УДК 004.042

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

АНАЛИЗ ТЕНДЕНЦИЙ РАЗВИТИЯ МЕТОДОВ МОНИТОРИНГА КОМПЬЮТЕРНЫХ СЕТЕЙ

Сегодня принятие эффективных решений по управлению компьютерными сетями (КС) невозможно без их мониторинга. Мониторинг различных показателей КС позволяет получить необходимую информацию об их состоянии. В работе рассматривается развитие методов мониторинга КС в контексте развития самой КС. Рассмотрены проблемы мониторинга КС в различных аспектах, таких, как построение распределенной архитектуры мониторинга, интеллектуализация методов мониторинга, сбор, хранение и анализ больших объемов сетевых данных, классификация и кластеризация сетевого трафика, визуализация сетевого мониторинга, QoS (Quality of Service) мониторинг, мониторинг Wi-Fi сетей, и кратко изложены существующие подходы к решению этих проблем.

Ключевые слова: *компьютерные сети, мониторинг, распределенная архитектура мониторинга, интеллектуализация методов мониторинга, классификация и кластеризация сетевого трафика, визуализация сетевого мониторинга, QoS мониторинг, мониторинг Wi-Fi сетей.*

Введение

Сегодня компьютерные сети стали одним из важных факторов эффективного функционирования и развития практически всех областей общества. КС представляет собой систему, в которой множество компьютеров соединено друг с другом для обмена информацией и ресурсами. КС и используемые в них сетевые приложения могут повысить производительность работ, проводимых как в государственных, так и в частных организациях. Однако при такой зависимости от КС появляются риски, связанные со сбоем, выходом из строя сетей или их низкой производительностью, нарушения безопасности и т.д. Эти риски могут привести к большому ущербу, как материальному, так и моральному (простаивание сотрудников, потеря репутации и недовольство клиентов и т.д.). Для снижения этих и других рисков необходимо постоянно проводить мониторинг КС.

Мониторинг является очень важным элементом эффективного управления современными 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 выведении агрегированной функции из этих измерений. Эти показатели описывают состояние и производительность сети с точки зрения использования ресурсов, перегрузки, потери пакетов и помогают администраторам выявлять потенциальные проблемы. Вместе с тем, измеряя и анализируя параметры сетевого трафика, может 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 состояние этих объектов и определяются актуальностью и полнотой. К этим объектам можно отнести такие элементы КС, как сетевое оборудование, сетевые соединения, сетевые трафики, сетевые сервисы и пользователи. На различных этапах развития КС осуществлялся мониторинг тех или иных объектов КС. А также на различных этапах развития КС определялись цели и задачи мониторинга и использовались различные методы.

Целью данной статьи является рассмотрение вопросов развития методов мониторинга КС в контексте развития самих КС. Потому что развитие методов мониторинга КС неразрывно связано с развитием самих КС. Вместе с тем в статье проводится анализ существующих концепций и методов мониторинга КС, а также имеющихся в этой области проблем.

Эволюция компьютерных сетей

Прежде чем анализировать развитие мониторинга КС, необходимо провести анализ развития самих КС. Так как анализ развития КС позволит нам понять направления развития их мониторинга, а также определить тенденции и перспективы развития этой области.

Изначально КС были созданы как сети коммутации данных или передачи данных, которые включали в себя результаты развития информационных и телекоммуникационных технологий [2]. Однако современные КС практически являются большим хранилищем постоянно растущей информации. Вместе с тем большое влияние КС, оказываемое на другие типы телекоммуникационных сетей, привело к их конвергенции, и цифровая передача голоса в телефонных сетях была одним из первых этапов этой конвергенции. С конца 1960-х годов в телефонных сетях передача голоса в цифровом формате стала более распространенной. Позднее в КС появились такие новые сервисы, как передача голоса по IP (Internet protocol), радио- и в телепередаче. Вместе с тем процесс конвергенции сетей происходит и сегодня.

