УДК 681.511.3 **Маракова И.И.**

МЕТОДИКА ИССЛЕДОВАНИЯ СЕКРЕТНЫХ СИСТЕМ С ЦИФРОВЫМИ ВОДЯНЫМИ ЗНАКАМИ В УСЛОВИЯХ АТАКИ В ВИДЕ АДДИТИВНОГО ШУМА И ЛИНЕЙНОЙ ФИЛЬТРАЦИИ

В [1] разработана методика оценки эффективности системы с цифровыми водяными знаками для заданных ограничений ее построения, а именно, рассмотрения атаки только аддитивным шумом. Были получены аналитические выражения, позволяющие проводить количественную оценку при построении реальных систем. Представляется интересным расширить предложенную методику для менее жестких ограничений, например, при атаке не только аддитивным шумом, но и линейной фильтрацией.

1. Разработка модели

Прежде всего необходимо выполнить корректировку модели. Пусть:

- $C(n)$, $n \in A_N = 1, \ldots, N$ - основное покрывающее сообщение (ОПС) с дискретизацией во времени. Если $C(n)$ – изображение, то аргумент будет векторный $n = \bar{n} = (n_1, n_2)$ И ОПС будет содержать $C(\bar{n})$ пикселей, $C(\bar{n}) \in R$, R - реальное число. Причем, $C(\bar{n})$ может быть квантовано.

- $w(n)$, $n \in A_N = 1, \ldots, N$ цифровые водяные знаки (ВЗ), дискретные во времени. Если ВЗ погружается в изображение, то $n = \bar{n} = (n_1, n_2)$, $w(n) \in R$. $w(n)$ может быть квантовано.

- $S(n)$, $n \in A_N = 1, \ldots, N$ – стеганографическое сообщение, т.е. результат соединения по определенному алгоритму $C(n)$ и $w(n)$.

- $S'(n)$ - стегасообщение после прохождения канала атакующего.

- $\varepsilon(n)$, $n \in A_N = 1, \ldots, N$ – аддитивный шум атаки, .

- η_w - отношение сигнал/шум после погружения ВЗ или параметр искажений ОПС после погружения ВЗ.

- η_α - отношение сигнал/шум после прохождения стегасообщения через канал атаки.

- N – длина $C(n)$, $w(n)$, $\varepsilon(n)$, $S(n)$, $S'(n)$. В общем случае будем рассматривать одинаковую длину для $C(n)$, $w(n)$, $\varepsilon(n)$, $S(n)$, $S'(n)$. В отдельных случаях необходимо уточнение, а именно N_0 – длина ОПС, стегасообщения, помехи, N – длина ВЗ, причем $N < N_0$.

Уточним модель погружения ВЗ для рассматриваемой атаки.

Для кодера ВЗ

$$S(n) = f(C(n), R(n)), \qquad (1)$$

где $f(,)$ - некоторая функция двух последовательностей;

$R(n)$ - некоторая последовательность, случайная для атакующего, но известная кодеру и декодеру ВЗ.

В простейшем случае погружения ВЗ посредством побитового сложения

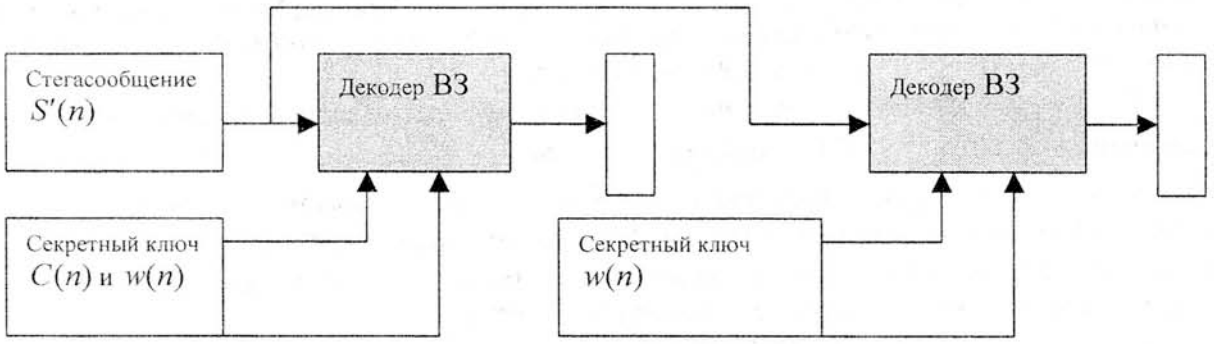
$$S(n) = C(n) + w(n), \quad n \in A_N = 1, \ldots, N, \qquad (2)$$

где $w(n)$ не зависит от $S(n)$.

