УДК 681.142.33:681.14
doi:10.15217/issn1684-8853.2018.3.61

МЕТОД И АЛГОРИТМЫ ОБНАРУЖЕНИЯ АНОМАЛИЙ В ТРАФИКЕ МУЛЬТИСЕРВИСНЫХ СЕТЕЙ СВЯЗИ, ОСНОВАННЫЕ НА НЕЧЕТКОМ ЛОГИЧЕСКОМ ВЫВОДЕ

С. А. Агеев[a], *канд. техн. наук, доцент, ведущий научный сотрудник, serg123_61@mail.ru*
И. Б. Саенко[a], *доктор техн. наук, профессор, ведущий научный сотрудник, ibsaen@comsec.spb.ru*
И. В. Котенко[a], *доктор техн. наук, профессор, заведующий лабораторией проблем компьютерной безопасности, ivkote@comsec.spb.ru*
[a]*Санкт-Петербургский институт информатики и автоматизации РАН, 14-я линия В. О., 39, Санкт-Петербург, 199178, РФ*

Введение: *важнейшим требованием, предъявляемым к системам обнаружения и предупреждения вредоносных вторжений в современные телекоммуникационные инфраструктуры, является способность обнаруживать аномалии и, соответственно, угрозы вторжения в реальном времени. Сложность этой задачи во многом обусловлена нестационарностью, неполнотой, неточностью априорных знаний о законах распределения, которым подчиняются потоки в трафике мультисервисных сетей связи, их многообразием, а также изменяющимся характером злонамеренных действий со стороны атакующего, которые приводят компьютерные системы в небезопасное состояние.* ***Цель:*** *повышение оперативности и достоверности процесса обнаружения аномалий в сетевом трафике в условиях неполноты и высокой разнородности анализируемой информации.* ***Результаты:*** *предложены гибридные адаптивные метод и алгоритмы обнаружения аномалий в трафике мультисервисных сетей связи, работающие в режиме реального времени. Гибридный метод объединяет механизм безыдентификационной адаптации к изменяющимся параметрам трафика и нечеткий логический вывод, используемый для регулирования параметров алгоритмов и анализа выходных данных. Адаптивные алгоритмы ориентированы на комбинированную реализацию процедур модифицированной стохастической аппроксимации и псевдоградиентного поиска. Проведенная экспериментальная оценка показала, что алгоритмы имеют функциональные характеристики, максимально близкие к потенциально достижимым.* ***Практическая значимость:*** *разработанные метод и алгоритмы могут быть реализованы на существующих аппаратно-программных платформах на основе технологии интеллектуальных агентов. Их совместное использование с уже существующими методами и алгоритмами обнаружения вторжений может существенно повысить эффективность систем защиты информации в мультисервисных сетях связи.*

Ключевые слова *— мультисервисная сеть связи, обнаружение аномалий, трафик, стохастическая аппроксимация, нечеткий логический вывод.*

Цитирование: Агеев С. А., Саенко И. Б., Котенко И. В. Метод и алгоритмы обнаружения аномалий в трафике мультисервисных сетей связи, основанные на нечетком логическом выводе // Информационно-управляющие системы. 2018. № 3. С. 61–68. doi:10.15217/issn1684-8853.2018.3.61
Citation: Ageev S. A., Saenko I. B., Kotenko I. V. Method and Algorithms of Anomaly Detection in Multiservice Network Traffic based on Fuzzy Logical Inference. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 3, pp. 61–68 (In Russian). doi:10.15217/issn1684-8853.2018.3.61

Введение

В настоящее время в различных информационных инфраструктурах (системах управления, мобильных системах, на транспорте, в энергетике, экономике и т. д.) успешно внедряются технологии высокоскоростных телекоммуникаций и сетей нового поколения [1, 2]. Достижения в развитии этих технологий привели к концепции мультисервисной сети связи (МСС), ядром которой являются опорные IP-сети, интегрирующие услуги передачи речи, данных и мультимедиа и реализующие принцип конвергенции услуг электросвязи [3, 4].

Множество основных сервисов, предоставляемых пользователям с помощью МСС, хорошо известно. Однако появление большого количества дополнительных сервисов у МСС делает достаточно острой проблему обеспечения ее информационной безопасности. Серьезность этой проблемы возрастает по следующим причинам: 1) из-за реализации процедур динамического изменения топологии МСС; 2) из-за возможного добавления или исключения из сети различного, априори неопределенного, числа абонентов; 3) в связи с динамическим изменением пространственного расположения абонентов; 4) из-за взаимодействия и сопряжения МСС друг с другом и т. д. Оперативность реагирования системы управления МСС на внешние и внутренние деструктивные воздействия приобретает особое значение для безопасности сети. Поэтому отсутствие аномалий в трафике сети является одним из критериев безопасного функционирования МСС.

При этом считается, что нормальный трафик соответствует политике безопасности в сети.

