УДК 004.048

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

ОБ ОДНОЙ КОНЦЕПТУАЛЬНОЙ МОДЕЛИ СИСТЕМЫ ИНТЕЛЛЕКТУАЛЬНОГО МОНИТОРИНГА КОМПЬЮТЕРНЫХ СЕТЕЙ

Эффективное управление компьютерными сетями (КС) невозможно без объективных данных об их состоянии и функционировании, что обеспечивается сетевым мониторингом. Для достоверного и эффективного мониторинга КС необходимо использовать системный подход. В статье предлагается концептуальная модель системы интеллектуального мониторинга КС, целью которой являются создание эффективной инфраструктуры сбора, хранения и анализа данных мониторинга, а также принятие решений по управлению сетью.

Ключевые слова: *компьютерные сети, сетевой мониторинг, данные мониторинга, структура системы интеллектуального мониторинга.*

1. Введение

Сетевой мониторинг является одним из составляющих элементов процесса управления компьютерными сетями (КС) и источником получения объективных данных об их состоянии и функционировании. Без этих данных невозможно принять обоснованные решения по управлению КС, особенно если масштаб КС очень большой. Вместе с тем без проведения сетевого мониторинга трудно объективно оценить конфигурацию аппаратного и программного обеспечения КС, а также происходящих в нем изменений. На основе анализа результатов сетевого мониторинга осуществляются управление трафиком, реконфигурация сети, идентификация неисправностей и т.п., чтобы обеспечить оптимальную производительность и надежность КС.

Для того чтобы управление КС было эффективным, необходимо постоянно осуществлять их мониторинг. Однако постоянный мониторинг КС может привести к некоторым проблемам, связанным со сбором, хранением, обработкой и анализом большего объема сетевого трафика, передаваемого по сети. Так как постоянно меняются масштаб и сложность КС и по сути сетевой трафик КС является сложным динамическим процессом и состоит из различных потоков трафика. Эти потоки трафика имеют множество взаимосвязанных характеристик и генерируются различными аппаратами, сервисами, приложениями, протоколами и т.п. Прежде всего потоки трафика связаны с управлением КС, например, трафики инициализации клиентов, трафики серверов и т.п., которые генерируются периодически. Другие потоки трафика – это трафики сетевых сервисов, приложений и протоколов, например, веб-сервис, DNS (Domain Name System), FTP (File Transfer Protocol), запросы WINS (Windows Internet Naming Service), ARP (Address Resolution Protocol), сеанс NetBIOS, HTTP (Hypertext Transfer Protocol), P2P (Peer-to-Peer), SMTP (Simple Mail Transfer Protocol), POP3 (Post Office Protocol v. 3), Telnet и т.п., которые и составляют основную часть сетевого трафика КС [1].

В условиях постоянно изменяющихся масштаба и сложности КС, а также требований к самим КС (например, к производительности, пропускной способности, безопасности и т.д.) для осуществления достоверного и эффективного мониторинга КС необходимо использовать системный подход. Системный подход к мониторингу КС заключается в том, что процесс мониторинга рассматривается как совокупность связанных элементов, к которым относятся сбор (регистрация), хранение, анализ данных мониторинга и поддержка принятия решений по управлению сетью, а также обратная связь с КС, осуществляемая администратором, который

выполняет конкретные управленческие действия. При этом модель системы мониторинга должна основываться на использовании интеллектуальных технологий, так как они позволяют минимизировать роль человека при мониторинге, уменьшить потери нужной информации, минимизировать влияние системы мониторинга на нормальную работу КС и т.д. [2].

Сегодня на рынке информационных технологий существуют различные системы мониторинга, которые могут использоваться для мониторинга КС [3]. Сравнительный анализ этих систем показал, что они различаются по различным критериям, например, используемым технологиям (например, с использованием протокола SNMP ((Simple Network Management Protocol)) или агентов), способам сбора и хранения данных, архитектурам мониторинга, условиям использования этих систем, то есть являются коммерческими, условно бесплатными, свободными и т.д.

Известно, что основными недостатками коммерческих систем мониторинга являются дороговизна и закрытость программного кода. Эти недостатки особенно важны, когда эти системы мониторинга используются для мониторинга крупных КС, например национальных КС. Поэтому актуальной является задача разработки моделей построения системы мониторинга КС.