Для простоты аналитических выкладок первоначально рассмотрим систему ВЗ с нулевым битом, т.е. возможно присутствие или отсутствие в стегасообщении ВЗ (декодер формирует только два вида сигнала, свидетельствующие о наличие или отсутствие ВЗ). В общем случае ВЗ может содержать значительно больше бит, например, идентификатор

владельца. Аналогично в системах связи один бит информации передается кодом или последовательностью. Но даже в случае системы с ВЗ с нулевым битом для каждого пользователя будут свои ВЗ.

В общем случае возможны секретная и открытая структура системы с ВЗ. При секретной версии, декодер знает секретный ключ, не известный атакующему. Секретным ключом может быть только ВЗ, $w(n)$, или только ОПС, $C(n)$, или $C(n)$ и $w(n)$ одновременно. В любом случае для секретной системы детектор должен быть информированным относительно $f(,)$. Рассмотрим две структуры секретной системы с ВЗ: когда $C(n)$ и $w(n)$ известны и известно только $w(n)$.



а). б).

Рис.1. Секретная структура системы с ВЗ с различными способами формирования ключа: а). секретный ключ $C(n)$ $w(n)$; б). секретный ключ $w(n)$.

Для открытых систем с ВЗ декодер не использует при обработке принятого сигнала секретного ключа. При этом на выходе так же формируется 0 или 1 и структура аналогична изображенной на рис.1 с тем лишь отличием, что не используется секретный ключ., т.е. ВЗ – также известны. Необходимо отметить, что ОПС должно быть не известно для атакующего даже в случае открытых систем с ВЗ. В противном случае представляется возможным тривиально удалить ВЗ, взяв $S'(n)=C(n)$.

Рассмотрим модель атаки.

Для секретной системы

$$S'(n)=\varphi(S'(n)),\ n\in A_N=1,\ ...,\ N, \qquad (3)$$

где $\varphi()$ - некоторая функция, возможно рандомизированная.

Для открытой системы

$$S'(n)=\varphi(S'(n),w(n)),\ n\in A_N=1,\ ...,\ N, \qquad (4)$$

Полагаем, что для двух структур систем атакующий знает встроенную функцию $f(,)$, структуру кодера ВЗ. Однако для секретной версии системы с ВЗ $C(n)$ и $w(n)$ (либо только $w(n)$) не известны для атакующего.

При атаке в виде аддитивного шума и фильтрации

$$S'(n)=S(n)*h(n)\ +\ \varepsilon(n),\quad n\in A_N=1,\ ...,\ N, \qquad (5)$$

где * означает операцию свертки $S(n)$ и некоторой импульсной функции фильтра $h(n)$, дискретной во времени и выбранной атакующим. Причем, атакующая функция $\varphi(S'(n))$ может быть известна или не известна кодеру.

2. Разработка методика исследование системы с ВЗ в условиях атаки аддитивным шумом и линейной фильтрацией

Предположим, что после погружения ВЗ и после прохождения канала атаки стегасообщение надежно. Если ОПС – изображение, то это означает, что визуально нет отличия между ОПС, сформированным кодером стегасообщением и стегасообщением после атаки. Проблема аналитического критерия надежности трудна при ОПС в виде картинке, видео и т.д. Это относится к области задач искусственного интеллекта.

Один из важнейших параметров, характеризующих систему с ВЗ, – визуально оцениваемое качество системы с ВЗ, означающее, что погружение ВЗ в ОПС не изменяет качество последнего ниже допустимого уровня. Другими словами, при восприятии человеком (изображения, видео) различия между стегаобразом (в данном случае ОПС и ВЗ) и ОПС должны быть не видимы.

