УДК 004.738.52:004.031

В.И. Саенко

Харьковский национальный университет радиоэлектроники, Харьков

РАСШИРЕННЫЙ МЕТОД ВЫБОРА НАБЛЮДАЕМЫХ ПЕРЕМЕННЫХ ДЛЯ МОНИТОРИНГА КОМПЬЮТЕРНОЙ СЕТИ

Рассматриваются вопросы теории, методологии и практики мониторинга компьютерных сетей. Акцент сделан на задачах снижения служебного трафика в процессе сбора данных за счет выбора необходимого и достаточного набора контролируемых переменных. Все положения подтверждаются экспериментально в рамках технологии WMI.

Ключевые слова: *компьютерная сеть, мониторинг, WMI, наблюдаемая переменная.*

Введение

Одна из актуальных задач мониторинга компьютерных сетей – снижение нагрузки на сеть служебного трафика. Сложность структуры компьютерной сети приводит к росту потоков служебной информации и уменьшению полезного трафика [1]. В итоге задача уменьшения служебного трафика остается актуальной.

Общая схема реализации мониторинга, например, представленная в [1], показывает, что чем больше измеряется переменных и чем выше частота измерений, тем больше требуется вычислительных, информационных и финансовых затрат.

Существуют разные пути уменьшения этого трафика. Например, можно уменьшить число точек измерения (частоту измерения). Это может быть выполнено путем применения специальных оптимизационных процедур [2] или адаптивных процедур [3]. Может учитываться текущее состояние сети в целом [4] или прогнозировано значение уже измеренных переменных [5]. Можно основную обработку данных проводить локально, используя агентную технологию [7], пересылая менеджеру готовые усредненные результаты. Можно уменьшить набор подлежащих контролю переменных [6]. В этом случае выбор переменных ставит вопрос о необходимости и достаточности такого набора переменных, которые обеспечат определенную информативность задач мониторинга.

Задача выбора переменных для мониторинга в рассматриваемых условиях не соответствует классическим задачам факторного анализа [8]. В классических задачах необходима статистическая информация о поведении переменной в различных условиях эксперимента. Априорная информация о значимости переменной отсутствует. В нашем случае имеем высокий уровень априорной определенности. Эту особенность предлагается использовать при формировании экспертных оценок для выбора переменных.

Рассматриваемая задача не является тривиальной, так как объем доступной для измерения и передачи информации может достигать тысячи переменных. Отметим, что в [6] рассматривался вариант предварительного оценивания переменных на основании признаковых переменных, принимающих дискретные значения {0,1}. Если допустить, что степень важности переменных будет оцениваться вместо дискретной формы в виде некоторой интервальной оценки [0,1], то предложенный в [6] метод изменится.

Целью работы является дальнейшее развитие метода выбора наблюдаемых переменных для определенных условий задач мониторинга.

Структура статьи. В п. 1 дано формализованное описание постановки задачи. В п. 2 представлены концептуальные положения для выбора переменных наблюдения, в п. 3 представлены положения по экспертному оцениванию, в п. 4 описан метод выбора переменных, в п. 5 обобщены результаты анализа, в п. 6 поясняется достаточность полученных решений, в п. 7 приведен пример реализации метода.

1. Постановка задачи

Пусть сеть относится к классу корпоративных, следовательно, требуется формировать большие потоки служебного трафика по сбору данных о состоянии сети. В то же время можно формировать единую политику мониторинга, определяя технологии сбора, архитектуру всей системы и объемы передаваемых данных.

По аналогии с [6] предположим, что в некоторой компьютерной сети решается задача менеджмента конфигураций или производительности [6]. Пусть планируется проведение мониторинга состояния компьютерной сети. Цель мониторинга G известна. Пусть для измерения переменных (объектов мониторинга) выбрана технология CIM-WMI [9], предоставляющая сгруппированное множество переменных V.

Множество переменных, которые можно рассматривать как кандидаты в переменные мониторинга, будем называть *начальным множеством* V_0. Оно избыточно и требуется выбрать из него набор переменных $v_i \in V_M \subset V_0$, которые будем называть *значимыми.*

Фактически общая постановка задачи не меняется по сравнению с [6].

Задача исследования сводится к развитию метода, выбора набора наблюдаемых переменных при использовании гибкого оценивания оценок значимости переменных в процесс мониторинга.

