УДК 004.042 DOI: 10.25045/jpit.v11.i1.11

Шыхалиев Р.Г.
Институт Информационных Технологий НАНА, Баку, Азербайджан
ramiz@science.az

ОБ ОДНОЙ МОДЕЛИ МОНИТОРИНГА КОМПЬЮТЕРНЫХ СЕТЕЙ В РЕАЛЬНОМ ВРЕМЕНИ

Поступила: 17.10.2019 Исправлена: 22.10.2019 Принята: 30.10.2019

Для обеспечения нормального и безопасного функционирования современных компьютерных сетей (КС) требуются надежные и эффективные модели мониторинга. Эти модели должны позволить анализировать большой объем потоков данных сетевых трафиков в режиме реального времени. Однако используемые сегодня традиционные подходы интеллектуального анализа данных не могут справиться с этой задачей. Для ее решения более подходящим является использование методов интеллектуального анализа потоков данных. В данной статье предложена модель мониторинга КС в реальном времени, в которой используются алгоритмы интеллектуального анализа потоков данных. Предложенная модель является многозадачной, то есть, в зависимости от целей мониторинга КС, для анализа потоков данных сетевых трафиков могут быть использованы соответствующие алгоритмы интеллектуального анализа потоков данных. Для этого используются такие алгоритмы, как алгоритмы кластеризации потоков данных, классификации потоков данных, анализа шаблонов и анализа временных рядов. Таким образом, предложенная модель может позволить осуществлять мониторинг КС в реальном времени в самых различных контекстах, например, обнаруживать тренды, аномалии и закономерности, а также делать прогнозы в реальном времени и т.д.

Ключевые слова: *мониторинг, потоки данных сетевых трафиков, кластеризация потоков данных, классификация потоков данных, анализ временных рядов.*

Введение

Сегодня увеличение масштабов, производительности, скорости и сложности компьютерных сетей, а также объема сетевого трафика и количества пользователей и устройств, подключенных к сети, становится обычным явлением. В таких условиях решение задач выявления и идентификации тех или иных проблемных ситуаций, а также инцидентов безопасности, влияющих на нормальное функционирование КС, становится очень трудным. Иногда для решения этих задач могут потребоваться дни или даже недели. Поэтому необходимо сократить время, затрачиваемое на решение возникших в КС проблем, а также для предотвращения их возникновения. Таким образом, требуется создать системы мониторинга и безопасности сетей, работающие в реальном режиме.

Для обеспечения нормального функционирования и безопасности КС сегодня используются различные аппаратно-программные средства, такие как системы обнаружения аномалий и предотвращения атак, межсетевые экраны и т.д. Несмотря на это, невозможно полностью исключить влияние вышеуказанных факторов на работу сети. Поэтому сетевым администраторам необходимо вести мониторинг КС и анализировать данные в режиме реального времени, что позволит им за короткое время определять и реагировать на различные проблемные ситуации.

Одним из перспективных подходов к повышению эффективности мониторинга КС является минимизация времени анализа потока данных сетевых трафиков. Время анализа должно быть настолько оптимальным, чтобы процесс анализа данных был близок к режиму реального времени, то есть скорость анализа данных должна быть очень близка к скорости сбора данных. Очевидно, что чем ближе будут скорость сбора и скорость анализа данных,

тем больше будет объем анализируемых данных. В таком случае в течение единицы времени будет проанализирован максимальный объем данных, что позволит определить эффективность и масштабность мониторинга КС. Однако скорость анализа в используемых сегодня методах анализа данных ниже, чем скорость сбора данных.

При мониторинге КС для анализа выборки статических данных сетевых трафиков используются методы интеллектуального анализа данных [1]. Однако эти традиционные методы не могут быть непосредственно использованы для анализа потоков данных сетевых трафиков в реальном времени. Это, в основном, связано с тем, что потоки данных сетевых трафиков имеют такие характеристики, как большой размер, бесконечность, непрерывность, высокая скорость, быстрое изменение и т.д. Поэтому для мониторинга КС в реальном времени требуется использовать иные методы интеллектуального анализа сетевых трафиков, а именно методы интеллектуального анализа потоков данных. Интеллектуальный анализ потоков данных является процессом обнаружения и извлечения скрытой полезной информации и знаний из потоков данных [2].

