проектирование и внедрение систем информационной безопасности на предприятиях почтовой связи;

организация технической учебы, повышения квалификации сотрудников предприятий почтовой связи в области информационной безопасности.

ВЫБОР КОДА ДЛЯ СИСТЕМЫ СВЯЗИ, ОБЕСПЕЧИВАЮЩЕЙ ИНФОРМАЦИОННУЮ БЕЗОПАСНОСТЬ

А.И. МИТЮХИН

Одним из требований, предъявляемых к современным системам связи является способность противостоять подслушиванию и преднамеренным помехам. Во избежание обнаружения кодированного сигнала несущего сообщение, передача в такой системе ведется с минимальным излучением мощности. Кодирование реализуется посредством использования кодов большой мощности $M=q^k$, где q и k основание и размерность кода соответственно. При этом период сигнала $T=n/f_т$ должен быть соизмерим со временем между сменами кодов ($f_т$ – тактовая частота в системе, n – значность кода).

Обнаруживающая способность подслушивающей стороны ограничивается отношением Q энергии $E_в$ (приходящейся на один бит сообщения) перехваченного сигнала к спектральной плотности мощности шума N_o. Возникает задача выбора класса кодов, определения его мощности, других его параметров, обеспечивающих минимальную вероятность ошибки декодирования $P_{ош}$ в основном канале при заданном минимальном отношении $Q=E_в/N_o$.

Пусть {G} является [n, k]-кодом над полем из q элементов. В системе используется M кодовых слов кода G. Для удобства назовем совокупность M действительных векторов $X=(x_1...x_n)$ множеством сигналов

$G=\{x^1,x^2,...,x^S,...,x^M\}$, $S\in\{1,2,...,M\}$.

Оптимальная процедура декодирования M сигналов на основе стратегии максимального правдоподобия заключается в нахождении номера S одного из M корреляторов с максимальным по абсолютной величине выходным сигналом. Декодирование сводится к сравнению входного вектора $Y=(x+E)$ с каждым словом кода G, где $Y=(y_0y_1...y_i...y_{n-1})$; $X=(x_0x_1...x_i...x_{n-1})$, $X\in G$; $E=(e_0e_1...e_i...e_{n-1})$ – вектор ошибок; $y_i,x_i,e_i\in\{0,1\}$. При условии, что все кодовые слова равновероятны, вектор Y декодируется в ближайшее по расстоянию Хэмминга кодовое слово. Это равносильно определению номера i, для которого вычисляется значение

$|F_i| = G\cdot Y^T$, для $i\in\{1,2,...,M\}$,

где $F_i=(f_0f_1...f_i...f_{n-1})^T$; G – матрица кодовых слов кода.

Если взаимное влияние сигналов отсутствует, то на величину вероятности ошибки декодирования $P_{ош}$ кодового слова X^S влияет только отношение сигнал/шум Q. Для того, чтобы в системе не было взаимного влияния сигналов должно выполняться условие

$R_{X^jX^S}(\tau)=0$ при всех $j\neq S$; $j, S\in\{1,2,...,M\}$.

Здесь $R_{X^jX^S}(\tau)=n-2wt(x^j+Д^\tau x^S)$, (1)

для $0\le\tau\le n-1$ — взаимная корреляционная функция; Д — оператор циклического сдвига последовательности X на одну позицию влево.

С точки зрения получения минимальной величины $P_{ош}$ или помехоустойчивого декодирования (приема в условиях воздействия организованных помех), множество сигналов {G} необходимо характеризовать коэффициентами ВКФ (1). Таким образом, оценка $P_{ош}$ для выбранного кода будет зависеть не только исключительно от отношения ($E_в/N_o$), но и корреляционной матрицы кодированных сигналов.

Рассмотрим, как можно осуществить реальный выбор кода для скрытной передачи информации. Будем исходить из того, что обнаружение подслушивателем передачи состоит в некогерентном накоплении энергии сигналов за период кодированных сообщений. В системе предусмотрена частая смена кодовых слов кода, затрудняющая правильное декодирование подслушивающей стороне. Такая тактика применения кодов требует тщательного анализа ВКФ больших множеств слов.

Известно, что большой совокупностью множеств слов кода G обладает двоичный симплексный $[2^k, k]$-код. К его достоинствам можно также отнести простоту формирования и относительно несложное декодирование. Недостатком симплексных кодов и их производных (Голда, Касами, ЛРД и др.) является сравнительно малое множество слов с хорошими взаимно-корреляционными свойствами. В качестве примера приведем М-код длиной 31. Всего существует 6 различных проверочных полиномов h(x) над полем GF(2) длиной 31. Полиномы h(x) запишем в восьмеричном представлении, в виде коэффициентов многочленов и в виде многочленов (см. табл.).