2. Концептуальные положения реализации мониторинга компьютерной сети

При выборе набора переменных мониторинга можно идти двумя путями. Первый – для заданной задачи мониторинга формируется набор необходимых для контроля переменных, будем называть его *первичным* (x_j). Далее разрабатываются процедуры их измерения и передачи. Второй – для заданной задачи мониторинга выбираются технологии с процедурами измерения определенных наборов переменных, *вторичные* v_p. Из имеющихся наборов процедур выбираем те, которые наиболее близки решаемой задаче мониторинга и первичным переменным. Второму подходу соответствуют технологии SNMP, WMI.

С одной стороны, существует очень большое число переменных, которые можно измерять локально на каждом узле сети (рабочей станции). С другой стороны, полное их измерение, контроль и последующая передача создадут значительную нагрузку на каналы передачи данных и на сами узлы.

В чем принципиально отличие реализации процедур контроля первичных и вторичных переменных? Первичные переменные требуют нестандартных, специальных трудоемких решений. Вторичные переменные используют стандартные процедуры, легко реализуемые, но требуют дополнительного перегруппирования.

В настоящей статье будем рассматривать задачу выбора набора подлежащих контролю переменных при условии, что используется технология WMI.

Идея состоит в использовании априорной информации о переменных, описывающих стояние компонент в процессе мониторинга.

Существует задача выбора такого набора переменных. При этом целесообразно учесть достаточно высокий уровень априорной определенности о выбираемых переменных. Как следствие, предлагается использовать экспертные оценки, которые позволяют наиболее полно учитывать эту информацию.

Для определения значимости каждой переменной (кандидата) введем следующую систему экспертного оценивания, идея которой предложена в [6]. Будем полагать, что заданы задачи мониторинга $g_i \in G$, например, «мониторинг загрузки сети трафиком TCP», или «мониторинг конфигурации узлов компьютерной сети» и т.п. Создадим две группы экспертных оценок, по которым будем выбирать переменные мониторинга.

Первая группа P_x – *основные признаки*, т.е. те, на основе которых строятся критерии оптимизации для задачи мониторинга. Фактически это признаки привязки переменной к определенной задаче мониторинга, это первичные переменные.

Вторая группа P_a – это дополнительные признаки, характеризующие определенные требования к наблюдаемой переменной при выборе первичного признака.

Имеем $x_j \in P_x$, $a_i \in P_a$. Если $T(S)$ обозначим как список свойств объекта S, то $x_j = T(g_q), a_i = T(v_p)$, где g_q, v_p – задача и переменная наблюдения соответственно. Т.е. x_j – свойство задач, a_i – свойство переменных.

Формирование x_j не составляет труда. Например, для задачи «мониторинг загрузки сети трафика TCP» определяющими могут быть $< x_1, x_2 >$ = <(пропускная способность логических каналов), (задержка выполнения запросов)>. Соответственно критериальные выражения будут $x_1 \to \max\limits_{\Delta T}$, $x_2 \to \min\limits_{\Delta T}$, ΔT – интервал мониторинга.

Признаки a_i отражают особенность переменных кандидатов по отношению к конкретному признаку x_j.

Например, «переменная количественная», «переменная, быстро изменяющаяся в широком диапазоне», «переменная отражает двунаправленный процесс обмена данным» и т.п. Благодаря такому подходу можно указать, какими свойствами должна обладать рассматриваемая переменная, при условии ее значимости для заданной функциональной задачи или соответствующего признака.

Фактически P_a привязываются к x_j. Выбор количества признаков $x_j, j = 1,...,n; a_i, i = 1,...,k$, т.е. m, k – остается за экспертом.

Правило 1.

Рекомендуется для одной задачи выбирать 1-2 признака x_j *и не более 7 признаков* a_i *так, чтобы для каждого признака* x_j *было не менее 3-х признаков* a_i.

3. Методология оценивания значимости признаков

Для каждой рассматриваемой переменной (кандидата) определим значимость по признаку x_j в виде $x_j(v_p)$. Оценку будем формировать в интервале [0,1]. Такой подход позволяет помимо явного определения значимости (незначимости) $x_j = \{0,1\}$, задать также промежуточные оценки (некоторой значимости), например, $x_j(v_p) = \{0, 0.1, 0.2, 0.3, ..., 0.9\}$. Это оценивание означает, что рассматриваемая переменная v_p значима по признаку x_j с оценкой $x_j(v_p)$, следовательно, переменная значима для определенной задачи мониторинга, так как оценивание производится по всем признакам, все задачи будут покрыты.

