ОПТИМИЗАЦИЯ ВЫЯВЛЕНИЯ АНОМАЛИЙ ОБЛАЧНЫХ СЕРВИСОВ

Шишкин Ю.Е. Email: Shishkin1134@scientifictext.ru

Шишкин Юрий Евгеньевич – аспирант,
кафедра информационных технологий и компьютерных систем,
Севастопольский государственный университет, г. Севастополь

Аннотация: *в статье анализируется математическая модель, предназначенная для выявления аномального поведения сетевого трафика в сложных вычислительных системах. Метод решения основан на применении гибких решающих правил, использующих систему статистических метрик на основе эффекта гетероскедастичности. Выдвинутые гипотезы экспериментально подтверждены с использованием разработанной программной дискретно-событийной имитационной модели. Область применения модели – оптимизация процесса мониторинга в облачных сервисах и выявления несанкционированных атакующих воздействий.*

Ключевые слова: *Большие Данные, оптимизация мониторинга, система поддержки принятия решений, облачные сервисы, имитационное моделирование, аномалии сетевого трафика, визуализация.*

OPTIMIZATION OF CLOUD SERVICES ANOMALIES DETECTION

Shishkin Yu.E.

Shishkin Yurij Evgenevich – Postgraduate,
INFORMATION TECHNOLOGY AND COMPUTER SYSTEMS DEPARTMENT,
SEVASTOPOL STATE UNIVERSITY, SEVASTOPOL

Abstract: *the article analyzes a mathematical model designed to detect abnormal behavior of network traffic in complex computer systems. The method of solution is based on the use of flexible decision rules using a system of statistical metrics based on the effect of heteroscedasticity. Experiments using the developed discrete-event simulation model software have confirmed the advanced hypothesis. The scope of the model is the optimization of the monitoring process in cloud services and the detection of unauthorized attacking influences.*

Keywords: *Big Data, monitoring optimization, decision support system, cloud services, simulation, network traffic anomalies, visualization.*

УДК 519.816:004.75

Введение

На сегодняшний день для решения задачи оптимального управления облачными сервисами требуется производить оперативное выявление аномального поведения сетевого трафика [1]. Понятие облачных сервисов подразумевает возможность мгновенного получения сетевых ресурсов по требованию, при этом оплата за выделенный ресурс происходит по факту использования [2-3]. Для осуществления оптимального управления любой сложной системой, к которой можно отнести и вычислительную систему, реализованную в виде облачных сервисов, необходимо обеспечить оперативную обратную связь объектом управления, которая реализуется системой мониторинга [4-5].

Решение поставленной задачи выполнено при следующих предположениях и ограничениях:

— модель исследуемой системы и имеет вид аддитивной функции [6-7]. Модель сетевого актора определяет его метрику в виде функционала, состоящего из функций принадлежности всех метрик в виде:

$$F(x)=\frac{1}{n}\sum_{i=1}^{n} f_i(x_i), \quad F(x)\in[0;1] \qquad (1)$$

где n – число метрик, x – множество параметров системы.

— задача может быть разрешена в классе метрик функции принадлежности [8-9]. Признаком аномального поведения трафика в сети являются независимые от источника метрики, функция принадлежности которых задана в виде:

$$f(x)=e^{\frac{-(m-x)^2}{2\sigma^2}}, \quad f(x)\in[0;1], \qquad (2)$$

где m – математическое ожидание, σ^2 – дисперсия.

Статистические признаки, которые зависят от источника сигнала, определяются в виде некоторой меры отклонения коэффициента утилизации вычислительной системы от ожидаемого значения после обслуживания актора [10-11]. Функциональная метрика, в таком случае, будет представима в виде фильтра, пороговое значение которого:

$$\left|(1-\alpha)-\frac{1}{n}\sum_{i=1}^{n}\theta(p-F(x))\right|=\min(p), \qquad (3)$$

где p – порог детектирования, θ – единичная функция, α – допустимая погрешность.

В силу отмеченных обстоятельств известные методы для решения задач мониторинга в облачных вычислительных средах не могут являться совершенным операционным средством, так как не обеспечивают требуемого качества контроля состояния сетевого трафика, в частности, с их помощью затруднительно отследить моменты изменения таких свойств трафика как интенсивность, дисперсность, нестационарность [12]. С этой целью мы используем понятие гетероскедастичности, которое широко используется в эконометрии. Термин гетероскедастичность понимается как предположение о том, что дисперсии случайных отклонений являются значимо неоднородными выделенных совокупностей наблюдений, что приводит к нарушению принципов корректного использования методов множественной регрессии [13].

Основными преимуществами предлагаемого метода оценки состояний сетевого трафика на основе эффекта гетероскедастичности являются:

— чувствительность к изменениям состояния трафика,

— малая вычислительная трудоемкость,

— адаптивность к внешним воздействиям.

