, Україна.*

Korchinsky Vladimir, *Odessa National Academy of Telecommunications named after O. S. Popov, Ukraina*