УДК 681.391

Письмак Д.А., Клименко С.В.
Днепровский национальный университет имени Олеся Гончара

Помехоустойчивое кодирование сообщения электронной подписи

В современном обществе набирает популярность способ идентификации пользователя посредством электронной подписи. Современные методы довольно надежны, но и они имеют ряд недостатков, например влияние помех и искажения в сообщениях. Исходя из этого, предложен новый алгоритм передачи и обработки сообщений с электронной подписью. В ходе исследования проведен анализ существующих методов передачи сообщений с использованием электронной подписи посредством радиолинии связи. Рассмотрена задача скрытой передачи сообщения, которое содержит в себе электронную подпись при использовании обычной радиолинии связи, и при этом обеспечивает высокую помехоустойчивость.

Для решения этой задачи необходимо разработать алгоритм, который позволит при минимальных модификациях использовать стандартную радиолинию связи для скрытной передачи электронной подписи. Для формирования сообщения, несущего в себе электронную подпись, необходимо создать две последовательности Хаффмана. Первая последовательность будет использована для формирования самой электронной подписи, а вторая это так называемой “несущей”, в которой и будет скрыта наша электронная подпись. Так как первые последовательности могут быть практически неограниченной длины реализован механизм однодневных электронных подписей (возможна реализация на один месяц или же одну неделю). Смена паролей осуществляется методом “нарезания” последовательности на кусочки заданной длины, и при этом длина задается исходя из начальных условий, в дальнейшем эти кусочки и есть сменные электронные подписи. Необходимым условием является то, что получатель так же должен иметь у себя список с такими подписями, для возможности сравнения и установления достоверности полученного сообщения. Вторая же последовательность будет так называемой “несущей” в ней и будет скрыта электронная подпись. Двоично-кодовая последовательность должна быть значительно длиннее (как минимум в 10 раз) электронной подписи для обеспечения секретности и помехоустойчивости.

На практике использованы два разностных уравнения последовательностей Хаффмана следующего вида:

$$S(k) = \sum_{i=1}^{m} a_i \cdot S(k-i).$$

Для повышения помехоустойчивости и дополнительного шифрования данных пропустим электронную подпись через рекурсивный фильтр. Секретность будет достигаться использованием пары фильтров (рекурсивного и нерекурсивного), и без знания их дискретной передаточной функции невозможно получить искомую электронную подпись, после того как она пройдет через нерекурсивный фильтр. Электронная подпись видоизменится по следующему математическому закону:

$$U(k) = S(k) \oplus \sum_{i=1}^{n} a_i \cdot S(k-i),$$

U(k) – электронная подпись после прохождения ее через нерекурсивный фильтр.

Полученную электронную подпись вставим в несущую последовательность на некое место, которое может изменяться статически или динамически, следуя некоторому заранее заданному алгоритму (по договоренности получателя и отправителя).

Так как сам факт передачи и приема сообщения в большинстве случаев происходит незаметно от возможного нарушителя и вероятность различного вида атак очень незначительна, то при этом появляется другая проблема – случайные помехи различного рода, которые будут воздействовать на сигнал во время передачи. Под влиянием помех двоичные сигналы перекручиваются, в результате чего символы инвертируются. Воздействие помех математически описываются следующим образом

$$X(k) = S(k) \oplus \xi(k),$$

S(k) – сигнал на входе;

ξ(k) – двоичный сигнал помехи, который вызывает инверсию;

X(k) – сигналы, которые поступает на вход приемника.

Для того чтобы нивелировать влияние помех используются длинные несущие последовательности и несколько фильтров (рекурсивный и нерекурсивный). Но помехи могут все равно появляться, Поэтому осуществляется проверка степени искажения сообщения путем сравнения его с эталонным значением, которое хранится у получателя и принятия решения о том, что подпись это либо нет.

Различия между эталонным и полученным сообщением определяется кодовым расстоянием по следующей формуле

$$r(i, j) = \sum_{k=1}^{n} S_i(k) \oplus S_j(k),$$

$S_i(k)$ – принятая электронная подпись;

$S_j(k)$ – эталонная электронная подпись.

Полученное кодовое расстояние сравнивается с пороговым значением, которое выбирается исходя из размера электронной подписи

$$r(i, j) < r_0, \qquad (1)$$

r(i,j) – кодовое расстояние полученное путем сложения подписей;

r_0 – некое пороговое значение, которое выбирается исходя из изначальных условий.

Достаточным кодовым расстоянием является половина длины электронной подписи. В определенных случаях, может выбираться другая длина электронной подписи. Если кодовое расстояние удовлетворяет данному условию (1), то мы принимаем решение – принять данную электронную подпись, в противном случае – признать ее недействительной, или же подделанной.

Таким образом, предложенный алгоритм базируется на использовании двоично-кодовых последовательностей Хаффмана, для скрытой передачи сообщения, которое содержит в себе электронную подпись и при этом обеспечивает высокую помехоустойчивость. В ходе исследования проведены вычислительные эксперименты, которые подтверждают работоспособность представленного алгоритма.

Список использованных источников

1. *Дронь, М. М. Основы теории защиты информации: Учебное пособие / М. М. Дронь, В. П. Малайчук, А. Н. Петренко – Д.: ДНУ имени Олеся Гончара, 2001. – 125с.*
2. *Малайчук, В. П. Основы теории кодирования и декодирования: Учебное пособие / В. П. Малайчук, В. Ф. Рожковський – Д.: ДНУ имени Олеся Гончара, 2001.– 68с*
3. *Малайчук, В. П. Основы теории кодирования и передачи информации: Учебное пособие / В. П. Малайчук, О. М. Петренко – Д.: ДНУ имени Олеся Гончара, 1999. – 165с*
4. *Королев, А. И. Коды и устройства помехоустойчивого кодирования информации / А. И. Королев – Мн.: Бестпринт, 2002. – 286 с.*