Концептуальная архитектура интеллектуального мониторинга компьютерных сетей на основе мобильных мульти-агентов

Рамиз Шыхалиев

Институт Информационных Технологий НАНА

ramiz@science.az

***Аннотация*— Данная статья посвящена разработке концептуальной архитектуры интеллектуального мониторинга компьютерных сетей (КС). Для этого используются интеллектуальные мобильные мульти-агенты, каждый из которых осуществляет мониторинг отдельных компонентов КС, таких как сетевое оборудование, сетевые соединения, сетевые трафики, сетевые сервисы и пользователей. Такая архитектура может расширить охват системы мониторинга и обеспечить полноту данных мониторинга КС. А также, архитектура легко масштабируема, так как при необходимости мониторинга новых компонентов могут быть введены новые соответствующие интеллектуальные агенты.**

Ключевые слова— компьютерные сети; сетевой мониторинг; архитектура мониторинга; компоненты КС; интеллектуальные мобильные мульти-агенты

I. Введение

Сегодня наряду с широким применением сетевых технологий, увеличивается сложность и масштаб компьютерных сетей (КС). При этом повышение производительности, качества обслуживания, диагностика неисправностей и обеспечение безопасности сетей стали очень важными задачами. В решении этих задач мониторинг играет очень важную роль и позволяет эффективно управлять КС. Причем, для эффективного управления КС необходимо анализировать данные мониторинга, без чего трудно принять обоснованные решения. При этом практически все события происходящие в КС имеют большое значение в принятии решений и поэтому необходимо осуществить всеобъемлющий мониторинг КС. В результате, эффективность управления КС в большей степени зависить от эффективности мониторинга.

Анализ существующих систем мониторинга показал, что они имеют ряд недостатков. Во первых, они имеют характер централизации, то есть сбор и обработка данных мониторинга осуществляется одним монитором, и мониторинг осуществляется в отношении определенного компонента КС (например, сетевого трафика, сетевых соединений, сетевых сервисов, поведении пользователей и т.д.). Это очень затрудняет сбор, обработку и анализ огромного количества данных, которые должны быть переданы в центр мониторинга. Другим недостатком является то, что для сбора и обработки данных мониторинга не используются интеллектуальные методы, а если используются, то не известно какие методы рассматриваются. Третьим недостатком является то, что при необходимости не возможно расширить функции мониторинга.

Поэтому, для повышения эффективности мониторинга КС актуальным является использование интеллектуальных технологий (ИТ), так как они способны значительно упростить и облегчить процесс мониторинга КС. Кроме того, использование ИТ позволяет минимизировать роль человека при мониторинге КС, уменьшить потери нужной информации, минимизировать влияние мониторинговой системы на нормальную работу КС и т. д. [1]

Основной целью данной статьи является разработка архитектуры мониторинга КС с использованием элементов искуственного интеллекта. А именно, для интеллектуального мониторинга КС предлагается архитектура основанная на интеллектуальных мобильных мульти-агентах. Так как, имеющиеся архитектуры мониторинга КС не эффективны в условиях динамически изменяющихся особенностей трафика и топологии современных сетей. Вместе с тем, архитектуры централизованного мониторинга имеют проблемы с масштабируемости, а статические распределенные иерархические архитектуры мониторинга имеют проблемы с гибкостью и производительностью.

Парадигма мобильных агентов (МА) возникла в области распределенных вычислительний. Они являются самостоятельными программами, которые для решения данных задач могут перемещаться по сети от одного хоста к другому и возобновить или перезапустить выполнение своей работы, а также действовать от имени пользователей [2]. Таким образом, МА являются мобильными, автономными, реактивными и коммуникативными субъектами. Интеллект агентов может включать в себя способность к обучению, адаптации, анализирования и принятия решений, планировать и осуществлять сложные задачи, которые включают в себя сотрудничество с другими агентами или пользователями, возможность передвижения по сети и выполнять поставленные задачи на каждой запланированной точке остановки и т.д.

II. Обзор литературы

Как известно, сегодня сетевая среда КС очень изменилась, так как, в них совместно используюся множество различных сетевых сервисов, аппаратных и программных обеспечений, разработанных различными производителями, а так же происходило многократное увеличение количество пользователей. Конечно, такое изменение привело к повышению вероятности появления в сети различных проблем и усложнению мониторинга КС.

В литературе имеются различные подходы построения системы мониторинга КС. При этом имеющеюся архитектуры мониторинга не могут обеспечить полноту данных мониторинга, чтобы выявить и оценить всевозможные проблемы происходящие в КС. Так как, эти архитектуры направлены на мониторинг определенного аспекта функционирования КС (например, безопасности, производительности и т.д.) [3, 4] и одного определенного компонента КС (например, сетевого оборудования, сетевого трафика, сетевых сервисов, пользователей и т.д.)

