О методах мониторинга компьютерных сетей

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

***Аннотация* — Сегодня принятие эффективных решений по управлению и безопасности компьютерных сетей (КС) невозможно без их мониторинга. Мониторинг различных показателей КС позволяет получить необходимую информацию об их состоянии. В работе проводится анализ методов мониторинга КС в различных аспектах, таких как распределенный мониторинг, классификация сетевого трафика, визуализация сетевого мониторинга, QoS (Quality of Service) мониторинг.**

Ключевые слова — компьютерные сети, мониторинг, распределенный мониторинг, классификация сетевого трафика, визуализация сетевого мониторинга, QoS мониторинг

I. ВВЕДЕНИЕ

Мониторинг является очень важным элементом эффективного управления и обеспечения безопасности современных компьютерных сетей (КС). Основной целью мониторинга является получение необходимой информации о состоянии КС, чтобы принять эффективные управленческие решения. При этом мониторинг в основном заключается в измерении определенных показателей КС, а также выведение агрегированной функции из этих измерений. Эти показатели описывают состояние и производительность сети с точки зрения использования ресурсов, перегрузки, потери пакетов и помогают администраторам выявить потенциальные проблемы. Вместе с тем, измеряя и анализируя параметры сетевого трафика можеть быть обеспечена безопасность сети и пользователей от внешних и внутренних атак [1].

С точки зрения мониторинга, КС состоит из объектов имеющих различные параметры, которые характеризуют состояния этих объектов и определяются актуальностью и полнотой. К этим объектам можно отнести такие элементы КС, как сетевые оборудования, сетевые соединения, сетевые трафики, сетевые сервисы и пользователей. А также на различных этапах развития КС отличались цели и задачи мониторинга и использовались различные методы.

Целью данной статьи является анализ существующих концепций и методов мониторинга КС, а также существующих в этой области проблем.

II. РАСПРЕДЕЛЕННЫЙ МОНИТОРИНГ КС

С увеличением масштабов современных КС появляется необходимость в эффективных и масштабируемых системах распределенного управления. Основой этих систем является распределенный мониторинг. В литературе имеются различные подходы к распределенному мониторингу КС. Например, для распределенного и динамического мониторинга сети были использованы мобильные агенты [2]. В качестве агентов авторы использовали систему IBM Aglets и показали, что приложения распределенного мониторинга КС основанные на Java могут эффективно осуществлять сбор и анализ данных и адаптироваться к изменениям характеристик сети. Вместе с тем, эффективность осуществления распределенного мониторинга КС зависит от эффективности масштабируемой инфрастркутруры мониторинга. Чтобы снизить издержки развертывания такой системы была предложена оптимальная иерархическая архитектура мониторинга [3], суть которой заключалась в оптимальном распределении ресурсоемких задач по сети. Одной из таких задач является опрос отдельных узлов сети. При этом выбор количества опрашивающих узлов имеет существенное влияние на стоимость инфраструктуры измерений и пропускную способность сети. Для решения этой задачи авторы оптимизировали масштабируемую распределенную систему опроса. Также для создания оптимальной инфраструктуры мониторинга были использованы элементы искусственного интеллекта, а именно сети Хопфилда [4]. Кроме того, для эффективного и масштабируемого распределенного мониторинга КС необходимы эффективные алгоритмы распределенного мониторинга. В работе [5] автором были предложены два алгоритма, которые позволяют снизить коммуникационные издержки. Первый из которых был назван DSM (Distributed Subnetwork Monitoring) алгоритмом, в котором предполагается, что сеть состоит из нескольких подсетей и в каждой имеется свой локальный менеджер. Основная идея алгоритма заключается в том, что каждый локальный менеджер осуществляет сбор и обработку данных мониторинга своей подсети. А когда сумма переменных превышает значение локального порога, то менеджер начинает постепенно собирать данные из других подсетей. При этом, так как локальный менеджер находится ближе к данным своей подсети, то связь между узлами и локальным менеджером является более эффективной. При превышении в некоторых узлах значений переменных