Используем Эвклидову матрицу, т.е. среднеквадратический критерий, когда по минимуму $E(|C(n)-S'(n)|^2)$ выбирается наиболее надежное ОПС. Возможно использование и других критериев, например, так называемую, перцептуальную (perceptual) модель. Поскольку $C(n)$ является дискретным во времени стохастическим процессом, вполне естественным будет использовать в качестве критерия качества параметры искажения, а именно отношения сигнал/шум

$$\frac{\mathrm{var}(C(n))}{\mathrm{var}(S(n)-C(n))} \geq \eta_w, \qquad (6)$$

$$\frac{\mathrm{var}(C(n))}{\mathrm{var}(S'(n)-C(n))} \geq \eta_a, \qquad (7)$$

где $\mathrm{var}(x)$ - дисперсия случайной величины x.

Определим основные цели разработки системы ВЗ и атакующего (оптимальная стратегия атакующего должна быть известна разработчику системы для адаптации системы с ВЗ). Очевидно, что основная цель разработчика системы ВЗ и атакующего противоречат друг другу. Основная цель разработчика – сделать такой кодер и декодер ВЗ, чтобы обеспечить заданные величины вероятностей ошибок, а именно, вероятности ложного обнаружения ВЗ P_{fa} и зероятности пропуска ВЗ P_m и ограничения (7) для возможной атаки. Эффективность системы ВЗ зависит от длины N, но очень большие N могут быть практически нереализуемы или не оправданы для практической реализации. Поэтому разработчик должен найти минимально допустимое значение N, решая компромисс между теоретическими требованиями и практическими ограничениями. Иногда разработчик знает атакующую функцию $\varphi(n)$ и может использовать эти значения при формировании стегасообщения. Практически более ценным является рассмотрение сценария, когда разработчик не знает функцию $\varphi(n)$.

Основная цель атакующего – построить такую атаку, удовлетворяющую (7), чтобы P_{fa} и P_m были недопустимо большими при максимально возможном N. Если система ВЗ секретная, то атакующий не знает ключ, т.е. ОПС и ВЗ и поэтому постарается оптимизировать стратегию для любого ключа, но примет во внимание статистику ключа и ОПС.

Модель атаки в соответствие с (6)

$$S'(n) = S(n) * h(n) + \varepsilon(n) = \sum_{n'} S(n) * h(n-n') + \varepsilon(n), \quad n \in A_N = 1, \ldots, N, \qquad (8)$$

где $h(n)$ - некоторая реальная последовательность, являющаяся импульсной характеристикой линейного дискретного во времени фильтра;

$\varepsilon(n)$ - случайная последовательность, не зависимая от $S(n)$ для которой среднее и дисперсия, соответственно

$$E(\varepsilon(n)) = \varepsilon_0, \quad \text{var}(\varepsilon(n)) = \sigma_\varepsilon^2 \ . \qquad (9)$$

Более детально $\varepsilon(n)$ описывается плотностью распределения, которая может быть в частном случае гауссова. Модель погружения ВЗ может быть разной. Первоначально рассмотрим простейший случай аддитивного погружения ВЗ (2). При рассмотрении сценария, когда ОПС не известно декодеру будет использоваться так называемая кодовая книга W, содержащую много слов. Выбор $w(n) \in W$ будет осуществляться так, чтобы обеспечить наименьшие значения вероятностей ошибок кодера.

Если ОПС $C(n)$ является гауссовским процессом с нулевым средним и некоторой известной автокорреляционной функцией, $C(n)$, $w(n)$, $\varepsilon(n)$ - независимые последовательности, то (6) и (7) определяться как

$$\frac{\text{var}\, C(n)}{\text{var}\, W(n)} \geq \eta_w \ , \qquad (10)$$

$$\frac{\text{var}\, C(n)}{\text{var}(C(n) * h(n) - \delta(n) + \text{var}(W(n) * h(n)) + \text{var}\, \varepsilon(n)} \geq \eta_a \qquad (11)$$