Трафик в МСС является достаточно разнообразным [2]. Он состоит, в том числе, из следующих компонентов: 1) мультимедийного трафика, который очень чувствителен к задержкам; 2) трафика передачи данных; 3) трафика передачи сигнальной информации; 4) трафика электронной почты. При этом заданные требования к качеству сервисов должны выполняться полностью. Однако существуют объективные трудности в построении системы управления МСС и в защите сетевой и абонентской информации. Эти трудности вызваны сложностью структуры МСС, разнородностью сети, необходимостью анализа большого количества различных сетевых и информационных параметров. Поэтому оперативное обнаружение аномалий сетевого трафика является одной из ключевых задач управления МСС и представляет собой актуальную научную проблему.

В настоящей статье рассматривается новый подход к обнаружению аномалий трафика в МСС, основанный на применении нечеткого логического вывода. При этом правила такого вывода используются совместно с модифицированными безыдентификационными алгоритмами.

Основной теоретический вклад работы заключается в следующем. Во-первых, обоснована модель мультисервисного трафика. Во-вторых, предложены методы и алгоритмы обнаружения аномалий трафика в МСС, основанные на применении нечеткого логического вывода. Наконец, экспериментально подтверждено, что предложенные алгоритмы обладают практически максимально возможным быстродействием.

Состояние исследований

Основные архитектурные решения, связанные с построением МСС, отражены во многих работах, например [1–4]. В них подчеркивается, что важная особенность построения МСС заключается в сильной сегментации топологии сети и в наличии нескольких точек сопряжения МСС с другими сетями. В результате общий трафик МСС уже нельзя контролировать из одной точки сети.

Для контроля трафика сетей, подобных МСС, в работах [4, 5] предлагается применять технологию интеллектуальных агентов. Интеллектуальные агенты выполняют сбор данных о трафике сети, предварительную обработку этих данных и передачу данных в центральные устройства системы управления. Таким образом, интеллектуальные агенты самостоятельно вырабатывают и реализуют часть управляющих решений.

Отмечается высокая важность задачи обеспечения функционирования систем обнаружения аномалий трафика в режиме времени, близком к реальному [6]. Автор предлагает использовать смешанную централизованно-децентрализованную структуру для построения системы управления МСС. Такая структура позволяет значительно повысить оперативность принятия решений по противодействию деструктивным воздействиям на сеть, а также снизить служебный трафик управления.

Идея использования интеллектуальных агентов для контроля трафика МСС получила дальнейшее развитие в работе [7]. Там утверждается, что для реализации в МСС технологии интеллектуальных агентов необходимо разрабатывать и применять алгоритмы обнаружения аномалий мультисервисного трафика, которые являются простыми в реализации и устойчивыми к изменению параметров трафика. При этом данные алгоритмы должны функционировать в режиме времени, близком к реальному. Однако алгоритмы, предложенные в этой работе, не учитывали нечеткие факторы.

Таким образом, решения по алгоритмам обнаружения аномалий сетевого трафика, представленные в известных работах, не отвечают требованиям МСС. Это в основном связано с необходимостью обработки в этих алгоритмах нечеткой информации. В то же время известен ряд работ [8–17], в которых сделаны отдельные попытки применения методов обработки нечетких знаний для моделирования и оценки сетевого трафика. Однако непосредственное применение результатов, полученных в этих работах, для МСС является невозможным. Это объясняется тем, что статистические свойства трафика в МСС сильно отличаются как для различных условий эксплуатации, так и для различных приложений в МСС.

Известны другие подходы к обнаружению аномального трафика в сети, например, использующие непараметрические кумулятивные суммы [18], максимальную энтропийную оценку [19], историю изменений сетевого трафика [20], временные ряды от базы данных управления [21]. Однако эти подходы не могут быть отнесены к методам и алгоритмам, которые обеспечивают функционирование сети с данным качеством в режиме реального времени и могут быть достаточно просто реализованы. В нашей статье мы намереваемся устранить этот недостаток.

Модель мультисервисного трафика

Для разработки методов обнаружения аномалий в трафике МСС необходимо прежде всего сформировать модель мультисервисного трафика.

Модель мультисервисного трафика в общем виде представляет собой объединение множе-

ства различных стохастических процессов (СП). Поэтому предлагаемый подход к формированию модели мультисервисного трафика основан на учете следующих факторов: законов распределения СП; стационарности СП; самоподобия СП; характеристик, выбранных для анализа СП.

Отмечается [8, 9], что трафик для различных приложений в МСС может быть аппроксимирован с помощью многих вероятностных распределений, основными из которых являются распределения Пуассона, Парето, Вейбулла, логнормальное и экспоненциальное. Для моделирования различных типов трафика применяются различные законы распределения. Например, если моделируемый трафик является «Аудио» или «Видео», то тогда он наделяется эффектом самоподобия, и для его моделирования применяется распределение Парето. Если моделируемый трафик сформирован протоколами SMTP/TCP, то тогда применяются распределение Пуассона или экспоненциальное распределение. Полный перечень законов распределения трафика в МСС и их распределение по уровням модели ISO/OSI можно найти в статье [22].