Целью данной статьи является создание модели мониторинга КС в реальном времени. Эта модель должна позволять анализировать потоки данных сетевых трафиков, чтобы обнаруживать в них тренды, аномалии и закономерности, а также делать прогнозы по функционированию КС во времени. Для этого предлагается использовать методы интеллектуального анализа потоков данных.

Мониторинг компьютерных сетей

Мониторинг КС является сложной задачей и для достижения конкретных целей требуется использовать различные системы мониторинга. Известно, что сетевой мониторинг включает в себя методы наблюдения и количественной оценки функционирования КС. Мониторинг КС позволяет: выявлять, диагностировать и локализовывать неисправности сетей; управлять производительностью сетей, то есть обеспечить сетевым приложениям требуемую производительность; выявлять и устранять узкие места; идентифицировать необычное поведение; планировать сети, то есть прогнозировать масштаб и характер сетевых ресурсов и т.д.

Мониторинг КС в основном осуществляется на основе анализа сетевых трафиков, а анализ сетевых трафиков в свою очередь основывается на анализе выборок пакетов [3−5] и анализе характеристик потоков [6−10]. При этом в каждом подходе, в зависимости от задач мониторинга КС, используются определенные характеристики. Однако из-за увеличения масштаба, производительности, скорости и сложности, а также объема сетевого трафика и количества пользователей и устройств КС пакетно-ориентированный анализ трафика не справляется со своей задачей. Поэтому анализ потоков сетевых трафиков считается самым перспективным решением для мониторинга сетей.

Потоки сетевых трафиков могут включать в себе такие данные, как HTTP, P2P, EMAIL и т.д. Генерируемые в современных КС потоки сетевых трафиков имеют очень большой объем, масштабность и неоднородность, к тому же информация, содержащаяся в потоках сетевых трафиков, обычно бывает недостаточно детализированной. Поэтому традиционные системы мониторинга КС не могут идентифицировать новые сетевые peer-to-peer приложения, которые используют случайные порты, передачу мультимедийных потоков и т.д. Следовательно, для эффективного мониторинга КС в реальном времени необходимо использовать методы интеллектуального анализа потоков данных. В литературе изложены различные подходы к мониторингу КС в реальном времени, которые направлены на решение конкретных задач сетевого мониторинга [11−16].

Интеллектуальный анализ потоков данных

Потоки данных (data streams) являются последовательностью элементов данных,

поступающих в реальном времени, и имеют такие характеристики, как бесконечность, непрерывность, большая размерность, высокая скорость, быстрая изменчивость во времени и т.д. [17−19]. Потоки данных могут быть формализованы в виде упорядоченной последовательности элементов данных.

$$Y = \langle y_1, y_2, y_3, \dots y_n \rangle,$$

где n являются индексами элементов данных, которые отражают их порядок в потоках, и $n \to \infty$, то есть потоки являются бесконечностью. В качестве индекса также могут быть использованы временные отметки, то есть время появления данных в потоке. В свою очередь каждый элемент данных описывается n-мерным вектором атрибутов $y_i = \left[y_i^j\right]_{j=1}^{n}$, принадлежащим пространству атрибутов, которое может быть непрерывным [20].

Наличие перечисленных выше характеристик потоков данных приводит к тому, что алгоритмы анализа потоков данных должны удовлетворять некоторым требованиям, таким, как ограничения объема хранимых данных, обработка данных за один проход, обработка данных в режиме реального времени и адаптация к изменениям структуры данных во времени (concept drift).

