УДК 519.873
DOI: 10.25206/1813-8225-2018-159-133-136

Н. Р. СТОРОЖЕНКО
А. И. ГОЛЕВА

Омский государственный
технический университет,
г. Омск

ПОСТРОЕНИЕ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ПРОЦЕССА МОНИТОРИНГА ПАРАМЕТРОВ ИНФОРМАЦИОННОЙ СИСТЕМЫ

Стремительное развитие информационных сетей в наше время требует высоких показателей доступности, быстродействия и отказоустойчивости. Для достижения наилучших характеристик этих параметров существует необходимость их мониторинга. В работе выделены наиболее актуальные состояния в процессе мониторинга сети, на основе чего, с помощью аппарата цепей Маркова, была построена математическая модель, учитывающая зависимость вероятностей событий от времени и описывающая процесс мониторинга неисправных параметров сетевого оборудования. Предложен метод вероятностного прогнозирования состояния полного отказа сети.

Ключевые слова: вероятностное прогнозирование, информационная система, математическая модель, мониторинг сетевых параметров, надежность сетевых ресурсов.

Введение. Стремительное развитие информационных систем (ИС) в последние годы повысило интерес к проблемам надежности, безопасности, эффективного использования ресурсов и оперативного доступа к ним. Эти проблемы особенно остро проявляются в крупных компьютерных системах научно-исследовательских центров, промышленных предприятий и объектов оборонного комплекса. Такие системы должны отвечать требованиям отказоустойчивости и доступности для каждого зарегистрированного пользователя, так как от настройки и функционирования сетей зависит работоспособность всего предприятия [1].

Таким образом, современные информационные системы и сети нуждаются в постоянном контроле и мониторинге, так как работа производственных цехов, конструкторов и технологов невозможна без отлаженной системы связи, мгновенного обмена данными, систем контроля, диагностики и информационной безопасности.

Исследования в области мониторинга ИС. Проблема обеспечения надежности, безопасности и доступности сетевых ресурсов любой организации сейчас стоит довольно остро.

В связи с нарастающей сложностью, масштабом и интенсивным развитием сети становится трудно осуществлять контроль и прогнозирование возможных отклонений в параметрах серверного и коммутационного оборудования. Тем не менее необходимо непрерывно проводить контроль и диагностику оборудования и в случае обнаружения сбоев сообщать администратору.

Эти задачи можно отнести к множеству задач управления сетью.

Под мониторингом информационных систем понимают функции постоянного контроля и наблюдения за техническим состоянием объектов в пределах сети с целью обнаружения замедлений, неисправностей, отказов и аномалий в их работе и оповещения сетевых администраторов.

Системы мониторинга позволяют автоматизировать проверку оборудования и сбор статистики о функционировании сети, ускоряют обнаружение проблем и способствуют минимизации времени их устранения.

В отличие от систем обнаружения и предотвращения вторжений, мониторинг не только предполагает управление безопасностью, выявляя и не допуская потенциально опасную деятельность неавторизованных пользователей, но и обеспечивает функционирование подсистем управления конфигурацией сети, контроля и анализа производительности и надежности объектов сети, обработки ошибок и управления устранением неисправностей.

Проблемы анализа состояния надежности и безопасности технических систем и средств описаны в работах отечественных и зарубежных авторов [1–8].

Так, в работах Дружинина Г. В. и Ушакова И. А. описываются общие принципы построения математических моделей и подходы к расчету и моделированию параметров классической теории надежности [3].

В качестве математического аппарата Можаев С. А. в работе [4] рассматривает возможность применения графических и аналитических средств алгебры логики для моделирования работоспособ-

Рис. 1. Схема алгоритма мониторинга

ности систем, не учитывая при этом функции контроля и мониторинга.

В работе [5] рассматривается нейросетевой подход к выявлению неисправностей, а также разрушительных последствий от действий в ИС; данный подход сочетает достаточно «высокую скорость обработки сетевого трафика и результативность в определении сетевых атак», кроме того, предложена «система, реализующая как проверку подлинности, так и проверку целостности программного обеспечения» [6].

В работе [7] рассматриваются причины и последствия применения систем контроля и мониторинга сетевых ресурсов, а также описываются основные принципы работы таких систем без применения математического аппарата.

Анализ литературных источников по теме контроля и мониторинга сетевых ресурсов, посвященных вопросам повышения непрерывности функционирования информационных систем, позволил сделать ряд выводов.

1. На сегодняшний день одним из основных и приоритетных направлений деятельности в сфере информационных технологий является создание и применение систем мониторинга состояния и поведения сегментов сети с целью своевременного выявления и предотвращения влияния деструктивных факторов.