Примитивные многочлены степени 5

$h_1(x)$	45	100101	x^5+x^2+1
$h_2(x)$	75	111101	$x^5+x^4+x^3+x^2+1$
$h_3(x)$	67	110111	$x^5+x^4+x^2+x+1$
$h_4(x)$	51	101001	x^5+x^3+1

$h_5(x)$	57	101111	$x^5+x^3+x^2+x+1$
$h_6(x)$	73	111011	$x^5+x^4+x^3+x+1$

Выбор множеств пар М-кодов, кодовые слова которых обладают только определенными значениями ВКФ, основывается на следующем утверждении [1]. При всех $k \neq 0 \bmod 4$ существуют пары М-кодов с ВКФ, принимающими трехуровневые значения:

(-1), t(k), t(k)-2, (2)

где $t(k)=1+2^{\lceil (k+2)/2 \rceil}$, $\lceil \alpha \rceil$ — обозначает наибольшее целое число меньшее или равное α.

Пары примитивных многочленов, порождающие пары М-кодов с ВКФ, принимающими значения (2) образуют пары предпочтительных М-кодов. Для рассматриваемой системы связи важны не пары, а множества кодов с хорошими взаимно-корреляционными свойствами, в которых любая входящая в нее пара предпочтительна. Для приведенного выше примера М-кода значности 31 можно построить 8 различных множеств, в каждом из которых по 3 пары предпочтительных М-кодов. Распределение полиномов h(x) в множествах предпочтительных пар М-кодов выглядит так:

$M_3^1=\{h_1(x), h_2(x), h_6(x)\}$;
$M_3^2=\{h_1(x), h_2(x), h_3(x)\}$;
$M_3^3=\{h_1(x), h_3(x), h_5(x)\}$;
$M_3^4=\{h_1(x), h_5(x), h_6(x)\}$;
$M_3^5=\{h_2(x), h_4(x), h_6(x)\}$;
$M_3^6=\{h_2(x), h_3(x), h_4(x)\}$;
$M_3^7=\{h_3(x), h_4(x), h_5(x)\}$;
$M_3^8=\{h_4(x), h_5(x), h_6(x)\}$;

Заметим, что каждый предпочтительный многочлен h(x) входит в четыре из восьми множеств. Абсолютное максимальное значение коэффициента корреляции между всеми кодовыми словами каждого множества пар предпочтительных М-кодов M_3^i (j=1...8) равно (2)

$t(5)=1+2^{\lceil (5+2)/2 \rceil}=9$.

Относительное максимальное значение выбросов ВКФ не превышает величины 9/31 = 0,29. Выбранное для передачи множество M_3^i содержит $3\cdot(2^5-1)=93$ кодовых слов длиной 31. Если в системе предусматривается смена используемых множеств предпочтительных пар М-кодов, то количество применяемых слов для кодирования сообщений достигает величины

$M=8M_3^i = 8\cdot 93=744$.

Как видно, даже для малой длины кода можно построить сравнительно большое множество кодовых слов, удовлетворяющее основным требованиям скрытой системы: обеспечение заданной $P_{ош}$ декодирования для всех кодовых слов кода мощностью М.

Если переходить к большим значностям кода (n>100), когда число пар предпочтительных полиномов симплексного кода (его модификацией) увеличивается вместе с увеличением совокупности множеств M_r^j, эффективность защиты от подслушивания будет также расти. При низких отношениях Q и больших М для обнаружения слабых сигналов подслушивающей стороне потребуются значительные временные затраты во многих случаях несоизмеримые с реальным временем передачи информации по основному каналу.

Литература

1.Сарвате Д.В., Персли М.Б. Взаимно-корреляционные свойства псевдослучайных и родственных последовательностей. ТИИЭР. 1980. Т. 68. № 5.

СОХРАНЕНИЕ КОРПОРАТИВНЫХ ДАННЫХ С ПОМОЩЬЮ СИСТЕМЫ АВТОМАТИЧЕСКОГО РЕЗЕРВНОГО КОПИРОВАНИЯ

Д.С. ПРИЩЕПА

Работа любой организации немыслима без создания надежной и удобной информационной системы, в которой должны находиться все корпоративные данные. При этом остро встает вопрос сохранности этих данных, так как их потеря может привести к остановке работы всего предприятия. Одним из самых надежных путей решения данной проблемы является резервное копирование.

Современные корпоративные СУБД представляют подобные сервисы [1, 2], однако доступ к такому инструментарию имеет лишь администратор СУБД, что приводит к усложнению процесса. Возможно также использование файлового копирования, предоставляемого сервисами ОС, но в таком случае требуется предоставить пользователю сведения об архитектуре распределенной БД, что является грубым нарушением политики безопасности. В данной работе реализован внешний по отношению к СУБД сервис, основанный на механизмах аутентификации, используемых для доступа к корпоративным данным. За основу взята технология DataSnap компании Borland Software Corp [3].

Разработанная система состоит из трех частей: сервер расписания, сервер копирования и клиентское приложение. Первый является дополнительным сервисом бизнес-уровня корпоративной сети и представляет собой DCOM-сервер, реализованный в виде службы NT. Сервер расписания выполняет следующие функции: посредничество между СУБД и пользователем (в том числе аутентификация), поддержка расписания (добавление, редактирование и удаление заданий), обработка таймера и запуск сервера копирования по появлению события задания. Сервер копирования является COM-сервером и