Обрабатывать потоки данных традиционными методами интеллектуального анализа данных невозможно, так как для этого требуются большая память и вычислительная мощность. Поэтому потоки данных должны быть обработаны в режиме реального времени без предварительного хранения. Например, в методе анализа потоков данных, так называемое дерево Хоффдинга, обучающие примеры предварительно не сохраняются. Следовательно, требуемый размер памяти может быть независимым от размера анализируемых наборов данных. Для этого алгоритм дерево Хоффдинга использует так называемую границу Хеффдинга, чтобы обучить модели с использованием минимального числа примеров. При этом граница Хеффдинга определяет, что, учитывая n независимых наблюдений случайной величины со средним значением выборки r с вероятностью $1 - \delta$, истинное среднее значение переменной, которая по крайней мере равна $r - \epsilon$, где δ является заданной допустимой ошибкой оценки, и $\epsilon = \sqrt{In(1/\delta)/2n}$ [21].

Анализ потоков данных является процессом анализа непрерывных потоковых данных в реальном времени. Интеллектуальный анализ потоков данных же является извлечением знаний, представленных в моделях и шаблонах бесконечных потоков данных. С точки зрения методов интеллектуального анализа данных потоки данных могут быть представлены как последовательность обучающих примеров, которые поступают непрерывно и с высокой скоростью из одного или нескольких источников. При этом весь процесс обучения должен постоянно повторяться с учетом новых примеров.

В общем процесс анализа потоков данных состоит из генерации потоков данных, анализа потоков данных и извлечения знаний (рис.1) [22−23]. В этом процессе генерируемые источниками потоки данных являются входными данными для методов анализа потоковых данных. При этом источниками могут быть различные приложения, генерирующие потоки данных. В свою очередь процедура анализа потока данных состоит из выбора части потока данных, предварительной обработки данных, инкрементального обучения и извлечения знаний. Причем процедура анализа потока данных должна быть однопроходной, то есть все этапы процедуры анализа данных должны выполняться за один проход и данные могут быть обработаны только один раз. Результатом анализа потоков данных является знание, которое может быть использовано для принятия обоснованных решений. Для извлечения знания из потоков данных должны быть использованы методы, которые способны анализировать многомерные данные в многоуровневом, однопроходном и интерактивном режимах. А также с проведением некоторых изменений в самих потоках данных могут быть использованы традиционные методы интеллектуального анализа данных [24].

Методы анализа потоков данных условно делятся на методы, основанные на данных, и методы, основанные на задачах [17, 18, 22]. В методах, основанных на данных, для анализа производится обобщение всех данных входящего потока или выбирается некоторое подмножество.

Рис.1. Общая схема анализа потоков данных

К этим методам относятся взятие выборок данных (sampling), снижение нагрузки (load shedding) [25], создание эскизов (sketching) [26], синопсис структур данных (synopsis data structures) [27] и агрегирование (aggregation) [28]. А в методах, основанных на задачах, используются существующие алгоритмы анализа с модификацией или же новые алгоритмы, которые решают вычислительные проблемы, связанные с анализом потоков данных. К этим методам относятся алгоритмы аппроксимации [29], метод скользящего окна и степень детализации алгоритма (algorithm output granularity) [30].

Наиболее распространенными задачами по анализу потоков данных являются кластеризация, классификация, анализ шаблонов и анализ временных рядов [31−32]. Процесс кластеризации заключается в разбиении непрерывно поступающих потоков данных на различные кластеры. Однако из-за того, что данные потоков со временем могут изменяться, то базовые кластеры также могут изменяться. Поэтому при нахождении кластеров за определенный промежуток времени в качестве входных данных также используется временной интервал.

Основными проблемами кластеризации потоков данных являются ограничение памяти, быстрая обработка данных, обнаружение изменения структуры данных во времени, установление выбросов из имеющихся кластеров. При этом алгоритм кластеризации потока данных должен быть способен изучать данные последовательно и реагировать на изменения шаблонов в потоках. Однако во многих случаях шаблоны в потоках могут значительно изменяться. Поэтому необходимо, чтобы процесс кластеризации был адаптивным к таким изменениям и позволил получить представление во времени. Для этого необходимо использовать инкрементальное обучение, то есть процесс обучения должен постоянно повторяться с учетом новых примеров. В литературе в последнее десятилетие появились различные алгоритмы кластеризации потоков данных [33].