Для получения аналитических выражений, описывающих оптимальную систему с ВЗ, необходимо упростить модель с обоснованием вносимых упрощений. Если $\varepsilon(n)$ - гауссовская последовательность, то оптимальная модель Неймана-Пирсона хорошо известна. Детектор в таком случае формирует величину

$$\Lambda = \sum_{n=0}^{N} S''(t)(w(n) * h(n)) \qquad (12)$$

и сравнивает с заранее выставленным в зависимости от требуемого уровня вероятностей ошибок порогом λ. Если $\lambda \geq \Lambda$, то принимается решение о присутствие ВЗ. Но проблема оценки $h(n)$ для детектора не проста. Одним из подходов является построение подоптимального приемника для неизвестного фильтра с $h(n)$, который вычисляет

$$\Lambda' = \max_{h(n) \in (14)} \sum_{n=0}^{N} S''(t)(w(n) * h(n)) \qquad (13)$$

и сравнивает с порогом λ'.

Если детектор ВЗ является обычным корреляционным детектором, который будет оптимальным в случае атаки без фильтрации, то формируемая величина

$$\Lambda'' = \sum_{n=0}^{N} (S'(n) - C(n))w(n) \qquad (14)$$

и сравнивается с порогом λ''.

Получим выражения для вероятностей ошибок P_{fa} и P_m для идеального детектора ВЗ, когда ему точно известен фильтр атакующего, т.е. $h(n)$. Если в стегасообщении есть ВЗ, то получим

$$\Lambda = \Lambda_1 = \sum_{n=0}^{N-1} [w(n) * h(n) + \varepsilon(n))(w(n) * h(n)] = \qquad (15)$$

$$= \sum_{n=0}^{N-1} [(w(n) * h(n)]^2 + \sum_{n=0}^{N-1} \varepsilon(n)[h(n) * w(n)]$$

Если в стегасообщении ВЗ отсутствуют, то получим

$$\Lambda = \Lambda_0 = \sum_{n=0}^{N-1} \varepsilon(n)[h(n) * w(n)] \ . \qquad (16)$$

Поскольку $\varepsilon(n)$ - гауссовская величина, то Λ_1 и Λ_0 должны быть гауссовскими при больших N. Математические ожидания и дисперсии для Λ_1 и Λ_0

$$E(\Lambda_0) = 0 \ . \qquad (17)$$

$$E(\Lambda_1) = \alpha^2 \sum_{n=0}^{N-1}\sum_{n'=0}^{N-1} h^2(n-n') \approx N\alpha^2 \sum_{n=0}^{N-1} h^2(n), \qquad (18)$$

$$\mathrm{var}\,\Lambda_0 = \sigma_\varepsilon^2 \sum_{n=0}^{N-1} E[w(n) * h(n)]^2 \ , \qquad (19)$$

$$\mathrm{var}\,\Lambda_1 = \mathrm{var}[\sum_{n=1}^{N-1} (w(n) * h(n))^2 + \mathrm{var}\,\Lambda_0 \ , \qquad (20)$$

где $\alpha^2 = \dfrac{\sigma_c^2}{\eta_w}$.

Моделированием было проверено справедливость равенства $\mathrm{var}\,\Lambda_1 \approx \mathrm{var}\,\Lambda_0$. Сравнивая количественные оценки $\mathrm{var}\,\Lambda_1$ и $\mathrm{var}\,\Lambda_0$ можно отметить, что они зависят от N, σ_ε^2, α^2 и результат сравнения существенно зависит от исходных параметров. Например, если выбрать $\sigma_\varepsilon^2 << 1$, то это приведет наименьшей величине $\mathrm{var}\,\Lambda_0$ и если положить $\alpha^2 << 1$, то это приведет к наименьшей величине $\mathrm{var}\,\Lambda_1$.

Аналитические оценки вероятностей ошибок

$$P_m = 1 - Q\frac{(\lambda - E(\Lambda_1))}{\sqrt{\mathrm{var}\,\Lambda_1}} \approx 1 - Q((\frac{\lambda - E(\Lambda_1)}{\sqrt{\mathrm{var}\,\Lambda_0}}) \ , \qquad (21)$$

$$P_{fa} = Q\frac{\lambda}{\sqrt{\mathrm{var}\,\Lambda_0}} \ , \qquad (22)$$

где $Q(x) = 1/\sqrt{2\pi} \int_x^\infty e^{-\frac{t^2}{2}} dt$.