Стационарность или нестационарность СП также является важным фактором. Проще всего решать задачу обнаружения аномалий в трафике, если он является стационарным. Однако во многих работах, например в [8, 9], отмечается, что трафик в МСС является нестационарным по своей природе. Это существенно осложняет обнаружение аномалий в трафике, так как аномалии могут восприниматься как нормальное поведение трафика.

Анализ трафика может вестись с помощью различных характеристик случайного процесса. Основными такими характеристиками являются максимальное, минимальное и среднее значение интенсивности процесса, среднее квадратическое отклонение и другие. Ниже в работе будет рассматриваться среднее значение интенсивности процесса, которое рассчитывается по формуле

$$S_{mid} = \frac{1}{N}\sum_{i=1}^{N} S_i, \qquad (1)$$

где N — размер выборки; S_i — элемент i в выборке.

Выражения для расчета остальных характеристик стохастических процессов приведены в работе [22].

Метод и алгоритмы обнаружения аномалий трафика

К разработанным алгоритмам обнаружения аномалий в трафике МСС предъявляются следующие требования: функционирование в режиме реального или близкого к реальному времени; поддержание заданного качества сервиса; простота реализации. Алгоритмы относятся к классу гибридных адаптивных алгоритмов идентификации параметров трафика. Они применяются как для стационарных, так и для нестационарных трафиков. Трафики моделируются посредством СП. Каждый СП относится к соответствующему классу, определяемому законом распределения СП.

Сущность гибридного метода обнаружения аномалий в трафике МСС состоит в том, что, с одной стороны, используются алгоритмы безыдентификационной адаптации к изменяющимся параметрам СП. С другой стороны, для настройки параметров алгоритмов и принятия решений используется нечеткий логический вывод. Применение такого гибридного подхода вызвано необходимостью оценки как текущих точечных, так и интегральных параметров трафика. Оценка интегральных параметров трафика производится в скользящем окне. Оценка текущих точечных параметров выполняется от точки к точке одновременно с процедурой интегральной оценки. При этом оценки, полученные в скользящем окне, используются как начальные значения для безыдентификационной процедуры. Для проведения этой процедуры используются два алгоритма, отличающиеся своими возможностями по аппроксимации СП. Комбинация таких подходов позволяет как оценивать интегральные свойства СП, так и отслеживать динамику его поведения. Применение нечеткого логического вывода позволяет строить параметрические оценки параметров алгоритма по малому числу наблюдений. В этом случае становится возможным делать нечеткие выводы относительно аномалий трафика.

Пусть СП задан в дискретных значениях времени $t_i = i$, $i = 1, 2, \ldots$. Первый алгоритм является алгоритмом *модифицированной стохастической аппроксимации* (МСА) [11]

$$S_{i+1} = S_{i-1} + \mu_i (S_i - S_{i-1}), \qquad (2)$$

где S_i — среднее значение интенсивности трафика в момент времени i; μ_i — параметр алгоритма на шаге i.

Второй алгоритм используется в случае, когда плотность вероятности значений СП является симметричной. Он основан на применении *псевдоградиентных процедур* (ПГП) вида

$$S_{i+1} = S_{i-1} + \mu_i \mathrm{sign}\,(S_i - S_{i-1}). \qquad (3)$$

Такой выбор первого и второго алгоритмов обеспечивает оценку динамических свойств СП. Из-за того, что алгоритмы МСА и ПГП относятся к классу безыдентификационных алгоритмов, время анализа трафика и обнаружения аномалий существенно сокращается.

В качестве целевой функции предлагается квадратичная функция вида

$$M\{(S_i - S_{i-1})^2\}, \quad (4)$$

где $M\{*\}$ — функция вычисления математического ожидания.

Параметр μ_i для МСА и ПГП должен удовлетворять следующим условиям:

$$0 < \mu_i < 1,\ \mu_i = \text{const}. \quad (5)$$

Особенностью алгоритмов МСА и ПГП является тот факт, что необходимо подстраивать значение параметра μ_i для различных оцениваемых СП и их статистических свойств. Предлагается процедуру подстройки этих алгоритмов осуществлять на основе метода нечеткого вывода Мамдани [5, 11], согласно которому идентификация параметров алгоритмов МСА и ПГП производится с помощью правил, имеющих в общем случае следующий вид:

$$\textbf{IF} < S_i = A > \textbf{AND} < \sigma = B > \textbf{AND} < \rho = D > \textbf{THEN}\ \mu = R, \quad (6)$$

где A, B и D — нечеткие пороговые значения, определяемые в ходе обучения системы нечеткого логического вывода.

Идентификация аномалий в трафике МСС осуществляется на основе нечеткого логического вывода следующего вида:

$$\textbf{IF} < S_i = A > \textbf{AND} < \textbf{A}\ \text{соответствует политике безопасности} > \textbf{THEN}\ R, \quad (7)$$

где R — значение лингвистической переменной, оценивающей наличие аномалий.

Для выполнения процедуры идентификации аномалий необходимо предварительно проводить обучение системы нечеткого логического вывода по экспериментальным данным. Экспериментальные данные формируются заранее.

