ПОИСК АНОМАЛИЙ ПРИ ПРОВЕДЕНИИ РАСПРЕДЕЛЕННЫХ РАСЧЕТОВ В СИСТЕМЕ МЕТАКОМПЬЮТИНГА X-COM

Ю.А. Жолудев

Введение

Для распределенных вычислительных систем, построенных с помощью инструментария X-Com[1], ввиду их неоднородности, динамичности и масштабности, актуальна задача обнаружения различного рода неполадок и вмешательств при проведения расчетов. Участвующих в расчете клиентов X-Com может быть много, в то время как данные, которые можно от них получить централизованно на сервере, содержат в себе минимум служебной информации; при этом необходимы внешние средства анализа, основанные на шаблонном поведении компонентов среды.

В настоящей работе рассматривается один из подходов к анализу активности клиентов X-Com [1] с целью выявления функционирующих неверно или показывающих характерную для вредоносного вмешательства активность.

Задача анализа активности клиентов

В базовой конфигурации [2] среди компонентов распределенной вычислительно среды выделяются сервер задачи и клиент. Ответственностью сервера задачи является обработка следующих запросов клиентов:

- TSR — запрос на получение описания задачи. Клиент в запросе отправляет данные о программно-аппаратных характеристиках своего вычислительного узла, в ответ клиент получает идентификатор сессии, сохраняющийся за клиентом на все время его участия в расчете, и описание задачи, содержащее в себе список необходимых для участия в расчете файлов прикладной задачи.
- TFILE и DFILE — запросы на загрузку файлов задачи (исполняемая часть и файлы данных).
- REQ — запрос на получение порции данных для обработки. При получении REQ-запроса сервер X-Com посредством серверной части прикладной задаи готовит порцию данных и отправляет её клиенту.
- ASW — запрос на отправку результатов обработки порции данных.

  Задачей клиента в распределенной среде является получение порции данных от сервера, их обработка с помощью клиентской части задачи и отсылка полученных результатов серверу задачи. Порции данных и соответствующие им порции результатов нумеруются.

Под активностью клиентов понимается последовательность запросов клиентов к серверу, атрибутами которых являются такие параметры как тип запроса, время начала и конца его обработки сервером, размеры передаваемых данных и любые другие данные, которые клиентская часть может предоставляет вместе со своими запросами. Для запросов TSR это информация о конфигурации системы (операционная система, архитектура процессора, размер оперативной памяти, производительность). Для ASW это время обработки порций данных на узле клиента. Информация такого рода отображается и сохраняется во время работы среды в журналах сервера.

Результатом анализа журналов служит список клиентов, продемонстрировавших признаки нежелательного поведения. Для распределенных вычислительных систем анализ такой информации может быть существенно затруднен в связи со следующими особенностями их построения и функционирования:

- В связи с потенциально высокой интенсивностью запросов, требования к скорости обработки запросов к серверу высоки, поэтому дополнение к процессу обработки запросов вычислений дополнительных параметров запроса (например, оценка правильности присланных клиентом результатов путем репликации части вычислений на серверной стороне) крайне нежелательно.
- Различные клиенты могут вести себя по-разному, время счета порций на различных конфигурациях оборудования может сильно различаться, время передачи данных сильно зависит от пропускной способности каналов связи. Зачастую перед проведением расчета нельзя определить какие-либо основанные на априорных оценках характеристики задачи: например, размеры передаваемых данных в запросе или время их обработки. Даже если теоретически обоснованные оценки времени работы задачи есть, нет никакой гарантии того, что при нормальном функционировании клиентов на разнородных узлах реальные показатели времени счета будут им соответствовать: многое зависит от особенностей конкретной версии ОС вычислительного и программно-аппаратной архитектуры узла. На клиентском узле могут работать и другие задачи, не принимающие участие в работе распределенной вычислительной среды, однако влияющие на ход распределенного расчета.

Обнаружение аномальных клиентов

Обнаружение аномалий [3] заключается в предварительном формальном описании правильного поведения компонентов системы. Если поведение компонента не соответствует такому описанию, то он помечается как аномалия.

В средах X-Com каждый принимающий участие в расчете клиент начинает своё взаимодействие с запроса описания прикладной задачи, поставляя при этом серверу данные о характеристиках узла и получая в результате идентификатор сессии, которым в дальнейшем помечаются все его запросы. Затем следуют запросы файлов задачи, с помощью которых клиент получает все необходимое для начала работы над задачей, а дальнейшее функционирование клиента описывается последовательным чередованием запросов на порцию исходных данных (REQ) и посылки порции результатов их обработки (ASW). При этом для каждой пары REQ-ASW, следующих друг за другом, верно, что значение параметра номера порции у них одно и то же.

