Math-Net.Ru

Общероссийский математический портал

П. А. Ушаков, О способе организации скрытого канала и оценка его устойчивости к помехам, *Дискрет. матем.*, 2007, том 19, выпуск 1, 60–66

DOI: <https://doi.org/10.4213/dm8>

Использование Общероссийского математического портала Math-Net.Ru подразумевает, что вы прочитали и согласны с пользовательским соглашением

<http://www.mathnet.ru/rus/agreement>

Параметры загрузки:

IP: 54.162.85.209

26 апреля 2023 г., 16:49:36

О способе организации скрытого канала и оценка его устойчивости к помехам

© 2007 г. П. А. Ушаков

В работе рассматривается модель скрытого канала взаимодействия агентов в глобальной сети и в закрытом сегменте локальной сети. Находится предельное распределение статистик, на основании которых возможно построение канала. Анализируется возможность противодействия организации скрытого канала с помощью случайных помех и доказывается устойчивость данного канала к случайным помехам.

В статье [1] была описана модель скрытого канала взаимодействия агентов в глобальной сети и в закрытом сегменте локальной сети. В данной работе находится предельное распределение статистик, на основе которых строится данный канал, и исследуется поведение распределения этих статистик в случае наличия случайных перестановок, противодействующих организации данного канала.

Пусть имеется $m + 1$ сегмент локальных сетей $S_0, S_1, \dots, S_m$, с адресами шлюзов $s_0, s_1, \dots, s_m$, которые соединены в виртуальную частную сеть (VPN) посредством глобальной сети. Мы предполагаем, что нарушитель глобальной сети (НГС) пытается организовать скрытый канал и передать информацию программно-аппаратному агенту, находящемуся в одной из сетей, например, в s_0 . Передача пакета от компьютера x в сегменте S_i компьютеру y в сегменте S_j выглядит следующим образом:

- пакет передается от машины с адресом x к шлюзу сегмента S_i ;
- далее пакет передается на узел защиты, который шифрует пакет и инкапсулирует его в пакет с адресом получателя s_j и адресом отправителя s_i ;
- пакет попадает на шлюз глобальной сети, который через глобальную сеть направляет этот пакет на аналогичный шлюз, соединяющий сегмент S_j с глобальной сетью;
- пакет попадает на узел защиты, где он дешифруется, и восстанавливается исходный пакет с адресом получателя y и адресом отправителя x ;
- этот пакет направляется к шлюзу сегмента S_j , который пересылает его машине с адресом y в этом сегменте.

Все данные, пересылаемые между сегментами VPN, шифруются на узлах защиты (УЗ), которые соединяют шлюзы с глобальной сетью и НГС не может строить канал на основе содержимого пакетов, а единственной информацией, которая может послужить для организации скрытого канала, является относительный порядок сообщений.

Построим следующую вероятностную модель. Пусть дан алфавит

$$A = \{\alpha_{11}, \dots, \alpha_{1|S_1|}, \alpha_{21}, \dots, \alpha_{2|S_2|}, \dots, \alpha_{m,|S_m|}\},$$

здесь символ α_{ij} соответствует сообщению из компьютера j в i -м сегменте. Предположим, что сообщения появляются независимо с вероятностями p_{ij} соответственно, при этом для p_{ij} выполнено соотношение

$$\sum_{i=1}^m \sum_{j=1}^{|S_i|} p_{ij} = 1.$$

В данном случае скрытый канал можно организовать следующим образом. НГС разбивает сегменты локальных сетей на K частей $S(1), S(2), \dots, S(K)$. Предположим, что разбиение можно выполнить таким образом, что вероятности появления сообщений из каждой из K частей будут равными, то есть

$$\sum_{i \in S(1)} \sum_{j=1}^{|S_i|} p_{ij} = \sum_{i \in S(2)} \sum_{j=1}^{|S_i|} p_{ij} = \dots = \sum_{i \in S(K)} \sum_{j=1}^{|S_i|} p_{ij}$$

Потом НГС начинает отправлять пакеты программно-аппаратному агенту в S_0 , посылая сообщения последовательно из разных сегментов. Для простоты предположим, что K равно 2, то есть НГС чередует отправку пакетов, вначале он шлет пакет из $S(1)$, потом из $S(2)$, потом из $S(1)$ и так далее. Для удобства предположим, что компьютер с адресом α_{ij} находится в сегменте, относящемся к $S(2)$

Предположим, что УЗ пытается противостоять попыткам организации скрытого канала, для этого он производит перемешивание пакетов стараясь нарушить статистические зависимости, которые используются программно-аппаратным агентом для активизации скрытого канала. Алгоритм действий УЗ может быть следующим: он получает D сообщений и перед отправкой их в локальную сеть производит равномерное перемешивание. Рассмотрим случай с D равным 2. В этом случае УЗ разбивает все приходящие сообщения на пары, после чего в каждой паре с вероятностью $1/2$ меняет порядок пакетов и с вероятностью $1/2$ оставляет его без изменений.

