К.С. ТКАЧЕНКО

Динамическая реструктуризация однородных сетей и распределенных сред при условии вирусных атак и несанкционированного доступа

ФГБОУ ВО
«Севастопольский
государственный
университет»,
г. Севастополь

УДК 004.75

Рассматривается решение задачи динамической реструктуризации однородных сетей и распределенных сред при условии априорной неопределенности входных данных, связанной с возможными вирусными атаками и несанкционированным доступом в вычислительные системы. При этом используется подход на основе алгоритмов стохастической аппроксимации.

На сегодняшний день остро стоит вопрос защиты различных сложных вычислительных систем, в том числе в основе которых лежат однородные сети и распределенные среды, от различных вредоносных вторжений. К таким вторжениям можно отнести разнообразные вирусные атаки (ВА) и атаки несанкционированного доступа, которые для удобства дальнейшего рассмотрения можно включить в класс ВА. Нерешенной прежде частью общей проблемы является решение частной задачи динамической реструктуризации с использованием рекуррентных методов автоматного управления.

Книга [1] посвящена адаптивному управлению стохастическими системами с конечным множеством управляющих воздействий, а именно, проблеме адаптивного выбора вариантов. При этом с единых позиций рассматриваются задачи безусловного и условного выбора, игровые задачи и задача адаптивного управления конечными однородными марковскими цепями. В работе [2] исследуются простейший и иерархический автоматные алгоритмы и демонстрируется, что учет дополнительной априорной информации

о специфике структуры решаемой задачи позволяет повысить эффективность автоматных алгоритмов. В статье [3] анализируется задача принятия решений по управлению рисками, возникающими при оценке состояния объектов критического применения. Показаны примеры экспериментального исследования применимости статистических критериев для случайных выборок. В публикации [4] подвергаются разбору задачи системной динамики сетей обработки данных в условиях действия ВА. Предлагается совокупность оптимизационных задач выбора структуры и параметров комплементарных детекторов ВА. В материалах [5] производится решение задачи обнаружения ВА на основе разработанного программного стенда при использовании непараметрических статистических критериев.

Целью данной публикации является исследование решения задачи динамической реструктуризации однородных сетей (и распределенных сред) при условии априорной неопределенности входных данных, связанной с возможными ВА и несанкционированным доступом в вычислительные системы, на основе алгоритмов стохастической аппроксимации.

Пусть в вычислительной системе, на основании которой реализуются однородные сети и распределенные среды, имеется диспетчер. Диспетчер имеет возможность выполнять динамическую реструктуризацию системы, а именно, управлять подключением отдельных узлов системы между собой. Это позволяет определенным образом видоизменять процесс обработки пакетов заданий на узлах системы, их поступлением в среду и выдачу результатов обработки (в том числе пользователям).

При этом ВА может быть подвергнута с неизвестной функцией распределения вероятностей каждая группа вычислительных узлов и, при возникновении результативной ВА их производительность линейно убывает в зависимости от времени начала атаки. Интенсивность ВА не зависит от интенсивности входного потока заданий. Диспетчеризация заданий с целью обнаружения ВА осуществляется с заданной периодичностью. Возможно изменение дисциплины функционирования групп узлов при наличии ВА путем увеличения их производительности до определенного предела.

Среда представляет собой сложную, разветвленную компьютерную систему, организованную в иерархические и многоуровневые структуры. Поступление пакетов заданий (заявок) в узлы нижних уровней осуществляется из более высокого уровня, а именно, центрального крупного маршрутизатора, который обслуживает все узлы низкого уровня, осуществляющие вычислительные работы.

Организация управления вычислительными процессами этой иерархической разветвленной системы состоит в нахождении стратегий управления, обеспечивающих необходимое качество функционирования каждой из подсистем. Это возложено на диспетчер.

Структура изображается на рисунке 1.