При выборе размера скользящего окна необходимо найти разумный компромисс между скоростью изменения значений СП, размером окна и репрезентативностью выборки значений СП. Этот компромисс необходим для устранения эффекта излишнего сглаживания значений СП.

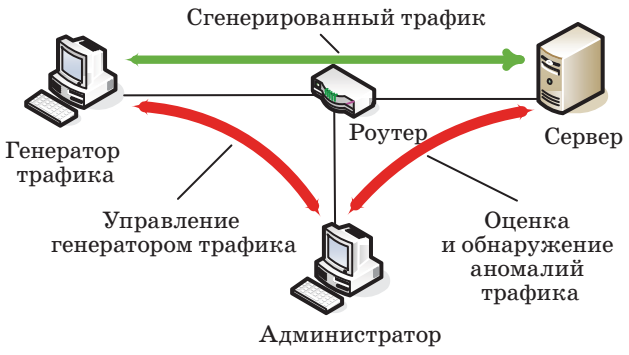
Вывод о характере поведения трафика в МСС также осуществляется на основе метода Мамдани.

Анализ экспериментальных данных

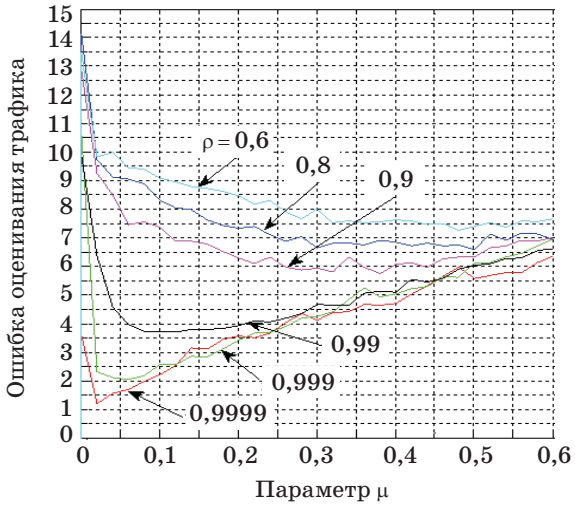
Для экспериментальной проверки предложенных методов и алгоритмов был использован инструментальный стенд (рис. 1). Стенд состоял из сервера и двух рабочих станций, объединенных в сеть с помощью маршрутизатора. Одна рабочая станция являлась генератором трафика. На второй станции работал администратор сети. Администратор сети управлял генератором. Генератор формировал трафик с заданным законом распределения. При этом аномалии внедрялись в трафик случайным образом в соответствии с выбранным типом компьютерной атаки. Трафик проходил через маршрутизатор на сервер. Задача администратора заключалась в оценке и определении аномалий трафика.

Генератор формировал стационарные и нестационарные трафики с распределениями Пуассона и Парето. Эти распределения являются наиболее характерными для МСС. Для генерации аномалий использовались атаки типа DoS, приводящие к перегрузке канала связи. Нестационарные процессы моделировались как мультипликативные СП с детерминированными и случайными модулирующими функциями. Случайные модулирующие функции представляли собой случайные процессы авторегрессии первого порядка с различными коэффициентами корреляции. Адаптация к параметрам пуассоновского СП осуществлялась с помощью алгоритма МСА. Для СП с законом Парето применялся алгоритм ПГП.

Настройка параметров алгоритмов адаптации осуществлялась с помощью правил, имеющих вид (6). Нечеткие константы A, B и D для этих правил определялись предварительно по результатам обучения. Для этой цели использовались экспериментальные результаты, представленные на рис. 2, на которых показаны зависимости среднеквадратического значения ошибки оценивания интенсивности трафика нестационарного СП от значения коэффициента шага алгоритма МСА при различных значениях коэффициента корреляции, модулирующего СП для пуассоновских трафиков. Случайный процесс имел среднее значение $a_0 = 100$ и среднеквадратическое отклонение $\sigma = 10$. Коэффициент корреляции тренда ρ



■ ***Рис. 1.*** Структура инструментального стенда
■ ***Fig. 1.*** Testbed structure



■ ***Рис. 2.*** Зависимость ошибки оценивания трафика от величины параметра μ

■ ***Fig. 2.*** Dependence of the traffic assessment error on the parameter μ

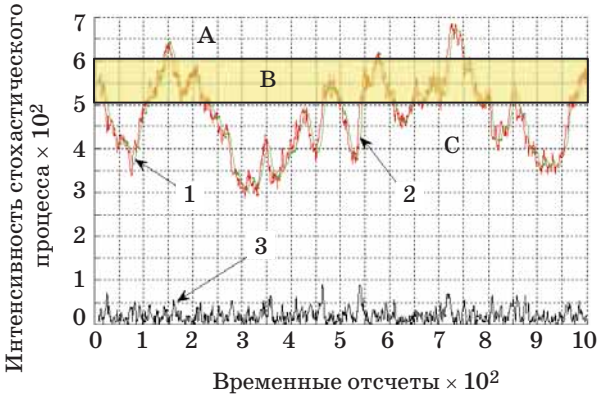
для различных зависимостей изменялся в диапазоне от 0,6 до 0,9999. Видно, что при малых значениях μ погрешности оценки трафика сильно отличаются друг от друга в зависимости от значения ρ.