Классификация является процессом прогнозирования класса данных на основе модели, основанной на обучении. В традиционных алгоритмах классификации используется статический набор данных, которые разделяются на наборы обучающих и тестовых данных. Однако, в отличие от них, алгоритмы классификации потоков данных изначально не имеют всех данных, и поэтому классификация из входящих обучающих наборов данных и тестирования происходит одновременно. В литературе имеются различные подходы к классификации потоков данных [34]. При этом возможности алгоритмов и решаемые проблемы анализа потоков данных отличаются.

Целью анализа шаблонов является обнаружение часто встречающихся шаблонов в

больших наборах данных. Шаблоны позволяют обобщать наборы данных и могут дать определенное представление о данных. В литературе имеются различные подходы к анализу шаблонов [35].

Анализ временных рядов позволяет решать задачи, связанные с обнаружением в потоках данных трендов, определенных событий и т.д. В литературе были предложены различные подходы к анализу временных рядов [36].

Модель мониторинга КС в реальном времени

Мониторинг КС в реальном времени в общем может быть описан следующим образом. В точку мониторинга поступают бесконечные и непрерывные потоки данных сетевых трафиков. Необходимо обнаруживать тренды, аномалии и закономерности, а также делать прогнозы в реальном времени и т.д. Для решения этих и других задач могут быть использованы различные алгоритмы интеллектуального анализа потоков данных, такие, как кластеризация потоков данных, классификация потоков данных, анализ шаблонов и анализ временных рядов и т.д.

Для решения задач мониторинга КС в реальном времени предлагается модель, которая позволит осуществлять мониторинг КС в реальном режиме (рис.2). Предложенная модель состоит из потоков сетевых трафиков, сетевого монитора, который состоит из блока формирования целей (задач) мониторинга, анализатора потоков данных и выхода.

Модель мониторинга КС в реальном времени работает следующим образом. В сетевой монитор (анализатор потоков данных) поступают потоки данных сетевых трафиков. При этом потоки данных сетевых трафиков могут быть определены как последовательность непрерывных и последовательных записей, поступающих в реальном времени.

В блоке формирования целей (задач) мониторинга КС формируются запросы на мониторинг, например, обнаружить тренды, аномалии, закономерности или дать прогнозы во времени и т.д. На основании этих запросов в анализаторе потоков данных выбирается соответствующий алгоритм анализа, например, алгоритм анализа шаблонов, алгоритм кластеризации потоков данных, алгоритм классификации потоков данных, алгоритм анализа временных рядов и т.д.