DOI: 10.25045/NCInfoSec.2017.07

среднего значения для узла, результат сглаживается другими переменными подсети, что уменьшает необходимость опроса всех узлов в больших КС. Второй алгоритм был назван FDM (Fully Distributed Monitoring – полностью распределенный мониторинг) алгоритмом потому, что в этом алгоритме нет подсетей и локальных менеджеров. Узлы сети взаимодействуют друг с другом и выполняют задачу мониторинга, а когда узел превышает их предел, то ищет другие узлы с более доступными ресурсами. Другой подход для распределенной сетевой архитектуры мониторинга предлагается в [6], суть которого состоит из децентрализованного сбора и хранения данных сетевого трафика. В таком подходе сетевой трафик собирается и хранится прямо на соответствующих устройствах по всей сети. При этом обработка данных происходит параллельно на соответствующих локальных данных и для этого используется технология Map-Reduce [7].

III. Классификация сетевого трафика КС

Сетевой трафик является одним из важнейших фактических показателей работы КС, то есть трафик является носителем информации о поведении пользователей и функционировании КС. Использование в современных КС большего количества сетевых сервисов и приложений, аппаратного и программного обеспечения приводит к появлению в сети большого разнообразия трафиков. Для проведения эффективного мониторинга и управления КС, решение задачи точной классификации трафиков относительно сетевых сервисов, приложений и протоколов является очень важной [8].

Классификация сетевого трафика особенно важна для решения таких задач, как определение приоритетов при формировании полосы пропускания для отдельных трафиков, установление правил по управлению сети, обеспечение безопасности сети, диагностический мониторинг КС и т.д. [9]. Например, для того, чтобы обеспечить нормальную работу приложений, важных для корпорации, администратор сети должен идентифицировать и ограничивать (или заблокировать) P2P (peer-to-peer) трафик. Кроме того, эффективное решение большинства технических задач, таких как определение параметров и моделирование рабочей нагрузки каналов связи, планирование загрузки сетевых оборудований, инициализация маршрутов и т.д., также зависит от точной идентификации и классификации сетевого трафика.

Однако классификация сетевого трафика в реальном масштабе времени является одной из основных проблем мониторинга современных КС. Классификация позволяет идентифицировать приложения на основании используемых конкретных «известных» портов TCP или UDP (обычно информация о номере порта имеется в заголовках TCP или UDP-пакетов). Однако все номера портов, используемые большинством приложений предсказать невозможно [10]. Поэтому нужны более эффективные методы классификации сетевого трафика, которые позволяют определить тип приложения на основе данных, имеющихся в основной части TCP или UDP-пакетов (или на основе известных поведений протоколов). Однако из-за детальности проверки содержимого пакетов уменьшается эффективность таких методов классификации сетевого трафика. Поэтому, большинство исследователей считают методы машинного обучения (МО), которые являются частью дисциплины искусственного интеллекта, более подходящими для классификации сетевого трафика. В работе [11] предложен инспектор сетевого трафика, основанный на методах МО и предназначавшийся для минимизации длительности вызовов в телекоммуникационных сетях с канальной коммутацией. Эта работа является началом применения методов МО в области телекоммуникационных сетей. А после этого МО было использовано для классификации интернет-трафика в целях обнаружения вторжений [12]. Эта работа положила начало применению методов МО для классификации интернет-трафика.