Создание многотерминальных систем. КС появились в конце 1960-х годов, и первыми прототипами были многотерминальные системы. В таких системах один центральный компьютер (мэйнфрейм) использовался множеством пользователей. Каждый пользователь из своего собственного терминала мог обращаться к центральному компьютеру. При этом время, необходимое центральному компьютеру для ответа на запрос пользователей, было достаточно малым, чтобы он мог параллельно обслуживать нескольких пользователей. Необходимо подчеркнуть, что такие системы в основном эксплуатировались в вычислительных центрах. Позже терминалы из вычислительных центров переместились на рабочие места организаций. При этом вычисления проводились централизованно, а ввод и вывод данных осуществлялись распределенно. Пользователи могли использовать общие файлы и периферийные устройства, а также в любое время на центральном компьютере запускать любую программу и получать результаты практически мгновенно. При этом было такое ощущение, что все вычисления осуществляются на терминалах, и появление таких систем можно считать первыми шагами в создании локальных вычислительных сетей (ЛВС).

Создание глобальных сетей (ГС). Следующий этап развития КС связан с необходимостью соединения компьютеров, расположенных на большом расстоянии друг от друга, то есть созданием глобальных сетей. При этом основная задача заключалась в обеспечении доступа к центральному компьютеру из терминалов, расположенных за сотни, а иногда и тысячи километров друг от друга. Вместе с тем соединение было обеспечено не только между терминалами и центральными компьютерами, но также и между центральными компьютерами. В результате этого компьютеры стали обмениваться данными в автоматическом режиме и появились первые ГС, которые соединяли географически удаленные компьютеры, то есть компьютеры, находящиеся в разных городах или странах. В таких сетях разработчиками были реализованы такие сервисы, как обмен файлами, синхронизация баз данных, электронная почта и т.д. При этом развитие ГС главным образом зависело от развития телефонных сетей. Вместе с тем необходимо подчеркнуть, что именно при развитии ГС было введено и развито много фундаментальных разработок, которые лежат в основе современных КС, такие, как: многослойная

архитектура протоколов коммуникаций (взаимодействия); технология пакетной коммутации; технология маршрутизации пакетов в гетерогенных сетях и т.д.

Несмотря на то, что ГС унаследовали много свойств от телефонных сетей, впоследствии было решено отказаться от использования технологии коммутации каналов, которая успешно использовалась в телефонных сетях в течение десятилетий. Эксперименты и математическое моделирование, проведенные специалистами, показали, что сети, основанные на коммутации пакетов, в принципе могут более эффективно передавать трафик пакетов. Однако ввиду того, что построение высококачественных коммуникационных линий, соединяющих удаленные узлы, было очень дорого, то в первых ГС часто использовались имеющиеся коммуникационные линии, изначально предназначенные для различных целей. Например, ГС в течение длительного времени были построены на основе телефонных линий. Поэтому скорость передачи цифровых данных с использованием таких связей была довольно низкой и составила сотни килобит в секунду (Kbps). А набор сервисов, предоставляемых такими сетями, был ограничен передачей файлов, которая в основном осуществлялась в фоновом режиме и по электронной почте. В дополнение к низкой скорости передачи данных такие каналы имели еще один недостаток – они существенно искажали передаваемые сигналы. Таким образом, сетевые протоколы ГС, использующие коммуникационные линии низкого качества, характеризовались сложными процедурами управления и восстановления данных, в качестве примера можно показать протокол X.25 [3]. Обычно в таких сетях для подключения компьютеров и коммутаторов использовались низкоскоростные аналоговые каналы.

Создание Интернет. В 1969 году Министерство обороны США начало исследования по подключению к сети компьютеров научно-исследовательских центров. Эта сеть была названа ARPANET (Advanced Research Project Agency Network) [4] и являлась началом построения первой и наиболее широко известной ГС, ныне известной как Интернет. К ARPANET были подключены различные типы компьютеров, использующие различные операционные системы и дополнительные модули для реализации коммуникационных протоколов, общих для всех компьютеров. Эти операционные системы могут быть рассмотрены как первые сетевые операционные системы, которые отличались от многотерминальных тем, что кроме распределения ресурсов сети между пользователями также позволяли проводить распределенную обработку и организовывать хранение данных.

