Об одном подходе к интеллектуальному активному мониторингу компьютерных сетей

Рамиз Шихалиев

Институт Информационных Технологий НАН Азербайджана

ramiz@science.az

***Аннотация*— В данной статье предлагается архитектура интеллектуального активного мониторинга компьютерных сетей (КС). Для интеллектуализации процесса мониторинга, совместно с активным монитором, который основывается на опросе сетевых узлов, предлагается использовать экспертную систему реального времени. В результате экспертная система позволит изменить дисциплину опроса узлов КС, то есть интеллектуально управлять списком опрашиваемых устройств, частотой, длительностью и параметрами опроса узлов КС. В целом, эта архитектура позволит оптимизировать активный мониторинг КС за счет уменьшения мониторингового трафика.**

Ключевые слова— компбютерные сети; интеллектуальный активный мониторинг; опрос узлов; экспертные системы реального времени

I. ВВЕДЕНИЕ

Непрерывно растущая сложность современных компьютерных сетей (КС) увеличивает потребность в их постоянном активном мониторинге. При этом, активный мониторинг КС заключается в измерении характеристик сетевых узлов и каналов связи и позволяет контролировать ключевые рабочие параметры сети, значения которых могут быть получены посредством опроса узлов в режиме реального времени. Активный мониторинг КС может быть смоделирован как система опроса сетевых узлов.

Как правило, активный мониторинг осуществляется только в отношении основных (или критических) сетевых узлов [1], к которым относятся серверы, маршрутизаторы, коммутаторы, хабы и межсетевые экраны. Кроме основных сетевых узлов при необходимости также может быть осуществлен мониторинг и других сетевых узлов, например, рабочих станций, терминалов и т.д. Конечно, самой лучшей стратегией активного мониторинга КС был бы постоянный периодический опрос всех ее узлов. Однако, основным недостатком такого подхода является значительно большой процент использования сетевых ресурсов КС (например, полосы пропускания), так как в этом случае сам процесс мониторинга может генерировать большой служебный трафик и потреблять огромные системные ресурсы, что может привести к нарушению работы КС, а также повлиять на результаты мониторинга. Поэтому такой подход к мониторингу является неприемлемым, особеннно при больших размерах КС, так как при этом увеличивается потребность к полосе пропускания и другим ресурсам сети (например, к памяти, процессорным ресурсам и т.п.).

Исходя из вышесказанного можно сказать, что необходимо разработать новый подход к активному мониторингу, основанному на опросе узлов КС с использованием элементов искусственного интеллекта. При этом, применение элементов искусственного интеллекта позволит снизить объем служебных трафиков и потребление системных ресурсов, что может повысить эффективность мониторинга. Это связано с тем, что интеллектуальный опрос узлов КС позволит интеллектуально управлять списком опрашиваемых узлов, частотой и длительностью опроса и определит параметры опроса узлов. Кроме того, интеллектуальный опрос узлов КС позволит при ограниченных сетевых ресурсах оптимизировать частототу, длительность и параметры опроса узлов. При этом, можно интеллектуально определить для каждого узла сети частоту, длительнсть и параметры опроса, и таким образом, интеллектуализация опроса узлов КС позволит сетевым администраторам с минимальным использованием сетевых ресурсов осуществить эффективный мониторинг КС и принимать более обоснованные решения по ее управлению.

В статье проводится анализ проблем активного мониторинга КС, предлагается архитектура интеллектуального активного мониторинга КС, целью которой является минимизация использования сетевых ресурсов КС. Для достижения интеллектуализации процесса активного мониторинга КС предлагается совместно с активным монитором использовать эксперную систему реального времени. Экпертные системы реального времени – это он-лайн системы основанные на знаниях, которые сочетают аналитические модели процессов управления с обычными процессами управления. Вместе с тем, при оценке текущих событий и планов надлежащих мер, учитывается информация о прошлом, настоящем и будущем управляемой системы.

