УДК 519.713

Д.И. АЛЕКСЕЕВ, А.И. ГРИЦЕНКО

МЕТОД НЕПРЕРЫВНОГО МОНИТОРИНГА ПРИ ОБНАРУЖЕНИИ ОТКАЗОВ МАРШРУТИЗАТОРОВ

Рассматривается метод организации непрерывного мониторинга при обнаружении отказов маршрутизаторов в компьютерной сети произвольной топологии методом построения логических деревьев компьютерной сети. Метод предназначен для использования в системах непрерывного мониторинга и основан на решении логических уравнений состояния маршрутизаторов для обнаружения их отказов и на выборе необходимых моментов измерения.

1. Введение

Существующие на сегодняшний день многосегментные корпоративные компьютерные сети требуют реализации процедур постоянного мониторинга для обеспечения функциональной поддержки основных ресурсов и сервисов и обеспечения стабильности показателей QoS. К сожалению, технологии постоянного мониторинга оказывают большую нагрузку на сеть и снижают эффективность ее использования. К задачам постоянного мониторинга относятся задачи обнаружения отказов маршрутизаторов, а также задачи поддержки функций QoS. Реализация процедур экономного мониторинга является актуальной для компьютерной сети в целом.

Общая цель мониторинга – сбор пакетов в различных точках сети и получение информации для раскрытия пути любого пакета [1].

Эффективность решения задачи непрерывного экономного мониторинга состояния сложных систем, таких как компьютерные сети, может рассматриваться в контексте двух показателей – достоверности получаемой информации о наблюдаемом объекте и величины информационных затрат, связанных с передачей данных от наблюдаемого объекта к системе мониторинга.

Актуальной проблемой мониторинга является нахождение оптимального соотношения величины информационных затрат и достоверности получаемой информации.

Один из путей реализации экономного мониторинга основывается на сокращении количества моментов измерений. В рамках данного подхода широко используются неадаптивные методы с систематическим, стохастическим или стратифицированным способом выбора моментов измерений [2-4].

Однако ведение непрерывного мониторинга состояния узлов сети, даже с выбором моментов измерения, существенно сокращает возможность сети обеспечить необходимые для большого количества потоков ресурсы, поэтому решение проблемы должно состоять не только в оптимизации процесса непрерывного мониторинга, но и в разработке более эффективных архитектур процесса мониторинга. В связи с этим возникает проблема синтеза архитектуры процесса мониторинга и формирования соответствующих эффективных методов диагностики [5].

Из существующих технологий мониторинга [6-8] наиболее удачной является технология, основанная на реализации процедур выборочного тестирования маршрутизаторов [8]. При этом предлагается формировать специальные логические деревья и тестировать их, решая логические уравнения.

Эти методы, к сожалению, позволяют осуществлять только общую диагностику состояния узлов или предъявляют слишком высокие требования к пропускной способности сети или к хранилищам данных, собранных в процессе мониторинга.

Исходя из сказанного выше, предлагаем разработку путей реализации экономически эффективного непрерывного мониторинга при выявлении отказов передачи данных в корпоративной компьютерной сети.

Описание объекта. Пусть существует некоторая многосегментная корпоративная компьютерная сеть. В сети существует единая политика, разрешающая использование специальных агентов и технологий для тестирования маршрутизаторов и рабочих станций. В такую сеть входят рабочие станции, серверы, внутрисегментные и внешние относительно сегментов маршрутизаторы.

Согласно [8], представим компьютерную сеть в виде древовидного графа, узлами которого являются корневые маршрутизаторы – маршрутизаторы, образующие магистраль $\{C_1, C_2, ..., C_5\}$, а вершинами (листьями) – граничные маршрутизаторы – маршрутизаторы, находящиеся на границе локальных сетей $\{E_1, E_2, ..., E_7\}$. Пусть $\{R_j\}$ - множество всех маршрутизаторов, тогда $\{C_1, C_2, ..., C_5\} \subset \{R_j\}$, $\{E_1, E_2, ..., E_7\} \subset \{R_j\}$ и $\{C_1, C_2, ..., C_5\} \cup \{E_1, E_2, ..., E_7\} = \{R_j\}$. Введем множество $\{Q^-\}$ - сбойные маршрутизаторы. В случае стабильно работающей сети имеем $\{Q^-\} = O$.

Постановка задачи сводится к разработке методов непрерывного мониторинга компьютерной сети для выявления в ней отказов связей (сегментов) и маршрутизаторов.

2. Непрерывный мониторинг при выявлении отказов маршрутизаторов

Предлагается метод мониторинга, который слабо нагружает магистральные маршрутизаторы, поскольку не использует их для проведения измерений. Предполагается, что если сеть правильно спроектирована и построена, а также если пользователи ведут себя в соответствии с правилами, то потоки, проходящие сквозь эту сеть, не испытывают больших задержек и потерь.