В 1990-х годах началось построение ГС на основе высокоскоростных цифровых каналов, что значительно расширило спектр используемых сервисов, часть из которых была разработана для ЛВС. Из-за использования высокоскоростных каналов стала возможной передача большого количества мультимедийной информации в режиме реального времени, в том числе изображения, видео и голоса. World Wide Web (WWW) [5] – гипертекстовый информационный сервис стал главным информационным сервисом в Интернет.

Создание локальных вычислительных сетей (ЛВС). Следующий этап развития КС связан с созданием ЛВС [6]. В начале 1970-х годов были разработаны большие интегральные схемы, которые имели низкую стоимость и высокие функциональные возможности, что привело к созданию мини-компьютеров. Мини-компьютеры были способны решать задачи гораздо быстрее, чем центральные компьютеры (мэйнфреймы). Из-за относительно низкой стоимости даже небольшие организации могли иметь свои собственные мини-компьютеры. Это было началом концепции распределенных вычислений, при которой вычислительные ресурсы распределялись по всей организации. Вместе с тем все мини-компьютеры организации функционировали самостоятельно. В результате объединения мини-компьютеров организаций в единую сеть были образованы первые ЛВС.

Далее появились персональные компьютеры (ПК), которые стали идеальным элементом ЛВС. Так как они были достаточно мощными, чтобы поддерживать сетевое программное обеспечение. Вместе с тем была возможность объединить их вычислительные

мощности для решения сложных задач и разделить дорогие периферийные устройства и дисковые пространства. Из-за этого ПК стали широко использоваться в ЛВС и играли роль не только клиентов, но также выполняли функции центров хранения и обработки данных. При этом используемые в ЛВС стандартные технологии основывались на том же методе коммутации, который применялся при передаче трафика в ГС, т.е. на методе коммутации пакетов. Таким образом, для построения ЛВС стали использовать стандартные сетевые технологии (например, стандартные сетевые кабели и адаптеры, а также Ethernet [7] технологию и популярную в те времена сетевую операционную систему Novell NetWare [8]). При этом доступ к общим сетевым ресурсам стал значительно проще, и, в отличие от ГС, пользователям не было необходимости запоминать сложные идентификаторы разделяемых ресурсов. На следующих этапах развития КС различия между ЛВС и ГС начали уменьшаться и разработчики сетей стали объединять отдельные ЛВС посредством ГС. В результате такой интеграции произошло значительное взаимопроникновение соответствующих технологий. Кроме того, использование IP также способствовало интеграции ЛВС и ГС.

Сегодня с развитием информационных технологий КС становятся очень сложными, разнообразными и распределенными системами. Это в свою очередь приводит к появлению все новых проблем в их мониторинге. Проблемы мониторинга КС можно рассмотреть в различных аспектах, таких, как построение распределенной архитектуры мониторинга, интеллектуализация методов мониторинга, сбор, хранение и анализ больших объемов сетевых данных, классификация и кластеризация сетевого трафика, визуализация сетевого мониторинга, QoS (Quality of Service) мониторинг, мониторинг Wi-Fi сетей и т.д.

Развитие методов мониторинга компьютерных сетей

Исходя из анализа эволюции развития КС, можно сделать вывод о том, что с развитием КС развивались и методы мониторинга. При этом каждый этап развития КС так или иначе определял цели, задачи и проблемы мониторинга. С ростом сложности КС выросла сложность методов их мониторинга. Например, на начальном этапе эры информатизации для того, чтобы обеспечить непрерывность работы, а также безопасность центральных компьютеров, были необходимы автоматические системы мониторинга, которые контролировали бы их общее использование. Однако такие системы были уязвимы к человеческим ошибкам, которые могли привести к уничтожению системной информации или информации пользователей, а также сохранить контроль над системой после того, как все необходимые вычисления закончились [9].

К концу 60-х годов для мониторинга систем с разделением времени появились как аппаратные системы мониторинга [10], так и программные с графическими интерфейсами [11, 12]. Такие системы мониторинга осуществляли периодический сбор, хранение и обработку некоторых показателей сетей. При этом появились проблемы с выбором наиболее значимых данных и методов их отображения.