При анализе последовательности запросов любой клиент, показавший несоответствие этим требованиям поведение, считается функционирующим неверно или со сбоями.

Однако такой анализ не позволит выявить клиентов, считающих порции данных слишком медленно или быстро, также анализу не подвергаются передаваемые данные. При этом, учитывая отсутствие каких-либо априорных представлений о решаемой в средах X-Com задачах, зафиксировать такие значения, как ожидаемое время счета порции на клиенте или размер порций результатов не представляется возможным.

Поэтому второй частью анализа является поиск контекстных аномалий [3]. Аномальными будут считаться те клиенты, для которых значения эффективности проводимых вычислений, среднего времени простоя между отсылкой результатов и получений очередной порции данных, среднего объема порций результатов и других числовых характеристик сильно отличаются от этих же характеристик для множества остальных клиентов. Для выявления контекстных аномалий среди клиентов используется алгоритм «ближайший K-й сосед».

Для каждого клиента рассматривается вектор характеристик:

- периодичность однотипных запросов;
- время между запросами ASW и REQ (время простаивания клиента);
- время обработки порции данных, помноженное на заявленную производительность узла клиента;
- размеры порций данных и порций результатов.

Для каждого элемента из множества векторов производится поиск ближайшего K-го элемента. Рассматриваемое значение является аномальным, если расстояние до ближайшего K-го элемента превышает некий заданный наперед порог D. На рис. 1 представлена иллюстрация работы алгоритма на двумерном случае. Клиент A при указанных параметрах алгоритма не является аномалией, так как расстояние до ближайшего 3-го клиента (отмечен цифрой 3) не превышает значения параметра D. Точка B, напротив, не входит в основное скопление клиентов и не имеет ни одного другого клиента в своей D-окрестности.

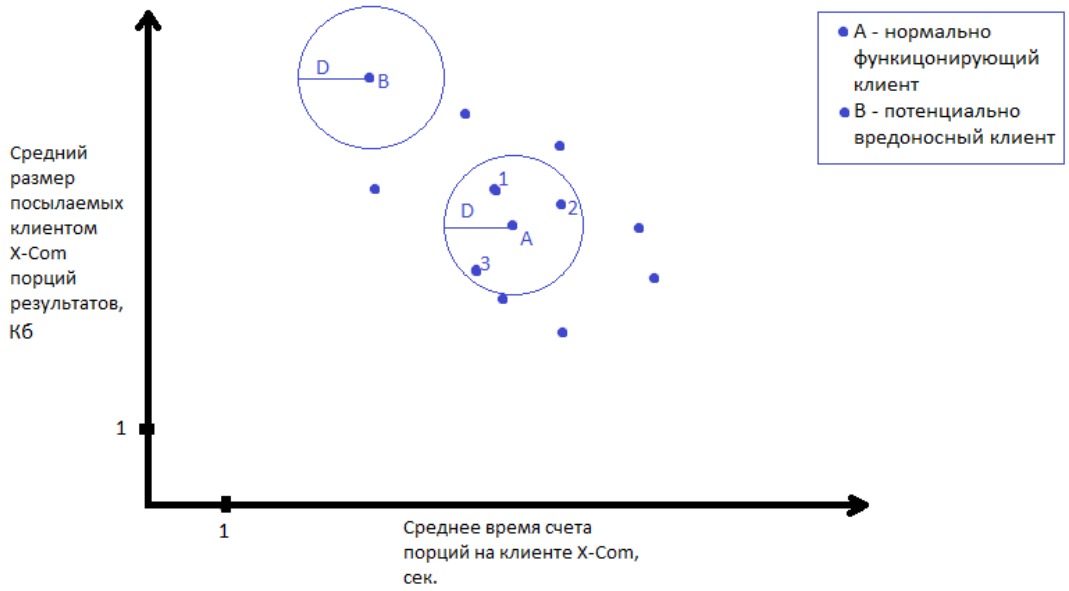

Рис.1 Иллюстрация работы алгоритма «ближайший K-й сосед» с параметрами K=3, D=1 для 2 координат характеристик клиентов X-Com

Аномалиями, определенные таким алгоритмом, будут считаться те элементы, которые не входят ни в один кластер значений мощности больше K, при этом кластером считается множество элементов, в котором для каждого элемента A найдется K элементов, находящихся внутри его D-окрестности.

