

странственном расположении F_i считаем атаку успешной, если при работе сервиса S_M передатчики F_t и F_{t+1} были выбраны на i и $i+1$ этапе передачи, $t \in [1, n]$, $i \in [1, f]$:

$$p_A = \frac{2}{n - a_0} \cdot \frac{1}{n - 1 - a_1} + \frac{2}{n - 1 - a_1} \cdot \frac{1}{n - 2 - a_2} + \dots + \frac{2}{n - (f - 1) - a_{f-1}} \cdot \frac{1}{n - f - a_f}.$$

Эта формула легко распространяется на случай подконтрольных злоумышленнику участков между s доверенными серверами $F_t, F_{t+1}, \dots, F_{t+s}$. Так, при достаточно большом n и достаточно малых a_i и f , причем $n \gg f$ и $n \gg a_i$, оценка p_A представляется в виде

$$p_A = O\left(\frac{1}{n^2}\right).$$

При использовании мультиплексирования ($c > 1$) задача злоумышленника еще более усложняется. Варианты атак злоумышленника на разнесенный трафик рассматриваются в [3].

ЛИТЕРАТУРА

1. Ефимов В. И., Файзуллин Р. Т. Система мультиплексирования разнесенного TCP/IP трафика // Вестник Томского госуниверситета. Приложение. 2005. № 14. С. 115–118.
2. Avi Kak. Port Scanning, Vulnerability Scanning, and Packet Sniffing // Computer and Network Security. 2008. № 23. С. 29–38.
3. Ефимов В. И. Атака на систему разнесенного TCP/IP трафика на основе анализа корреляции потоков // Информационные технологии моделирования и управления. 2005. № 6(24). С. 859–863.

УДК 519.8

АППРОКСИМАЦИЯ СЕТЕВОГО ТРАФИКА МОДЕЛЮ АЛЬТЕРНИРУЮЩЕГО ПОТОКА СОБЫТИЙ

О. В. Ниссенбаум, И. Б. Пахомов

Трафик пользователя в сети, как правило, имеет переменную интенсивность и с той или иной степенью достоверности может быть представлен потоком событий с кусочно-постоянной стохастически изменяемой интенсивностью [1]. Рассмотрим трафик пользователя компьютерной сети с точки зрения соответствия модели асинхронного альтернирующего потока. Такой поток имеет два состояния, в первом из которых наблюдается пуассоновский поток с параметром λ , а во втором события потока отсутствуют. Интервалы, на которых поток находится в первом или втором состоянии, распределены по экспоненциальному закону с параметром α_1 и α_2 соответственно. Сравним полученные результаты с результатами для модели пуассоновского потока с интенсивностью λ_P .

Статистика трафика в виде временных моментов получения пакетов данных была собрана с компьютеров одной локальной сети. Данные сгруппированы по 1 мин, в каждой группе производилась оценка параметров. Использованы оценки параметров асинхронного альтернирующего потока, полученные в [2], и оценка моментов для интенсивности пуассоновского потока [3]. На рис. 1 черными штрихами обозначены моменты поступления пакетов данных за два отрезка времени по 2 мин. На верхней части рисунка (эксп. 1) трафик достаточно равномерен, на нижней (эксп. 2) выделяются периоды высокой интенсивности трафика и периоды «молчания». Оценки параметров

для эксп. 1: $\hat{\lambda} = 0,0458$, $\hat{\alpha}_1 = 0,0004$, $\hat{\alpha}_2 = 0,0011$, $\hat{\lambda}_P = 0,0332$. Для эксп. 2: $\hat{\lambda} = 0,0522$, $\hat{\alpha}_1 = 0,0002$, $\hat{\alpha}_2 = 0,0003$, $\hat{\lambda}_P = 0,0338$. Оценка $\hat{\lambda}_P$ для обоих случаев близка, с точки зрения простейшего потока эти случаи неразличимы. Оценки параметров альтернирующего потока отличаются существенно, эта модель — более гибкая.

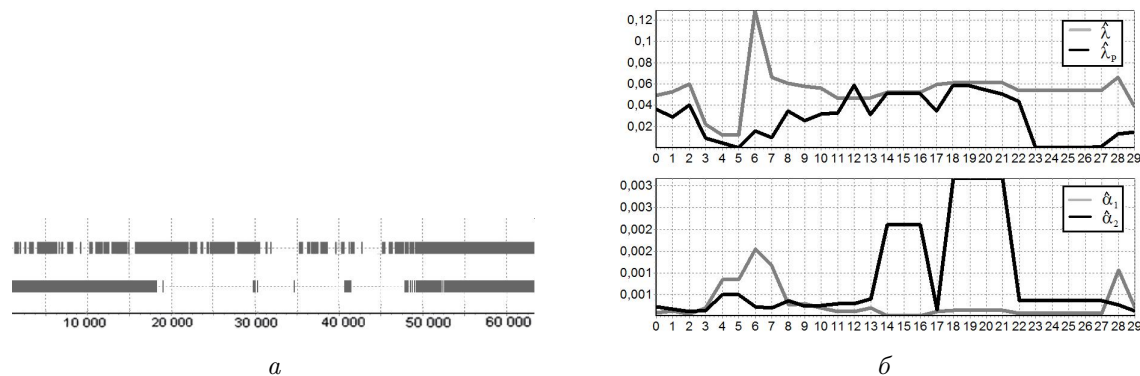


Рис. 1. Моменты поступления пакетов данных (2 эксперимента) (а). Динамика оценок (б)

На рис. 1,а представлена динамика оценок параметров трафика пользователя, работавшего с сетевыми сервисами и посещавшего сайты, в течение часа. Средние оценок, представленных на рис. 1,б, составили: $\bar{\lambda}=0,0534$, $\bar{\alpha}_1=0,0003$, $\bar{\alpha}_2=0,0009$, $\bar{\lambda}_P=0,0281$. Выборочные дисперсии оценок: $D_{\hat{\lambda}}=0,0003$, $D_{\hat{\alpha}_1}=0,00001$, $D_{\hat{\alpha}_2}=0,00001$, $D_{\hat{\lambda}_P}=0,0004$. Анализ результатов позволяет сделать следующие выводы: 1) стабильность оценок говорит о том, что модель альтернирующего потока более адекватно описывает трафик пользователя, чем модель пуассоновского; 2) резкое изменение оценок для альтернирующего потока позволяет использовать их для анализа сетевой активности.

ЛИТЕРАТУРА

1. Головкин Н. И., Каретник В. О., Танин В. Е., Сафонюк И. И. Исследование моделей систем массового обслуживания в информационных сетях // Сиб. жур. индустр. матем. 2008. Т. XI. № 2(34). С. 50–58.
2. Васильева Л. А., Горцев А. М. Оценивание параметров дважды стохастического потока событий в условиях его неполной наблюдаемости // Автоматика и телемеханика. 2002. № 3. С. 179–184.
3. Вентцель Е. С., Овчаров Л. А. Теория случайных процессов и ее инженерные приложения. М.: Высш. шк., 2000. 383 с.

УДК 004.412

К ОПРЕДЕЛЕНИЮ СТЕПЕНИ ИНТЕГРИРОВАННОСТИ ПРОГРАММНЫХ ПОДСИСТЕМ

Д. А. Стефанцов

При разработке защищённых систем обработки информации (СОИ) строится модель нарушителя в виде формального описания набора угроз и/или атак и формулируется политика безопасности (ПБ) в виде набора формальных требований [1]. С изменением модели нарушителя появляется необходимость внесения изменений в ПБ.