В разработанной программной дискретно-событийной имитационной модели, реализующей исследуемую систему в виде системы массового обслуживания, применена система решающих правил, детерминировано определяющих поведение системы поддержки принятия решений по управлению облачным сервисом в зависимости от значений данных мониторинга [14-15]. Метрики эффективности взаимодействия сетевых акторов вычисляются на основе сравнения вектора фактических параметров объекта управления и его идеализированной математической моделью, в зависимости от допустимых погрешностей первого и второго рода происходит выбор порогового значения фильтра [16].

Экспериментально выявлено, что внедрение в систему управления облачными сервисами параметризованных функций оптимизации с ограничениями и метрики эффективности позволяет оптимизировать процесс выявления аномалий сетевого трафика в облачных сервисах.

Список литературы / References

1. *Шишкин Ю.Е.* Актуализация данных в системах мониторинга сложных объектов с использованием информационных метрик // Проблемы современной науки и образования, 2017. № 6 (88). С. 22-27. doi:10.20861/2304-2338-2017-88-001.
2. *Шишкин Ю.Е., Шишкин В.Е.* Повышение эффективности распределенных вычислений на основе использования имитационной модели // Academy, 2017. № 4 (19). С. 19-20.
3. *Пасынков М.А.* Комплексная система интеграции баз данных мониторинга физических параметров и позиционирования в акваториях // Научный журнал, 2017. № 2 (15). С. 29-31.
4. *Магжанова А.Т.* Применение облачных технологий для реализации решений интернета вещей // Современные инновации, 2016. № 7 (9). С. 30-34.
5. *Шишкин Ю.Е.* Оптимизация функционирования супермаркета на основе процедур эвристической диспетчеризации // Мир компьютерных технологий: материалы внутривузовской студенческой научно-технической конференции. Севастополь 2-5 апреля 2012 г. Севастополь: СевНТУ, 2012. С. 3.
6. *Шишкин Ю.Е.* Разработка инструментальных средств и математических моделей для оптимизации мониторинга // Наука, техника и образование, 2017. № 3 (33). С. 55-60. doi:10.20861/2312-8267-2017-33-002.
7. *Шишкин Ю.Е.* Использование широтно-импульсной модуляции на базе микроконтроллера pic12f629 для плавного включения галогенных ламп высокой мощности // Мир компьютерных технологий: материалы внутривузовской студенческой научно-технической конференции. Севастополь 2-5 апреля 2012 г. Севастополь: СевНТУ, 2012. С. 22.
8. *Шишкин Ю.Е.* Облачные сервисы в системах поддержки принятия решений // Научный журнал. 2017. № 1 (14). С. 19-20.
9. *Шишкин Ю.Е.* Адаптивная система построения пиксельных карт для управления движением автономных роботов // Мир компьютерных технологий: материалы внутривузовской студенческой научно-технической конференции. Севастополь 1-3 апреля 2013 г. Севастополь: СевНТУ, 2013. С. 17.
10. *Шишкин Ю.Е.* Оптимизация выявления и моделирования сетевых вирусных атак // Мир компьютерных технологий: материалы внутривузовской студенческой научно-технической конференции. Севастополь 1-3 апреля 2013 г. Севастополь: СевНТУ, 2013. С. 4.

11. *Неменко А.В., Никитин М.М.* Прогнозная оценка выносливости конструкционных материалов при циклическом нагружении // Фундаментальные и прикладные проблемы техники и технологии, 2015. Т. 1. № 5 (313). С. 11-23.
12. *Шишкин Ю.Е.* Анализ информационных процессов по технологии «Большие Данные» // Автоматизация: проблемы, идеи, решения: материалы международной научно-технической конференции. / под науч. ред. В.Я. Коппа. Севастополь 8-12 сентября 2014 г. Севастополь: СевНТУ, 2014. С. 157-159.
13. *Шишкин Ю.Е.* Построение системы управления компьютерной сетью с использованием Больших Данных // Мир компьютерных технологий: материалы внутривузовской студенческой научно-технической конференции. Севастополь 1-3 апреля 2014 г. Севастополь: СевНТУ, 2014. С. 14.
14. *Кодолов П.А.* Облачное хранилище данных // Наука, техника и образование, 2016. № 4 (22). С. 51-53.
15. *Шишкин Ю.Е.* Построение гибридной модели критической инфраструктуры // Мир компьютерных технологий: материалы внутривузовской студенческой научно-технической конференции. Севастополь 1-3 апреля 2015 г. Севастополь: СевГУ, 2015. С. 11.
16. *Шишкин Ю.Е.* Визуальный анализ Больших Данных с применением познавательных паттернов // Проблемы современной науки и образования, 2017. № 2 (84). С. 24-26.