II. СВЯЗАННЫЕ РАБОТЫ

При активном мониторинге состояние КС может быть определено регулярным опросом ключевых параметров ее узлов. Однако, проведение эффективного активного мониторинга КС (особенно больших КС) на основе опроса с минимальным использованием системных ресурсов является проблемой. Для решения этой проблемы в различных работах были предложены различные подходы. Например, для того чтобы оптимизировать мониторинг КС в работе [2] управление частотой опроса узлов КС осуществляется на основе значений установленного порога или предыдущих измерений параметров. Необходимость оптимизации мониторинга также рассмотрена в работе [3], в которой определены проблемы мониторинга, для решения которых предложены эффективные алгоритмы. Однако несмотря на классификацию проблем мониторинга сети, для снижения служебного трафика в предложенных алгоритмах не учитывается стратегия опроса узлов сети. Также в работе [4] были предложены способы для

снижения служебного трафика динамического опроса узлов основанные на управлении частотой опроса. Однако, в этой работе не рассматриваются вопросы оптимизации потребления сетевых ресурсов. В работе [5] рассмотрена задача оптимизации системы распределенного опроса узлов сети, целью которой является определение минимального количества узлов на которых размещаются системы запроса, так что пропускная способность для каждого сетевого соединения была бы максимальной. Однако эта задача оптимизации является NP-трудной, и авторами был предложен эвристический подход для ее решения. Вместе с тем, при таком подходе также необходимо минимизировать ресурсы используемые для мониторинга.

Несмотря на то, что предложенные выше методы могут оптимизировать мониторинг КС и при опросе узлов КС в определенных сценариях снизить размер служебного трафика и используемых системных ресурсов, они не имеют интеллектуальных возможностей выбора дисциплины опроса узлов при активном мониторинге КС. Исходя их этого, для интеллектуализации активного мониторинга КС целесообразно совместно с активным монитором использовать эксперную систему реального времени.

В работах [6, 7, 8, 9] были даны различные подходы к управлению и мониторингу КС на основе экспертных систем. В результате анализа этих работ, для интеллектуализации активного мониторинга КС предлагается использовать эксперную систему реального времени.

Большинство современных экспертных систем реального времени представляет собой графическую объектно-ориентированную среду разработки для приложений реального времени. Они позволяют на структурированном естественном языке создать различные правила, аналитические выражения, функции и процедуры, а также механизмы вывода, которые контролируют выполнение правил в базе знаний.

III. АРХИТЕКТУРА ИНТЕЛЛЕКТУАЛЬНОГО АКТИВНОГО МОНИТОРИНГА КОМПЬЮТЕРНЫХ СЕТЕЙ

Как правило, для принятия эффективных решений по управлению КС в режиме реального времени, используется активный мониторинг, который заключается в опросе текущего состояния узлов КС. При этом частота, длительность, параметры опроса узлов и список опрашиваемых узлов определятся задачей мониторинга.

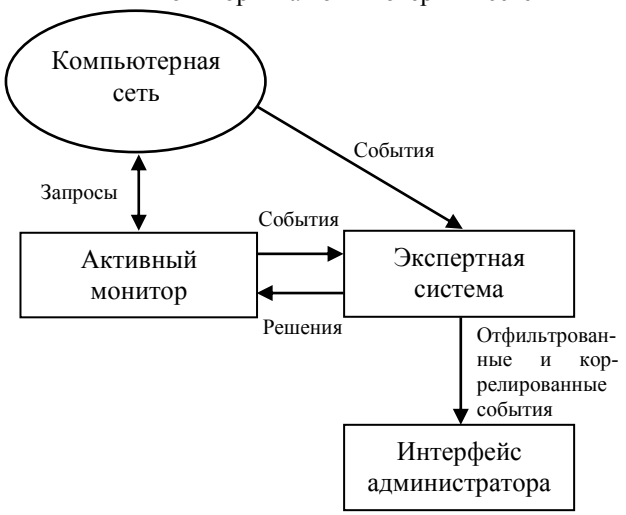
Обычно активный мониторинг осуществляется с помощью ICMP (Internet Control Message Protocol) и SNMP (Simple Network Management Protocol) протоколов, которые позволяют опрашивать сетевые узлы КС. При этом, опрос узлов КС представляет собой процесс, в котором система опроса посылает запросы к сетевым узлам, чтобы получить информацию об их состоянии. Как правило, опрос проводится периодически с фиксированной частотой определяемой временным окном, в котором могут быть обнаружены неисправности и на основе определения корректности ответа сетевых узлов на стандартные запросы администраторы сетей могут определить их состояние.