В работе предлагается концептуальная модель системы интеллектуального мониторинга КС, целью которой являются создание эффективной инфраструктуры сбора, хранения и анализа данных мониторинга и принятие решений по управлению сетью. При этом интеллектуальность системы мониторинга КС в основном заключается в использовании интеллектуальных технологий для анализа собранных данных мониторинга и принятия решений по управлению сетью.

2. Концептуальная модель системы интеллектуального мониторинга компьютерных сетей

Мониторинг КС в целом может быть условно разделен на мониторинг сетевой инфраструктуры и мониторинг сетевого трафика. Мониторинг сетевой инфраструктуры используется для повышения производительности и надежности сетевой инфраструктуры. К задачам мониторинга сетевой инфраструктуры можно отнести обнаружение неисправностей (отказов), мониторинг производительности сетевых узлов, а также управление уровнем загрузки каналов связи, выявление «узких» мест, оптимальное распределение и использование сетевых ресурсов и т.д. А мониторинг сетевого трафика относится к коммуникационной инфраструктуре, задача которой состоит из управления сетевого трафика, обеспечения необходимых параметров качества обслуживания, таких, как пропускная способность, минимальные значения задержек и потерь пакетов, а также мониторинг поведения пользователей и т.д. Исходя из сказанного, можно сделать вывод о том, в какой мере задачи мониторинга сетевой инфраструктуры и мониторинга сетевого трафика пересекаются. Так как управление трафиком имеет цель достижения максимальной производительности каналов связи и может быть применено для повышения эффективности использования ресурсов каналов связи и избежания заторов в сети, а также для изменения конфигурации маршрутизации в сети в случае сбоев или проблем, связанных с перегрузкой.

Для решения задач мониторинга в целом предлагается концептуальная модель системы интеллектуального мониторинга КС, которая является информационной моделью взаимодействия компонентов системы мониторинга. Эти компоненты могут входить в состав любой системы мониторинга независимо от ее архитектуры. Предложенная модель является модульной и состоит из нескольких подсистем (рис.1), она также позволяет легко включать новые подсистемы по конкретным аспектам процесса мониторинга и реорганизовывать взаимодействие подсистем. Таким образом при необходимости можно масштабировать систему и решить любую задачу по мониторингу КС, что позволит адаптировать систему под любое функциональное и инфраструктурное изменение,

происходящее в КС. А также очень важным аспектом модульности модели системы интеллектуального мониторинга КС является возможность распределять и интегрировать подсистемы в масштабе КС, что особенно важно при очень больших масштабах КС.

Предложенная модель системы интеллектуального мониторинга включает следующие подсистемы: сбора (регистрации) данных мониторинга; хранения собранных данных мониторинга; интеллектуального анализа данных мониторинга и поддержки принятия решений по управлению сетью. Вместе с тем администратор (или консоль администратора) сети также является составной частью структуры интеллектуального мониторинга КС. Потому что на основании выданных решений подсистемой поддержки принятия решений по управлению сетью администратор осуществляет обратную связь с КС и выполняет конкретные действия. При этом первые три подсистемы решают задачи систематического долговременного накопления и анализа данных о КС и не предусматривают какую-либо реакцию на получаемые данные.

