СКРЫТЫЕ СЕТИ

А.А. Грушо, Н.А. Грушо, Е.Е. Тимонина

Российский государственный гуманитарный университет
Кировоградская 25, г. Москва, Россия
телефон: + 7(495) 2506699; e-mail: grusho@yandex.ru

Работа посвящена построению моделей сетей скрытой передачи информации. Для этих моделей найдены достаточные условия существования состоятельных последовательностей критериев выявления скрытых сетей статистическими методами. Наибольший интерес представляют условия несуществования состоятельных последовательностей критериев в этой задаче, т.к. они определяют условия неэффективности поиска скрытой сети.
Работа выполнена при поддержке РФФИ, грант № 07-07-00236, грант № 07-01-00484.

Ключевые слова - безопасность распределенных компьютерных систем, статистические методы, скрытые сети.

Скрытым каналам (СК) посвящено много работ. Однако вероятностно-статистических моделей скрытых сетей в литературе мало [3]. Практически такие сети существуют, например, бот сети [4]. В связи с такими скрытыми сетями возникают следующие математические задачи. В каких условиях можно выявить существование таких сетей статистическими методами? Можно ли это сделать, рассматривая выборочные данные по сетевому трафику? Данная работа посвящена построению формальных моделей.

Допустим, что в глобальной сети содержится перенумерованное натуральными числами счетное множество узлов, но количество возможных связей каждого узла ограничено константой C. Будем считать, что множество логических связей каждого узла i фиксировано и обозначается Y_i. Это предположение усложняет задачу выявления скрытой сети, т.к. означает, что скрытые передачи идут по традиционным связям хостов. Множества Y_i, $i \in \mathbf{N}$, определяют бесконечный граф G, вершины которого перенумерованы натуральными числами, а ребра определяются множествами смежности Y_i. Корректное определение графа G связано с выполнением условий

$$i \in Y_j \Leftrightarrow j \in Y_i .$$

Скрытая сеть представляет собой конечное множество $M \subseteq \mathbf{N}$ вершин графа и множество конечных маршрутов в сети $i_1 i_2 ... i_s$, где все вершины i_j, $j = \overline{1,s}$, лежат в M, а ребра (i_j, i_{j+1}), $j = \overline{1,s-1}$, присутствуют в определенном выше графе. Мы предполагаем, что пути в скрытой сети постоянны и устойчивы. При этом промежуточные вершины маршрутов скрытой сети могут оказаться «зомби» компьютерами, но исключать их из рассмотрения нельзя. На каждое ребро графа G можно поместить неотрицательную метку $\rho(i, j)$, равную, например, числу пакетов, передаваемых за заданный период времени по связи (i, j). Будем считать, что все метки ограничены константой C". На самом деле метка лишь характеризует интенсивность связи и должна удовлетворять условию аддитивности и конечнозначности.

Ограничение графа G на первые n вершин будем обозначать через G_n. Множество графов $\{G_{n+1}\}$ получается из множества графов $\{G_n\}$ следующим образом. Любой граф G_{n+1} получается из некоторого G_n добавлением допустимых помеченных ребер, связывающих вершину $(n+1)$ с вершинами $\{i,\ i=1,...,n\}$. Обозначим множество всех возможных допустимых добавлений X_{n+1}, а набор добавлений x_{n+1}, $x_{n+1} \in X_{n+1}$, к графу G_n определяет вместе с графом G_n граф G_{n+1}. Тогда каждый допустимый граф G_{n+1} представим в виде вектора $(x_2, x_3, ..., x_{n+1})$, где x_i - это числовой вектор меток допустимых ребер, связывающий i с предыдущими вершинами.

В пространстве $\{G\}$ граф G взаимно-однозначно представим в виде бесконечной последовательности $(x_2, x_3, ...)$, являющейся элементом бесконечного произведения $\prod_{i=2}^{\infty} X_i = X^{\infty}$.

Элементарные цилиндрические множества в таком представлении соответствуют произведению $(x_2, x_3, ..., x_n) \times \prod_{i=n+1}^{\infty} X_i$. Цилиндрические множества порождают на X^{∞} σ-алгебру $\mathcal{A}$.