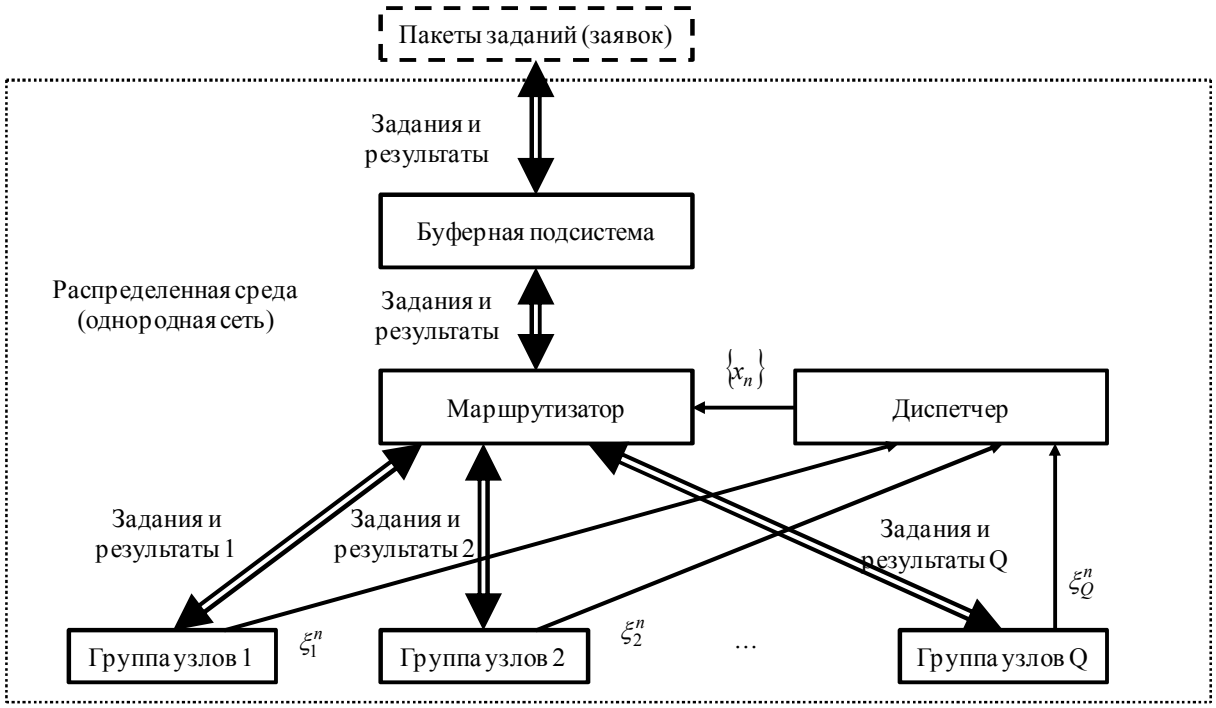

Рис. 1. Структура вычислительной среды

Пусть группы вычислительных узлов, действуя независимо друг от друга, могут выполнять обработку пакетов задач от управляемого диспетчером маршрутизатора и возвращать через него же результат и значение ограниченной функции текущих потерь ξ_j^n, где n — номер такта T ($T = 1,2,\ldots$), j — номер группы вычислительных узлов. При этом в векторе управляющих воздействий

$\{x_n\} = (x_n^1, \ldots, x_n^Q)$ $x_n^j = 0$, если j-ая группа вычислительных узлов отключена от маршрутизатора, и $x_n^j = 1$, если j-ая группа вычислительных узлов подключена к маршрутизатору. В случае отключения от маршрутизатора информационного обмена между группой и конечным получателем результатов не происходит, в случае подключения, соответственно, происходит.

Задается ξ_j^n в виде:

$$\xi_j^n = C_{очер}\left(\frac{\overline{l_{ocher}}}{\overline{l_{porog}}}\right) + C_{про}\left(\frac{\mu}{\mu_{\min}}\right) + C_{съем}\left|\frac{\Delta t_j^A}{\Delta t_j} - 1\right|. \qquad 1)$$

Пусть для удобства проведения расчетов в (1) группа узлов является процессором переменной производительности. Тогда в (1) $\mu_{\min}$ — это минимальная производительность процессора, минимально возможное значение параметра μ. $\mu_{\min}$ — максимальная производительность процессора, максимально возможное значение параметра μ. $\Delta\mu$ — квант изменения производительности процессора, шаг изменения μ. μ — мгновенная оценка производительности процессора. $\overline{l_{porog}}$ — пороговое значение средней длины очереди, критическое значение средней длины очереди. $\overline{l_{ocher}}$ — оценка значения средней длина очереди. Δt_j — это время, которое проходит между двумя измерениями параметров модели. Δt_j^A — вероятное пороговое время между двумя атаками, которое может проходить между двумя ВА.

При использовании подхода на основе проекционных алгоритмов стохастической аппроксимации и разработанной программной системы поддержки принятия решений (СППР) управление в диспетчере осуществляется следующим образом:

Шаг 1. Получение ограниченных небинарных потерь;

Шаг 2. Реализация одного шага алгоритма оптимизации;

Шаг 3. Выбор варианта методом деления отрезка;

Шаг 4. Пока нет останова переход к шагу 1.

При этом выполняется оптимизация для заданного числа шагов и заданных параметров алгоритмов, обеспечивается обработка

ошибок и исключений, поддерживается графический пользовательский интерфейс.

Входными данными для СППР являются: выбранный алгоритм оптимизации, его параметры, число шагов оптимизации, характер функций текущих потерь, текущие потери. Выходными данными являются: набор результирующих выбранных вариантов управления, величины средних текущих потерь, их статистические оценки, график величин текущих средних потерь.

Вывод. В работе приводится описание подхода решения задачи динамической реструктуризации распределенной среды и однородной сети в условиях ВА. Перспективой дальнейших изысканий станет нахождение эффективных значений Δt_j и $\Delta\mu$.

Литература

1. Назин А.В. Адаптивный выбор вариантов. Рекуррентные алгоритмы / А.В. Назин, А.С. Позняк. — М.: Наука, 1986. — 288 с.

2. Назин А.В. О повышении эффективности автоматных алгоритмов адаптивного выбора вариантов / А.В. Назин // Адаптация и обучение в системах управления и принятия решений. — Новосибирск: Наука, 1982. — 208 с.

3. Маловик К.Н. Управление рисками при непараметрической статистической оценке состояния объектов критического применения / К.Н. Маловик, Н.А. Скаткова, В.С. Ловягин // Вісник СевНТУ: зб. наук. пр. Вип. 131/2012. Серія: Інформатика, електроніка, зв'язок. — Севастополь, 2012. — С.55—62.

4. Скатков А.В. Комплементарное детектирование атак в телекоммуникационных системах критического применения / А.В. Скатков // Information technologies in education, science and production, 2013, ed. № 4 (5). — С.136—146.

5. Скатков А.В. Анализ мощности непараметрических критериев при оценивании состояния объектов критического применения / А.В. Скатков, К.Н. Маловик, Л.П. Луговская, В.С. Ловягин // Радіоелектронні і комп'ютерні системи, 2012, № 6 (58). — С.271—275.

TKACHENKOKIRILLSTANISLAVOVICH@MAIL.RU,
TKACHENKOKIRILLSTANISLAVOVICH@GMAIL.COM