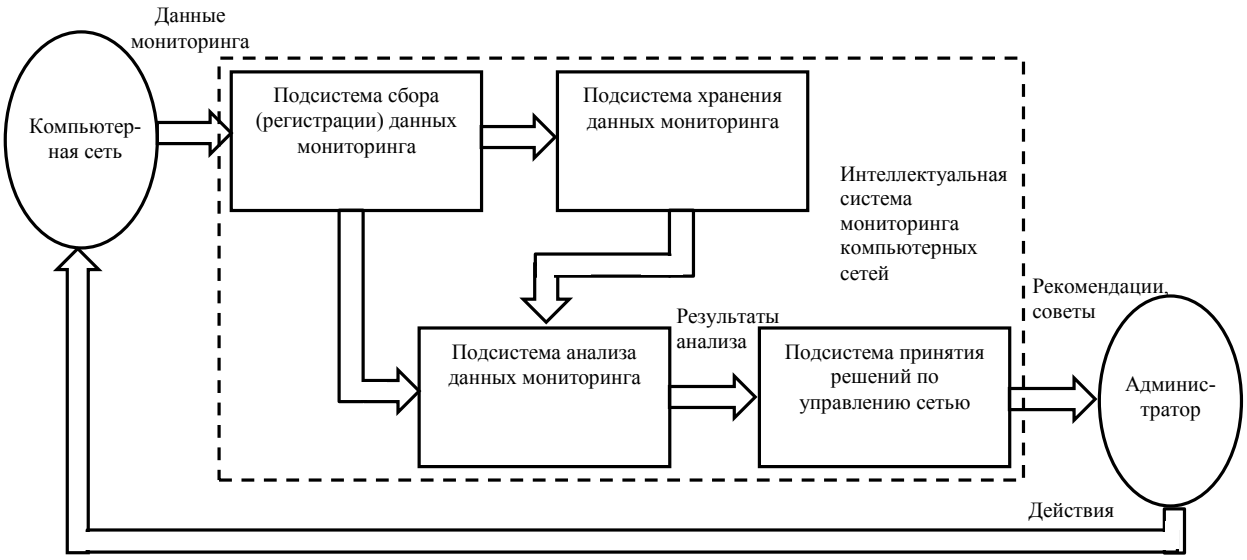

Рис.1. Концептуальная структура интеллектуального мониторинга КС

3. Взаимодействие и функции подсистем

В предложенной выше модели системы интеллектуального мониторинга КС взаимодействие подсистем происходит следующим образом. Сначала в подсистеме сбора (регистрации) данных мониторинга с помощью сетевых сенсоров осуществляется сбор сетевого трафика (данных мониторинга). Она также может осуществлять предварительный анализ этих данных. При этом большинство средств сбора сетевого трафика записывают полученные данные в файлы (лог-файлы) и обычно имеют собственные форматы файлов. Поэтому очень важно знать формат хранимого файла, чтобы без затруднения организовать передачу данных между приложениями сбора и анализа данных, так как большинство из них поддерживают определенные форматы файлов [4]. Однако имеются некоторые общие форматы (например, pcap), которые поддерживаются большинством приложений сбора и анализа данных, но форматы создаваемых файлов могут определить необходимые объемы для хранения файлов. Вместе с тем, как было сказано выше, постоянный мониторинг КС может привести к некоторым проблемам, связанным со сбором, хранением, обработкой и анализом большего объема сетевого трафика, передаваемого по сети. Для решения проблем, связанных со сбором и хранением большего объема данных мониторинга, в работе [5] авторами был предложен метод, который позволяет преобразовывать формат собранных данных мониторинга. Этот метод позволяет минимизировать потери точности данных мониторинга и уменьшить пространство, необходимое для их хранения.

В зависимости от задач мониторинга могут быть использованы различные методы: сбор всех пакетов; сбор сетевого потока и так называемый сбор расширенного потока [4, 6, 7]. Причем эти методы имеют различные требования к объему памяти, необходимому для хранения собранных данных.

Целью сбора пакетов является сбор всего сетевого трафика, который генерируется компьютерами и устройствами КС, при котором осуществляются сбор и хранение данных заголовка каждого пакета и передаваемой в пакетах информации. Другими словами, производятся сбор, обработка и хранение копии каждого пакета трафика для последующего анализа. Эти собранные данные обеспечивают аналитиков полной информацией о трафике: информацией заголовков пакетов и передаваемой в пакетах информацией. Следовательно, такой метод сбора данных мониторинга может быть наиболее универсальным, так как большой объем информации может интенсивно храниться и обрабатываться.

Сетевой поток определяется как множество IP-пакетов, проходящих через точку наблюдения в сети в течение определенного интервала времени. Все пакеты, принадлежащие к определенному потоку, имеют набор общих свойств. Требования к потокам IP-пакетов определены в RFC 3917 [8].

Сбор расширенного потока включает в себя сбор всех пакетов и сетевого потока. При этом к информации потока добавляется информация, взятая непосредственно из заголовков пакетов или из передаваемой в пакетах информации. Вместе с тем расширенный поток также может содержать дополнительную информацию о каком-то внешнем источнике, например, о географическом расположении IP-адресов источника и назначения.