Обычно, в системах опроса узлов КС используются простые ICMP-ping тесты и SNMP-опросы, где ICMP-ping применяются для опроса состояния сетевых устройств и определения их доступности, а SNMP-опрос используется для определения производительности устройств в сети. Использование SNMP для управления и мониторинга сети широко обсуждалось в работах [10, 11]. Вместе с тем, наличие связи с удаленными узлами и характеристики каналов связи могут быть проверены путем ввода в КС стандартных тестовых пакетов (например, пакетов traceroute, pathcharu и т.п.). С помощью опроса узлов могут быть получены текущие параметры узлов, а также QoS (Quality of Service) параметры, показатели производительности, такие как потери, флуктуация, задержка, пропускная способность, информация о свободной памяти, загрузке процессора и характеристики каналов связи и сетевого трафика и т.д.

Несмотря на то, что активный мониторинг служит для повышения производительности КС, однако опрос узлов может привести к снижению ее производительности, если не эффективно использовать сетевые ресурсы. Так как, частый опрос узлов КС может привести к использованию больших сетевых ресурсов. Однако, с другой стороны, редкий опрос узлов КС может привести к снижению точности определения состояния узлов сети, а в целом – состояния КС. Обычно не известно, какой узел и с какой частотой должен быть опрошен. Поэтому, для оптимизации частоты опроса узлов КС предлагается совместно с системой опроса использовать экспертную систему, которая не только контролирует трафик опроса, а также в соответствии с изменением производительности сети может определить дисциплину опроса.

На рисунке 1 показана архитектура интеллектуального активного мониторинга КС. Эта архитектура состоит из следующих основных компонентов: активного монитора, экспертной системы и интерфейса администратора.

Рис.1. Архитектура интеллектуального активного мониторинга компьютерных сетей



Вместе с тем, дополнительная интеллектуальность может быть в эксперт агентах, однако для простоты здесь они не показаны и не обсуждаются. Рассматривается только экспертная система, хотя они часто используются вместе.

Активный монитор – это компонент, который периодически опрашивает состояние всех узлов КС

(например, с помощью SNMP-запросов) и осуществляет сбор ключевых параметров узлов КС. При этом активный монитор тесно интегрирован с экспертной системой и вся информация о мониторинге передается ей.

Активный монитор на основе предварительного анализа может определить являются ли те или иные ситуации аномальными (например, превышается определенные пороги) и генерировать предупреждения об этом, а также о том, что запросы не доходят до тех или иных узлов. Если активным монитором определяется аномальная ситуация, то информация об этом передается в экспертную систему. Однако следует отметить, на основе окончательного анализа этой информации, экспертной системой принимается решение об аномальности тех или иных ситуаций. В результате этого, экспертна система может вносить изменения в список опрашиваемых устройств, частоту, параметры и длительности опроса узлов КС. При этом из-за того, что в активном мониторе осуществляется предварительный анализ параметров узлов сети, то снижаются нагрузки на экспертную систему и в итоге повышается производительность системы в целом.

Экспертная система является ключевым компонентом интеллектуализации активного мониторинга КС. В предложенной архитектуре целесообразно использовать эксперную систему реального времени, которая подробно обсуждается в работах [12, 13, 14, 15].

События генерируемые активным монитором и полученные непосредственно от КС фильтруются и коррелируются экспертной системой. При этом, экспертная система является единственной точкой где все события о КС собираются, фильтруются и коррелируются. Затем, только отфильтрованные и коррелированные события передаются к интерфейсу администратора, и отношение отфильтрованных событий к необработанным событиям зависит от сложности экспертной системы. Также, сложность экспертной системы определяется качеством информации предоставляемой администратору сети.

Экспертные системы также должны быть способны обрабатывать правила, процедуры и быть орентированными на пользователя. Кроме того, экспертные системы должны иметь стандартный интерфейс для обмена данными с другими системами.

Существуют некоторые стандартные интерфейсы основанные на SNMP, TCP/IP, HTTP (Hyper-Text Transmission Protocol), JavaRMI (Remote Method Invocation) и CORBA (Common Object Request Broker Architecture), которые используются в экспертных системах.

Интерфейс администратора обычно состоит из настраиваемого графического интерфейса, который позволяет администратору представить состояние сети. Основным компонентом интерфейса администратора является топологическая карта сети, которая представляет соединения сетевых компонентов КС.

