УДК 004.56(06)

Г.Н. Лиходедова, А.А. Орехова, А.И. Дементеев

Разработка защитного фильтра для противодействия нетрадиционному каналу в сетях пакетной передачи данных

Рассматривается имитационная модель нетрадиционного информационного канала (НИК) в сетях пакетной передачи данных и метода противодействия для канала по расстояниям.

1. Модель НИК (частный случай)

В реальной ситуации осуществление передачи информации по НИК возможно, если соблюдаются следующие условия:

- Существует закладное устройство 1 (ЗУ1) в НГС, модулирующее сетевой поток для образования НИК по определенному признаку.
- Существует ЗУ2 в ЛВС, способное произвести демодуляцию сетевого потока по определенному признаку.
- Признаки ЗУ1 и ЗУ2 совпадают.
- Имеется интенсивный сетевой поток.

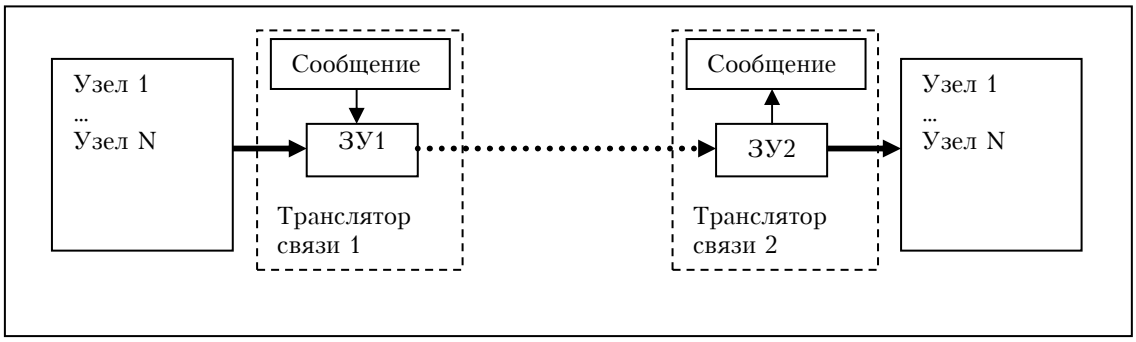

Рис. 1. Схема взаимодействия ЗУ по НИК

В роли узлов выступают объекты, формирующие сетевой поток (приложения или узлы сети). Трансляторами связи могут выступать управляющие сетевым потоком устройства, например маршрутизаторы. Для передачи сообщения согласно схеме (рис. 1) сетевой поток проходит через Транслятор связи 1 (аппаратный или программно-аппаратный комплекс), содержащий ЗУ1, которое накапливает очередь из n пакетов, переупорядочивает их и затем отправляет в сеть (модулирует сетевой поток по определенному признаку). ЗУ2 пытается получить сообщение, демодулируя входящий поток по тому же признаку. Таким образом, происходит скрытая передача информации. Наличие НИК очень сложно определить, так как сетевой поток не нарушается, а лишь меняются его неконтролируемые свойства.

2. Защитный фильтр

Для противодействия скрытым каналам по расстояниям авторами была разработана модель защитного устройства, цифрового рекурсивного фильтра, изменяющегося во времени:

$$y(x_n(t_n)) = \sum_{k=1}^{n-1} d_k(t_{n-1}) y(x_{n-k}(t_{n-1})),$$

где $n = 1 \ldots N$, $d_k = \begin{cases} -1, & \text{влево,} \\ 0, & \text{на месте,} \\ 1, & \text{вправо.} \end{cases}$ — коэффициент, показывающий направление сдвига в момент времени t_{n-1}, а сумма выступает в роли накопительного счетчика.

Его действие основано на лексикографическом упорядочении адресов пакетов, поступающих из глобальной сети на шлюз локальной сети. Опишем его работу.

Определим информационный канал в виде пары зависимых случайных величин $\{\xi_{in}, \xi_{out}\}$, одна из них называется входом, другая — выходом канала. Случайные величины дискретны и конечны, т.е. имеют конечные множества событий. Пусть $\Omega_{in} = \{x_1, \ldots, x_n\}$ — множество адресов пакетов на входе, каждому из которых присваивается порядковый номер входа; $\Omega_{out} = \{y_1, \ldots, y_n\}$ — множество тех же пакетов после работы фильтра, уже с другими порядковыми номерами. Ω_{in} и Ω_{out} изоморф-

ны множеству натуральных чисел N, следовательно, наше отображение биективно и может быть представлено в виде

$$\sigma(n,t_n)=\begin{pmatrix}1 & 2 & . & . & n\\ i_1(t_n) & i_2(t_n) & . & . & i_n(t_n)\end{pmatrix}.$$

