УДК 658.012

Д.И. АЛЕКСЕЕВ

НЕКОТОРЫЕ АСПЕКТЫ МЕНЕДЖМЕНТА ОШИБОК В КОМПЬЮТЕРНЫХ СЕТЯХ

Анализируются особенности менеджмента ошибок в компьютерных сетях. Предлагается подход к описанию и классификации ошибок. Обосновывается выбор математического аппарата описания процесса диагностики ошибок и разрабатываются основные формализованные описания данного процесса.

1. Основные особенности менеджмента ошибок в компьютерных сетях

Рост числа компьютерных сетей, которые представляют собой критические компоненты в инфраструктуре многих организаций, привел к тому, что интерес к менеджменту ошибок в течение прошлого десятилетия увеличился и в сфере образования, и в сфере промышленности.

Проблема менеджмента ошибок в компьютерных сетях состоит в том, чтобы своевременно обнаружить, изолировать, диагностировать и исправить возможные ошибки, не прерывая работы компьютерной сети. Она имеет следующие особенности:

1. Менеджмент ошибок имеет дело со сбоями системы, а не с ошибками проекта, так что основная его задача - диагностика ошибки, а не создание устойчивого к ошибкам проекта системы.

2. Аналитическое диагностирование ошибок является более целесообразным, чем прямое тестирование системы, поскольку это более дорогостоящий процесс.

3. Система менеджмента ошибок должна производить диагностику как можно большего количества вариантов ошибки, чтобы удовлетворять заданному соотношению стоимость–эффективность даже при неверной диагностике ошибки.

При современном состоянии развития компьютерных сетей диагностика ошибок представляет собой решаемую задачу. Менеджер сети, основываясь на своей базе знаний, отчетах пользователей и предупреждениях системы, в состоянии своевременно произвести диагностику и определить причину большинства отказов, но при росте компьютерных сетей, их разбиении на подсети увеличивается динамика их работы и соответственно увеличивается сложность процесса диагностики ошибок. В таких сложных компьютерных сетях ошибка, происшедшая в одной подсети, может послужить причиной системных предупреждений в других подсетях. В этой ситуации менеджер сети, загруженный множеством системных предупреждений, не сможет правильно и своевременно локализовать ошибку, основываясь только на своей базе знаний и отчетах пользователей. Поэтому эффективный менеджмент ошибок требует соответствующего уровня автоматизации и применения более действенных методов по обработке ошибок и предупреждений.

2. Постановка задачи менеджмента ошибок

Поскольку основная проблема – диагностика ошибки, решения затрагивают собственно процесс диагностики ошибок. Для диагностики ошибок предлагается несколько методов, имеющих свои достоинства и недостатки: метод диагностирования ошибки по конечному состоянию [1–3], метод построения авторегрессионной (Auto Regressive) модели [4], метод обобщенного коэффициента вероятности (Generalized Likelihood Ratio) [5]. Однако они применяются в основном в системах, построенных с использованием для управления сетью протокола SNMP или с применением фиксированного интерфейса управления агентом. Эти подходы имеют недостатки при переходе на большие и гетерогенные сети. Так, при использовании SNMP (централизованный подход) менеджер может

заблокироваться в потоке данных от всех агентов, а при применении фиксированного интерфейса теряется гибкость управления агентом.

В данной статье предложены методы менеджмента ошибок сети.

Пусть имеется некоторая компьютерная сеть. Процесс обнаружения ошибок в ней должен быть непрерывным и своевременно отображать возникающие ситуации сбоя, т.е. отклонения от нормального поведения сети.

Нормальное поведение системы – это взаимодействие конечного пользователя и поставщика службы при условии отсутствия сообщений о неисправности. Так, если пользователь замечает ухудшение работы системы, он может подать сообщение о неисправности. Диагностика ошибки сводится к процессу идентификации наиболее вероятной причины для обнаруженных признаков ошибки. Сам процесс идентификации основан на моделировании причины ошибки и ее действия на интересующие исследователя процессы в моделируемой проблемной области (компьютерной сети). Начальными данными для диагностики ошибки служат обнаруженные ее признаки в виде системных сообщений и информация о неисправностях, полученная от пользователей или обслуживающего персонала.

После обнаружения и идентификации ошибки проводятся действия по корректировке работы системы в целях восстановления нормальной работы системы.

3. Разбиение областей поиска ошибок

Процедуру диагностики ошибок следует интерпретировать в терминах областей поиска и соответствующих действий. Предлагается метод интерпретации данных, основанный на разбиении областей поиска и классификации ошибок (тяжелые и легкие ошибки):

1. Область данных, в которой данные измерений вместе с предупреждениями и сообщениями от пользователей сопоставляются с некоторыми гипотезами об ошибке. В этой области выполняется сбор данных, их анализ и испытание гипотезы.