С развитием информационных технологий началось широкое использование КС. Вместе с тем появились проблемы с их обслуживанием (администрированием). Это в основном было связано с тем, что не хватало специалистов по информационным технологиям, а также стоимость их услуг была очень высокой. В результате стоимость владения КС было очень высока. Поэтому для анализа данных мониторинга КС начали разрабатывать различные экспертные системы [13, 14]. Эти системы в основном использовали характеристики трафика и сети, информацию о приложениях и значительно облегчили выполнение работы сетевых администраторов по управлению КС.

В 1995 году для осуществления распределенного управления КС IETF (Internet Engineering Task Force) был предложен метод удаленного мониторинга, который назывался Remote MONitoring (RMON) [15]. Суть метода заключалась в использовании мониторов –

устройств, которые осуществляли мониторинг сетевого трафика. Мониторы могли быть реализованы как в виде устройств с вложенными приложениями, так и в виде отдельных устройств. Задачи мониторов заключались в мониторинге сетевого трафика в сегментах сети, в котором они находились, и предупреждении администраторов сетей об аномалиях в виде сигналов тревоги. При этом администраторы сетей посредством определения типов и значений порогов срабатывания сигналов тревоги могли регулировать объем собираемых данных, то есть осуществлять фильтрацию событий, и в результате облегчить процесс принятия решений. Вместе с тем сами мониторы могли выполнять некоторую предварительную обработку данных перед тем, как передавать их администратору сети. Однако при таком подходе мониторинга КС все же основная нагрузка по принятию решений для управления КС лежала на администраторах сетей. Для решения этой задачи был использован искусственный интеллект, а именно интеллектуальные агенты [16, 17], которые могли быть успешно применены для мониторинга сетевого трафика, диагностики неисправностей, контроля перегрузки, доступа и т.д.

Рост использования в КС приложений реального времени, таких, как аудио и видео, а также необходимость добавления веб-функциональности к сетевым приложениям привели к необходимости управления сетями на основе веб. Существенным элементом такого управления является мониторинг трафика. В работе [18] для мониторинга потоков трафика в реальном времени авторы предлагают систему мониторинга трафика на основе CORBA (Common Object Request Broker Architecture) [19]. Такой подход позволяет веб-приложениям управления сетями найти соответствующие мониторы потока трафика в режиме реального времени и извлекать из них информацию о трафике. Эта информация может быть отображена в графическом виде, а также использована для получения дополнительных параметров, связанных с потоками трафика в реальном времени.

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 можно найти описание различных подходов к распределенному мониторингу КС. Например, для распределенного и динамического мониторинга сети были использованы мобильные агенты [20]. В качестве агентов авторы использовали систему IBM Aglets и показали, что как приложение распределенного мониторинга КС основанная Java может эффективно осуществлять сбор и анализ данных и адаптироваться к изменениям характеристик сети. Вместе с тем эффективность осуществления распределенного мониторинга КС зависит от эффективности масштабируемой инфраструктуры мониторинга. Чтобы снизить издержки развертывания такой системы, была предложена оптимальная иерархическая архитектура мониторинга [21], 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 оказывает 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 [22]. Кроме того, для эффективного и масштабируемого распределенного мониторинга КС необходимы эффективные алгоритмы распределенного мониторинга. В работе [23] автором были предложены два алгоритма, которые позволяют снизить коммуникационные издержки. Первый из них был назван DSM (Distributed Subnetwork Monitoring) алгоритмом, который предполагает, 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 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 ищут другие узлы с более доступными ресурсами. Другой подход для распределенной сетевой архитектуры мониторинга предлагается в [24], сутью которого являются децентрализованный сбор и хранение 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 [25].

Сбор и классификация сетевого трафика КС

Большая часть современных исследований в области сбора сетевого трафика посвящена вопросам сбора пакетов в скоростных сетях с минимальной потерей данных и сжатию данных после сбора, то есть снижению объемов. Например, в работах [26, 27] авторы соответственно обсуждают вопросы преобразования данных для их эффективного хранения и обработки и мониторинга в облаке (cloud). В работах [28, 29] авторы предлагают подход к разработке приложений по сбору данных в скоростных сетях, основанный на стандартных аппаратных средствах. А в работе [30] для полного анализа сетевого трафика авторы предлагают метод агрегации потоков. Альтернативой централизованного хранения данных является распределенное хранение данных, однако при таком подходе хранения усложняется процесс анализа данных, а также администрирования и обслуживания. Другим видом распределенного хранения данных можно считать облачное хранение данных [31, 32], которое может также осуществлять и сбор данных.