После сбора данные мониторинга должны передаваться подсистеме хранения данных мониторинга, которая осуществляет накопление, хранение, архивацию данных. При этом данные мониторинга должны сохраняться достаточно долго и надежно, чтобы при необходимости быть переданными для анализа в подсистему анализа данных мониторинга или же могут быть переданы непосредственно подсистеме анализа данных мониторинга. Такой подход может позволить проводить мониторинг КС как в оффлайн, так и в онлайн-режимах.

В зависимости от места и способа хранения данных могут существенно изменяться требуемый объем памяти для хранения, а также возникать проблемы, связанные с администрированием и обслуживанием, и т.д. Поэтому эта подсистема должна включать в себя средства сжатия данных, работы с базами данных различного типа и т.п. Вместе с тем данные могут быть сохранены локально, в облаке или другом внешнем хранилище и использованы различные способы хранения данных, такие, как: файлы (например, лог-файлы); базы данных и их комбинации [4, 6, 7]. А также для хранения и обработки данных в большом масштабе могут быть использованы такие технологии, как облачное вычисление (Cloud Computing) [9], MapReduce, Hadoop [10].

Следующим этапом обработки данных мониторинга является их анализ, который позволяет извлечь информацию из собранных данных мониторинга и создать новые знания о функционировании КС. Для достижения этих целей должны быть решены такие основные задачи анализа данных, как классификация и кластеризация, нахождение ассоциативных правил, статистических закономерностей, нахождение корреляционного отношения и т.п. Для этого могут быть использованы различные методы интеллектуального анализа данных, в том числе методы слияния данных [11], а также методы извлечения знаний из данных (data mining) [12]. При этом анализ сетевого трафика может быть осуществлен на нескольких абстрактных уровнях: на уровне номера портов, содержимого пакета, потока, заголовка пакета и на уровне бита (т.е. объема трафика). Естественно, на каждом уровне анализируемые характеристики сетевого трафика будут отличаться, например, на уровне пакета сетевой трафик характеризуется размером пакета и временным интервалом между пакетами. А анализ на уровне бита в основном касается количественных характеристик сети, таких, как интенсивность передачи и пропускная способность обмена в каналах связи сети. На уровне

пакета рассматривается процедура прибытия IP-пакетов, т.е. интенсивность их задержки и потери пакетов. В итоге всеобъемлющий и эффективный анализ сетевого трафика позволит решать такие основные задачи мониторинга, как выявление реального состояния КС, идентификация неисправностей, определение приоритетов при формировании полосы пропускания для отдельных трафиков, обеспечение безопасности КС и т.д.

Далее, извлеченная из собранных данных мониторинга информация передается и хранится в подсистеме поддержки принятия решений по управлению сетью. Вместе с тем в этой подсистеме накапливается опыт принятия решений администраторов сетей по управлению КС. На основании извлеченных из данных мониторинга знаний и собранных в подсистеме поддержки принятия решений по управлению сетью администратором сети принимаются соответствующие решения и выполняются определенные конкретные действия.

Подсистема поддержки принятия решений по управлению сетью является информационной системой и представляет из себя интерактивную систему, основанную на программном обеспечении и предназначенную для поддержки лиц, принимающих решения. Эта подсистема позволит администраторам КС из множества альтернативных решений по управлению сетью выбрать одно. При этом процесс принятия решений должен быть автоматизирован, чтобы можно было быстро проанализировать большой объем информации. Это позволит администраторам быстро реагировать на критические ситуации, происходящие в КС, например, при сбое узлов и каналов связи, атаках на безопасность сети и т.д. Фактически, для администраторов КС эта подсистема является средством для мониторинга сети и принятия оперативного решений по управлению сетью.

Создание систем поддержки принятия решений по управлению КС является отдельной областью исследования, и в этой статье не будем ее рассматривать. Однако в литературе имеются различные подходы к созданию систем поддержки принятия решений в той или иной области. Эти системы разделяются на пять типов: системы поддержки принятия решений, управляемые связями; системы поддержки принятия решений, управляемые данными; системы поддержки принятия решений, управляемые документами; системы поддержки принятия решений, управляемые знаниями, и системы поддержки принятия решений, управляемые моделями [13].

Заключение

Масштаб и сложность современных КС, а также требования к самим КС постоянно растут, что усложняет их эффективное управление. Для эффективного управления КС необходимы объективные данные об их состоянии и функционировании, которые могут быть собраны сетевым мониторингом.