2. Область гипотез, в которой подтвержденные на основании данных гипотезы об ошибках сопоставляются с некоторыми возможными причинами ошибки. Обычно в этой области получают модель ошибки, на основании которой проводятся дальнейшие рассуждения.

3. Область восстановления, в которой причины сопоставляются с набором возможных действий в целях рассмотрения или восстановления неисправных компонентов системы наиболее эффективным способом.

4. Классификация ошибок и их описание

В некоторых исследованиях по менеджменту ошибок термин «ошибка» обычно сопоставлялся с термином «отказ», что означает сбой компонента (аппаратных средств или программного обеспечения), например, отказ датчика, нарушение соединения или сбой программного обеспечения. Ошибки в работе аппаратных средств происходят обычно из-за повреждения аппаратных средств, окончания гарантийного срока работы и т.д. Ошибки программного обеспечения обычно появляются из-за неправильного или неполного проекта программы или ошибок в реализации программ. Назовём такие ошибки *тяжелыми*. Однако в компьютерных сетях есть еще некоторые другие важные виды ошибок. Например, работа коммутатора ухудшается или появляется перегрузка на одном из соединений. Такой пример позволяет представлять ошибки как отклонения от нормального поведения. Поскольку в этих случаях нет отказа любого из компонентов, мы называем такие ошибки *легкими*.

Тяжелые ошибки могут быть исправлены заменой аппаратных элементов или путем отладки программного обеспечения. Такую диагностику называют реактивной в том смысле, что она состоит в основном из реакций на фактические отказы. Легкие ошибки в большинстве случаев сигнализируют о некоторых серьезных проблемах, и по этой причине диагностику таких ошибок называют *превентивной*. Посредством раннего предупреждения и диагностики такой превентив-

ный менеджмент опознает и предотвратит отказы и, таким образом, может увеличить жизнеспособность и эффективность сетей. В дальнейшем для удобства будем использовать термин «ошибка», чтобы представить и тяжелые, и легкие ошибки.

Основанные на знаниях экспертные системы являются примерами автоматизированных систем, предназначенных для комплексной системной диагностики ошибок. Большинство экспертных систем разработаны для какого-то определенного класса задач и предназначены только для приема и хранения знаний, полученных путем формализации опыта эксперта. Как правило, такие системы базируются на детерминированных моделях компьютерной сети. Серьезная проблема использования детерминированных моделей - их неспособность отделить первичные источники отказов от нескоординированных системных предупреждений, которые усложняют автоматизированную идентификацию ошибки. Замечено, что отношения причины и эффекта между признаками и возможными причинами являются неотъемлемо недетерминированными, соответственно с помощью *вероятностных* моделей можно получить более точное представление для сетей. Более естественной и эффективной моделью для логического рассуждения человека являются доверительные сети, которые представляют собой общую схему представления знания и являются ключевой технологией для диагностики при условии неопределенности. Для построения вероятностной модели ошибок предлагается использовать именно доверительные сети.

Доверительная сеть (сеть Байеса) – подходящая структура для объединения знаний экспертов и статистических данных, которая представляет собой модель *окружающей среды*, а не модель процесса рассуждения, как во многих других схемах представления знания. Фактически доверительные сети моделируют механизмы, которые работают в окружающей среде, и таким образом учитывают различные виды выходной информации. Преимущества их состоят в следующем:

1. Естественная и ключевая технология для диагноза.
2. Основа для лучших, более последовательных экспертных систем.
3. Поддержка новых подходов к планированию и моделированию действия.
4. Планирование использования марковских процессов принятия решения.

5. *Процесс диагностики с использованием интервенции сети Байеса*

В компьютерных сетях зонды присоединены к некоторым компонентам аппаратной или программной части. Обычно необработанные данные, получаемые от зонда, группируются в вектор $d \in R^n$ и далее подвергаются обработке для получения обобщенных значений (например, средние значения, пиковые значения и т.д.). Статистика, получаемая как функция от R, ставит в соответствие вектору необработанных данных d числовые значения. Такая статистика, как правило, представляется как набор дискретных переменных. Обозначим через NS нормальное состояние, а все остальные положительные значения будут представлять собой анормальное состояние с различными уровнями тяжести. Узел v в сети модели $B=(V,L,P)$ называется наблюдаемым тогда и только тогда, когда он представляет собой статистику о состоянии сети или ссылается на отчет пользователя. Набор наблюдаемых узлов обозначим через O. Ненаблюдаемые узлы – это те, которые не входят в набор O. Набор доказательств R содержит те узлы, которые подвергаются наблюдению в течение мониторинга сети. Узлом симптома называется каждый узел $r \in R$. Тестовый набор ST содержит все остальные наблюдаемые узлы, которые не входят в набор R. Набор ошибок F - это набор корневых узлов, которые не находятся под наблюдением. Узлы, которые не входят в набор O и не входят в набор F, - это скрытые узлы H. Скрытые узлы – это посредники между узлами ошибок и узлами симптомов, и в процессе диагностики они не рассматриваются.