При больших значениях μ эти погрешности принимают приблизительно равные значения.

По данным, показанным на рис. 2, формируются правила настройки параметров МСА. Например, при $S_i \approx 100$, $\sigma \approx 10$ и $\rho \approx 0{,}9999$ параметр алгоритма μ приблизительно равен 0,025. Для $\rho \approx 0{,}99$ параметр μ будет иметь значение, приблизительно равное 0,12. Параметры σ и ρ оцениваются в скользящем окне.

Пример численного моделирования нестационарного пуассоновского СП представлен на рис. 3. Коэффициент корреляции процесса изменялся в экспериментах от 0,9 до 0,99999. СП имел следующие параметры: начальное значение среднего значения тренда $m_0 = 500$, коэффициент корреляции тренда $\rho = 0{,}99$, размер скользящего окна $r = 10$, параметр $\mu = 0{,}05$, среднеквадратическое отклонение тренда $\sigma = 100$. Как видно из рисунка, предложенный алгоритм работает практически без задержек и имеет достаточно высокую точность оценивания.

С определением аномалий связаны три зоны (см. рис. 3). Зона **A** определяет, что риск наличия аномалий есть, и уровень риска является неприемлемым. Зона **B** показывает, что риск наличия аномалий есть, и уровень риска является приемлемым. В трафике, расположенном в зоне **C**, аномалий нет. Границы зон **A**, **B** и **C** определяются на этапе предварительной настройки базы знаний машины нечеткого вывода в соответствии



■ ***Рис. 3.*** Оценка нестационарного тренда с распределением Пуассона: *1* — истинное значение тренда; *2* — оценка тренда; *3* — ошибка оценивания тренда

■ ***Fig. 3.*** Assessment of a non-stationary trend with the Poisson distribution: *1* — the true value of a trend; *2* — trend assessment; *3* — estimation error of a trend

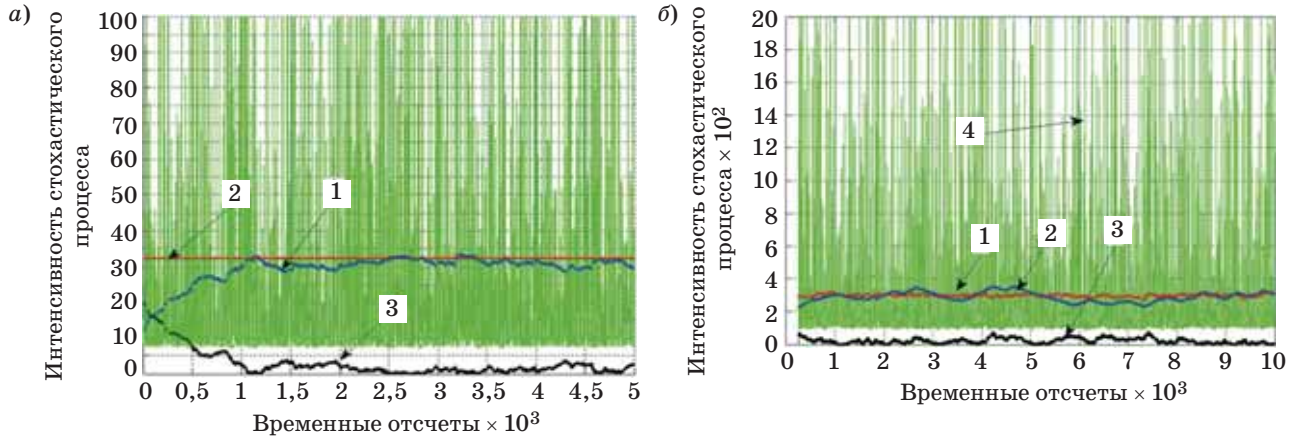
■ ***Таблица 1.*** Параметры стационарного и нестационарного процесса

■ ***Table 1.*** Parameters of stationary and nonstationary process

Параметр	Стационарный процесс	Нестационарный процесс
Параметр Херста H	0,85	0,75
Среднее значение СП	32,5	250
Параметр распределения СП	1,3	—
Параметр алгоритма МСА μ	0,004	0,13
Относительная погрешность оценивания Δ, %	≤6,2	≤9,1

с принятыми правилами политики безопасности. Значения оценок тренда на границах зон **A**, **B** и **C** используются для построения правил Мамдани по формуле (7). Например, правило для вывода об отсутствии аномалий имеет следующий вид: **IF** $<S_i \in$ *Зона C* $>$ **THEN** *Аномалий трафика нет*.

Результаты оценки параметров (табл. 1) самоподобных трафиков с распределением Парето представлены на рис. 4, *а* и *б*.