2. В рассмотренных работах при построении математических моделей в расчет берутся лишь базовые показатели надежности технической системы, при этом не учитываются функции, выполняемые в процессе контроля системой мониторинга. В данной статье делается попытка устранения указанных недостатков путем моделирования процедур обнаружения аномалий и прогнозирования состояния полного отказа сети, что позволяет повысить адекватность модели.

Прежде чем приступать к моделированию мониторинга информационной системы, следует детально рассмотреть процессы, связанные с ним.

Объект моделирования. Комплексный процесс мониторинга включает две основные процедуры — процедуру сбора исходных параметров и данных о работе узлов в сети: статистики по циркулирующим в сети пакетам различных протоколов, состоянии портов коммуникационных устройств и т.п. [9]. Затем выполняется процедура анализа полученных на первом этапе параметров с последующим сравнением их с заданными эталонными значениями для принятия решения о нормальном функционировании или обнаружения причин замедленной или ненадежной работы элементов сети:

$$Z = \{Z_H, Z_З, Z_O\}, \quad (1)$$

где Z — множество возможных значений опрашиваемых параметров; Z_H — подмножество значений, указывающих на нормальное функционирование; $Z_З$ — подмножество значений, указывающих на замедления в работе устройств; Z_O — подмножество значений, указывающих на отказ.

Схема алгоритма мониторинга представлена на рис. 1.

В структуре управления сложной системы мониторинг решает следующие задачи:

1) проверка работоспособности и анализ состояний объекта диагностики;

2) поиск дефектных элементов и причин отказа;

3) прогнозирование технического состояния объекта диагностики.

Мониторинг сети может выполняться с помощью различных программных или аппаратных решений. Выбор способов и объектов мониторинга в сети зависит от нескольких факторов — конфигурации сети, коммутационного оборудования и серверов, действующих сервисов и служб и т.п. В данной статье при моделировании процесса мониторинга рассматривался обобщенный принцип функционирования современных систем мониторинга, а не какое-либо конкретное решение, для возможности универсального применения модели.

В общем случае к объектам мониторинга можно отнести следующие параметры:

— физическая доступность оборудования;

— состояние оборудования, служб и сервисов сети;

— параметры функционирования сети: уровни загрузки процессора, свободное место на дисках, производительность, время отклика, память, резкое увеличение сетевого трафика;

— журналы и отчеты на наличие ошибок (помогает выявить частые или систематические отказы).

Для определения степени обнаружения различных аномалий, неисправностей и отказов в данной работе предлагается постановка и решение задачи математического моделирования процесса мониторинга параметров оборудования информационной системы. Ввиду реализации модели для удобства и наглядности целесообразно представить процесс мониторинга в виде схемы алгоритма (рис. 1).

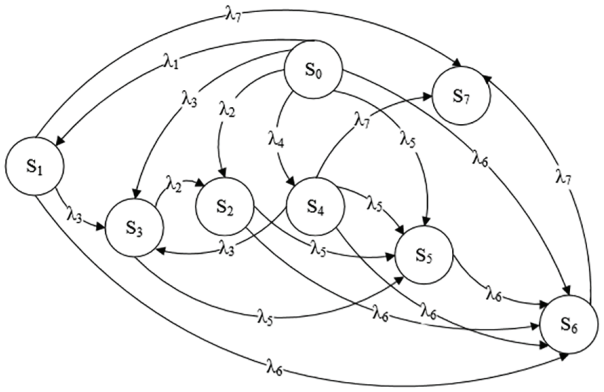

Рис. 2. Граф обнаружения неисправных параметров в процессе мониторинга

Постановка задачи и описание модели. Поскольку события, происходящие в ИС и сетях, носят случайный характер, для их изучения наиболее подходящими являются вероятностные математические модели теории массового обслуживания. В данном случае предлагается использовать теорию марковских цепей.

Цепи Маркова представляют собой широко известный математический аппарат для описания разнообразных проблем вероятностного характера. Цепь может записываться в виде графа с вершинами (состояниями системы) и ребрами (интенсивностями перехода) в данные состояния. По построенному графу можно найти вероятности каждого из состояний как в условиях изменения параметров во времени, так и в условиях предельного стационарного режима работы системы [10].

На начальном этапе моделирования необходимо определить входные данные: в качестве состояний рассматриваемой системы мониторинга предлагается рассмотреть события, связанные с обнаружением неисправностей в ходе диагностики и контроля исследуемых системой параметров оборудования в сети.

Исходя из вышеизложенного, опишем возможные состояния в процессе мониторинга параметров сетевого оборудования:

— S_0 — отсутствие неисправностей;
— S_1 — проблемы с жестким диском;
— S_2 — проблемы с оперативной памятью;
— S_3 — перегрузка процессора;
— S_4 — перегрузка трафика;
— S_5 — недоступность порта;
— S_6 — физическая недоступность устройства;
— S_7 — полный отказ системы.