Теперь рассмотрим множество пронумерованных векторов характеристик клиентов X-Com X и применим для него алгоритм «ближайший K-й сосед», взяв в качестве функции расстояния

$$\rho(x,y) = max_{i:0 \le i < m} |x_i - y_i|,$$

задав K и D:

$$K = |X|/2 \; D = 1/3,$$

и нормализовав значения координат векторов характеристик по формуле

$$x_i' = \varepsilon + (1-2\varepsilon)\frac{(x_i - m_i)}{(M_i - m_i + 2\varepsilon)},$$

где ε - любое пренебрежительно малое неотрицательное число,

m - вектор минимальных координат множества X, M - максимальных.

Перенос на $+\varepsilon$ и масштабирование координат с коэффициентом $(1-2\varepsilon)$ гарантируют, что в идеальном или близком к идеальному случае (значения координат элементов множества X равны между собой или отличаются друг от друга не более чем на ε) расстояние между любыми двумя элементами $X' = \{x'\}$ не будет превышать $D = 1/3$ и аномалии не будут обнаружены.

Наличие хотя бы одного неаномального клиента x' в множестве X' означает, что как минимум половина элементов из множества X' размещается в гиперкубе со стороной 2/3 (|X'|/2 элементов находятся на расстоянии не более 1/6 до элемента x), а для неаномальности каждого из них достаточно, чтобы все они находились внутри гиперкуба со стороной 1/3.

Такое применение алгоритма «ближайшего K-го соседа» опирается на предположение об относительной инвариантности внутри каждого из уровней иерархии соответствующих им характеристик, допуская при этом незначительные отклонения друг от друга для неаномальных клиентов.

Интерпретировать полученные в результате работы алгоритма аномалии можно, если при вычислении расстояния между элементами множества X сохранять номер координаты, для которой модуль разности между её значениями максимален: зная этот номер, можно определить, какая характеристика сессии клиента "ответственна" за его аномальность. Тогда найденные аномалии будем помечать номером такой координаты.

Возможные причины аномалий характеристик клиентов:

- координата "размер результатов данных" - вероятнее всего, аномальный клиент поставляет заведомо ложные результаты или используется для проведения DoS-атаки на сервер X-Com;
- координата "время обработки запроса ASW" - клиент посылает результаты, сложность обработки которых на серверной стороне высока или канал связи между клиентом и сервером обеспечивает нестабильную скорость отправки данных; возможна фальсификация результатов вычислений или проведение DoS-атаки;
- координата "время обработки запроса REQ" - канал связи между клиентом и сервером обеспечивает нестабильную скорость скачивания данных;
- координаты "периодичность запросов ASW и REQ" и "время простаивания клиента" - клиент X-Com или клиентская часть задачи выполняются на узле неэффективно или некорректно из-за вмешательства на стороне узла или наличия на узле клиента других задач, занимающих вычислительные ресурсы; клиент X-Com или клиентская часть задачи были подменены, возможна фальсификация результатов вычислений;
- координата "время обработки порции данных" - клиент X-Com или клиентская часть задачи были подменены или на стороне узла имеет место вмешательство в работу клиента; возможна фальсификация результатов вычислений и/или времени обработки порций данных.

Описание реализации

Для обнаружения аномалий реализация алгоритма представлена в виде библиотеки классов C# 3.0, фронтальный класс которой поддерживает запросы следующих типов:

1. добавление записи очередного события (параметр - запись журнала);
2. запрос списка аномалий, где параметрамы запроса - перечисленные в строке через запятую имена характеристик для анализа, параметры K и D для алгоритма «ближайшего K-го соседа», типы объектов для анализа (сети как множества клиентов с одинаковым префиксом подсети IP-адреса, множества клиентов из одной сети с одинаковыми конфигурациями, узлы или сессии клиентов) и тип множеств, внутри которых производится поиск аномалий.