В работе [5] для обеспечеия отказоустойчивости и безопасности сервисов КС (например, финансовых, коммерческих и других корпоративных сервисов) авторами была предложена архитектура мониторинга SLA (Service Level Agreement). Отказ сервисов указанных в SLA может привести к значительным убыткам и поэтому необходимо ровести их мониторинг. Вместе с тем, предложенная авторами архитектура позволяет определять стратегию управления отказоустойчивостью сети. В работе [6] авторами предложена архитектура «конец в конец» мониторинга сети по требованию, названная как gd2. Предложенная архитектура позволяет провести динамический мониторинг производительности Grid среды и решить проблему масштабируемости вводимой Grid средой. Тогда как, имеющиеся известные системы мониторинга не способны провести мониторинг производительности сети в режиме реального времени. В работе [7] авторами предложена архитектура распределенной системы активного мониторинга сетей. на основе мобильных агентов (МА). Так как, распределенные системы мониторинга КС основанные на протоколе управления сетью, как SNMP (Simple Network Management Protocol) или распределенных объектных технологий, как CORBA (Common Object Request Broker Architecture) не могут решить с проблему масштабируемости системы. Они также не очень хорошо подходят для мониторинга больших и динамичных систем, какой является КС. Вместе с тем, несмотря на то, что системы мониторинга являются распределенными, принцип их функционирования предопределен при разработке. В системе мониторинга предложенной авторами агенты действуют как мониторы определенных сегментов сети и не связаны с какими-либо конкретными сетевыми узлами, а также могут перемещаться для достижения оптимального местоположения. По существу, МА являются автономными объектами, предназначенными для выполнения конкретных задач и могут перемещаться от узла к узлу сети.

В работах [8] и [9] предложены архитектуры для мониторинга высокоскоростных сетей. В частности, в первой работе авторами предложена, так называемая HISTORY (High Speed Network Monitoring and Analysis) архитектура, которая предназначена для мониторинга высокоскоростных сетей. Этот подход основывается на высокоскоростном мониторинге, который позволяет обрабатывать до одного гигабита в секунду. Архитектура мониторинга опирается на стандарные протоколы, такие как IPFIX (Internet Protocol Flow Information Export) и PSAMP (Packet Sampling Protocol), которые используются для передачи данных мониторинга между элементами мониторинга и последующего анализа трафика. А во второй работе авторами предложена архитектура (так называемая NG-MON ((Next Generation MONintoring)) для мониторинга высокоскоростных (10 Gbps и высше) сетей. NG-MON использует пассивный мктод мониторига и в нем используются как посследовательная, так и параллельная обработка пакетов трафика, что намного снижает потери пакетов. Кроме того такой подход обработки пакетов использует небольшой и фиксированный обьем диского пространства для каждого потока, так как обьем памяти линейно зависим от скорости.

III. Методы мониторинга компьютерных сетей

В литературе имеются различные методы мониторинга КС, такие как централизованый и распределенный мониторинг [10]. При централизованном мониторинге единственный мониторинговый сервер непосредственно осуществляет мониторинг всей системы (рис.1). При этом мониторинг сервер осуществляет сбор, агрегацию и обработку сетевых данных. Централизованный метод мониторинга в основном используется для мониторинга и управления относительно небольших сетей и при этом используется SNMP протокол. Однако такой метод монитогринга имеет некоторые недостатки, такие как низкая эффективность и точность, отсутствие масштабируемости и т.д. Сбор и обработка большого количества сетевых данных в одной точке приводит к перегрузке самого центра мониторинга и сетевых коммуникаций. В результате ограничивается количество элементов сети, в отнешении которых может быть проведен мониторинг, а также снижается скорость поступления данных в центр мониторинга. Кроме того, SNMP протокол постоянно использует поллинг, что приводит к генерации дополнительного трафика, даже если в сети не происходит никаких существенных изменений.

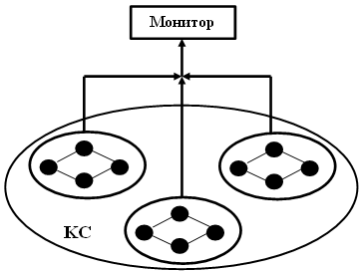

Рис.1. Централизованный мониторинг компьютерных сетей

Распределенный метод мониторинга позволяет повысить производительность и масштабируемость системы мрниторига (рис.2). Этот метод в основном используется для мониторинга и управления больших сетей. Распределенные системы мониторинга имеют иерархическую архитектуру, которая состоит из нескольких мониторов, один из которых выступает в качестве основного, а другие функционируют как мониторы отдельных сегментов сети или подсетей и собирают данных мониторинга элементов сегментов. При этом функции мониторинга распределяются между центральным и распределенными мониторами.