Описанную цепь событий в ходе мониторинга сети можно представить в виде графа состояний (рис. 2).

После определения входных параметров системы можно приступать к математическому описанию.

Для построения модели полагаем, что обнаружение любых неисправностей описываемой системой мониторинга рассматривается как случайный процесс с конечным числом состояний. При этом события происходят поодиночке, а не группами по нескольку сразу, что означает ординарность модели. Кроме того, модель не содержит последействия в силу того, что для любых двух непересекающихся участков времени число событий, попадающих на один из них, не зависит от того, сколько событий попало на другой.

Вероятность i-го состояния определяется в данном случае как вероятность нахождения системы в состоянии S_i, то есть вероятность обнаружения системой мониторинга i-го неисправного параметра в сети.

На графе состояний каждой стрелке соответствует интенсивность того потока событий, который переводит систему из одного состояния в другое.

Мониторинг, предусматривающий постоянный операторский контроль, представляет собой систему упорядоченного опроса [11]. Последовательность опроса определяется назначенным администратором приоритетом. Чем выше приоритет у параметра сетевого устройства, тем выше интенсивность его опроса. За интенсивности переходов в данном случае принимается λ_i — интенсивность опроса i-го параметра в системе мониторинга.

С учетом изложенного описания работы системы мониторинга следует, что она из состояния S_0 при выполнении опроса сетевых устройств при отказе любого компонента переходит в состояние обнаружения неисправности S_i с интенсивностью λ_i.

По графу состояний (рис. 2) составляется математическая модель процесса мониторинга в виде системы уравнений (2):

$$\begin{cases} \frac{dp_0}{dt} = -p_0 \cdot (\lambda_1 + \lambda_2 + \lambda_3 + \lambda_4 + \lambda_5 + \lambda_6), \\ \frac{dp_1}{dt} = p_0 \cdot \lambda_1 - p_1 \cdot (\lambda_3 + \lambda_6 + \lambda_7), \\ \frac{dp_2}{dt} = p_0 \cdot \lambda_2 + p_3 \cdot \lambda_2 - p_2 \cdot (\lambda_5 + \lambda_6), \\ \frac{dp_3}{dt} = p_0 \cdot \lambda_3 + p_1 \cdot \lambda_3 + p_4 \cdot \lambda_3 - p_3 \cdot (\lambda_2 + \lambda_5), \\ \frac{dp_4}{dt} = p_0 \cdot \lambda_4 - p_4 \cdot (\lambda_3 + \lambda_5 + \lambda_6 + \lambda_7), \\ \frac{dp_5}{dt} = p_0 \cdot \lambda_5 + p_2 \cdot \lambda_5 + \\ + p_3 \cdot \lambda_5 + p_4 \cdot \lambda_5 - p_5 \cdot \lambda_6, \\ \frac{dp_6}{dt} = p_0 \cdot \lambda_6 + p_1 \cdot \lambda_6 + p_2 \cdot \lambda_6 + \\ + p_4 \cdot \lambda_6 + p_5 \cdot \lambda_6 - p_6 \cdot \lambda_7, \\ \frac{dp_7}{dt} = p_1 \cdot \lambda_7 + p_4 \cdot \lambda_7 + p_6 \cdot \lambda_7. \end{cases} \quad (2)$$

Решение системы дифференциальных уравнений (2) позволяет отследить динамику диагностирования неисправных параметров в процессе сетевого мониторинга путем отслеживания вероятностей в определенные промежутки времени.

В случае, если необходимо рассмотреть вероятности состояния системы мониторинга в предельном установившемся режиме, следует перейти к линейной системе уравнений, приравняв левые части дифференциальных уравнений к нулю.

Для моделирования функций прогнозирования системы мониторинга необходимо учесть тот факт, что состояния на последующих шагах зависят от предыдущих. Исходя из этого, будущие состояния можно характеризовать при помощи условных вероятностей (2):

$$p(AB) = p(A) \cdot p(B \mid A), \quad (3)$$

где $p(AB)$ — совместная вероятность событий A и B; $p(A)$ — вероятность события A; $p(B \mid A)$ — вероятность возникновения события B при условии возникновения события A.

Тогда вероятность состояния S_n с учетом вероятностей на предыдущих состояниях определяется по формуле:

$$p(S_0 S_2 ... S_n) = p(S_0) \prod_{j=1}^{n} p\left(S_j \mid S_0 S_1 .... S_{j-1}\right). \quad (4)$$

Процесс является n-связным, если на исход испытания основное влияние оказывают результаты n предыдущих испытаний.