■ ***Рис. 4.*** Оценка стационарного (*а*) и нестационарного (*б*) тренда самоподобного трафика с распределением Парето: *1* — оценка тренда; *2* — истинное значение тренда; *3* — ошибка оценивания тренда; *4* — значения СП

■ ***Fig. 4.*** Assessment of a stationary (*а*) and non-stationary (*б*) trend of a self-similar traffic with the Pareto distribution: *1* — trend assessment; *2* — the true value of a trend; *3* — estimation error of a trend; *4* — stochastic process values

■ ***Таблица 2.*** Экспериментальные результаты оценки алгоритмов

■ ***Table 2.*** Experimental results of the algorithms assessment

Распределение	Коэффициент корреляции ρ	Средняя относительная погрешность оценки, %	Время обнаружения, временные отсчеты
Парето (H = 0,75)	0,99	12,0	80
	0,999	10,0	65
	0,9999	8,0	50
Пуассона	0,9	8,6	34
	0,99	7,6	27
	0,999	6,4	20
	0,9999	5,3	15

Итоговые результаты оценки разработанных алгоритмов определения аномалий в трафике МСС для рассмотренных выше распределений приведены в табл. 2.

Из этой таблицы видно, что величина относительной погрешности алгоритмов не превышает 12 % от истинного значения тренда. Этот результат следует считать достаточно хорошим, учитывая, что алгоритмы работают в реальном времени, так как полученные для времени обнаружения значения лежат в диапазоне от 15 до 80 временных отсчетов. Таким образом, разработанные алгоритмы обнаружения аномалий в трафике МСС полностью удовлетворяют требованиям оперативности и точности.

Заключение

В настоящей работе предложен гибридный метод обнаружения аномалий в трафике МСС, использующий алгоритмы безыдентификационной адаптации и нечеткого вывода Мамдани.

Ключевой особенностью мультисервисного трафика как объекта оценивания на существование аномалий является наличие в нем стохастических процессов, подчиненных различным законам распределения. Для экспериментальной оценки предложенных метода и алгоритмов были выбраны законы распределения Пуассона и Парето, определяющие предельные случаи регулярности трафика.

Экспериментальная оценка предложенных метода и алгоритмов показала, что они позволяют оценивать тренды указанных стохастических процессов в реальном времени, с высокой точностью и с сохранением качества обслуживания.

Дальнейшие направления исследований связаны с разработкой методов обучения предложенных алгоритмов с использованием тестовых трафиков.

Работа выполнена при частичной финансовой поддержке РФФИ (проекты 16-29-09482, 18-07-01369 и 18-07-01488), бюджетной темы № АААА-А16-116033110102-5, а также при государственной финансовой поддержке ведущих университетов Российской Федерации (субсидия 074-U01).

Литература

1. **Гольдштейн А. Б., Гольдштейн Б. С.** SOFTSWITCH. — СПб.: БХВ, 2006. — 368 с.
2. **Kanáliková A.** Services in NGN — Next Generation Networks // Journal of Information, Control and Management Systems. 2005. Vol. 3. N 2. P. 97–102.
3. **Агеев С. А., Шерстюк Ю. М., Саенко И. Б., Полубелова О. В.** Концептуальные основы автоматизации управления защищенными мультисервисными сетями // Проблемы информационной безопасности. Компьютерные системы. 2011. № 3. С. 30–39.
4. **Агеев С. А., Бушуев А. С., Егоров Ю. П., Саенко И. Б.** Концепция автоматизации управления информационной безопасностью в защищенных мультисервисных сетях специального назначения // Автоматизация процессов управления. 2011. № 1. С. 50–57.
5. **Gorodetski V., Kotenko I., Karsaev O.** Multi-Agent Technologies for Computer Network Security: Attack Simulation, Intrusion Detection and Intrusion Detection Learning // International Journal of Computer Systems Science & Engineering. 2003. N 4. P. 191–200.
6. **Paxson V.** A System for Detecting Network Intruders in Real-Time // Proc. of the 7th USENIX Security Symp. 1998. P. 2435–2463.
7. **Paxson V.** A System for Detecting Network Intruders in Real-Time // Computers Networks. 1999. N 31. P. 2435–2463.
8. **Laskin N., Lambadaries I., Harmatzis F. C., Devetsikiotis M.** Fractional Levy Motion and its Application to Network Traffic Modeling // Elsevier Comp. Network. 2002. Vol. 40. P. 363–375.
9. **Шелухин О. И., Осин А. В., Смольский С. М.** Самоподобие и фракталы. Телекоммуникационные приложения. — М.: Физматлит, 2008. — 368 с.
10. **Ageev S., Vasil'ev K.** Adaptive Algorithms for Decorrelation to Image Processing // Pattern Recognition and Image Analysis. Advances in Mathematical Theory and Application. 2001. Vol. 11. N 1. P. 131–134.
11. **Takagi T., Sugeno M.** Fuzzy Identification of Systems and its Applications to Modeling and Control // IEEE Trans. on System, Man and Cybernetics. 1985. Vol. 15. N 1. P. 11–132.
12. **Derrac J., García S., Herrera F.** Fuzzy Nearest Neighbor: Taxonomy, Experimental Analysis and Prospects // Inf. Sci. 2014. Vol. 260. P. 98–119.
13. **Li X., Lara-Rosano F.** Adaptive Fuzzy Petri Nets for Dynamic Knowledge Representation and Inference // Expert System Applications. 2000. Vol. 19. N 3. P. 235–241.
14. **Xing-zhu W.** Network Information Security Situation Assessment based on Bayesian Network // International Journal of Security and its Applications. 2016. Vol. 10. N 5. P. 129–138.
15. **Papageorgiou E. I.** Fuzzy Cognitive Maps for Applied Sciences and Engineering: from Fundamentals to Extensions and Learning Algorithms. — Springer-Verlag Berlin Heidelberg, 2014. — 395 p. doi:10.1007/978-3-642-39739-4
16. **Astanin S. V., Zhukovskaya N. K.** Business Processes Control via Modeling by Fuzzy Situational Networks // Automation and Remote Control. 2014. Vol. 75. N 3. P. 570–579.
17. **Nikolaev A. B., Sapego Yu. S., Jakubovich A. N., Berner L. I., Stroganov V. Yu.** Fuzzy Algorithm for the Detection of Incidents in the Transport System // International Journal of Environmental & Science Education. 2016. Vol. 11. N 16. P. 9039–9059.
18. **Wang H., Zhang D., Shin K. G.** Detecting SYN Flooding Attacks // Proc. of IEEE INFOCOM. 2002. 10 p.
19. **Staniford S., Hoagland J., McAlerney J. M.** Practical Automated Detection of Stealthy Portscans // J. Comput. Secur. 2002. Vol. 10. N 1–2. P. 105–136.
20. **Brutlag J. D.** Aberrant Behavior Detection in Time Series for Network Service Monitoring // Proc. of the 14th Systems Administration Conf. 2000. P. 139–146.
21. **Thottan M., Ji C.** Anomaly Detection in IP Networks // IEEE Trans. Signal Processing. 2003. Vol. 51. N 8. P. 2191–2204.
22. **Котенко И. В., Саенко И. Б., Агеев С. А., Копчак Я. М.** Обнаружение аномального трафика в сетях Интернета вещей на основе нечеткого логического вывода // XVIII Междунар. конф. по мягким вычислениям и измерениям (SCM'2015): сб. докл. 2015. Т. 1. С. 9–14.