Программно-аппаратный агент в сегменте S_0 видит слово $a = (a_1, a_2, \dots, a_N)$ длины N из алфавита A , анализирует распределение расстояний между одинаковыми адресами. В случае попытки активации скрытого канала и отсутствия помех все расстояния между пакетами из одного адреса должны быть четными. Программно-аппаратный агент анализирует распределение числа расстояний, равных j , между вхождениями произвольного символа α_{fg} из алфавита A в слово a . Так как нас интересует в слове a только символ α_{fg} , данную схему можно свести к схеме с алфавитом $B = \{0, 1\}$, где 1 соответствует α_{fg} , а 0 любому другому символу. Случайному слову a будет соответствовать слово $b = (b_1, b_2, \dots, b_N)$, где b_l — независимые случайные величины с $\mathbf{P}\{b_l = 1\} = p_{fg} = p$

Комбинации возможной активности НГС и УЗ дают нам четыре возможных сценария:

- (1) НГС не пытается организовать скрытый канал, УЗ не вносит помехи.
- (2) НГС активизирует скрытый канал, УЗ не вносит помех, в этом случае для отличия от первого сценария случайные величины будут обозначаться теми же символами с крышкой $(\hat{a}_i, \hat{b}_i, \dots)$

- (3) НГС не пытается организовать скрытый канал, УЗ противодействует попытке скрытой передачи информации, задействовав перемешивание, случайные величины будут обозначаться теми же символами со штрихом ($a'_i, b'_i, \dots$)
- (4) НГС пытается организовать скрытый канал, УЗ противодействует попытке скрытой передачи информации, задействовав перемешивание, случайные величины будут обозначаться теми же символами с крышкой и со штрихом ($\hat{a}'_i, \hat{b}'_i, \dots$)

Основная трудность при анализе данной схемы заключается в конечности слова b , поэтому рассмотрим слово b^* бесконечной длины, а ограничение на его размер добавим потом. Обозначим λ_k номер k -го появления единицы в слове b^* .

Положим $r_i = \lambda_i - \lambda_{i-1}$, для удобства будем считать, что $\lambda_0 = 0$ и $r_0 = 0$. Тогда мы получим схему из независимых случайных величин $r_1, \dots, r_n, \dots$, имеющих геометрическое распределение с параметром p .

Число расстояний, равных j , среди первых l расстояний есть

$$S_l^j = I_{\{r_1=j\}} + \dots + I_{\{r_l=j\}}$$

Обозначим через τ_N номер последнего появления единицы среди $b_1, b_2, \dots, b_N$, то есть

$$\tau_N = \max\{n \geq 0: r_1 + \dots + r_n \leq N\}$$

и $\tau_N = 0$, если $r_1 > N$. Применительно к данной задаче $S_{\tau_N}^j$ имеет смысл числа расстояний между пакетами из машины с адресом α_{fg} , равных j , среди N сообщений. Именно статистику $S_{\tau_N}^j$ удобнее всего использовать для выявления активации скрытого канала.

Найдем предельное распределение случайной величины $S_{\tau_N}^j$, для этого вначале докажем вспомогательную лемму.

Лемма 1. Случайная величина τ_N при N , стремящемся к бесконечности, асимптотически нормальна, точнее, при $N \rightarrow \infty$

$$\frac{\tau_N - Np}{\sqrt{(1-p)pN}} \Rightarrow N(0, 1).$$

Доказательство. Для начала отметим основные свойства случайной величины r_i ; нетрудно видеть, что

$$\begin{aligned} \mathbf{E}I_{\{r_i=j\}} &= \mathbf{P}\{r_i = j\} = p(1-p)^{j-1}, & \mathbf{D}I_{\{r_i=j\}} &= p(1-p)^{j-1}(1-p(1-p)^{j-1}), \\ \mu = \mathbf{E}r_i &= \sum_{j=1}^{\infty} jp(1-p)^{j-1} = \frac{1}{p}, & \mathbf{E}r_i^2 &= \sum_{j=1}^{\infty} j^2 p(1-p)^{j-1} = \frac{2-p}{p^2}, \\ \sigma^2 = \mathbf{D}r_i^2 &= \frac{1-p}{p^2}. \end{aligned} \quad (1)$$