Так как для v_p имеется явная избыточность, исходя из технологий WMI, эти переменные дополнительно оцениваем по a_i. Фактически формируем экспертные оценки значимости переменной v_p по признакам a_i. Оценки выбираем в интервале [0,1].

Признаки a_i выбираем так, чтобы они характеризовали наиболее важные свойства всех переменных v_p и соответствовали задачам мониторинга. В этом случае часть признаков a_i учитывается для одних признаков x_j, а часть для других. Факт принадлежности признака определенной переменной будем задавать дополнительным коэффициентом b_{ij}:

$$b_{ij} = \begin{cases} 1, \text{if}(a_i(x_j, v_p) > 0, \\ 0, \text{if}(a_i(x_j, v_p) \le 0. \end{cases} \quad (1)$$

При этом будем допускать и боле слабые ограничения

$$b_{ij} = \begin{cases} 1, \text{if}(\text{bool}(a_i(x_j, v_p) = \text{TRUE}), \\ 0, \text{if}(\text{bool}(a_i(x_j, v_p) = \text{FALSE}), \end{cases} \quad (2)$$

где $\text{bool}(a_i(x_j, v_p) = \text{TRUE}$ означает, что признак a_i используется для признака x_j независимо от значимости $a_i(x_j, v_p)$.

Формирование правила выбора переменных

Для выбора переменных для каждой из них определяем показатель ее значимости. Введем выражение оценки значимости

$$R_2(v_p) = 1/n \sum_{j=1}^{n} x_j \left(\sum_{i=1}^{k} b_{ij} a_i \setminus \sum_{i=1}^{k} b_{ij}\right), \quad (3)$$

где x_j – основной признак, a_i – дополнительные признаки, b_{ij} – коэффициенты принадлежности.

С учетом (1) введем правило выбора

$$\Re: \; v_p \in V_M \mid R_2(v_p) \ge \lambda_v, \; p=1,..,m, \quad (4)$$

где V_M – множество значимых переменных, m – мощность начального множества переменных.

Правило $\Re$ предполагает выполнимость условия, при котором рассматриваемая переменная принадлежит множеству V_M по определенным свойствам. В основе правила используется выражение (2), которое утверждает следующее: рассматриваемая переменная будет считаться *значимой*, если ее оценка (суммарная значимость переменной) не меньше некоторого порогового значения.

В результате получим подмножество переменных с меньшей мощностью $M(V_M) < M(V_0)$. Выбранные переменные будем называть *значимыми*. Они будут образовывать итоговое множество переменных мониторинга.

4. Модифицированный метод выбора наблюдаемых переменных

Предлагаемый метод M_2 состоит из двух этапов. На первом этапе, на основании исходной цели мониторинга и признаков пространства P_x из *исходного множества переменных* формируется *начальное множество переменных* V_0 путем выбора *групп переменных*. На втором этапе с помощью признаков пространств P_x и P_a проводится экспертное оценивание переменных *начального множества* V_0 для получения *итогового множества переменных* V_M.

Метод M_2, предназначенный для выбора наблюдаемых переменных для процесса мониторинга компьютерной сети, является модифицированным вариантом предложенного ранее метода M_1 [0]. Шаги 1 – 4 метода идентичны исходному методу M_1.

Описание метода:

1. Формируются задачи мониторинга $g_p \in G$ и критерии оптимизации.
2. Выбирается базовая технология мониторинга (WMI).
3. На основании $\{g_p\}$ формируются основные признаки $\{x_j\}$.
4. В соответствии $\{g_p\}$ проводится первый этап и выбирается ***начальное множество*** априорные группы V_0 переменных (кандидатов для мониторинга) из групп переменных CIM\ROOT в соответствии с технологией WMI.
5. Учитывая предварительно выбранные переменные $v_p \in V_0$ и требования к реализации задач мониторинга, формируются признаки $a_i \in P_a$.

6. Учитывая предварительно выбранные переменные и сформированные $a_i \in P_a$, задаются коэффициенты значимости каждого признака $a_i \in P_a$ для каждой переменной V_0 в виде матрицы $\| b_{ij} \|$.

7. Формируются экспертные оценки признаков $x_i(v_p)$. Всем признакам ставится значение в диапазоне [0,1] в зависимости от оцениваемой степени значимости переменной. Результаты оценивания записываются в таблицу.

8. Формируются экспертные оценки признаков $a_i(x_j, v_p)$. Всем признакам ставится значение в диапазоне [0,1] в зависимости от степени значимости переменной. Результаты оценивания записываются в таблицу.