3. Моделирующий программный комплекс

Для проверки возможности образования нетрадиционного информационного канала в сетях пакетной передачи данных и оценки эффективности фильтра противодействия был разработан моделирующий комплекс программного обеспечения, имитирующий работу закладных устройств (ЗУ) и фильтра противодействия НИК. Программа разработана на языке C# в виде нескольких консольных модулей и основного управляющего приложения с графическим интерфейсом. Каждый модуль имитирует работу одного звена системы передачи информации по НИК. Роль сетевого трафика выполняет файловый поток. Так как необходимо, чтобы все измерения были максимально точными, для имитации сетевого потока был выбран двухмесячный отпечаток реальной сетевой активности одного из учебных заведений города Краснодара. Технически отпечаток представляет собой список из примерно 51 000 записей об отправленных пакетах (адреса назначения, дата и время отправки пакетов, количество переданной информации и др.) из гетерогенной сети, которая состоит из 25 персональных компьютеров и сервера-шлюза. В программном комплексе воссозданы 2 способа модуляции сетевого потока:

- по расстояниям между одинаковыми IP-адресами,
- по расстояниям между четными IP-адресами.

Пример. Рассмотрим НИК по расстоянию между одинаковыми адресами. Пусть размер буфера ЗУ1 равен 10 пакетам. На вход поступает последовательность: *AABACDFCAB*. Выбраны пакеты с часто встречающимися адресами, в нашем случае «*A*». После работы закладки получено уже закодированное сообщение: $A\underbrace{CD}_{0}A\underbrace{BFC}_{1}AA\underbrace{B}_{*}$. ЗУ2 игнорирует «*», так как в связи со случайным появлением пакетов (равномерно распределенных) невозможно осуществлять непрерывную трансляцию сообщения. Если ЗУ1 ожидает необходимые адреса для кодировки «0» или «1», из-за задержки во времени оно может быть обнаружено.

При тестировании программы, моделирующей работу фильтра, выбирались последовательности определенной длины: 25, 1000, 7000 бит и т.д. Получены кривые эмпирического распределения вероятности появления ошибки при распознавании ЗУ2 передаваемого ЗУ1 сообщения (рис. 2).

Рис. 2. Кривая распределения ошибок в сообщении

Доказана нормальность распределения по критерию Пирсона с уровнем значимости 0,05 и объемом выборки 100.

4. Вывод

По результатам исследования ЗУ2 распознает в среднем 20% модулированного потока, причем только 50% бит из них совпадают с исходными данными.

Вероятность инвертирования бита среди полученных равна 0,5, т.е., достигнуто равномерное перемешивание. Такая ситуация является наиболее неблагоприятной для злоумышленника, так как неизвестна степень «обучаемости» закладного устройства 2 и его возможности расшифровывания. Данный вывод основан на утверждении, что максимальная энтропия достигается в равновесной системе.

Пусть ЗУ1 сообщение отправляет с помощью кодов, исправляющих ошибки, т.е. вносит избыточность настолько, что, анализируя полученные данные, можно не только заметить ошибки или группы ошибок, но и указать, где именно возникли искажения. Транспортный уровень традиционного

канала является физическим для нетрадиционного, а разрушение битов с помощью фильтра происходит на сетевом уровне легальной передачи, следовательно, разрушаются не только информационные биты, но и контрольные. Поэтому предполагается, что ЗУ2 не сможет восстановить даже частично исходную информацию.

В дальнейшем планируется усовершенствовать работу фильтра для других типов НИК и провести оценку его эффективности.

Литература

1. Ушаков П.А. О способе организации скрытого канала и оценка его устойчивости к помехам // Дискретная математика. – 2007. – Т. 19, вып. 1. – С. 60–66.

2. Научно-исследовательская работа «Апология-2003»: Отчет / ИТМ и ВТ РАН; Рук. Д.А. Ловцов. М., 2003.

Лиходедова Галина Николаевна
ГОУ ВПО «Кубанский государственный технологический университет»
Преподаватель кафедры общей математики
Тел.: +7-918-4856046
Эл. почта: absk@mail.ru

Орехова Анна Александровна
ГОУ ВПО Кубанский государственный технологический университет
Студентка 4-го курса группы 04-К-ИБ1, специальность: информационная безопасность
Эл. почта: sly-boots@ya.ru.

Дементеев Александр Ильич
ГОУ ВПО Кубанский государственный технологический университет
Студент 4-го курса группы 04-К-ИБ1, специальность: информационная безопасность
Эл. почта: sly-boots@ya.ru

G.N. Likhodedova, A.A. Orekhova, A.I. Dementeev

Elaborations of defensive filter for covert channel's counteraction in the data packets nets

Abstract. An imitation model of covert channel in the data packet's nets is considered in this article, and a new method of counteraction for interval subliminal channels is presented. The method is based on the lexicographical regulation which is realized in the special filter.