Рассмотрим случайный процесс

$$X_N(t) = \frac{1}{\sigma\sqrt{n}} \sum_{i=1}^{[Nt]} (r_i - \mu)$$

Так как случайные величины r_i независимы, одинаково распределены и имеют конечную дисперсию, для $X_N(t, w)$ выполнена функциональная центральная предельная теорема и

этот процесс сходится по распределению к винеровскому процессу при $N \rightarrow \infty$. Отсюда на основании теоремы 17.3 из [2] следует, что процесс

$$Z_N(t) = \frac{\tau_N t - Nt/\mu}{\sigma\mu^{-3/2}\sqrt{N}}$$

также сходится по распределению к винеровскому процессу, откуда следует слабая сходимость случайной величины $(\tau_N - Np)/\sqrt{(1-p)pN}$ к стандартному нормальному распределению.

Следствие 1. Из леммы 1 следует, что случайная величина $\tau_N/(N\sqrt{(1-p)p})$ сходится по распределению к константе, то есть при $N \rightarrow \infty$

$$\frac{\tau_N}{N\sqrt{p(1-p)}} \Rightarrow \sqrt{\frac{p}{1-p}}. \quad (2)$$

Найдем предельное распределение числа расстояний между пакетами с одинаковыми адресами, равных произвольной константе j , в описанной схеме (случай 1) при длине сообщения N стремящейся к бесконечности.

Теорема 1. При $N \rightarrow \infty$

$$\frac{S_{\tau_N}^j - \tau_N p(1-p)^{j-1}}{\sqrt{p(1-p)^{j-1}(1-p(1-p)^{j-1})\tau_N}} \Rightarrow N(0, 1) \quad (3)$$

Доказательство. Определим случайным процесс $X_N^j(t)$, полагая

$$X_N^j(t) = \frac{S_{[Nt]}^j - [Nt]p(1-p)^{j-1}}{\sqrt{p(1-p)^{j-1}(1-p(1-p)^{j-1})N}}.$$

Для X_N^j справедлива функциональная центральная предельная теорема, так как S_k^j является суммой независимых одинаково распределенных случайных величин с конечным вторым моментом. Но из этого условия совместно с условием (1) на основании теоремы 17.2 из [2] следует сходимость процесса

$$Y_N(t) = X_{\tau_N(w)}^j(t)$$

к винеровскому процессу. Отсюда следует, что при $N \rightarrow \infty$

$$\frac{S_{\tau_N}^j - \tau_N p(1-p)^{j-1}}{\sqrt{p(1-p)^{j-1}(1-p(1-p)^{j-1})\tau_N}} \Rightarrow N(0, 1)$$

сходится по распределению к стандартной нормальной случайной величине при стремлении числа пакетов к бесконечности в описанной выше схеме, при условии, что скрытый канал не активен.

Найдем теперь, как ведет себя случайная величина $\hat{S}_{\hat{\tau}_N}^j$, имеющая смысл числа расстояний между пакетами из машины с адресом α_{fg} , равных j , среди N сообщений, в случае если НГС пытается передать информацию программно-аппаратному агенту для активации скрытого канала. В этом случае НГС шлет сообщения парами, первое из $S(1)$, второе из $S(2)$. Предположим что α_{fg} принадлежит $S(2)$.

Для начала найдем предельное распределение для $\hat{\tau}_N$.

Лемма 2. Распределение $\hat{\tau}_N^p$ совпадает с распределением $\tau_{N/2}^{2p}$.

Доказательство. В этом случае в слове $\hat{b} = (\hat{b}_1, \dots, \hat{b}_N)$ нечетные символы всегда нули, а четные символы $\hat{b}_{2l}$ являются независимыми случайными величинами, равными единице с вероятностью $2p$, то есть $\hat{b}_{2l+1} = 0$, а $\mathbf{P}\{\hat{b}_{2l} = 1\} = 2p$. Из этого следует, что все расстояния $\hat{r}_i$ могут принимать только четные значения, а случайные величины $\hat{b}_2, \hat{b}_4, \dots, \hat{b}_N$ имеют тоже распределение, что и $b_1, \dots, b_{N/2}$ при условии появления единицы с вдвое большей вероятностью. Отсюда следует утверждение леммы.