9. Проводится оценивание каждой рассматриваемой переменной с помощью выражения (3).

10. Задается порог значимости наблюдаемых переменных λ_v и с помощью правила выбора (4), формируется итоговый набор переменных.

5. Анализ полученных результатов

1. Предлагаемый метод позволит достаточно гибко осуществить выбор переменных, которые будут участвовать в задачах мониторинга.

2. Ориентация на технологию WMI позволяет охватывать любые, реализованные в Windows OS, процедуры оценивания показателей работы системы. При этом возможно подключать базы Registry, Events, Counters, SNMP.

3. Предлагаемые процедуры позволяют более полно использовать достаточно высокий уровень априорной определенности о наблюдаемых процессах в компьютерной сети. Именно эти предпосылки позволяют упростить процедуру экспертного оценивания.

4. Недостаток предложенной методики – использование экспертных оценок, т.е. зависимость конечных результатов от квалификации эксперта. Но так как это разовая процедура и можно корректировать список переменных в текущем режиме, то недостаток можно не учитывать.

5. Использование широко известных методов оценивания значимости переменных в исследованиях, такие как статистическое оценивание или корреляционный анализ, в данном случае нецелесообразен. Они требуют дополнительного проведения экспериментов по формированию начальной статистики.

6. Необходимость и достаточность выбора переменных

В результате использования предложенного метода должен быть получен достаточный и необходимый набор переменных для поставленных целей непрерывного мониторинга.

Необходимость выбора той или иной переменной обусловлена использованием соответствующего признака x_j. Т.е. для каждого x_j должны быть кандидаты v_p.

Достаточность обуславливается тем, что в результате решения задачи выбора для признака x_j должно выполняться условие, что для каждого x_j должна быть хотя бы одна переменная v_p, значимость которой будет $x_j(v_p) \geq \lambda_v$.

7. Пример реализации метода

Рассмотрим на примере реализацию предложенного метода:

1. Пусть планируется решить задачу менеджмента производительности компьютерной сети. Согласно общей задаче цель задается как G – контроль производительности рабочих станций компьютерной сети. Исходное множество переменных сформируем из переменных, характеризующих сетевое взаимодействие узлов компьютерной сети. В CIM эти переменные определены и описаны как «Formatted Performance Counters», они сгруппированы по 47 группам (наследники WMI класса Win32_PerfFormattedData [13]).

2. Согласно предложенному методу в соответствии с заданной целью зададим признаки пространства P_x. К таким признакам отнесем: контроль пропускной способности сети (x_1), контроль задержек, потерь и ошибок в процессе передачи данных (x_2) и контроль загруженности узлов базовыми сетевыми службами (x_3).

3. Определим начальное множество рассматриваемых переменных V_0. Прежде всего, отмечаем, что в CIM\ROOT предлагается 47 базовых групп переменных. Основываясь на выбранной цели и сформированных признаках X, выберем из 47 рассматриваемых групп переменных следующие группы: ICMP, IP, TCP, UDP. В WMI эти группы представлены классами
Win32_PerfFormattedData_Tcpip_ICMP,
Win32_PerfFormattedData_Tcpip_IPv4,
Win32_PerfFormattedData_Tcpip_TCPv4 и
Win32_PerfFormattedData_Tcpip_UDPv4.

Рассматриваемые группы состоят из следующего числа переменных: TCP – 9, UDP – 5, IP – 17, ICMP – 27 (всего 58 переменных).

4. По аналогии с [6], учитывая особенность рассматриваемых групп переменных и решаемых функциональных задач, сформируем дополнительные признаки пространства P_a.

Таблица 1

Результаты экспертного и классификационного оценивания наблюдаемых переменных группы IP для метода M_2