В определенный момент времени можно сказать, что сеть работает в нормальном режиме с набором R тогда и только тогда, когда каждый узел в R принимает нулевое значение, или полностью вектор $r = 0$, где $r = (r_1, r_2, ..., r_{|R|})$. Сеть имеет анормальный режим работы тогда и только тогда, когда хотя бы одно из $r \in R$ отличается от 0. Такая ситуация включает процесс диагностики.

Рассмотрим различия между двумя видами семантики для определения конкретного узла в сети Байеса: пассивное наблюдение и активную установку. Вся конкретизация узлов, о которой мы до этого говорили, получена вследствие пассивного наблюдения, и при такой организации мы можем узнать результаты и возможные причины для полученных наблюдений. При использовании альтернативной семантики мы можем устанавливать значение узла в течение активного эксперимента.

Рассмотрим вариант корректировки сети Байеса путем оценки результатов, без изменения активных установок (рис. 1). Такое внешнее вмешательство назовем *интервенцией.*

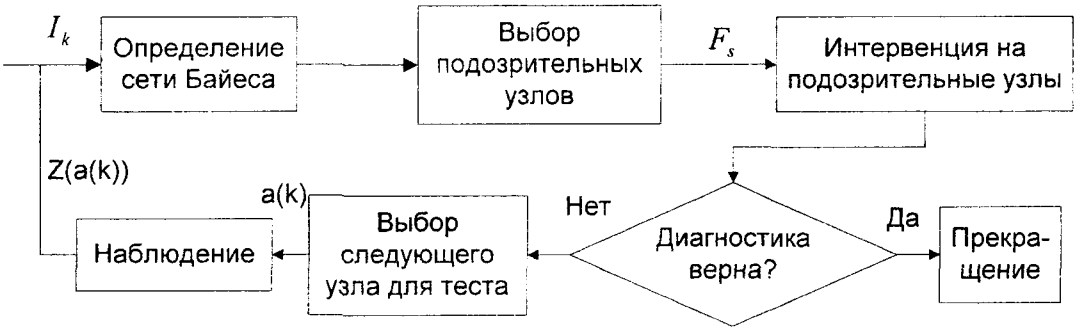

Рис. 1. Процесс диагностики ошибок с использованием интервенции

Сеть Байеса после интервенции $\overline{B} = (V, L, P, S, F_S)$ получается из оригинальной сети Байеса $B = (V, L, P)$ с теми же самыми V, L, P. S - это набор симптомов, а $F_S \in F$ - набор подозрительных узлов. Для каждого $s \in S$ подсчитаем вероятность $P(s = 0 \mid \text{setting}(F_S = 0))$ для использования в $\overline{B}$.

При данном малом ε можно сказать, что узел S_1 становится ε-нормализованным посредством интервенции на f_1 тогда и только тогда, когда $P(s1 = 0 \mid \text{setting}(f_1 = 0)) < \varepsilon$.

Непустой набор подозрительных узлов F_S будет называться правильной диагностикой тогда и только тогда, когда каждый узел в наборе S, включая начальные и найденные симптомы, становится ε-нормализованным, если мы устанавливаем каждый узел в F_S в состояние нормального функционирования в сети Байеса после интервенции $\overline{B} = (V, L, P, S, F_S)$. И как только F_S объяснит набор S, можно останавливать процесс диагностики, так как в этом случае будет найден неисправный узел.

Если неисправный узел не найден, то после произведенных действий a_k определяется переменная Z_{a_k}, принимающая некоторое значение после действия a_k, *по которой можно определить историю процесса диагностики в* каждый момент времени k, $I_k = (I_{k-1}, (a_k, Z_{a_k}))$, что в свою очередь является свойством марковского процесса.

6. *Парадигмы создания систем управления сетью*

Обычная система управления сетью состоит из двух классов компонентов: менеджеры и агенты (рис. 2). Приложения на станции управления принимают роль

