8. *TrippingPoint* Threat Suppression Engine. http://www.tippingpoint.com/technology_tse.html
9. *TippingPoint* Intrusion Prevention Systems http://www.tippingpoint.com/pdf/resources/datasheets/400917-002_TP-IPS.pdf
10. *Sourcefire* Intrusion Agent for Snort http://www.sourcefire.com/products/is_agent.html
11. *Sourcefire* IS5800 – A Revolutionary Approach to Enterprise Inrtusion Prevention http://www.sourcefire.com/products/is5800.html
12. *The Snort* Project, "Snort, Users Manual 2.4.0RC1" http://cvs.snort.org/viewcvs.cgi/snort/doc/ snort_manual.pdf/rev=1.31.2.3.2.4
13. *Snort* 2.0 Hi-performance Multi-rule Inspection Engine. Sourcefire, 2004.
14. *Raven Alder*, Jacob Babbin, Adam Doxtater. Snort 2.1. Second Edition Syngress Publishing, 2004.
15. *Лукацкий А.В.* Обнаружение атак. -БХВ-Петербург, 2001. -С.144-149.

Надійшла 19.09.2006

УДК 004.681 **Кулагин Е.А.**

ОЦЕНКА СТОЙКОСТИ СКРЫТЫХ КАНАЛОВ В ПРОВОДНЫХ ТЕЛЕФОННЫХ ЛИНИЯХ ПРОТИВ ПАССИВНЫХ АТАК

Введение

В условиях информационного противоборства большое значение приобретают проблемы сохранения секретности и имитостойкости информации. Одними из наиболее распространенных во многих странах сред передачи информации являются телефонные сети, абонентский участок которых представляет собой проводные линии, по которым передаются сигналы аналогового канала тональной частоты (ТЧ).

При обеспечении секретности связи по аналоговым каналам ТЧ чаще всего используются различные методы скремблирования речи. Несмотря на то, что современные методы скремблирования позволяют обеспечить высокую криптостойкость сообщений [1], у них есть один существенный недостаток. Факт передачи скремблированного сообщения может привлечь внимание противника и в случае невозможности раскрыть содержимое сообщений он может применить активные атаки по их уничтожению. Сокрытие факта передачи сообщения позволит существенно повысить секретность передаваемой информации за счет того, что противник не знает против какого, из большого множества каналов, он должен применять вычислительно емкие атаки.

Обеспечение имитостойкости речевых сигналов при современных методах синтеза речи так же является актуальной задачей. Обмен парольными фразами является малоэффективной защитой, так как параллельно требуется иметь секретную систему передачи паролей. Одним из наиболее эффективных решений этой проблемы является встраивание в сообщение цифровых водяных знаков.

Задачи обеспечения скрытности передаваемого сообщения и обеспечения имитостойкости телефонного канала можно решить методами стеганографии, путем встраивания в открытый телефонный канал скрытного канала передачи секретных сообщений либо передачи меток идентификации.

Теоретическая возможность создания таких скрытых каналов основывается на нечувствительности человеческого слуха к незначительным изменениям параметров

речевого сигнала во временной либо частотной области. В настоящее время имеется большое количество научных работ, посвященных методам создания таких каналов [2] – [5].

В данной статье рассмотрены современные подходы к оценке стойкости стеганографических систем против пассивных атак по обнаружению скрытых каналов передачи информации и разработан алгоритм оценки стойкости этих каналов, применительно к проводным телефонным линиям связи.

Основные подходы к оценке стойкости стегосистем против пассивных атак

Целью пассивных атак является выявление факта передачи скрытых сообщений. Структура информационных потоков в стеганографической системе при проведении противником пассивных атак изображена на рис. 1.