IV. Визуализация мониторинга КС

Непрерывное и быстрое поступление данных в систему мониторинга приводит к накоплению большого количества данных, что затрудняет их обработку и анализ в числовой форме. Поэтому, появляется необходимость в использовании методов визуализации сетевых данных, которые позволят администраторам сетей буквально мгновенно зрительно провести мониторинг сети. Визуализация сетевых данных позволяет кратко представить и отобразить большой объем сетевых данных в графическое представление и является эффективным механизмом мониторинга характеристик сетевого трафика. Визуализация сетевых данных особенно важна для экспресс оценки состояния сети, которая дает возможность администрам сетей легко и быстро интерпретировать результаты мониторинга. Визуализация сетевых данных также позволяет динамически представить состояние сети и определить узкие места, отказы, нецелевое использование ресурсов сети и т.д. При этом, детализация визуализации может быть проведена на различных уровнях, таких как нагрузка сети, пропускная способность, типы пакетов и т.д. Для выразительности полученного в результате визуализации изображения используются различные цвета, которые облегчают их интерпретацию [13].

Сегодня, для визуализации сетевых данных предлагаются различные методы [14]. При этом, обшей чертой этих методов является отображение большого обьема данных на меньшее пространство. Обычно, методы визуализации сетевых данных включают в себя простые линейные графики и диаграммы, которые отображают изменение параметров сетевого трафика и используемые метрики могут варьироваться от общих

измерений (например, использование пропускной способности сети), до более конкретных показателей.

Простые линейные графики и диаграммы являются весьма эффективными для отображения большинства метрик сети, поскольку просты для понимания и интерпретации. Поэтому простые линейные графики являются одним из самых распространенных видов визуализации и наиболее часто используются. Простые линейные графики предназначены для визуализации изменения параметров трафика сети во времени. При этом, каждому параметру присваивается уникальный цвет. Для анализа сети, простые линейные графики обеспечивают интуитивно понятное изображение и в зависимости от характера отображения графической линии, администратор сети может легко провести анализ трафика и принять соответствующие решения.

Простые графики используются в многих средствах мониторинга, например, в системах мониторинга MRTG [15] и RRDTool [16]. MRTG используется для визуализации использования текущей пропускной способности во времени. Кроме того, в работе [17] для мониторинга сетевого трафика был предложен, так называемый радиальный анализатор трафика, который использует концентрические кольца и изображает иерархические отношения между различными измерениями. В общем, этот метод визуализации предназначен для количественного анализа иерархически структурированных данных и очень хорошо подходит для визуального анализа сетевых данных. Также, этот метод может быть использован для любых наборов данных, имеюших иерархическое отношение.

V. Мониторинг качества сервисов КС

Используемые в КС сетевые протоколы, приложения, сервисы и мультимедиа имеют различные требования к QoS (Quality of Service). Обеспечение для каждого сетевого приложения, сервиса и мультимедиа требуемого уровня QoS является серьезной проблемой.

Так как QoS имеет комплексный характер, то его количественное определение и гарантированное обеспечение становится трудным. Поэтому проведение в режиме реального времени постоянного мониторинга и управления параметрами QoS КС становится очень важным. Однако QoS все же остается одним из самых неоднозначно определенных понятий КС. В зависимости от задач по обеспечению сетевого сервиса QoS может быть определен различными способами и может включать в себя множество различных требований сервиса, такие, как производительность, доступность, надежность, безопасность и т.д. Все эти требования являются очень важными аспектами для комплексного обеспечения QoS. Поэтому для обеспечения QoS компьютерных сетей необходимым является создание QoS структуры, которая включала бы в себя принципы, спецификации и механизмы мониторинга и управления QoS [18].

Созданное ITU (International Telecommunications Union) SLA (Service Level Agreements), которое заключается между провайдерами интернет услуг и абонентами, позволило определить QoS параметры сетевых сервисов. Однако SLA не основывается на объективных стандартах и может различаться в зависимости от клиента, провайдера интернет-услуг и предлагаемых услуг [19]. Поэтому отсутствие единого стандарта QoS не позволяет должным образом определить QoS сетевых сервисов.

На протяжении более десятка лет было проведено множество исследований и были разработаны различные архитектуры, технологии и механизмы мониторинга QoS [20–23]. Множество исследований и разработок было выполнено IETF (Internet Engineering Task Force), например, IETF RFC 1633 [24], IETF RFC 2430 [25], IETF RFC 2475 [26] и т.д. CAIDA (Cooperative Association for Internet Data Analysis) создала среду мониторинга сетевого трафика, которая используется для сбора и анализа данных QoS.