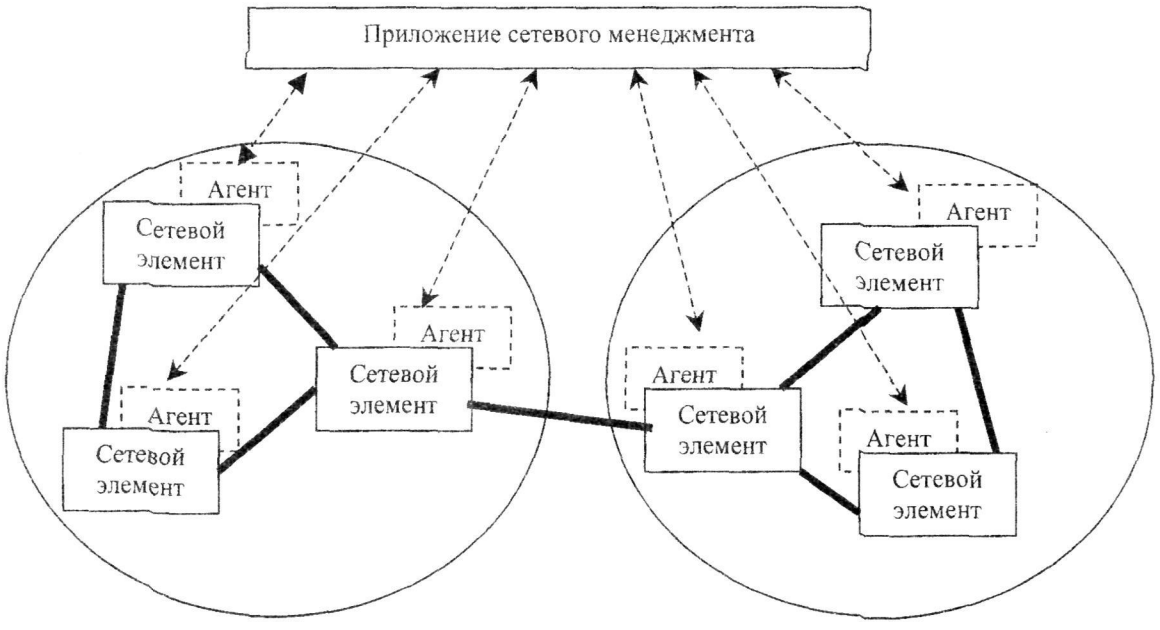

Рис.2. Компоненты системы менеджмента и мониторинга сети

менеджера; агенты в данном случае - это процессы сервера, запущенные на каждом управляемом объекте сети. Эти агенты собирают данные об устройствах сети, хранят их в некотором формате и поддерживают некоторый протокол управления, например, SNMP (Simple Network Management Protocol). Приложения-менеджеры получают данные от агентов, посылая соответствующие запросы по протоколу управления. Все, что должен делать агент, – это обеспечивать менеджера только необходимыми данными.

Собственно менеджер выполняет все вычисления по статистике, шаги по диагностике ошибки и другие приложения. Такая система представляет собой централизованную структуру и хорошо работает для маленьких сетей. Но поскольку сети становятся большими, более сложными и гетерогенными (например, мультимедийные сети), централизованная парадигма будет пересылать большие объемы данных между менеджером и агентом и, таким образом, неэффективно занимать слишком большую часть полосы пропускания. Поскольку не все данные уместны и необходимы для обработки менеджером и есть много случаев, когда обработка может быть сделана на месте, нет необходимости централизовать всю обработку на стороне менеджера.

Поэтому более целесообразным оказывается создание распределенных систем управления сетью, когда часть проблем решается собственно агентом, установленным на управляемом объекте сети. А приложение-менеджер, со своей стороны, выполняет действия, координирующие работу агентов.

Заключение

Предложены методы интерпретации, классификации методологии описания ошибок. Развитие решения рассмотренной задачи в перспективе станет основой для создания автоматизированных систем менеджмента ошибок на ранних стадиях их появления.

Список литературы: 1. *Боулотас А., Харт Г.В., Шварц М.* Простейшие датчики ошибок в компьютерных сетях // IEEE конференция по связи. 1992. Т. 40, № 3. С. 477-479. 2. *Ли Д., Нетравали А.Н., Сабнани К.К. и др.* Пассивное тестирование и его применение к менедж-

менту компьютерных сетей // Тезисы на международной конференции по протоколам сети. 1997. С. 113-122. 3. *Ванг С., Шварц М.* Обнаружение ошибок по множественным наблюдениям // Доклад на конференции IEEE INFOCOM. 1992. 4. *Худ С., Дзи С.* Превентивное обнаружение ошибок в сети // Доклад на конференции IEEE INFOCOM. 1997. С. 333-341. 5. *Тоттан М., Дзи С.* Адаптивная установка порогового значения параметров при превентивном обнаружении ошибок в сети // Доклад на 3-м международном симпозиуме IEEE по системному менеджменту. 1998. Ньюпорт. P1. С. 108-116.

Поступила в редколлегию 27.06.2003

Алексеев Дмитрий Игоревич, ассистент кафедры ИУС ХНУРЭ. Научные интересы: методы мониторинга и администрирования компьютерных сетей. Адрес: Украина, 61166, Харьков, пр. Ленина, 14, тел. 70-21-451.