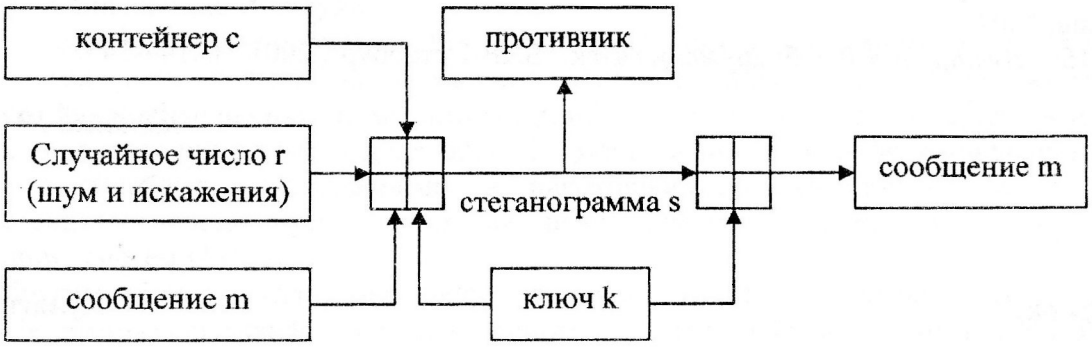

Рис. 1. Информационные потоки в стеганографической системе при противодействии пассивным атакам

Стегосистема является стойкой против пассивных атак, если противник не может обнаружить сообщение m в стеганограмме s без знания ключа k.

Существует несколько подходов к теоретической оценке стойкости стеганографических систем.

В информационно-теоретической модели, описанной в [6], предполагается, что противник знает точные вероятностные характеристики контейнеров, стегограмм, скрываемых сообщений и ключей; что передаваемые стегограммы и пустые контейнеры не претерпевают никаких искажений в процессе их доставки по каналу связи. В этой модели любое отклонение статистики, наблюдаемого нарушителем в канале связи, сообщения от среднестатистических характеристик пустых контейнеров рассматривается как факт выявления стегоканала. Для определения стойкости стегосистемы в [6] используется относительная энтропия $D(P_C \parallel P_S)$ между распределениями вероятностей P_C – контейнеров и P_S – стегограмм. Стегосистема называется совершенно стойкой против пассивного противника если

$$D(P_C \parallel P_S) = 0;$$

и стегосистема называется ε-стойкой против пассивного противника если

$$D(P_C \parallel P_S) \le \varepsilon.$$

В [6] также доказывается что если α – это вероятность ошибки ложного обнаружения скрытой связи, а β – вероятность ошибки не обнаружения скрытой связи, то для ε-стойкой стегосистемы выполняется соотношение:

$$d(\alpha,\beta) \le \varepsilon,$$

где $d(\alpha,\beta)$ – относительная двоичная энтропия.

В частности, если $\alpha=0$, тогда $\beta \ge 2^{-\varepsilon}$.

Описанная в [6] модель является идеальной и не всегда соответствует реальным условиям информационного противоборства. Например, противник часто не имеет точной информации о действительных характеристиках используемых контейнеров, и часто

пользуется усредненными характеристиками множества сообщений, которые могут применяться в качестве контейнера. В проводных каналах ТЧ многие параметры могут быть установлены только с определенной конечной точностью, в связи с шумами каналов и линий связи и нестационарностью их параметров. Кроме вносимых искажений, параметры самих информационных сигналов также являются величинами случайными, заданными в определенном диапазоне значений.

В [7] предлагается другой подход к оценке теоретической стойкости стегосистемы и доказывается, что стегосистема не может быть совершенной, если противнику одновременно известен контейнер и стегограмма. Для решения этой проблемы предлагается перейти от детерминированных стегосистем к недетерминированным. В недетерминированных стегосистемах даже если противник способен определить то что статистика контейнера отличается от известной ему, он не может доказать или опровергнуть факт наличия стегоканала. Это обусловлено тем, что противник во-первых знает только усредненные характеристики контейнера, а во-вторых источники контейнеров обычно являются нестационарными, или канал не идеален, или сам контейнер при передаче трансформируется с определенными погрешностями.

В недетерминированных стегосистемах противник знает только параметры источника контейнеров C_s, но не знает параметры самого контейнера C, то есть неопределенность в знании контейнера, при известном источнике контейнеров, должна быть строго больше нуля: $H\ (C/C_S) > 0$. Обеспечить выполнения данного условия можно путем добавления к контейнеру случайного числа r, как это показано на рисунке 1. Физически такое добавление шума к сигналу может происходить при преобразовании речи (источника контейнеров) в электрические сигналы (шумы и искажения микрофона, усилителя, АЦП), или при передаче сигнала по каналу связи.