В предлагаемом методе все граничные маршрутизаторы исследуют своих соседей в направлениях по часовой стрелке и против часовой стрелки.

В процессе инициализации формируется логическое дерево сети с использованием всех граничных маршрутизаторов. После этого запускается процесс сбора и измерения данных, которые могут характеризовать существующие связи между маршрутизаторами. В результате процесса сбора данных о потерях и задержках в сети не подсчитывается процент потерь для каждого индивидуального соединения, вместо этого определяются соединения, которые находятся в состоянии перегрузки, т.е. имеют большой процент потерь пакетов.

Так как необходимо минимизировать нагрузку на сеть, предлагается проводить измерения состояния маршрутизаторов через строго фиксированные интервалы времени Δt_0 с пропущенными плановыми измерениями. Будем различать такие последовательности: $x[i]$– истинные значения наблюдаемого процесса, $x'[i]$ – накапливаемые значения наблюдаемого процесса, $\tilde{x}[i]$ – измеряемые значения наблюдаемого процесса, $\hat{x}[i]$ – оцениваемые значения наблюдаемого процесса. Для того чтобы определить моменты времени, в которые необходимо производить последующие измерения, предлагается выполнить следующие действия: на первом шаге формируется опорная выборка $\tilde{x}[i]$, $i = \overline{1,k}$, состоящая из измеренных значений наблюдаемого процесса, на втором шаге осуществляется выбор интервала прогнозирования Δt_p с помощью процедуры экстраполяции полученных измерений. На третьем шаге используется метод коррекции накопленных данных для процессов непрерывного мониторинга.

Метод коррекции накопленных данных для процессов непрерывного мониторинга основан на методах интерполяции измеренных значений. Он необходим для обработки результатов наблюдения в целях увеличения их достоверности путём уточнения экстраполированных данных.

После процедуры сбора данных о потерях и задержках производится тестирование полученного дерева компьютерной сети в целях получения реальных значений для анализа существующей архитектуры. В этот момент определяется проблемный участок сети, ограниченный парой маршрутизаторов.

После определения проблемного участка компьютерной сети производится уточнение проблемного узла (маршрутизатора). Для уточнения используются рабочие станции, находящиеся по разные стороны маршрутизаторов проблемного участка. Важным условием является то, что рабочие станции исправны, т.е. функционируют без сбоев.

На основании рассмотренных выше решений можно сформулировать метод непрерывного мониторинга при обнаружении отказов маршрутизаторов.

1. Формируем логическое дерево сети τ, выбираем граничные $\{R\}$ и корневые маршрутизаторы $\{C\}$, логические каналы (пути) $\{P\}$.

2. По истечении некоторого времени начинаем процедуру сбора данных о состоянии маршрутизаторов, основанную на экономном методе активного мониторинга. Осуществляем выбор интервала прогнозирования Δt_p. Для этого формируем опорную выборку значений $\tilde{x}[i],\ i=\overline{1,k}$.

3. Принимаем решение о выборе интервала прогнозирования Δt_p на основании процедуры экстраполяции накопленных данных, экстраполируемое значение рассчитываем с помощью модели метода линейной регрессии [9]:

$$\hat{x}[i] = a_0 + a_1 t[i],$$

где $\hat{x}[i]$ – экстраполируемое значение; a_0, a_1 – коэффициенты модели, рассчитывающиеся по следующим формулам:

$$a_0 = \Big(\sum_i x'[i] - a_1 \sum_i t[i]\Big) \Big/ w,\quad a_1 = \Big(w\sum_i x'[i]t[i] - \sum_i x'[i]\sum_i t[i]\Big) \Big/ \Big(w\sum_i t[i]^2 - \sum_i t[i]\sum_i t[i]\Big),$$

где w – длина окна прогнозирования.

4. Оцениваем адекватность экстраполяции на основании опорной выборки $\{\tilde{x}[i]\},\ i=\overline{1,k}$ с помощью вычисления ошибки прогнозирования по формуле

$$e[k] = \left|x'[k] - \hat{x}[k]\right|.$$

Для накапливаемых значений $x'[i],\ i>k$ используются либо измеренные значения ($\tilde{x}[i]$), либо прогнозированные ($\hat{x}[i]$).

5. Для обработки результатов наблюдения в целях увеличения их достоверности путём уточнения экстраполированных данных осуществляем коррекцию накопленных данных. На множестве накопленных значений $x'[i],\ i=\overline{1,n}$ интерполируем значения, которые были экстраполированы в процессе наблюдения. Интерполяции осуществляется по формуле

$$\hat{x}[i] = \tilde{x}[i-l] + \alpha(\tilde{x}[i+r] - \tilde{x}[i-l]),$$

где $\hat{x}[i]$ – интерполируемое значение; $\tilde{x}[i-l]$ – ближайшее к $\hat{x}[i]$ ранее измеренное значение; $\tilde{x}[i+r]$ – ближайшее к $\tilde{x}[i]$ значение, измеренное позже; α – коэффициент модели, рассчитываемый по формуле

$$\alpha = \frac{t[i] - t[i-l]}{t[i+r] - t[i-l]}.$$

В результирующей выборке экстраполированные значения заменяются уточнёнными.