№ п/п	Счетчик	x_1	x_2	x_3	a_1	a_2	a_3	a_4	a_5	R_2
1	Дейтаграмм/сек	1,00	0,00	0,25	0,20	1,00	1,00	0,50	1,00	**0,94**
2	Доставлено полученных дейтаграмм/сек	0,00	0,25	0,75	0,00	0,00	1,00	1,00	0,00	**0,67**
3	Исходящих дейтаграмм отброшено	0,00	0,00	1,00	0,20	0,00	1,00	1,00	1,00	**1,00**
4	Исходящих дейтаграмм с ошибкой 'Нет маршрута'	0,00	1,00	0,00	0,20	0,00	0,10	1,00	1,00	**0,70**
5	Полученных дейтаграмм отброшено	0,00	0,00	1,00	0,20	0,00	1,00	1,00	1,00	**1,00**
6	Отправлено дейтаграмм/сек	1,00	0,00	0,25	0,20	0,00	1,00	1,00	1,00	**0,65**
7	Ошибок при сборке фрагментов	0,00	1,00	0,25	0,20	0,00	1,00	0,00	1,00	**0,83**
8	Ошибок при фрагментации	0,00	1,00	0,25	0,20	0,00	0,00	1,00	1,00	**0,83**
9	Переслано дейтаграмм/сек	1,00	0,00	0,50	0,20	1,00	1,00	0,30	1,00	**1,12**
10	Получено дейтаграмм неопознанного протокола	0,00	0,75	0,00	0,20	0,00	0,00	0,00	1,00	**0,25**
11	Получено дейтаграмм с ошибками адреса	0,00	0,75	0,00	0,20	0,00	0,00	0,00	1,00	**0,25**
12	Получено дейтаграмм с ошибками заголовка	0,00	1,00	0,00	0,20	0,00	0,00	0,00	1,00	**0,33**
13	Получено дейтаграмм/сек	1,00	0,00	0,25	0,20	0,00	1,00	0,00	1,00	**0,57**
14	Получено фрагментов/сек	1,00	0,00	0,25	0,20	0,00	0,70	0,00	1,00	**0,44**
15	Собрано фрагментов/сек	0,00	0,25	0,75	0,00	0,00	1,00	1,00	1,00	**1,00**
16	Создано фрагментов/сек	0,00	0,25	0,75	0,00	0,00	1,00	1,00	1,00	**1,00**
17	Фрагментировано дейтаграмм/сек	0,00	0,25	0,75	0,00	0,00	1,00	1,00	0,00	**0,67**

Зададим требования, чтобы эти признаки учитывали особенность и режим измерения наблюдаемых переменных. Предлагаем следующий набор признаков: единицы измерения переменной – байт/с (a_1), переменная характеризует двунаправленный поток данных (a_2), переменная вариабельна (a_3), переменная характеризует локальную сторону сетевого взаимодействия (a_4), переменная измеряется при нормальном режиме функционирования сети (a_5).

5. Будем полагать, что для первого признака значимы свойства переменных (a_1, a_2, a_3), для второго и третьего (a_3, a_4, a_5). Соответственно определим коэффициенты $\| b_{ij} \|$.

6. На основе априорной определенности проведем расширенное экспертное оценивание всех рассматриваемых переменных для каждого признака. Каждому признаку $x_j(v_i)$ и $a_j(v_i)$ ставим значение в диапазоне [0,1] в зависимости от степени значимости переменной по заданному признаку (риск эксперта). Результаты оценивания переменных группы IP приведены в табл. 1.

Проведем классификационное оценивание по каждой переменной, вычисляя выражение $R = 1/n \sum_{i=1}^{n} x_i (\sum_{j=1}^{k} b_{ij} a_j \setminus \sum_{j=1}^{k} b_{ij})$.

Результаты оценивания переменных группы IP приведены в табл. 1.

В соответствии с методом M_2 сформируем правило выбора $\Re_2$, задав пороговый уровень $\lambda_v = 0,75$.

$$\Re_2 : v_p \in V_M \mid R_2(v_p) \geq 0,75,\ i=1,..,58$$

В итоге по группе IP из 17 переменных выбираем 8 переменных. Рассматривая по аналогии группы TCP, UDP, ICMP получаем из 58 переменных набор из 29 переменных.

Как видим, метод M_2 оказался более гибким, так он позволяет варьировать порог значимости. Но он более трудоемкий на этапе экспертного оценивания.

Выводы

Представленные решения могут быть использованы при реализации процесса мониторинга ком-

пьютерных сетей в случае необходимости снижения уровня служебного трафика. При этом предполагается использование переменных репозитария CIM-WMI, оценивание значимости каждой переменно на основе двух типов признаков и интервальных оценок (новизна). Все положения подтверждаются примером п.7.

Сравнительный анализ. Полученные решения сравнимы, прежде всего, с результатами [6]. Основное отличие состоит в уточнении концептуальных положений о выборе переменных для задач мониторинга и использовании вместо дискретных оценок значимости – интервальных. Такой подход предоставляет более гибкие возможности оценивания и выбора переменных наблюдения, позволяя учесть условия, когда экспертная оценка не соответствует точному значению {0,1}. Использование интервальных оценок потребовало полное изменение основных правил выбора переменных.