По способу получения информации мониторинг QoS может быть разделен на мониторинг «точка-точка» [27] и распределенный мониторинг [28]. При мониторинге «точка-точка» в режиме реального времени проводится мониторинг QoS трафика между двумя точками, то есть между отправителем и получателем. А при распределенном подходе мониторинга QoS наряду с мониторингом «точка-точка» также проводится мониторинг QoS различных сегментов сети. В основе модели системы мониторинга QoS КС лежит традиционная модель сетевого мониторинга [29], включающая следующие функциональные компоненты: приложение мониторинга, QoS мониторинг, монитор и объекты мониторинга [30].

Заключение

С равитием информационных технологий, КС становятся все более масштабными и сложными. В результате появляются проблемы в управлении и безопасности КС. При этом, мониторинг играют важную роль в эффективном управлении и безопасности КС.

Проведенный в статье анализ методов мониторинга КС позволит выявить проблемы существующие в этой области и разработать более эффективные методы для мониторинга КС.

ЛИТЕРАТУРА

[1] Vokorokos L., Adam N., Balarz A., Application of intrusion detection systems in distributed computer systems and dynamic networks, Computer Science and Technology Research Survey, 2008, pp. 19–24.

[2] Kamangar F., Levine D., Záruba G. V., and Chitturi N., Distributed network monitoring using mobile agents paradigm, Proceedings of the International Conference on Parallel and Distributed Processing Techniques and Applications, 2003, pp. 951-957.

[3] Li L., Thottan M., Sanjoy B. Y. P., Distributed network monitoring with bounded link utilization in IP networks, Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies. 2003, vol. 2, pp. 1189-1198.

[4] Liu X., Yin J., Cai Z., Lu X., Chen S., Optimizing the distributed network monitoring model with bounded bandwidth and delay constraints by neural networks, Advances in Neural Networks – ISNN 2005, volume 3496 of the series Lecture Notes in Computer Science, pp. 805-810.

[5] Du X., Toward efficient distributed network monitoring, IEEE International Conference on Performance, Computing, and Communications, 2004, pp. 87-94.

[6] Elsen L., Kohn F., Decker C., Wattenhofer R., goProbe: a scalable distributed network monitoring solution, IEEE International Conference on Peer-to-Peer Computing, 2015, pp. 1-10.

[7] Lee Y., Kang W., Son H., An Internet Traffic Analysis Method with MapReduce, Proceedings of the Network Operations and Management Symposium Workshops (NOMS Wksps), 2010 IEEE/IFIP, 2010, pp. 357-361.

[8] Шыхалиев Р.Г., О применении интеллектуальных технологий в мониторинге компьютерных сетей, Искусственный интеллект, 2011, № 1, с. 124-132.

[9] Kim H., Fomenkov M., Barman D., Faloutsos M., and Lee K., Internet traffic classification demystified: myths, Caveats, and the Best Practices, Proceedings of the 4th Conference on Emerging Network Experiment and Technology, December 09 - 12, 2008, pp. 112-124.

[10] Karagiannis T., Broido A., Brownlee N., and Claffy K., Is P2P dying or just hiding?, Proceedings of the 47th annual IEEE Global Telecommunications Conference, 2004, vol. 3, pp. 1532-1538.

[11] Silver B., Netman: A learning network traffic controller, Proceedings of the Third International Conference on Industrial and Engineering Applications of Artificial Intelligence and Expert Systems, Association for Computing Machinery, 1990, vol. 2, pp. 923 – 931.

[12] Frank J., Machine learning and intrusion detection: Current and future directions, Proceedings of the National 17th Computer Security Conference, 1994, pp. 22-33.

[13] Shikhaliyev R.H., About Methods for Visualizing Network Monitoring, Proceedings of the 4th International Conference Problems of Cybernetics and Informatics, Baku, Azerbaijan, September 12-14, 2012, vol. 1. - B., pp. 69-70.