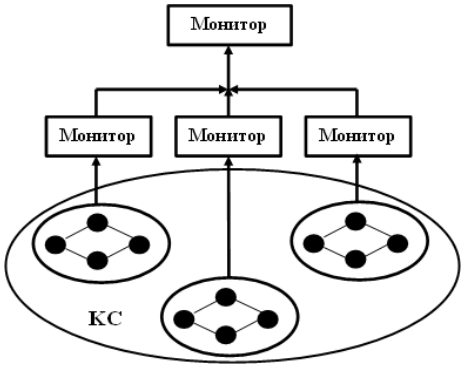

Рис.2. Распределенный мониторинг компьютерных сетей

Основным недостатком рапределенного мониторинга является то, что распределенные мониторы функционируют в определенных сегментах сети или подсетях и не могут адаптироваться к изменениям происходящим в КС. Таким образом, несмотря на то, что распределенные системы мониторинга позволяют решать проблемы производительности, масштабируемости и т.д., они не эффективны в часто изменяющихся динамических средах. Поэтому, в данной работе предлагается архитектура мониторинга КС, в которой в качестве распределенных мониторов используются интеллектуальные мобиьлные мульти-агенты, что на наш взгляд может позволить решить эту проблему.

IV. Многослойное представление взаимодействия компонентов компьютерных сетей

Для того, чтобы осуществить всеобъемлющий и эффективный мониторинг КС необходимо разработать архитектуру монитиоринга, которая позволить провести мониторинг таких основных компонентов, как сетевое оборудование, сетевые соединения, сетевые трафики, сетевые сервисы, пользователи и т.д. При этом такая архитектура мониторинга позволить выявить и оценить всевозможные проблемы происходящие в КС. Однако, прежде чем определить архитектуру мониторинга КС, для ясности взаимодействия основных компонентов КС, представим ее в виде пирамиды состоящей из взаимодействующих слоев-компонентов (рис.3).

В основании пирамиды, показанной на рисунке 3, лежит слой сетевое оборудование, к которому относятся компьютеры и сетевое коммуникационное оборудование. В этом слое происходит обработка и хранения информации, а также передача пакетов информации между компьютерами. На следующем уровне лежит слой сетевых трафиков, которые состоят из потоков пакетов информации передаваемых между компьютерами и Интернетом. Над слоем сетевых трафиков лежит слой сетевых соединений, которые имеются в сетевых трафиках. Следующий слой состоит из сетевых сервисов, которые инициируют эти сетевые соединения и генерируют сетевые трафики. Наконец на самом верхном уровне КС лежит слой пользователей которые используют эти сетевые сервисы.

Рис.3. Многослойное представление основных компонентов компьютерных сетей

V. Архитектура мониторинга компьютерных сетей

В этом разделе, для осуществления всеобъемлющего мониторинга КС предлагается концептуальная архитектура мониторинга основанная на интеллектуальных мобильных мульти-агентнах (рис.4). При этом, процесс функционирования МА заключается в следующем [1]. Изначально программный модуль МА создаются и хранятся на отдельном компьютере, так называемой исходной машине (home machine). Далее агент отправляется на удаленный компьютер, так называемый хост МА, для выполнения. Хост МА также называют сервером МА. Вместе с агентом хосту отправляют весь код МА и информацию о состоянии МА. Хост предоставляет агенту подходящую среду для выполнения. При этом, для выполнения своей задачи, МА используют ресурсы хоста (ресурсы центрального процессора, память и т.д.). После завершения своей задачи на хосте МА переходят на другой компьютер и миграция МА продолжается до тех пор, пока МА не возвратится к исходной машине после завершения выполнения задачи на последней машине в маршруте.

Предложенная концептуальная архитектруа мониторинга является многослойной и охватывает такие основные компоненты КС, как сетевое оборудование, сетевые соединения, сетевые трафики, сетевые сервисы и пользователей. Для мониторинга каждого элемента КС используется отдельный интеллектуальный агент, то есть агент мониторинга сетевого оборудования, агент мониторинга сетевых соединений, агент мониторинга сетевых трафиков, агент мониторинга сетевых сервисов, агент мониторинга поведения пользователей. При этом каждый агент использует различный протокол мониторинга. В этой архитектуре, интерфейс агент

является мостом между администраторои и агентами, который передает запросы администратора к агентам и представляет результаты мониторинга администратору.