Теорема 2. Случайная величина $\hat{S}_{\hat{\tau}_N}^j$ ведет себя следующим образом: $\hat{S}_{\hat{\tau}_N}^{2j+1} = 0$ для любого целого неотрицательного j , при $N \rightarrow \infty$

$$\frac{\hat{S}_{\hat{\tau}_N}^{2j} - \hat{\tau}_N 2p(1-2p)^{j-1}}{\sqrt{2p(1-2p)^{j-1}(1-2p(1-2p)^{j-1})\hat{\tau}_N}} \Rightarrow N(0, 1). \quad (4)$$

Доказательство. Теорема прямо следует из вида распределения $\hat{b} = (\hat{b}_1, \dots, \hat{b}_N)$, которое может быть получено из факта, доказанного в лемме 2, путем замены p на $2p$ и N на $N/2$ в распределении $S_{\tau_N}^j$.

Отметим что предельные распределения $\hat{S}_{\hat{\tau}_N}^j$ и $S_{\tau_N}^j$ различны, откуда следует, что программно-аппаратный агент может выявить сигнал от НГС статистическими методами.

Рассмотрим число $S_{\tau_N}^{'j}$ расстояний между пакетами из машины с адресом α_{fg} , равных j , среди N сообщений в случае, если НГС не пытается передать информацию программно-аппаратному агенту для активации скрытого канала, а УЗ перемешивает сообщения.

Теорема 3. При $N \rightarrow \infty$

$$\frac{S_{\tau_N}^{'j} - \tau'_N p(1-p)^{j-1}}{\sqrt{p(1-p)^{j-1}(1-p(1-p)^{j-1})\tau'_N}} \Rightarrow N(0, 1) \quad (5)$$

Доказательство. В этом случае случайные величины $S_{\tau_N}^j$ и $S_{\tau_N}^{'j}$ имеют одинаковое распределение, так как символы b_i независимы и одинаково распределены и поэтому их перемешивание не изменяет распределение вектора b , а значит и функций от него.

Рассмотрим число $\hat{S}^{'j}$ между пакетами из машины с адресом α_{fg} , равных j , среди N сообщений, в случае, если НГС пытается передать информацию программно-аппаратному агенту для активации скрытого канала, а УЗ перемешивает сообщения.

Теорема 4. При $N \rightarrow \infty$

$$\begin{aligned} \frac{\hat{S}_{\hat{\tau}_N}^{'2j} - \hat{\tau}_N p(1-2p)^{j-1}}{\sqrt{p(1-2p)^{j-1}(1-p(1-2p)^{j-1})\hat{\tau}_N}} &\Rightarrow N(0, 1), \\ \frac{\hat{S}_{\hat{\tau}_N}^{'2j+1} - \hat{\tau}_N p(1-p)(1-2p)^{j-1}}{\sqrt{p(1-p)(1-2p)^{j-1}(1-p(1-p)(1-2p)^{j-1})\hat{\tau}_N}} &\Rightarrow N(0, 1). \end{aligned} \quad (6)$$

Доказательство. Отметим, что $\hat{\tau}'_N = \hat{\tau}_N$, так как при перемешивании сообщений на УЗ число единиц в слове $\hat{b}$ не меняется.

Распределение вектора $\hat{b}'$, полученного как суперпозиция двух операций, переупорядочивания НГС для передачи сигнала об активации скрытого канала и перемешивания УЗ для нарушения работы скрытого канала, имеет вид

$$\begin{aligned}\mathbf{P}\{\hat{b}'_{2j+1} = 1\} &= (1/2)2p = p, \\ \mathbf{P}\{\hat{b}'_{2j} = 1\} &= (1/2)2p = p,\end{aligned}\quad (7)$$

то есть распределение элементов векторов b и $\hat{b}'$ совпадает, но, в отличие от b , элементы $\hat{b}'$ являются зависимыми.