Таким образом, для недетерминированных стегосистем условие стойкости против пассивных атака будет иметь вид:

$$H(M/(S,C_S)) = H(M)$$

Далее в [7] показано, что неопределенность знания контейнера должна быть больше или равна неопределенности знания сообщения:

$$H(C/S) \geq H(M) \quad (1)$$

$$H(C/C_S) \geq H(M) \quad (2)$$

При выполнении этих условий для нижней границы неопределенности о знании контейнера C, если известны S и C_S, противник не может получить информацию о скрываемом сообщении и условие стойкости выполняется.

Для того чтобы противник не мог получить ключ K при знании стего и источника контейнеров необходимо, чтобы выполнялось следующее условие:

$$H(K/(S,C_S)) \geq H(M)$$

На практике, в проводных стегосистемах условие (1) можно трактовать следующим образом: неопределенность знания встраиваемого в канал сообщения не должна превышать той погрешности, с которой противник может определить исходные параметры канала (контейнера), измеряя параметры канала со встроенным сообщением.

Условие (2) можно трактовать следующим образом: неопределенность знания встраиваемого в канал сообщения не должна превышать допустимого диапазона шумов и искажений канала при условии, что противник знает только допуска на параметры канала, но не знает реальные параметры данного канала без стегосообщения.

Среди возможных пассивных атак наиболее опасными являются статистические атаки [8], при которых производится анализ статистических характеристик контейнеров. Так как в большинстве случаев при передаче речи искажения и шумы в канале не являются абсолютно независимыми от передаваемого речевого сигнала, то при встраивании в канал скрытого сообщения, независимого от информации контейнера, возникает возможность его обнаружения. В [8], [9] приводятся результаты исследований различных стего при

проведении пассивных статистических атак. Из этих результатов можно сделать вывод, что для противодействия любой статистической атаке, можно выбрать такой уровень избыточности, при котором такая атака становится не эффективной.

Так как идеальную стегосистему на практике реализовать практически невозможно, а также в связи с ограниченностью вычислительных ресурсов противника, в [10] предлагается игровой подход к стегоанализу при котором противник с помощью оракулов производит генерацию пустых контейнеров и имитацию стегограмм. Если при ограниченной полиномиальной структуре контейнера и ключа противник не может с достаточной точностью принять решение о наличии стегограммы, тогда такую стегосистему называют условно стойкой. Для получения безусловно-стойкой стегосистемы, она должна быть стойкой при бесконечной длине полинома.

Алгоритм оценки стойкости скрытых каналов в проводных телефонных линиях против пассивных атак

Исходя из вышеизложенных теоретических положений, можно сделать вывод что, при проведении пассивных атак перед противником будут стоять следующие задачи:

– уточнение статистических характеристик контейнеров с целью уменьшения объема выборки C_S и, соответственно, уменьшения энтропии $H(C/C_S)$;

– генерация различных случайных стегограмм и исследование их статистических характеристик;

– сравнение параметров сигналов, предположительно содержащих встроенное сообщение, с имеющимися статистическими моделями каналов и принятие решения о принадлежности сообщения к множеству пустых контейнеров или к множеству стегограмм.

Стегосистему для проводной телефонной линии можно считать стойкой против указанной модели пассивных атак если:

– уровни вносимых шумов и искажений не превышают допустимого уровня, установленного оператором связи и откорректированного с учетом особенностей эксплуатации (длины линии, качества и срока службы кабеля и т.д.);

– статистические характеристики встраиваемого сообщения подобранны таким образом, чтобы они соответствовали статистическим характеристикам аналогичных шумов и искажений контейнера, с учетом предполагаемой вычислительной мощности противника.