При добавлении каждой новой записи журнала производится синтаксический анализ записи, после чего, в зависимости от того, впервые ли замечена запись с указанным номером сессии клиента, для сессии создается запись, содержащая в себе для неё минимальные, максимальные значения, а также сумму и количество слагаемых в сумме следующих значений:

- размер порции данных;
- размер порции результатов;
- заявленное клиентом время обработки порции, помноженное на заявленную при включении в расчет производительность (такое произведение дает теоретическую оценку сложности обработки порции данных на узле клиента);
- время между REQ-запросами;
- время между ASW-запросами;
- время между запросами любого типа;
- время между последовательными запросами REQ и ASW;
- время между последовательными запросами ASW и REQ (время простаивания клиента между счетами каждой порции);
- время обработки сервером запроса ASW;
- время обработки сервером запроса REQ;
- время обработки сервером любого запроса клиента;

Также для сессии хранится:
- тип последнего запроса;
- номер последней принятой клиентом порции данных;
- заявленная производительность;
- время последнего запроса ASW;
- время последнего запроса REQ;
- время последнего запроса описания прикладной задачи;
- время последнего запроса файлов задачи;
- время последнего запроса;
- количество внеочередных (нарушающих правила последовательности запросов) запросов REQ;
- количество внеочередных ASW;
- количество внеочередных запросов файлов задачи;
- количество внеочередных запросов описаний задачи.

Такие же данные хранятся для объектов-узлов клиента, доменов (множеств клиентов из одной сети с одинаковыми конфигурациями), сетей и среды целиком.

При запросе списка аномалий в зависимости от параметров производится выборка данных и нормализация значений по характеристикам рассматриваемого множества, внутри которого производится анализ:

1. для каждого множества указанного в запросе типа (узла, домена, сети или вся среда) производится выборка объектов запрошенного типа (узла, домена или сети);
2. по собранной выборке строится массив векторов характеристик, нормализованных по соответствующим характеристикам рассматриваемого множества;
3. производится поиск аномалий с использованием алгоритма «ближайший K-й сосед», в результате получается список идентификаторов аномалий и имен координат в векторе характеристик, указывающих на причину аномалии.

На основе данной библиотеки был разработан инструментарий для статического анализа журналов сервера X-Com. Рассмотренный в работе подход по обнаружению аномалий был успешно апробирован на журналах моделируемых экспериментов с искусственным введением клиентов, показывающих нестабильную эффективность вычислений, а также на журналах, полученных с помощью имитационного моделирования среды X-Com.

В экспериментах с реальными вычислительными узлами использовалась модельные задачи TesPl и Pi из дистрибутива X-Com [1]. Множество клиентов было распределено на 3х узлах кластера СКИФ МГУ «Чебышев» (Intel Xeon E5472 3.0 GHz, Linux, x86_64, по 8 клиентов на узел), при этом в множество клиентов было введено 4 искусственно аномальных клиента, работающих на отдельно портативном компьютере (Intel Pentium Dual CPU T2390 1.86GHz, Windows, x86), показывающих нестабильную эффективность расчетов из-за работы дополнительных задач на узле. Похожая ситуация моделировалась с помощью разработанного в рамках данной работы инструментария для моделирования поведения компонентов среды с участием 120 клиентов кластера, из которых 20 — искусственные аномалии, показывающие пониженную производительность при счете порций; и 23 клиента под управлением Windows. Анализ журналов экспериментов с реальной и моделируемой средой показал пригодность рассмотренного в работе подхода: при анализе всего множества клиентов по перодичености запросов REQ и ASW клиенты под управлением Windows были помечены как аномалии как на реальных, так и на моделируемых экспериментах; при анализе журналов моделируемого эксперимента были обнаружены все 20 аномалий внутри домена кластера, при этом алгоритм не показал ложных срабатываний.

Разработанный инструментарий ориентирован на базовую конфигурации среды, без участия очередей задач и промежуточных серверов; ведутся работы по адаптации технологии к любым конфигурациям среды X-Com.

Работа выполняется при поддержке научно-технической программы Союзного государства СКИФ-ГРИД и гранта Президента РФ для молодых ученых МК-3040.2009.9.

ЛИТЕРАТУРА:

1. Система метакомпьютинга X-Com: http://x-com.parallel.ru/
2. Воеводин Вл.В., Жолудев Ю.А., Соболев С.И., Стефанов К.С. Эволюция системы метакомпьютинга X-Com // Вестник Нижегородского государственного университета им. Н.И. Лобачевского. №4. 2009. С 157-164.
3. Chandola V., Banerjee A., Kumar V. Anomaly Detection: A Survey: http://www.cs.umn.edu/tech_reports_upload/tr2007/07-017.pdf