Использование в современных КС большего количества сетевых сервисов и приложений, аппаратного и программного обеспечения приводит к появлению в сети большого разнообразия трафиков. При этом для проведения эффективного мониторинга и управления КС решение задачи точной идентификации и классификации трафиков относительно сетевых сервисов, приложений и протоколов является очень важным [33]. Потому, что сетевой трафик является одним из важнейших фактических показателей работы КС, то есть трафик является носителем информации о поведении пользователей и функционировании КС.

Идентификация и классификация сетевого трафика особенно важны для решения таких задач, как определение приоритетов при формировании полосы пропускания для отдельных трафиков, установление правил по управлению сетью, обеспечение безопасности сети, диагностический мониторинг КС и т.д. [34]. Например, для того, чтобы обеспечить нормальную работу приложений, важных для корпорации, администратор сети должен идентифицировать и ограничивать (или блокировать) 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 зависят 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, используемых большинством приложений, предсказать невозможно [35]. Поэтому нужны более эффективные методы классификации сетевого трафика, которые позволят 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 [36] 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 [37]. Эта работа положила начало применению методов МО для классификации интернет-трафика.

Визуализация мониторинга КС

Другая проблема мониторинга КС связана с тем, что при непрерывном и быстром поступлении данных в системе мониторинга накапливается большое количество 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 графическом представлении и является эффективным механизмом мониторинга характеристик сетевого трафика. Визуализация сетевых данных является особенно важной для экспресс-оценки состояния сети, она дает возможность администраторам сетей легко и быстро интерпретировать результаты мониторинга. Визуализация сетевых данных также позволяет динамически отобразить 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 [38].

Сегодня для визуализации сетевых данных предлагаются различные методы [39]. При этом общей чертой этих методов является отображение большого объема данных на меньшее пространство. Обычно методы визуализации сетевых данных включают в себя простые линейные графики и диаграммы, которые отображают изменение параметров сетевого трафика. При этом 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. 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 во многих средствах мониторинга, например, в системах мониторинга MRTG [40] и RRDTool [41]. MRTG используется для визуализации использования текущей пропускной способности во времени.

В дополнение к указанным методам были предложены более сложные методы, например, в работе [42] 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, имеющих иерархические отношения.

Мониторинг качества сервисов КС

Сегодня в КС, в частности в сети Интернет, используются множества различных сетевых протоколов, приложений, сервисов и мультимедиа, которые имеют различные требования к QoS (Quality of Service). В таких условиях обеспечение для каждого сетевого приложения, сервиса и мультимедиа требуемого уровня QoS становится серьезной проблемой. Так как QoS имеет комплексный характер, то его количественное определение и гарантированное обеспечение становится делом 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 [43].

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 [44]. Поэтому отсутствие единого стандарта QoS не позволяет должным образом определить QoS сетевых сервисов.

На протяжении более десятка лет было проведено множество исследований и разработаны различные архитектуры, технологии и механизмы QoS [45–48]. Множество исследований и разработок было выполнено IETF (Internet Engineering Task Force), например, IETF RFC 1633 [49], IETF RFC 2430 [50], IETF RFC 2475 [51] 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» [52] и распределенный мониторинг [53]. 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 [54], включающая следующие функциональные компоненты: приложение мониторинга, QoS мониторинг, монитор и объекты мониторинга [55].