UDC 681.142.33:681.14
doi:10.15217/issn1684-8853.2018.3.61

Method and Algorithms of Anomaly Detection in Multiservice Network Traffic based on Fuzzy Logical Inference

Ageev S. A.[a], PhD, Tech., Associate Professor, Leading Researcher, serg123_61@mail.ru
Saenko I. B.[a], Dr. Sc., Tech., Professor, Leading Researcher, ibsaen@comsec.spb.ru
Kotenko I. V.[a], Dr. Sc., Tech., Professor, Head of Laboratory of Computer Security Problems, ivkote@comsec.spb.ru
[a]Saint-Petersburg Institute for Informatics and Automation of the RAS, 39, 14 Line, V. O., 199178, Saint-Petersburg, Russian Federation

Introduction: The major requirement imposed to the systems of detection and prevention of malicious invasions into modern telecommunication infrastructures is the ability to find anomalies and invasion threats in real time. The complexity of this problem is in many respects caused by the incompleteness, discrepancy and diversity of the a priori knowledge about the distribution laws peculiar

to the traffic of multiservice communication networks, as well as by the changing nature of malicious actions which make computer systems unsafe. **Purpose:** Increasing the speed and reliability of network traffic anomaly detection when the analyzed information is incomplete and highly heterogeneous. **Results:** A hybrid method and adaptive algorithms have been proposed for real-time anomaly detection in multiservice communication network traffic. The hybrid method unites the mechanism of non-identificational adaptation to the changing traffic parameters with the fuzzy logical inference used for regulating the algorithm parameters and for analyzing the output data. The adaptive algorithms are focused on combined implementation of modified stochastic approximation and pseudo-gradient search procedures. An experimental assessment has shown that the functional characteristics of the algorithms are close to the potentially achievable ones. **Practical relevance:** The developed method and algorithms can be implemented on available hardware-software platforms on the basis of intellectual agent technology. Sharing them with already existing methods and algorithms of invasion detection can considerably increase the efficiency of information security systems in multiservice communication networks.

Keywords — Multiservice Communication Network, Anomaly Detection, Traffic, Stochastic Approximation, Fuzzy Logical Inference.