Случайную величину $\hat{S}'_{\hat{\tau}_N}$ представим в виде

$$\hat{S}'_{\hat{\tau}_N} = I_{\{\hat{r}'_1=j\}} + \dots + I_{\{\hat{r}'_{\hat{\tau}_N}=j\}} \quad (8)$$

Процесс перемешивания символов на УЗ можно представить следующим образом:

$$\hat{r}'_i = \hat{r}_i + \xi_{i-1} - \xi_i,$$

где ξ_i , $i \geq 0$, — независимые одинаково распределенные случайные величины, принимающие значения 0 и 1 с вероятностью $1/2$, $\xi_0 = 0$, а $\hat{r}_i$ — независимые одинаково распределенные случайные величины такие, что $\mathbf{P}\{\hat{r}_i = 2j\} = 2p(1-2p)^{j-1}$.

Найдем математическое ожидание и дисперсию случайной величины $I_{\{\hat{r}'_i=j\}}$. Нетрудно видеть, что

$$\begin{aligned}\mathbf{E}I_{\{\hat{r}'_i=j\}} &= \mathbf{E}I_{\{\hat{r}_i+\xi_{i-1}-\xi_i=j\}} = \frac{1}{2}\mathbf{P}\{\hat{r}_i = j\} + \frac{1}{4}\mathbf{P}\{\hat{r}_i = j+1\} + \frac{1}{4}\mathbf{P}\{\hat{r}_i = j-1\}, \\ \mathbf{E}I_{\{\hat{r}'_i=2j\}} &= \frac{1}{2}2p(1-2p)^{j-1} = p(1-2p)^{j-1}, \\ \mathbf{E}I_{\{\hat{r}'_i=2j+1\}} &= \frac{1}{4}\mathbf{P}\{\hat{r}_i = 2j+2\} + \frac{1}{4}\mathbf{P}\{\hat{r}_i = 2j\} = p(1-p)(1-2p)^{j-1}, \\ \mathbf{D}I_{\{\hat{r}'_i=2j\}} &= p(1-2p)^{j-1}(1-p(1-2p)^{j-1}), \\ \mathbf{D}I_{\{\hat{r}'_i=2j+1\}} &= p(1-p)(1-2p)^{j-1}(1-p(1-p)(1-2p)^{j-1})\end{aligned}\quad (9)$$

Отметим, что последовательность $\{I_{\{\hat{r}'_k=j\}}\}$ является 1-зависимой, так как зависимыми являются только соседние случайные величины. Отсюда на основании теоремы 20.1 из [2] следует, что процесс

$$\frac{\hat{S}'_{Nt} - Nt\mathbf{E}I_{\{\hat{r}'_k=j\}}}{\sigma\sqrt{N}},$$

где

$$\sigma^2 = \mathbf{D}I_{\{\hat{r}'_1=2j\}} + 2\sum_{k=1}^{\infty} \text{cov}(\{I_{\{\hat{r}'_1=j\}}, I_{\{\hat{r}'_k=j\}}\}),$$

сходится к винеровскому процессу, откуда следует, что процесс, полученный случайной заменой времени на $\hat{\tau}_N$, на основании теоремы 17.1 из [2] тоже сходится к винеровскому процессу. Из этого факта вытекает утверждение теоремы.

Эффективность работы УЗ определяется близостью распределений $\hat{S}_{\tau_N}^j$ и $S_{\tau_N}^j$.

Сравнивая теоремы 3 и 4, мы видим, что распределение, полученное после операции перемешивания входных сообщений на УЗ, отличается от распределения в случае отсутствия активности скрытого канала. Несмотря на то, что это отличие довольно мало, оно означает, что программно-аппаратный агент внутри локальной сети может использовать статистический критерий для организации скрытого канала, используя четность расстояний между сообщениями из одного адреса.

Тем более, так как инициатором организации скрытого канала выступает НГС, он может выбрать упорядочивание с базой K , большей двух, в этом случае перемешивание с базой два не сможет внести помех в скрытый канал. А так как НГС может увеличивать K до тех пор пока не получит из сети ответ на свое сообщение, данный метод организации скрытого канала является довольно эффективным и устойчивым к помехам.

Из данной работы следует, что организация случайных перестановок на УЗ не может помешать организации скрытого канала, в дальнейшем планируется исследовать возможность выявления скрытого канала на УЗ и борьбы с ним с помощью специальных помех, которые будут специфическими для каждого скрытого канала.

Список литературы

1. Грушо А. А., Тимонина Е. Е., Оценка времени, требуемого для организации скрытого канала. *Дискретная математика* (2003) **15**, №2, 40–46.
2. Биллингсли П., *Сходимость вероятностных мер*. Наука, Москва, 1977.

Статья поступила 29.09.2005.