6. В соответствии с заданными путями определяем соответствующие логические переменные $P_{i,j}$, которые представляют собой результат проверки состояния пути между граничными маршрутизаторами от i к j. Они равны 1, если связь перегружена, и равны 0 при нормальном состоянии связи. Также $P_{i,j}=0$, если $i=j$. С другой стороны, $X_{i,k}$ – булева переменная, представляющая собой состояние перегрузки для связи (i,k), назовем ее переменной перегрузки. Уравнения пути для h корневых маршрутизаторов будут иметь вид

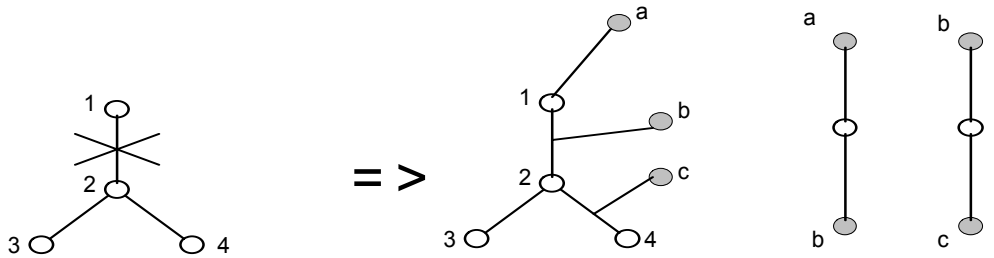
$$P_{i,j} = X_{i,k} + \sum_{n=k}^{n=h-1} X_{n,n+1} + X_{h,j}.$$

7. Формируем системы уравнений для каждого раунда по часовой стрелке (прямого) и против часовой стрелки (обратного).

8. Решаем полученные системы уравнений и выявляем сбойные сегменты $\{Q^-\}$.

9. Выявляем маршрутизаторы-претенденты в список отказавших $R_i \in Q^-$.

10. Для каждого выбранного маршрутизатора $R_i \in Q^-$ формируем логическое дерево τ_h, состоящее из пары рабочих станций и маршрутизатора (рисунок, поз. а). Формируем уравнения для путей



а б

Выделение в сегменте маршрутизатора и пары рабочих станций (а) и представление выделенных маршрутизаторов в виде отдельных деревьев (б)

$$\begin{cases} P_{bc} = X_{b2} + X_{2c} \\ P_{cb} = X_{c2} + X_{2b} \end{cases}, \quad \begin{cases} P_{ab} = X_{a1} + X_{1b} \\ P_{ba} = X_{b1} + X_{1a} \end{cases}.$$

11. Принимаем допущение, что рабочие станции работают нормально, т.е.

$$q_{a1} = q_{1a} = q_{1b} = q_{b1} = q_{2b} = q_{2c} = q_{c2} = 0.$$

12. Проводим тестирование для логических деревьев, состоящих из рабочих станций и маршрутизатора (рисунок, поз. б).

13. Формируем логические уравнения $X_{pr} = s_{pr} + q_{pr}$, где q_{pr} – состояние станции в направлении (p,r); s_{pr} – состояние маршрутизатора в направлении (p,r), решаем их и определяем отказавшие сегменты $\{(a,b)\}$:

$$\begin{cases} X_{a1} = q_{a1} + s_{a1} \\ X_{1b} = q_{1b} + s_{1b} \end{cases}, \quad \begin{cases} X_{b1} = q_{b1} + s_{b1} \\ X_{1a} = q_{1a} + s_{1a} \end{cases},$$

$$\begin{cases} X_{c2} = q_{c2} + s_{c2} \\ X_{2b} = q_{2b} + s_{2b} \end{cases}, \quad \begin{cases} X_{b2} = q_{b2} + s_{b2} \\ X_{2c} = q_{2c} + s_{2c} \end{cases}.$$

14. На основании полученных решений выявляем отказавшие маршрутизаторы $\{R_i\}$.

При наличии в сегменте отказавшего маршрутизатора одно из состояний пути Xij будет иметь значение 1, тогда при принятом допущении о работоспособности рабочих станций ($q_{ij} = 0$) одна из переменных s_{ij}, обозначающих состояние маршрутизатора, примет значение 1. Соответственно этот маршрутизатор и является отказавшим для данного направления.

Область применения полученных результатов. Предлагаемый метод может применяться для оперативной диагностики состояния компьютерных сетей.