Citation: Ageev S. A., Saenko I. B., Kotenko I. V. Method and Algorithms of Anomaly Detection in Multiservice Network Traffic based on Fuzzy Logical Inference. *Informatsionno-upravliaiushchie sistemy* [Information and Control Systems], 2018, no. 3, pp. 61–68 (In Russian). doi:10.15217/issn1684-8853.2018.3.61

References

1. Gol'dshtejn A. B., Gol'dshtejn B. S. *SOFTSWITCH* [SOFTSWITCH]. Saint-Petersburg, BkHV Publ., 2006. 368 p. (In Russian).
2. Kanáliková A. Services in NGN — Next Generation Networks. *Journal of Information, Control and Management Systems*, 2005, vol. 3, no. 2, pp. 97–102.
3. Ageev S. A., Sherstjuk Y. M., Saenko I. B., Polubelova O. V. Conceptual Basics of Protected Multiservice Networks' Control Automation. *Problemy informacionnoj bezopasnosti. Komp'juternye sistemy* [Information Security Problems. Computer Systems], 2011, no. 3, pp. 30–39 (In Russian).
4. Ageev S. A., Bushuev A. S., Egorov Y. P., Saenko I. B. The Concept of Information Security Control Automation in the Protected Multiservice Networks of a Special Purpose. *Avtomatizacija processov upravlenija*, 2011, no. 1, pp. 50–57 (In Russian).
5. Gorodetski V., Kotenko I., Karsaev O. Multi-agent Technologies for Computer Network Security: Attack Simulation, Intrusion Detection and Intrusion Detection Learning. *International Journal of Computer Systems Science & Engineering*, 2003, no. 4, pp. 191–200.
6. Paxson V. A System for Detecting Network Intruders in Real-Time. *Proc. of the 7th USENIX Security Symp.*, 1998, pp. 2435–2463.
7. Paxson V. A System for Detecting Network Intruders in Real-Time. *Computers Networks*, 1999, no. 31, pp. 2435–2463.
8. Laskin N., Lambadaries I., Harmatzis F. C., Devetsikiotis M. Fractional Levy Motion and its Application to Network Traffic Modeling. *Elsevier Comp. Network*, 2002, vol. 40, pp. 363–375.
9. Sheluhin O. I., Osin A. V., Smol'skij S. M. *Samopodobie i fraktaly. Telekommunikacionnye prilozheniya* [Self-Similarity and Fractals. Telecommunication Applications]. Moskow, Fizmatlit Publ., 2008. 368 p. (In Russian).
10. Ageev S., Vasil'ev K. Adaptive Algorithms for Decorrelation to Image Processing. *Pattern Recognition and Image Analysis. Advances in Mathematical Theory and Application*, 2001, vol. 11, no. 1, pp. 131–134.
11. Takagi T., Sugeno M. Fuzzy Identification of Systems and its Applications to Modeling and Control. *IEEE Trans. on System, Man and Cybernetics*, 1985, vol. 15, no. 1, pp. 11–132.
12. Derrac J., García S., Herrera F. Fuzzy Nearest Neighbor: Taxonomy, Experimental Analysis and Prospects. *Inf. Sci.*, 2014, vol. 260, pp. 98–119.
13. Li X., Lara-Rosano F. Adaptive Fuzzy Petri Nets for Dynamic Knowledge Representation and Inference. *Expert System Applications*, 2000, vol. 19, no. 3, pp. 235–241.
14. Xing-zhu W. Network Information Security Situation Assessment based on Bayesian Network. *International Journal of Security and its Applications*, 2016, vol. 10, no. 5, pp. 129–138.
15. Papageorgiou E. I. Fuzzy Cognitive Maps for Applied Sciences and Engineering: from Fundamentals to Extensions and Learning Algorithms. Springer-Verlag Berlin Heidelberg, 2014. 395 p. doi:10.1007/978-3-642-39739-4
16. Astanin S. V., Zhukovskaya N. K. Business Processes Control via Modeling by Fuzzy Situational Networks. *Automation and Remote Control*, 2014, vol. 75, no. 3, pp. 570–579.
17. Nikolaev A. B., Sapego Yu. S., Jakubovich A. N., Berner L. I., Stroganov V. Yu. Fuzzy Algorithm for the Detection of Incidents in the Transport System. *International Journal of Environmental & Science Education*, 2016, vol. 11, no. 16, pp. 9039–9059.
18. Wang H., Zhang D., Shin K. G. Detecting SYN Flooding Attacks. *Proc. of IEEE INFOCOM*, 2002, 10 p.
19. Staniford S., Hoagland J., McAlerney J. M. Practical Automated Detection of Stealthy Portscans. *J. Comput. Secur.*, 2002, vol. 10, no. 1–2, pp. 105–136.
20. Brutlag J. D. Aberrant Behavior Detection in Time Series for Network Service Monitoring. *Proc. of the 14th Systems Administration Conf.*, 2000, pp. 139–146.
21. Thottan M., Ji C. Anomaly Detection in IP Networks. *IEEE Trans. Signal Processing*, 2003, vol. 51, no. 8, pp. 2191–2204.
22. Kotenko I. V., Saenko I. B., Ageev S. A., Kopchak Y. M. Abnormal Traffic Detection in Networks of the Internet of Things based on Fuzzy Logical Inference. *Sbornik dokladov XVIII Mezhdunarodnoj konferentsii po myagkim vychisleniyam i izmereniyam (SCM'2015)* [Proc. of the XVIII Int. Conf. on Soft Computing and Measurements (SCM'2015)], 2015, vol. 1, pp. 9–14 (In Russian).