Ясно, что значение каждой метки является случайной величиной, и метки не являются независимыми. Мы получаем случайный помеченный граф, который определяется вероятностной мерой P_0 на вероятностном пространстве X^{∞} с σ-алгеброй $\mathcal{A}$, порожденной цилиндрическими множествами. Проекцию меры P_0 будем обозначать через $P_{0,n}$.

В случае существования скрытой сети появляется дополнительный трафик и другие специфические признаки скрытой передачи, например, специальные метки и транзитные пакеты через узлы маршрутов передачи данных в скрытой сети. Тогда скрытую сеть можно представить в виде графа G', метки которого складываются с метками графа G. Таким образом, образуется случайный граф $G''=G+G'$, который, удовлетворяет всем определенным ранее ограничениям. Так как M – конечное множество, то $\exists N$ такое, что все ненулевые метки ограничены графом G'_N. Поэтому число допустимых значений графа G' для фиксированного множества M конечно. Для любого конечного M и связанного с ним G' определим вероятностную меру $P_\theta(A) = P_\theta(A+G')$, где θ это некоторая нумерация возможных скрытых сетей и потоков в них. $P_{\theta,n}$ - проекция P_θ на первые n координат.

Мы считаем, что наблюдается конечный участок сети, который может расширяться, и куда входят вершины в соответствии с порядком нумерации узлов. Тогда для каждого n задача выявления скрытой сети (части скрытой сети) формулируется как задача проверки гипотезы

$$H_{0,n} : P_{0,n}.$$

против сложной альтернативы

$$H_{1,n} : \{P_{\theta,n},\ \theta \in \Theta\}.$$

Построенная модель позволяет выделить несколько случаев. Обозначим $D_{0,n}$ и $D_{\theta,n}$ носители вероятностных мер $P_{0,n}$ и $P_{\theta,n}$ для всех альтернатив. Определим также $\Delta_{0,n} = D_{0,n} \times \prod_{i=n+1}^{\infty} X_i$, $\Delta_{\theta,n} = D_{\theta,n} \times \prod_{i=n+1}^{\infty} X_i$. Нетрудно увидеть, что последовательности $\Delta_{0,n}$, $n\in\mathbf{N}$, и $\Delta_{\theta,n}$, $n\in\mathbf{N}$, $\theta \in \Theta$, - невозрастающие. Тогда существуют пределы

$$\Delta_0 = \bigcap_{n=2}^{\infty} \Delta_{0,n},\quad \Delta_\theta = \bigcap_{n=2}^{\infty} \Delta_{\theta,n},\ \Delta(\theta) = \Delta_0 \cap \Delta_\theta.$$

Пространство X^∞ является Тихоновским произведением [2], которое является топологическим пространством со счетной базой и компактным. Отсюда следует, что если

$$\Delta(\theta) = \varnothing, \qquad (1)$$

то $\exists N$ такое, что для любых $n \geq N$ существует критерий проверки $H_{0,n}$ против $H_{1,n}$ с критическим множеством S_n такой, что $P_{0,n}(S_n)=0$, $P_{\theta,n}(S_n)=1$. Отсюда следует существование состоятельной последовательности критериев [1] для всех альтернатив θ, удовлетворяющих (1).

Если $P_0(\Delta(\theta))>0$, то можно доказать, что состоятельной последовательности критериев не существует.

Последнее утверждение означает, что в достаточно широком классе случаев не существует эффективных статистических методов выявления скрытых сетей.

ЛИТЕРАТУРА

[1] Леман Э. Проверка статистических гипотез. – Наука, Москва, 1964.

[2] Прохоров Ю.В., Розанов Ю.А. Теория вероятностей. -- Наука, Москва, 1993.

[3] Eric D. Kolaczyk. Statistical Analysis of Network Data. Methods and Models. – Springer, 2009. – 386 p.

[4] John Kristoff. Botnets. – http://aharp.ittns.northwestern.edu.