Мониторинг Wi-Fi сетей

Появление такой беспроводной технологии подключения к сети, как Wi-Fi (например, IEEE 802.11), и сотовой сети передачи данных (например, 3G/LTE), позволило конечным пользователям иметь легкий доступ к КС (например, к Интернет). Сегодня этим очень широко пользуются. Поэтому вопросы обеспечения хорошего качества соединения пользователей в КС и безопасности приобретают очень важное значение. Однако решение этих вопросов, особенно в крупных КС, становится очень сложным из-за отсутствия адекватных схем мониторинга Wi-Fi сетей. Потому что, в отличие от обычных КС, для которых разработаны множества методов и моделей мониторинга, в Wi-Fi сетях имеются некоторые сложности, связанные с мониторингом. Во-первых, клиенты беспроводных сетей являются мобильными, что делает сложным сбор, хранение и анализ статистических данных каждого клиента. Во-вторых, сложность учета использования ресурсов каналов соединения, например в обычных КС, полоса пропускания канала и скорость передачи фиксированы (т.е. представляются как байты в секундах) и использование ресурсов канала может быть выражено в байтах, но в Wi-Fi сетях полоса пропускания представляется как время (т.е. нано-секунды) и скорость передачи динамически изменяется. Поэтому используя в Wi-Fi сетях мониторинг количества байтов и пакетов, невозможно определить процент используемого ресурса канала передачи в текущее время. В-третьих, ресурсы сети распределяются между различными сервисами и радиоустройствами, которые создают интерференцию, что не позволяет использовать полностью ресурсы сети.

В работе [56] проведено испытание технологий мониторинга и измерения их в используемых крупномасштабных Wi-Fi сетях, и для решения указанных проблем предлагается в модуле MIB (Management Information Base) иметь некоторые статистические счетчики, собирающие информацию, связанную с использованием радиоволн и интерференций.

Некоторые стандарты мониторинга КС

Наряду с методами мониторинга КС в целях обеспечения эффективности мониторинга также были созданы различные стандарты. Эти стандарты описывают свойства, состояние, методы, а также протоколы взаимодействия между объектами КС. В качестве примера стандартов, используемых при мониторинге КС, можно привести такие стандарты, как: Internet Control Message Protocol (ICMP) – протокол управляющих сообщений Internet, используется для определения доступности узлов, анализа различных показателей, определен в RFC (*Request For Comment*) 792 [57]; *Host Monitoring Protocol* (HMP) – протокол для сбора информации с узлов в различных сетях, определен в RFC869 [58]; Simple Network Management Protocol (SNMP) – простой протокол управления сетью, используется для получения информации с узлов сети, определен первоначально в 1988 году в RFC 1067 [59], а затем в качестве стандарта в 1990 году в RFC 1157 [60]; Management Information Base (MIB) – база управляющей информации, содержащая информацию о контролируемых и управляемых параметрах сетевых устройств, определена в RFC1156 [61] и т.д. Вместе с тем, были созданы различные приложения, позволяющие использовать эти протоколы для получения данных из сетевых объектов КС.

Заключение

Невозможно не согласиться с тем, что КС все больше и больше входят в нашу жизнь, с развитием информационных технологий постоянно развиваются и становятся все более масштабными и сложными. При этом появляются проблемы управления КС, и механизмы мониторинга играют решающую роль в их эффективном управлении. Поэтому рассмотрение вопросов мониторинга КС в контексте развития самих КС является актуальным, так как развитие методов мониторинга КС неразрывно связано с развитием

самих КС. В свете этих рассуждений можно с уверенностью сказать, что мониторинг является и будет являться одним из основных условий, способствующих развитию КС. Результаты проведенного анализа тенденций развития методов мониторинга КС позволят выявить проблемы, существующие в этой области, и разработать более эффективные методы.