Для обеспечения этих условий, при разработке стегосистемы, может применяться следующий алгоритм оценки эффективности стегоканала:

1) оценивается соответствие скрытого канала связи требованиям к его пропускной способности;

2) измеряются технические характеристики открытого канала при отключенном скрытом канале, измеряются параметры шумов и искажений в частотной и временной области;

3) измеряются технические характеристики канала связи при наличии скрытого канала, с учетом частотных и временных распределений искажений и помех. Система является стойкой, если изменения частотной и временной структуры искажений и помех, при включении скрытого канала, находится в пределах допусков поисковой аппаратуры, а уровни искажений и помех не превышают максимально допустимого значения.

Выводы

В проводных телефонных линиях стойкость скрытых каналов против пассивных атак обеспечивается за счет неопределенности знания противником точных параметров сигналов в линии, за счет случайного характера помех и случайности избыточных параметров самого речевого сигнала. Для обеспечения стойкости скрытого канала необходимо не только обеспечивать достаточно низкий уровень вносимых скрытым каналом помех, но и обеспечивать уровень отклонения статистических характеристик этих помех от помех

"пустого" канала ниже порога обнаружения аппаратуры противника. Необходимо постоянно совершенствовать методы построения скрытых каналов по мере увеличения вычислительной мощности поисковой аппаратуры противника.

Список литературы

1. *Хорошко В.А., Чекатков А.А.* Методы и средства защиты информации / Под ред. Ю.С. Ковтанюка. – К.: Издательство Юниор, 2003. – 504с.

2. *Bassia, P., Pitas, I.*: Robust audio watermarking in the time domain. In: Proc. EUSIPCO 98, vol. 1. Rodos, Greece. IEE (1998), P. 25–28.

3. *Swanson, M.D., Zhu, B., Tewfik, A.H., Boney, L.* Robust audio watermarking using perceptual masking. Signal Processing 66 (1998), P. 337–355.

4. *Gruhl, D., Lu, A., Bender, W.* Echo hiding. In: Anderson, R. (ed.): Information Hiding, Cambridge, UK. Lecture Notes in Computer Science, Vol. 1174. Springer-Verlag, Berlin/ Heidelberg (1996) , P. 295–315.

5. *Kirovski D., Malvar H.* Robust Covert Communication over a Public Audio Channel Using Spread Spectrum. Information Hiding Workshop, Pittsburgh, PA, (2001).

6. *Cachin C.* An Information-Theoretic Model for Steganography // Proceeding of the Workshop on Information Hiding. 1998.

7. *Zollner J., Federrath H., Klimant H.* Modeling the security of steganographic systems, 2nd Workshop on Information Hiding: April 1998, Portland, LNCS 1525, Springer Verlag, P. 345-355.

8. *Грибунин В.Г., Оков И.Н., Туринцев И.В.* Цифровая стеганография – М.: СОЛОН-Пресс, 2002.

9. *Provos N.* Defending Against on Statistical Steganalysis // Proceeding of the 10 USENIX Security Symposium. 2001. P. 323–335.

10. *Katzenbeisser S., Petitcolas F.* Defining Security in Steganographic Systems, Proceedings of the SPIE vol. 4675, Security and Watermarking of Multimedia Contents IV, 2002, P. 50-56.

Поступила 25.09.2006

УДК 681.3.06

Степанов В.Д, Хорошко В.А.

ПРИМЕНЕНИЕ СИСТЕМ АКТИВНОЙ ЗАЩИТЫ ИНФОРМАЦИИ В РАСПРЕДЕЛЕННЫХ КОРПОРАТИВНЫХ РЕСУРСАХ

Одной из основных задач при создании систем активной защиты (САЗ) является могокритериальная оптимизация оперативно-технических характеристик. Решение этой задачи предусматривает помимо количественного или качественного описания каждой характеристики, их сравнение с аналогичными характеристиками САЗ, использующих другие классы помех. Поэтому оценку их эффективности будем производить путем сравнения соответствующих технических характеристик.

Рассмотрим маскирующую способность прицельной помехи и ее зависимость от параметров, определяющих схемные и конструктивные особенности генераторов помех. Маскирующие свойства прицельной помехи в значительной степени обусловлены таким параметром, как число уровней квантования m. На рис. 1 и 2 приведены результаты расчетов средней вероятности ошибки для последовательных кодов с основанием n и равновероятным