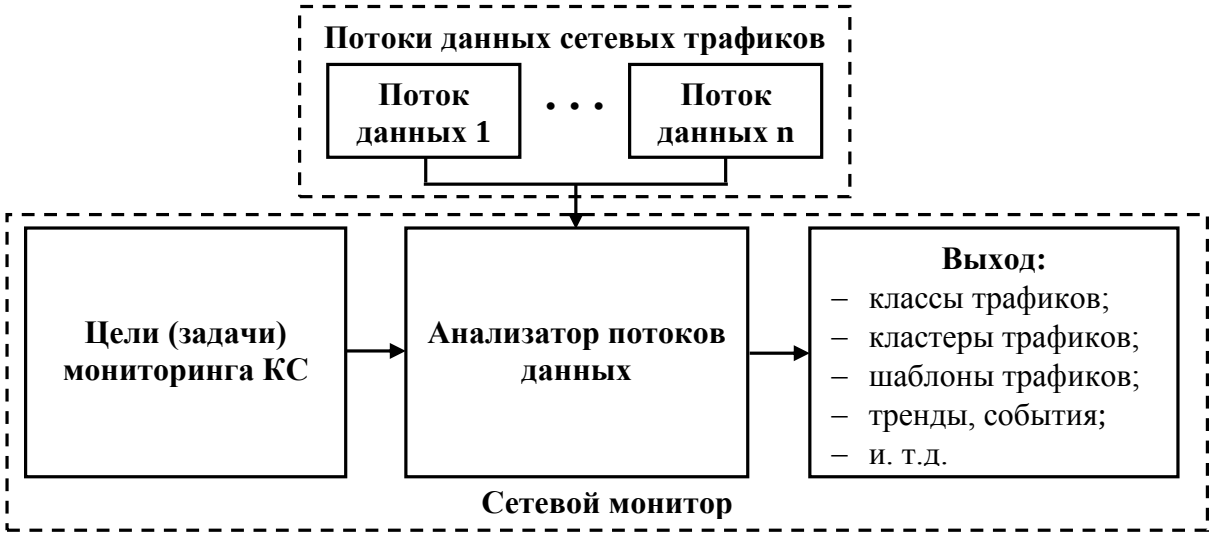

Рис.2. Модель мониторинга КС в реальном времени

После анализа потоков на выходе соответственно выдается информация о шаблонах трафиков, кластерах трафиков, классах трафиков, трендах, событиях и т.д., характеризующих потоки сетевых трафиков.

Заключение

Эффективный мониторинг является очень важным компонентом систем управления современных КС. Из-за увеличения скорости и объема, а также динамики сетевых трафиков КС процесс сбора данных мониторинга преобразуется в процесс динамического сбора потока данных. Следовательно, мониторинг КС может быть рассмотрен как проблема обработки потоков данных. Для повышения эффективности мониторинга КС необходимо минимизировать время анализа потоков данных сетевых трафиков. При этом время анализа должно быть настолько оптимальным, чтобы процесс анализа был близок к режиму реального времени. Анализ показал, что традиционные подходы интеллектуального анализа данных не могут быть непосредственно использованы для анализа потоков данных сетевых трафиков в реальном времени. Поэтому для анализа потоков данных сетевых трафиков требуется использовать методы интеллектуального анализа потоков данных, основными алгоритмами которых являются потоковая кластеризация, потоковая классификация, анализ шаблонов и анализ временных рядов.

В данной статье рассматриваются проблемы мониторинга сетевого трафика в реальном времени, основанного на методах интеллектуального анализа потоков данных. Для решения этой проблемы предложена модель, которая позволит осуществлять мониторинг КС в реальном времени в самых различных контекстах и использовать алгоритмы кластеризации, классификации, анализ шаблонов и анализ временных рядов. Предложенная модель позволит повысить эффективность мониторинга КС в реальном времени.

Литература

1. Шыхалиев Р.Г. О применении интеллектуальных технологий в мониторинге компьютерных сетей // Искусственный интеллект, 2011, №1, с.124−132.
2. Wesam S.B., Saud A.A. Anomaly detection in network traffic using stream data mining: review // Research Journal of Applied Sciences, 2016, vol.11, no.10, pp. 1076−1082.
3. Mohamed MG., Arkady Z., Shonali K. Mining Data Streams: A Review // SIGMOD Record, 2005, vol.34, no.2, pp.18−26.
4. Neha G., Indrjeet R. Stream Data Mining: A Survey // International Journal of Engineering Research and Applications, 2013, vol.3, no.1, pp.1113−1118.
5. Ryszard E.J., Miliosz M.H. Packet Sampling for Network Monitoring, Technical Report 2007. http://cern.ch/openlab
6. Davide T., Silvio V., Dario R., Antonio P. Exploiting packet sampling measurements for traffic characterization and classification // International Journal of Network Management, 2012, vol.22, no.6, pp.451−476.
7. Marco C., Damien F., David J.M., Andrew W.M., Raffaele B. Per flow packet sampling for high-speed network monitoring / Proceedings of the First International Conference on Communication Systems And NETworks, 2009, pp.463−472.
8. Song S., Ling L., Manikopoulo C.. Flow-based statistical aggregation schemes for network anomaly detection / Proceedings of the IEEE International Conference on Networking Sensing and Control, 2006, pp.786−791.
9. Bin L., Chuang L., Jian Q. A NetFlow based flow analysis and monitoring system in enterprise networks // Computer networks, 2008, vol. 52, no.5, pp.1074−1092.
10. Marco F., Kawahara R., Ishibashi K., Mori T. Detection accuracy of network anomalies using sampled flow statistics // International Journal of Network Management, 2011, vol. 21, no.6, pp.513−535.
11. Accurate and flexible flow-based monitoring for high-speed networks, Master Thesis. Autonomous University of Madrid, 2013, 38 p.
12. Wang B., Su J. A survey of elephant flow detection in SDN / Proceedings of the 6th International Symposium on Digital Forensic and Security, 2018, pp.208−213.