[14] D. A. Keim, Information Visualization and visual data mining, IEEE Transactions on visualization and computer graphics, 2002, vol. 7, no. 1, pp. 100-107.

[15] T. Oetiker, and D. Rand, Multi Router Traffic Grapher. http://www.mrtg.org.

[16] T. Oetiker, Round Robin Database Tool. http://www.rrdtool.org.

[17] Keim D. A., Mansmann F., Schneidewind J., and Schreck T., Monitoring Network Traffic with Radial Traffic Analyzer, IEEE Symposium On Visual Analytics Science And Technology, 2006, pp. 123-128.

[18] Шыхалиев Р.Г., О методах мониторинга и управления QoS компьютерных сетей, Проблемы Иформационных Технологий, 2013, № 1, с. 15-23.

[19] ITU-T, Support of IP-based services using IP transfer capabilities, Tech. Rep. Rec. Y.1241, 200.

[20] Firoiu V. et al., Theories and Models for Internet Quality of Service, Proc. of IEEE, Special issue on Internet Technology, 2002, Vol. 90, Is. 9 pp. 1565–1591.

[21] Soldatos J., Vayias E., Kormentzas G., On the Building Blocks of Quality of Service in Heterogeneous Ip Networks, IEEE Communications Surveys & Tutorials, 2005, vol. 7, No.1, pp. 70-89.

[22] Karam F., Jensen T., A Survey on QoS in Next Generation Networks, Advances in Information Sciences and Service Sciences, 2010, Vol. 2, No. 4, pp. 91–102.

[23] Aurrecoechea C., Campbell A., and Hauw L., A Survey of QoS Architectures, Multimedia Systems Journal, 1998, Vol. 6, No. 3, pp. 138–151.

[24] Braden R., Clark D., and Shenker S., Integrated Services in the Internet Architecture: an Overview, IETF RFC 1633, Tech. Rep., 1994. ftp://ftp.isi.edu/in-notes/rfc1633.txt

[25] Li T. and Rekhter Y., A Provider Architecture for Differentiated Services and Traffic Engineering (PASTE), IETF RFC 2430, Tech. Rep., 1998. ftp://ftp.isi.edu/in-notes/rfc2430.txt

[26] Blake S., Black D., Carlson M., Davies E., Wang Z., and Weiss W., An Architecture for Differentiated Services, IETF RFC 2475, Tech. Rep., 1998. ftp://ftp.isi.edu/in-notes/rfc2475.txt

[27] Jiang Y., Tham C.K., Ko C.C., A QoS distribution monitoring scheme for performance management of multimedia networks, Proc. of IEEE GLOBECOM’99, 1999, Vol. 1A, pp. 64-68.

[28] Foster I., Roy A., Sander V., and Winkler L., End-to-End Quality of Service for High-End Applications, Technical Report, Mathematics and Computer Science Division, Argonne National Laboratory, Argonne, 1999. www.mcs.anl.gov/qos/end to end.pdf

[29] Stallings W., SNMP, SNMPv2 and RMON: Practical Network Management, 2nd edition, Addison-Wesley, 1996.

[30] Jiang Y., Tham C.K., Ko C.C., Challenges and approaches in providing QoS monitoring, International Journal of Network Management, 2000, Vol. 10, No.6, pp. 323–334.

ON COMPUTER NETWORKS MONITORING METHODS

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

Abstract – Today, the adoption of effective solutions for the management of computer networks (CN) is not possible without their monitoring. Monitoring of various parameters allows the CN to receive the necessary information about their condition. The paper deals with the analysis of methods for monitoring in various aspects, such as the distributed monitoring, network traffic classification, network monitoring visualization, QoS (Quality of Service) monitoring.

Keywords – computer networks, monitoring, distributed monitoring, network traffic classification, network monitoring visualization, QoS monitoring