ЗАКЛЮЧЕНИЕ

Растущая сложность современных КС и предоставляемых ими услуг увеличивает потребность в их активном мониторинге. Активный мониторинг КС осуществляется для того, чтобы определить и гарантировать то, что сеть работает в пределах необходимых параметров. При этом, активный мониторинг заключается в измерении параметров сетевых узлов и осуществляется на основе их периодического опроса. Однако проведение такого мониторинга вносит в сеть ненужный избыточный трафик, который снижает общую эффективность мониторинга.

В статье анализируется проблема минимизации ненужного избыточного трафика при активном мониторинге КС. Для решения этой проблемы предлагается архитектура интеллектуального активного мониторинга КС. При этом, для достижения интеллектуальности процесса активного мониторинга предлагается совместно с активным монитором использовать эксперную систему реального времени, которая позволит минимизировать ненужный избыточный трафик и в результате минимизировать использование сетевых ресурсов КС. Использование экспертной системы позволит интеллектуально управлять списком опрашиваемых устройств, частотой, длительностью и параметрами опроса узлов КС.

БИБЛИОГРАФИЯ

[1] Ed Wilson, Network Monitoring and Analysis. A Protocol Approach to Troubleshooting, Prentice Hall PRT 2000, 350 pp.

[2] Gao, F., Gutierrez, J., A Trade-off Analysis Model: Towards Improving Polling Efficiency on Network Monitoring Problem, In Proc. of the eighth IEEE International Conference on Communication Systems, Vol.1, 2002, pp. 363- 367.

[3] Jiao, J., Naqvi, S., Raz, D., Sugla, B., Toward efficient Monitoring. IEEE Journal on Selected Areas in Communications (JSAC), special issue on recent advances in network management and operations Vol. 18, Issue: 5, 2000, pp. 723-732.

[4] K. Yoshihara, K. Sugiyama, H. Horiuchi, and S. Obana. Dynamic polling scheme based on time variation of network management information values. In Proc. of Integrated Network Management Symposium (IM 99), Boston, May 1999, pp. 141-154.

[5] Li, L., Thottan, M., Yao, B., Paul, S. (2003). Distributed Network Monitoring with Bounded Link Utilization in IP Networks, In Proc. of IEEE INFOCOM.

[6] Pedro Casas, Johan Mazel and Philippe Owezarski, Knowledge-Independent Traffic Monitoring: Unsupervised Detection of Network Attacks, IEEE Network Magazine, Vol. 26, Issue: 1, 2012, pp. 13-21.

[7] Rabie, S., Rau-Chaplin, A., and Shibahara, T., DAD: A Real-Time Expert System for Monitoring Data Packet Networks, IEEE Network Magazine, Vol. 2,, Issue: 5 1988, pp. 29-34.

[8] Bruce L. Hitson, Knowledge-based monitoring and control: an approach to understanding behavior of TCP/IP network protocols, The Proceeding SIGCOMM '88 Symposium proceedings on Communications architectures and protocols, 1988, pp. 210-221

[9] Robert Mathonet, Herwig Van Cotthem, and Leon Vanryckeghem. DANTES:An expert system for real-time network troubleshooting. In Intl. Joint Conference on Artificial Intelligence, 1987, pp. 527-530.

[10] Rose, M. and McCloghrie, K., How to manage your Network using SNMP: the network management practicum, Prentice Hall 1995, 576 pp.

[11] Stallings, W., SNMP, SNMPv2, and CMIP: the practical guide to network management standards, Addison-Wesley,1993, 613 pp.

[12] Amardeep Singh, Monika Verma, Real Time Expert System - Its Applications Polling engines, IJCSI Vol.1, Issue 2, 2010, pp. 150-.153.

[13] R. Moore, H. Rosenof, and G. Stanley, Process Control Using A Real Time Expert System, Proc. IFAC, Estonia, USSR, 1990, pp. 234-239.

[14] R L Ennis, J H Griesmer and others, A continuous real-time expert system for computer operations, IBM Journal of Research and Development, Vol. 30, Issue 1, 1986, pp. 14 – 28.

[15] http://projekter.aau.dk/projekter/files/45195788/main.pdf.