13. Gerald T. Real Time Network Traffic Monitoring. Technical Report: 5–99, Computing Laboratory, University of Kent, 1999.
14. Ahmed M. M. M. A real time distributed network monitoring platform (RTDNM), Doctoral Thesis, Universiti Sains Malaysia, 2009, 224 p.
15. Xu T., Qiong S., Xiaohong H., Yan M. A Dynamic Online Traffic Classification Methodology based on Data Stream Mining / Proceedings of the World Congress on Computer Science and Information Engineering, 2009, pp.298–302.
16. Kuai X., Feng W. Real-time behaviour profiling for network monitoring // International Journal of Internet Protocol Technology, 2010, vol.5, no.1/2, pp.65−80.
17. Aryan T.M., Tomasz W.W., Chunming R. Real-Time Handling of Network Monitoring Data Using a Data-Intensive Framework / Proceedings of the IEEE 5th International Conference on Cloud Computing Technology and Science, 2013.
18. Li L., Hu Z.-Y. The Research of Data Stream Technology in Computer Network Security Monitoring / Proceedings of the International Conference on Intelligent Systems Research and Mechatronics Engineering, 2015, pp.1904−1907.
19. John F., Matthew B., Michael H. Introduction to stream: A Framework for Data Stream Mining Research. http://www2.uaem.mx/r-mirror/web/packages/stream/vignettes/stream.pdf
20. Silva, J.A., Faria, E.R., Barros, R.C., Hruschka, E.R., de Carvalho, A.C., Gama, J., Data stream clustering: A survey // ACM Computing Surveys, 2013, vol.46, no.1, p.13.
21. Kholghi M., Keyvanpour M. An Analytical Framework for Data Stream Mining Techniques Based on Challenges and Requirements // International Journal of Engineering, Science and Technology, 2011, vol.3, no.3, pp.2507−2513.
22. Chao S.C., Lin K.C., Chen M.S. Flow Classification for Software-Defined Data Centers Using Stream Mining // IEEE Transactions on Services Computing, 2019, vol. 12 , no. 1, pp.105–116.
23. Sidda Reddy V., Rao T.V., Govardhan A. Data mining techniques for data streams mining // Review of computer engineering studies, 2017, vol.4, no.1, pp.31−35.
24. Golab L., Özsu M.T. Issues in data stream management // ACM SIGMOD Record, vol.32, no.2, 2003, pp.5−14.
25. Tatbul N., Cetintemel U., Zdonik S., Cherniack M., Stonebraker M. Load Shedding on Data Streams, Proceedings of the Workshop on Management and Processing of Data Streams, 2003.
26. Florin R., Alin D. Sketching Sampled Data Streams / Proceedings of the IEEE 25th International Conference on Data Engineering, 2009, vol.1−3, pp.381−392.
27. Babcock B., Babu S., Datar M., Motwani R., Widom J. Models and issues in data stream systems / Proceedings of the twenty-first ACM SIGMOD-SIGACT-SIGART symposium on Principles of database systems, 2002, pp.1−16.
28. Aggarwal C, Han J., Wang J., Yu P. S. A Framework for Projected Clustering of High Dimensional Data Streams / Proceedings of the Thirtieth international conference on Very large data bases, 2004, vol.30, pp.852−863.
29. Cormode G., Muthukrishnan S. What's hot and what's not: Tracking most frequent items dynamically // ACM Transactions on Database Systems, 2005, vol.30, no.1, pp.249−278.
30. Gaber, M, M., Zaslavsky, A., and Krishnaswamy, S. Towards an Adaptive Approach for Mining Data Streams in Resource Constrained Environments / Proceedings of the 6th International Conference on Data Warehousing and Knowledge Discoverey, 2004, Data Warehousing And Knowledge Discovery, Proceedings: Lecture Notes in Computer Science, vol.3181, pp.189−198.
31. Aggarwal C. An Introduction to Data Streams // Data Streams: Models and Algorithms, 2007, pp.1−18.
32. Gama J. Knowledge Discovery from Data Streams. 1st edition. Chapman & Hall/CRC, Boca Raton, 2010.