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. www3.nd.edu/~dwang5/courses/fall15/pdf/evolution.pdf
3. Poulton S., Packet Switching and x.25 networks, Taylor & Francis e-Library, 2003, 236 p.
4. http://en.wikipedia.org/wiki/ARPANET
5. http://en.wikipedia.org/wiki/World_Wide_Web
6. Clark D.D., Pogran K.T. and Reed D.P, An introduction to local area networks // Proceedings of the IEEE, 1978, vol.66, no.11, pp.1497–1517.
7. Boggs D.R. and Metcalfe R.M., Ethernet: Distributed packet switching for local computer networks // Communications of the ACM, 1976, vol.19, no.7, pp.395–404.
8. http://en.wikipedia.org/wiki/NetWare
9. Swift C., Machine Features for a More Automatic Monitoring System on Digital Computers // ACM (JACM), 1957, vol.4, no.2, pp.172–173.
10. Schulman F. Hardware measurement device for IBM system/360 time sharing evaluation / Proceedings of the 22nd national conference ACM Annual Conference/Annual Meeting, 1967, pp.103–109.
11. Grochow J., The graph display as an aid in the monitoring of a time shared computer system. Technical Report: TR-54, 1968.
12. Pikerton T., Performance monitoring in a time-sharing system // Communications of the ACM, November 1969, vol.12, no.11, pp.608–610.
13. Barton B., Switlik J., A real-time expert system for computer network monitor and control / // ACM SIGMIS Database, 1988, vol.19, no.2, pp.35–38.
14. Hitson B., Knowledge-based monitoring and control: an approach to understanding behavior of TCP/IP network protocols // ACM SIGCOMM Computer Communication Review, 1988, vol.18, no.4, pp.210–221.
15. Waldbusser S., Remote Network Monitoring Management Information Base. RFC 1757, Feb. 1995.
16. Cheikhrouhou M. M., Conti P., Labetoulle J., Intelligent Agents in Network Management: A State-of-the-art // Networking and Information Systems, 1998, vol.no.1, pp.9–38.
17. Koch F.L., Westphall C.B., Decentralized Network Management Using Distributed Artificial Intelligence // Network and Systems Management, 2001, vol.9, no.4, pp.375–388.
18. Yuming J., Chen-Khong T., Chi-Chung K., A Web-Based Real-Time Traffic Monitoring Scheme Using CORBA / Proceedings of the 2nd IFIP/IEEE International. Conference on Management of Multimedia Networks and Services, 1998, pp.16–18.
19. www.ois.com/Products/what-is-corba.html
20. 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.
21. 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.

22. 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.
23. Du X., Toward efficient distributed network monitoring / IEEE International Conference on Performance, Computing, and Communications, 2004, pp.87–94.
24. 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.
25. 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.
26. Aceto G., Botta A., Pescape A., Westphal C., 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.
27. Aceto G., Botta A., de Donato W., Pescape A., Cloud Monitoring: A Survey // Computer Networks, 2013, vol.57, no.9, pp.2093–2115.
28. Deri L., Cardigliano A., Fusco F., 10 Gbit Line Rate Packet-to-Disk Using n2disk / Proceedings IEEE INFOCOM, 2013, pp. 3399–3404.
29. Banks D., Custom Full Packet Capture System, SANS, 2013.
30. Francois J., State R., Engel T., Aggregated Representations and Metrics for Scalable Flow Analysis / IEEE Conference on Communications and Network Security (CNS), 2013, pp.478–482.
31. Sivashakthi T., 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.
32. Spoorthy V., Mamatha M., Santhosh Kumar B., A Survey on Data Storage and Security in Cloud Computing // International Journal of Computer Science and Mobile Computing, 2014, vol.3, no.6, pp.306–313.
33. Шыхалиев Р.Г. О применении интеллектуальных технологий в мониторинге компьютерных сетей // Искусственный интеллект, 2011, №1, с.124–132.
34. 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.
35. 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.
36. 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.
37. Frank J., Machine learning and intrusion detection: Current and future directions / Proceedings of the National 17th Computer Security Conference, 1994, pp.22–33.
38. 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. pp.69–70.
39. D.A.Keim, Information Visualization and visual data mining // IEEE Transactions on visualization and computer graphics, 2002, vol.7, no. 1, pp. 100–107.
40. Oetiker T., and Rand D., Multi Router Traffic Grapher. www.mrtg.org.
41. Oetiker T., Round Robin Database Tool. www.rrdtool.org.