3. Выводы

Предложен метод, позволяющий осуществлять непрерывный мониторинг сети при выявлении отказов маршрутизаторов. Результаты являются развитием методов, представленных в [10] и [11].

Основные ***научные результаты*** **можно представить в вербальном виде:**

- предложено для осуществления ненагружающего компьютерную сеть непрерывного мониторинга выбирать моменты времени, в которые производить необходимые измерения. Результаты получены для случайных процессов путём построения временных рядов в рамках скользящего окна и использования методов экстраполяции;

-усовершенствован метод выявления отказов сегментов и компонентов компьютерной сети, основанный на формировании логических деревьев и их тестировании. При этом строятся дополнительные деревья, позволяющие выявить отказавшие узлы. Метод основан на использовании алгебры логики. Используемый метод позволяет получить эффективный (с малым потреблением ресурсов) алгоритм тестирования сети.

Сравнение с лучшими аналогами. Предложенные методы в сравнении с методом, описанным в [8], позволяют выявлять не только отказавшие сегменты, но и отказавшие узлы. Кроме того, использование выбора моментов измерений для непрерывного мониторинга снижает информационные затраты процесса, что эквивалентно снижению стоимости мониторинга. Например, для таких систем, как компьютерная сеть, снижение информационных затрат в процессе мониторинга увеличивает полезную пропускную способность каналов связи, соответственно больше пользовательских данных может быть передано в единицу времени. В отличие от методов [2-4] предложенный метод является более экономным как с точки зрения затрат на полосу пропускания, так и с точки зрения других информационных затрат.

Направление дальнейших исследований. Результаты, полученные в данной работе, касались лишь одного из аспектов улучшения работы протокола управления качеством передачи потока данных. В дальнейшем предполагается рассмотрение реализации полученного метода для сетей со слабоинтеллектуальными узлами и гибридными сегментами Router-Switch.

Список литературы: 1. *Liotta A., Pavlou G., Knight G.* Exploiting agent mobility for large-scale network monitoring// IEEE Network. 2002, May/June. P. 112-117. 2. *Cochran W.*. Sampling Techniques. Wiley, New York, 1977. 3. *Amer Paul D., Cassel Lillian N.* Management of Sampled Real-Time Network Measurements. 14th Conference on Local Computer Networks, October 1989, Minneapolis. IEEE, 1989. P. 62-68,. 4. *Claffy K.C., Polyzos George C., Braun Hans-Werner.* Application of Sampling Methodologies to Network Traffic Characterization// Proceedings of ACM SIGCOMM'93, San Francisco, CA, USA, September 13-17, 1993. 5. *Breitbart Y., Chan C. Y. , Garofalakis M., Rastogi R. Silberschatz A*. Efficiently monitoring bandwidth and latency in IP networks// Proc. IEEE INFOCOM, Anchorage, AK. 2001. Apr. P. 72-76. 6. *Dilman M. , Raz D.* Efficient reactive monitoring// Proc. IEEE INFOCOM. Anchorage.AK. 2001. Apr. P. 34-37. 7. *Duffield N.G. , Horowitz J., Presti F. Lo, Towsley D.* . Network delay tomography from end-to-end unicast measurements / / Proc. of the 2001 International Workshop on Digital Communications 2001 Evolutionary Trends of the Internet, Italy. 2001. Sept. P. 121-132. 8. *Habib A. , Khan M. , Bhargava Bharat*. Edge-to-Edge measurement-based distributed network monitoring// Computer Networks Journal. 2004. Feb. Vol. 44. Issue 2. P. 211-233 . 9. *Draper N.R., Smith H.* Applied Regression Analysis Wiley Series in Probability and Statistics. 1998. 10. *Саенко В.И., Алексеев Д.И.* Метод обнаружения отказов маршрутизаторов в компьютерных сетях // Радиоэлектроника и информатика. 2007. № 3. С. 73-78. 11. *Саенко В.И., Гриценко А.И.* Метод выбора моментов измерений для процессов непрерывного мониторинга // Радиоэлектроника и информатика. 2007. № 4.С.17-20.

Поступила в редколлегию 24.06.2008

Алексеев Дмитрий Игоревич, ассистент кафедры информационных управляющих систем ХНУРЭ. Научные интересы: методы и технологии обнаружения и исправления ошибок в компьютерных сетях. Увлечения и хобби: компьютерные сети. Адрес: Украина, 61166. Харьков, пр. Ленина, 14, тел. 7021-451.

Гриценко Алексей Игоревич, соискатель кафедры информационных управляющих систем ХНУРЭ. Научные интересы: методы и технологии менеджмента компьютерных сетей. Увлечения и хобби: футбол, горный туризм, горные лыжи. Адрес: Украина, 61166. Харьков, пр. Ленина, 14, тел. 7021-451.