33. Sharma N., Masih S., Makhija P. A Survey on Clustering Algorithms for Data Streams // International Journal of Computer Applications, 2018, vol.182, no.22, pp.18−24.
34. Gaber M. M., Zaslavsky A., Krishnaswamy S. A Survey of Classification Methods in Data Streams // Data Streams: Models and Algorithms, 2007, pp.39−59.
35. Subbulakshmi B., Deis C., Periya Nayaki A. Survey on Frequent Pattern Mining over Data Streams // International Journal of Engineering Research and Technology, 2013, vol.2, no. 12, pp.2276−2283.
36. Jinlong W., Congfu X., Weidong C., Yunhe P. Survey of the study on frequent pattern mining in data streams / Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, 2004, vol.1−7, pp.5917−5922.

UOT 004.042

Şıxəliyev Ramiz H.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
ramiz@science.az

Kompüter şəbəkələrinin real zamanda monitorinqinin bir modeli haqqında

Müasir kompüter şəbəkələrinin (KŞ) normal və təhlükəsiz fəaliyyətini təmin etmək üçün etibarlı və effektiv monitorinq modelləri tələb olunur. Bu modellər böyük həcmdə şəbəkə trafiki verilənləri axınlarını real zaman rejimində analiz edə bilməlidir. Lakin bu gün istifadə edilən verilənlərin analizinin ənənəvi yanaşmaları bu məsələni həll edə bilməz. Bu məsələnin həlli üçün verilənlər axınlarının intellektual analizi metodlarının istifadəsi daha müvafiqdir. Bu məqalədə verilənlər axınlarının intellektual analizi alqoritmləri istifadə edilən, KŞ-in real zamanda monitorinqi modeli təklif edilmişdir. Təklif olunan model çoxməsələlidir, yəni KŞ-in monitorinqinin məqsədlərindən asılı olaraq, şəbəkə trafiki verilənləri axınlarının analiz edilməsi üçün verilənlər axınlarının intellektual analizinin müvafiq alqoritmlərindən istifadə edilə bilər. Bunun üçün, verilənlər axınlarının klasterizasiyası və klassifikasiyası, şablonların və zaman seriyalarının analizi kimi alqoritmlərdən istifadə edilir. Beləliklə, təklif olunan model KŞ-in real zamanda monitorinqini müxtəlif kontekstlərdə həyata keçirməyə, məsələn, trendlərin, anomaliyaların və qanunauyğunluqların aşkarlanmasına, habelə real zamanda proqnozların verilməsinə və s. imkan verə bilər.

***Açar sözlər**: monitorinq, şəbəkə trafiki verilənləri axınları, verilənlər axınının klasterizasiyası, verilənlər axınının klassifikasiyası, zaman sıralarının analizi.*

Ramiz H. Shikhaliyev
Institute of Information Technology of ANAS, Baku, Azerbaijan
ramiz@science.az

One model of real-time monitoring of computer networks

To ensure the normal and safe functioning of modern computer networks (CN), reliable and effective monitoring models are required. These models should allow analyzing a large volume of network traffic data streams in real time. However, the traditional data mining approaches used today cannot solve this task. To solve this problem, it is more suitable to use data stream mining techniques. This article proposes a real-time monitoring model of CN in which data stream mining algorithms are used. The proposed model is multitasking, that is, depending on the objectives of monitoring the CN, the corresponding algorithms for the intellectual analysis of data flows can be used to analyze data flows of network traffic. To do this, the algorithms, such as clustering data streams, classifying data streams, analyzing patterns, and analyzing time series, are used. Thus, the proposed model can allow real-time monitoring of CN in a variety of contexts, for example, detect trends, anomalies and patterns, as well as real-time forecasts, etc.

***Keywords**: monitoring, network traffic data stream, data stream clustering, data stream classification, time series analysis.*