42. 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.
43. Шыхалиев Р.Г., О методах мониторинга и управления QoS компьютерных сетей // Проблемы информационных технологий, 2013, № 1, с. 15–23.
44. ITU-T, Support of IP-based services using IP transfer capabilities, Tech. Rep. Rec. Y.1241, 200.
45. Firoiu V. et al., Theories and Models for Internet Quality of Service // Proc. of IEEE, Special issue on Internet Technology, 2002, vol.90, no.9, pp.1565–1591.
46. 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.
47. 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.
48. Aurrecoechea C., Campbell A., and Hauw L., A Survey of QoS Architectures // Multimedia Systems Journal, 1998, vol.6, no.3, pp.138–151.
49. 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
50. 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
51. 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
52. Jiang Y., Tham C.K., Ko C.C., A QoS distribution monitoring scheme for performance management of multimedia networks / Proc. of IEEE GLOBECOM'99, Brazil, Dec. 1999, Vol. 1A, pp. 64–68.
53. 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
54. Stallings W., SNMP, SNMPv2 and RMON: Practical Network Management, 2nd edition, Addison-Wesley, 1996.
55. 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.
56. irtf.org/raim-2015-papers/raim-2015-paper42.pdf
57. Postel J., Internet control message protocol, RFC 792, 1981, http://www.ietf.org/rfc/rfc792.txt
58. Hinden R. M., A Host Monitoring Protocol, RFC 869, 1983, http://tools.ietf.org/html/rfc869
59. Case J., Fedor M., Schoffstall M., Davin J., A Simple Network Management Protocol, RFC 1067, 1988, http://tools.ietf.org/html/rfc1067
60. Case J., Fedor M., Schoffstall M., Davin J., A Simple Network Management Protocol, RFC 1157, 1990, http://www.ietf.org/rfc/rfc1157.txt
61. McCloghrie K., Rose M., Management Information Base for Network Management of TCP/IP-based internets, RFC 1156, 1990, www.ietf.org/rfc/rfc1156.txt

UOT 004.042
Şıxəliyev Ramiz H.
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
ramiz@science.az

Kompüter şəbəkələrinin monitorinqi üsullarının inkişafı meyllərinin analizi

Bu gün kompüter şəbəkələrinin (KŞ) idarə olunması üçün effektiv qərarların qəbul edilməsi onları monitorinq etmədən mümkün deyil. KŞ-lərin müxtəlif göstəricilərinin mönitorinqi onların vəziyyəti haqqında lazımi informasiyanın əldə edilməsinə imkan verir. İşdə KŞ-lərin mönitorinqi üsullarının inkişafına, KŞ-lərin özlərinin inkişafı kontekstində baxılır. KŞ-lərin mönitorinqi problemlərinə monitorinqin paylanmış arxitekturasının yaradılması, monitorinq üsullarının intelletuallaşdırılması, böyük həcmdə şəbəkə verilənlərinin toplanması, saxlanması və analizi, şəbəkə trafikinin klassifikasiyası və klasterizasiyası, şəbəkə monitoriniqinin vizuallaşdırılması, QoS (Quality of Service) monitorinq Wi-Fi şəbəkələrin monitorinqi kimi aspektlərdən baxılmış və bu problemlərin həllərinə mövcud yanaşmalar qısa şərh edilmişdir.

Açar sözlər: *kompüter şəbəkələri, monitorinq, monitorinqin paylanmış arxitekturası, ölçmə və monitorinq üsullarının intelletuallaşdırılması, şəbəkə trafikinin klassifikasiyası və klasterizasiyası, şəbəkə monitoriniqinin vizuallaşdırılması, QoS monitorinq, Wi-Fi şəbəkələrin monitorinqi*.

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

Analysis of development tendencies of monitoring methods of computer networks

Nowadays, effective solutions for the management of computer networks (CNs) are impossible without their monitoring. Monitoring of various parameters of CNs allows obtaining the necessary information about their condition. The paper deals with the development of methods for CN monitoring in the context of the development of CN itself. CN monitoring issues are reviewed from various aspects, such as the construction of a distributed monitoring architecture, intellectualization of monitoring techniques, collection, storage and analysis of large volumes of network data, network traffic classification and clustering, network monitoring visualization, QoS monitoring, Wi-Fi networks monitoring. Available approaches to the problem solution are summarized.

Keywords: *computer networks, monitoring, distributed monitoring architecture, intellectualization of monitoring techniques, network traffic classification and clustering, network monitoring visualization, QoS monitoring, Wi-Fi networks monitoring*.