В статье для достоверного и эффективного мониторинга КС предложена концептуальная структура системы интеллектуального мониторинга КС, которая является модульной.

Предложенная система мониторинга позволит легко включить новые подсистемы по конкретным аспектам процесса мониторинга, реорганизовать взаимодействие подсистем, а также распределять и интегрировать подсистемы в масштабе КС. Таким образом при необходимости можно масштабировать систему и решить любую задачу по мониторингу КС, что позволит адаптировать систему под любое функциональное и инфраструктурное изменение, происходящее в КС.

Литература

1. Шыхалиев Р.Г. Анализ и классификация сетевого трафика компьютерных сетей // Проблемы информационных технологий, 2010, №2, с.15−23.
2. Шыхалиев Р.Г. О применении интеллектуальных технологий в мониторинге компьютерных сетей // Искусственный интеллект, 2011, №1, с.124−132.
3. Comparison of network monitoring systems.

http://en.wikipedia.org/wiki/Comparison_of_network_monitoring_systems
4. Шыхалиев Р.Г. О методах сбора, хранения и анализа большого сетевого трафика // Проблемы информационных техналогий, 2016, №2, с.56−62.
5. Aceto G., Botta A., and Pescape A. Efficient storage and processing of high-volume network monitoring data // IEEE Transactions on Network and Service Management, 2013, vol. 10, no. 2, pp.162−175.
6. Horneman A., Dell N. Smart collection and storage method for network traffic data. Technical Report CMU/SEI-2014-TR-011, 2014, p.62.
7. Shikhaliyev R.H. On the methods of collecting and storing big network traffic / 10th IEEE International Conference on Application of Information and Communication Technologies (AICT2016), Azerbaijan, Baku, 12−14 October 2016, pp.585−587.
8. Quittek J., Zseby T., Claise B., Zander S. RFC 3917: Requirements for IP Flow Information Export (IPFIX). Internet Engineering Task Force, 2004. http://tools.ietf.org/html/rfc3917.
9. Sivashakthi T. and Prabakaran N. A survey on storage techniques in cloud computing // International Journal of Emerging Technology and Advanced Engineering, 2013, vol. 3, no. 12, pp.125−128.
10. White T. Hadoop: The Definitive Guide. O'Reilly Media, 2015, p.768.
11. Bleiholder J., and Naumann F. Data fusion // ACM Computing Surveys, 2008, vol.41, no.1, pp.1−41.
12. Han J., Kamber M., Data mining concepts and techniques. Morgan Kaufmann, 2006, p.743.
13. Marin G. Decision support systems // Journal of Information Systems & Operations Management, 2008, vol.2, no.2, pp.513−520.

UOT 004.048

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

Kompüter şəbəkələrinin intellektual monitorinqi sisteminin konseptual modeli haqqında

Kompüter şəbəkələrinin (KŞ) effektiv idarə edilməsi onların vəziyyəti və fəaliyyəti haqqında verilənlər olmadan mümkün deyil və bu verilənlər şəbəkə mnitorinqi vasitəsi ilə təmin edilir. KŞ-nin doğru və effektiv monitorinq edilməsi üçün sistem yanaşmasının istifadəsi lazımdır. Məqalədə KŞ-nin intellektual monitorinqi sisteminin konseptual modeli təklif edilmişdir və məqsədi monitorinq verilənlərinin toplanması, saxlanması və analizi, həmçinin şəbəkə idarəetməsi üçün qərarların qəbul edilməsi üçün effektiv infrastrukturun yaradılmasıdır.

Açar sözləri: *kompüter şəbəkələri, şəbəkə monitorinqi, monitorinq verilənləri, intellektual monitorinq sisteminin strukturu.*

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

The conceptual model for the intellectual monitoring system of computer networks

The effective management of computer networks (CN) is impossible without data about their status and function, which is provided by network monitoring. It is necessary to use a systematic approach for reliable and effective monitoring of the CN. The paper proposes a conceptual model of intelligent monitoring system of the CN, which seeks to create an effective infrastructure for collecting, storing and analyzing of monitoring data, as well as making decisions on network management.

Keywords: *computer networks, network monitoring, monitoring data, structure of the intellectual monitoring system.*