Из (21) и (22) следует, что оптимальная атака фильтрацией должна минимизировать соотношение

$$\xi = \frac{E(\Lambda_1)}{\sqrt{\mathrm{var}\,\Lambda_0}} = \frac{\alpha}{\sigma_\varepsilon}\sqrt{\sum_{n=0}^{N-1} h^2(n)} \ . \qquad (23)$$

Представляется возможным переформулировать цель оптимальной атаки в терминах спектра, т.е. рассматривая ДПФ $h(n)$. Необходимо выбрать $h(n)$ и дисперсию шума σ_ε^2 так, чтобы минимизировать

$$\xi' = \frac{1}{\sigma_\varepsilon}\sqrt{\sum_{n=0}^{N-1} \left|\hat{h}(k)\right|^2} \qquad (24)$$

и выполнялось соотношение

$$\frac{1}{\frac{1}{N}\sum_{k=0}^{N-1} \hat{\Psi}_{cn}(k)\hat{h}_0(k) + \frac{1}{\eta_w N}\sum_{k=0}^{N-1}\left|\hat{h}(k)\right|^2 + \frac{\sigma_\varepsilon^2}{\sigma_c^2}} \geq \eta_\alpha \ , \qquad (25)$$

откуда представляется возможным вычисление оптимальной полосы частот фильтра атаки для минимизации ξ'.

Конечно, спектры реальных ОПС более сложны по форме, чем прямоугольные и поэтому потребуется дополнительная оптимизация частотного отклика фильтра. Как правило, точная форма спектра ОПС не известна и атакующему и разработчику системы с ВЗ. Конечно, атакующий может тестировать различные фильтры, наблюдая эффект

разрушения ОПС и выбирая лучший. Для того чтобы избежать ухудшения надежности ОПС можно ограничить частоту, тогда равномерная последовательность ВЗ в условиях фильтрующей атаки должна измениться и стать коррелированной последовательностью с некоторой оптимизированной корреляционной функцией. Данные исследования будут изложены в последующей публикации.

Литература:

1. 1.Маракова И.И., Мараков Д.А. Методика оценки эффективности систем с цифровыми водяными знаками в рамках заданных ограничений / Захист інформації – 2002. - №2. – с.с.58-64.

Поступила 20.02.2003

УДК 681.3

С.А.Чеховский, Ю.М. Рудаков

Побочные излучения и защита информации в локальных сетях

В связи с бурным развитием локальных и глобальных вычислительных сетей широкое развитие получили и методы разведки (промышленного шпионажа), направленные на перехват информации, обрабатываемой (передаваемой, хранящейся) в локальных сетях. Причем, трудно уверенно сказать, кто сейчас больше занимается разведывательной деятельностью: государства против других государств или коммерческие фирмы против других фирм. Соответственно, бурное развитие получили и методы противодействия разведке. Как правило, проникновение в локальную сеть какой либо организации возможно только при недостаточно квалифицированной настройке всех элементов локальной сети (включая и каждую рабочую станцию) администратором системы. В случае же грамотной настройки, применения дополнительных программных и аппаратных средств, выполнении необходимых организационных мероприятий, шпионам необходимо изыскивать методы добывания информации, не связанные с необходимостью проникновения в локальную сеть. В связи с этим в последнее время «второе дыхание» получают методы перехвата информации по каналам побочных излучений и наводок (ПЭМИН) элементов локальной сети.

Методика защиты отдельных компьютеров достаточно хорошо проработана, подкреплена необходимыми нормативными документами. Задача же защиты информации от утечки по каналам ПЭМИН в локальной сети существенно сложнее, чем для автономно используемых устройств.

Защита активного оборудования и рабочих станций.

Источниками электромагнитных излучений в локальной сети являются, безусловно, рабочие станции (компьютеры) и активное сетевое оборудование. Для защиты от утечки информации по каналам побочных излучений и наводок применяется экранирование этого оборудования.

Для снижения уровня излучений активного оборудования локальной сети это оборудование лучше всего размещать в экранированном шкафу. В частности, можно рекомендовать шкафы производства Schroff GmbH типа «HF». В конструкции этих шкафов приняты специальные меры по улучшению экранирующих свойств, такие, как, например, пружинящие контакты по всему периметру дверцы (рис. 1).