В отличие от других методов уменьшения служебного трафика, например [2, 3, 4, 5], данный метод может быть реализован до активной фазы мониторинга и вписан в процедуры реализации общей политики менеджмента компьютерной сети (поддержание заданного допустимого уровня служебного трафика).

Дальнейшее развитие методологии уменьшения служебного трафика в компьютерных сетях предполагает более широкое использование априорной информации о наблюдаемых процессах при их моделировании.

Научная новизна состоит в том, что получил дальнейшее развитие метод выбора наблюдаемых переменных для процесса непрерывного мониторинга компьютерной сети. Особенность метода заключается в использовании интервальных экспертных оценок при определении значимости каждой переменной.

Практическая ценность заключается в возможности более полного учета априорной информации о выбираемых для наблюдения переменных.

Такой подход позволяет регулировать поток собираемых данных в компьютерной сети. Это приводит к уменьшению затрат в процедурах мониторинга и оптимизации планирования процедур мониторинга.

Список литературы

1. *Clemm A. Network Management Fundamentals / A. Clemm. – Cisco Press. – 2006. – 510 c. – ISBN 1-58720-137-2.*
2. *Bulut A. Optimization Techniques for Reactive Network Monitoring / A. Bulut, N. Koudas, A. Meka, A.K. Singh, D. Srivastava // IEEE Transactions on Knowledge and Data Engineering. – 2009. – Volume 21, Issue 9. – P. 1343-1357.*
3. *Hernandez E. Adaptive Sampling for Network Management / E. Hernandez, M. Chidester, A. George // Journal of Network and Systems Management. – 2001. – Vol. 9, № 4. – P. 409-434.*
4. *Dilman M. Efficient Reactive Monitoring / M. Dilman, D. Raz // IEEE journal on selected areas in communications. – 2002. – Vol. 20, № 4. – P. 668-676.*
5. *Саенко В.И. Метод выбора моментов измерений для процессов непрерывного мониторинга / В.И. Саенко, А.И. Грищенко // Радиоэлектроника и информатика. – 2007. – №4. – С. 119-122.*
6. *Грищенко О.І. Метод вибору спостережуваних змінних для процесів безперервного моніторингу комп'ютерної мережі / О.І. Грищенко, В.І. Саєнко // Системи обробки інформації. – Х.: ХУ ПС, 2012. – Вип. 2 (100). – С. 188-194.*
7. *Yu Zhang. Theoretical and Practical Frameworks for Agent-Based Systems\IGI Global; 1 edition / Yu Zhang. (May 31, 2012). – 343 p.*
8. *Дж.-О. Ким. Факторный, дискриминантныи и кластерный анализ / Дж.-О. Ким, Ч.У. Мьюллер, У.Р. Клекка и др.; под ред. И.С. Енюкова. – М.: Финансы и статистика, 1989. – 215 с.*
9. *Lavy M. Windows Management Instrumentation (WMI) / M. Lavy, A. Meggitt. – New Riders. – 2001. – 432 c. – ISBN 1-57870-260-7.*

Поступила в редколлегию 21.05.2013

Рецензент: д-р техн. наук, проф. Н.И. Самойленко, Харьковская национальная академия городского хозяйства, Харьков.

РОЗШИРЕНИЙ МЕТОД ВИБОРУ СПОСТЕРЕЖУВАНИХ ЗМІННИХ ДЛЯ МОНІТОРИНГУ КОМП'ЮТЕРНОЇ МЕРЕЖІ

В.І. Саєнко

Розглядаються питання підвищення ефективності моніторингу шляхом зниження навантаження на комп'ютерну мережу службового трафіку. Запропоновані методологічні рішення для вибору достатнього числа контрольованих змінних. Метод використовує інтервальні оцінки значущості. Приклади розглядаються у рамках технології WMI.

Ключові слова: *комп'ютерна мережа, моніторинг, WMI, спостережувана змінна.*

EXTENDED METHOD OF CHOOSING OBSERVED VARIABLES FOR NETWORK MONITORING

V.I. Sayenko

The questions on increase of monitoring efficiency by a deloading on the service traffic in computer network are considered. Methodological solutions of choosing observed variables for network monitoring are offered. The method uses the interval meaningful estimations. Experimental data are got within the WMI network monitoring technology.

Keywords: *computer network, monitoring, WMI, observed variable.*