В нашем случае для рассматриваемой системы с графом состояний (рис. 2) S_0, S_1,..., S_7, $n=8$. Если учесть, что на состояние полного отказа системы S_n в процессе мониторинга основное влияние оказывают результаты $n-1$ предыдущих испытаний, то справедлива формула:

$$p(S_1 ... S_n) = p(S_1) \cdot \prod_{j=2}^{n} p\left(S_j \mid S_1 S_2 .... S_{j-1}\right). \quad (5)$$

Таким образом, полученная формула позволяет осуществить статистическое прогнозирование состояния полного отказа сети в процессе мониторинга на основе данных от предыдущих состояний неисправности, что дает возможность, в дополнение к моделированию обнаружения неисправных параметров (2), математически описать процедуру прогнозирования системы мониторинга.

Заключение. В данной работе на основе вероятностных методов построена модель, описывающая процесс сетевого мониторинга и обнаружения неисправностей. Кроме того, разработанная модель позволяет учесть вероятностное прогнозирование состояния полного отказа сети при учете вероятностей предыдущих состояний. Таким образом, решение представленной модели позволит получить конкретные значения вероятностей обнаружения неисправностей системой мониторинга в зависимости от времени наблюдения. Полученные значения дают наглядное представление о моделируемых процессах. Создание алгоритма и программной его реализации позволит не только оптимизировать процесс моделирования, но и предоставит возможность наблюдения за поведением системы в условиях изменения параметров.

Библиографический список

1. Цвитун А. А., Корнейчук В. И., Долголенко А. Н. Надежность компьютерных сетей. Киев: Корнійчук, 2010. 116 с. ISBN 966-7599-67-6.

2. Дружинин Г. В. Надежность автоматизированных систем. 3-е изд., перераб. и доп. М.: Энергия, 1977. 536 с.

3. Ушаков И. А. Надежность технических систем. М.: Радио и связь, 1985. 608 с.

4. Можаев А. С. Универсальный графоаналитический метод, алгоритм и программный модуль построения монотонных и немонотонных логических функций работоспособности систем // Моделирование и анализ безопасности, риска в сложных системах: тр. Междунар. науч. школы. СПб.: СПбГУАП, 2003. С. 101–110.

5. Талалаев А. А., Тищенко И. П., Фраленко В. П., Хачумов В. М. Анализ эффективности применения искусственных нейронных сетей для решения задач распознавания, сжатия и прогнозирования // Искусственный интеллект и принятие решений. 2008. № 2. С. 24–33.

6. Ачилов Р. Построение защищенных корпоративных сетей. М.: Наука и техника, 2013. 250 с. ISBN 978-5-94074-884-7.

7. Уилсон Э. Мониторинг и анализ сетей. Методы выявления неисправностей / пер. с англ. О. Труфанова. М.: Лори, 2013. 350 с. ISBN 5-85582-350-9.

8. Стороженко Н. Р., Голева А. И. Анализ и оценка отказоустойчивости сетевых ресурсов // Виртуальное моделирование, прототипирование и промышленный дизайн: материалы IV Междунар. науч.-практ. конф., 15–17 ноября 2017 г. Тамбов, 2017. Т. 3, вып. 4. С. 240–244. ISBN 978-5-8265-1839-7.

9. Куракин А. Мониторинг. Различение аномалий. Саарбрюккен (Германия): LAP Lambert Academic Publishing, 2014. 112 с. ISBN 978-3-659-54102-5.

10. Вентцель Е. С. Исследование операций: задачи, принципы, методология. 6-е изд., М.: Юстиция, 2018. 192 с. ISBN 978-5-4365-1925-8.

11. Бакланов А. И. Системы наблюдения и мониторинга. М.: Бином, 2014. 234 с. ISBN 978-5-94774-905-2.

СТОРОЖЕНКО Никита Русланович, аспирант кафедры «Информатика и вычислительная техника» Омского государственного технического университета (ОмГТУ); инженер-программист АО «Омский научно-исследовательский институт приборостроения» (АО «ОНИИП»).
Адрес для переписки: snikr@bk.ru
ГОЛЕВА Алина Игоревна, аспирант кафедры «Информатика и вычислительная техника» ОмГТУ; инженер-программист АО «ОНИИП».
Адрес для переписки: frybkf07.93@mail.ru

Для цитирования

Стороженко Н. Р., Голева А. И. Построение математической модели процесса мониторинга параметров информационной системы // Омский научный вестник. 2018. № 3 (159). С. 133–136. DOI: 10.25206/1813-8225-2018-159-133-136.

Статья поступила в редакцию 16.04.2018 г.