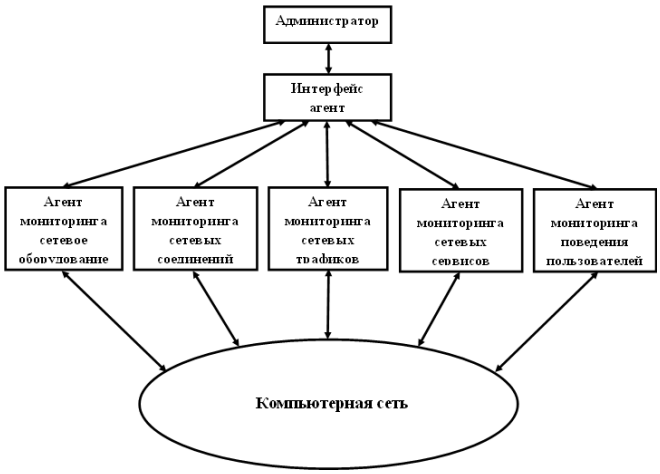

Рис.4. Концептуальная архитектура интеллектуального мониторинга КС

Преимуществами данной архитектуры являются то, что может быть расширен охват системы мониторинга и обеспечена полнота данных мониторинга КС. Кроме того, из-за интеллектуальности и гибкости МА, возможно быстрое принятие эффективных решений по мониторингу и управлению сетью. А также, система легко масштабируема, так как при необходимости мониторинга новых компонентов могут быть введены новые интеллектуальные агенты. Например, для того чтобы осуществить монитогринг безопасности КС нужно вводить в систему агент беопасности [11].

Заключение

В этой статье предлагается концептуальная архитектура интеллектуального мониторинга КС основанная на использовании мобильных мульти-агентов. Предложенная архитектура является многоуровневой. Каждый уровень представляет различные компоненты КС, такие как сетевое оборудование, сетевые соединения, сетевые трафики, сетевые сервисы и пользователей.

Архитектуры существующих систем мониторинга в основном имеют характер централизации, и мониторинг осуществляется в отношении определенного компонента КС, например, сетевого трафика, сетевых соединений, сетевых сервисов, поведения пользователей и т.д. Такие архитектуры мониторинга КС не эффективны в условиях динамически изменяющихся особенностей трафика и топологии современных сетей, кроме того появляются проблемы с масштабируемости системы мониторинга.

Предложенная архитектура может расширить охват системы мониторинга КС и обеспечить полноту данных мониторинга. А также, архитектура легко масштабируема, так как при необходимости мониторинга новых компонентов могут быть введены новые интеллектуальные агенты. Вместе с тем, из-за интеллектуальности и гибкости МА, возможно быстрое принятие эффективных решений по мониторингу и управлению сетью.

Благодарность

Данная работа выполнена при финансовой поддержке Фонда Развития Науки при Президенте Азербайджанской Республики – Грант № EİF-RİTN-MQM-2/İKT-2-2013-7(13)-29/27/1.

Литература

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

[2] D. Gavalas, D. Greenwood, G. M. O’Mahony M., “Hierarchical network management: A scalable and dynamic mobile agent-based approach,” Computer Networks, vol. 38 pp. 693-711, 2002.

[3] M. Ambika, R. V. Nataraj, “Architecture for real time monitoring and modeling of network behavior for enhanced security,” International Journal of Computer Applications, vol. 64, no.8, pp. 21-25, 2013.

[4] A. Phipps, “:Network performance monitoring architecture.” Technical Report EGEE-JRA4-TEC-606702-NPM NMWG Model Design, JRA4 Design Team, 2005.

[5] N. H. Shirazi, A. Schaeffer-Filho, D. Hutchison, “Service level agreement monitoring for resilience in computer networks,” 13th Annual Post Graduate Symposium on The Convergence of Telecommunications, Networking and Broadcasting. Liverpool John Moores University, 2012.

[6] A. Ciuffoletti, Y. Marchetti, A. Papadogiannakis, M. Polychronakis, “Prototype implementation of a demand driven network monitoring architecture,” Grid Computing - Achievements and Prospects. Springer, pp. 85-97, 2008.

[7] A. Liotta, G. Pavlou, G. Knight, “Exploiting agent mobility for large scale network monitoring,” IEEE Network, Special Issue on Applicability of Mobile Agents to Telecommunications, vol. 16, no. 3, pp. 7-15, 2002.

[8] Dressler F., Carle G., “HISTORY - High Speed Network Monitoring and Analysis,” 24th IEEE Conference on Computer Communications, Poster Session, 2005.

[9] Se-Hee Han, Myung-Sup Kim, Hong-Tack Ju, James Won-Ki Hong, “The Architecture of NG-MON: A passive network monitoring system for high-speed IP networks,” Lecture Notes in Computer Science, vol. 2506, pp.16-27, 2002.

[10] A. Liotta, G. Pavlou, “Exploiting agent mobility for large-scale network monitoring,” IEEE Network, vol. 16 issue 3, pp. 7-15, 2002.

[11] N. T. Nguyen et al, “A Multi-agent System for Computer Network Security Monitoring,” Proc. of the 2nd KES International Symposium on Agent and Multi-Agent Systems: Technologies and Applications, pp.842-849, 2008.