К.С. ТКАЧЕНКО

Особенности реализации моделирования методов своевременного обнаружения вирусных атак в однородных сетях

Севастопольский национальный технический университет, г. Севастополь

УДК 004.75

Исследуются особенности реализации моделирования методов своевременного обнаружения вирусных атак в однородных сетях. Разработанные методы позволяют выполнять управление процессами в однородных сетях критического применения при использовании непараметрических критериев и рандомизированных стратегий.

В общем виде проблема моделирования методов своевременного обнаружения вирусных атак (ВА) в однородных сетях актуальна, связана с важными научными и практическими задачами проектирования однородных сетей, компьютерных сетей, распределенных сред, сетей и систем, объектов критического применения. Имеется априорная неопределенность функции значений текущих затрат на своевременное обнаружение ВА ξ_n в интервал времени n. При этом возникает оптимизационная задача минимизации предельных значений средних текущих потерь:

$$\lim_{n\to\infty} \Phi_n = \lim_{n\to\infty} \frac{1}{n} \sum_{t=1}^{n} \xi_t = \Phi^{\min} \to \min \qquad (1)$$

Задача (1) не может быть решена аналитическими методами. В монографии [1] приводится решение ряда задач адаптивного управления стохастическими системами с конечным множеством управляющих воздействий. В статье [2] рассматривается вопрос повышения эффективности процесса мониторинга систем управления критического применения. В книге [3] обобщаются результаты исследо-

ваний в области распределенных вычислений в масштабируемых средах, в том числе кластерах. В конспекте лекций [4] предлагаются методы, позволяющие обнаруживать в статистических данных неслучайные и настораживающие закономерности. В публикации [5] формулируется информационная модель задачи динамической реструктуризации распределенных сред и описание системы поддержки принятия решений для решения этой задачи. В работе [6] приводятся имитационная модель и инструментальное средство поддержки принятия решений в распределенных средах типа открытых GRID-архитектур. Описание разработанной программной системы адаптивного принятия решений при априорной неопределенности входных данных и результаты применения системы имеются в [7].

Нерешенной прежде частью общей проблемы, которой посвящена данная публикация, является описание исследования особенностей реализации моделирования методов своевременного обнаружения вирусных атак в однородных сетях.

Целью данной работы является разработка методов, позволяющих выполнять управление процессами в однородных сетях критического применения при использовании непараметрических критериев и рандомизированных стратегий.

Рандомизированные стратегии [1] используют рекуррентные правила вида:

$$p_{n+1} = R_n\left(x_1, \ldots, x_n; p_1, \ldots, p_n; \xi_1, \ldots, \xi_n\right),\ n = 1, 2, \ldots, \qquad (2)$$

где R_n — вектор-функция движения со значениями в симплексе S^N, p_n — вектор условных вероятностей выбора вариантов $x(1), \ldots, x(N)$ в момент времени t_n. Перед выбором очередного варианта x_{n+1} происходит расчет непосредственно следующих значения вероятностей выбора вариантов p_{n+1} по (2). Выбор варианта может осуществляться методом деления отрезка.

Для обнаружения в статистических данных, накопленных во множественных прогонах имитационных моделей, закономерностей, которые могут свидетельствовать о наличии сбоев, отказов, нарушениях режима секретности, ВА используются непараметрические критерии [4], что позволяет выполнять накопление и обработку статистической информации непрерывно, без предположений о зави-

симости экспериментальных данных от ограниченного числа параметров.

Методы управления процессами в однородных сетях основаны обнаружении ВА непараметрическими критериями на основе результатов имитационного моделирования системы G/G/1 с управлением. Управление осуществляется рандомизированными стратегиями с перерасчетом величин условных вероятностей $P\left(H_0 \middle| H_0\right)$ — предположение об отсутствии ВА при её фактическом отсутствии, $P\left(H_1 \middle| H_1\right)$ — предположение о наличии ВА при её фактическом наличии, $P\left(H_1 \middle| H_0\right)$ — предположение о наличии ВА при её фактическом отсутствии, $P\left(H_0 \middle| H_1\right)$ — предположение об отсутствии ВА при её фактическом наличии.

Для удобства последующего масштабирования разрабатывалась имитационная модель для одного процессорного блока переменной производительности. Этот блок подвергается ВА с априорной неопределенностью об интенсивности атаки. При этом происходит падение производительности блока по линейному закону. Мониторинг осуществляется с переменной производительностью.

При формировании аддитивной штрафной функции учитываются потери от ВА и реализации контроля. Это связано с тем, что обнаружение ВА связано с затратами ресурсов, зависящих от частоты действий по обнаружению. При малой частоте затраты низкие, но велики риск существенных потерь от ВА. При большой частоте затраты высокие, но риска существенных потерь от ВА нет.

Фрагмент программы для имитационного моделирования написан на языке программирования высокого уровня Java:

```
F_v = Cocher*(queue.size() / l_porog) + Cproiz*(mu / mu_min) +
Cdt*(dt_porog / dt - 1);
if (queue.size() > l_porog) {
   PH0H0 = Math.max(0.05, PH0H0 - 0.10);
   PH1H1 = Math.min(0.95, PH1H1 + 0.10);
   PH1H0 = Math.max(0.05, PH1H0 - 0.05);
   PH0H1 = Math.min(0.95, PH0H1 + 0.05);
     if (mu < mu_max - eps) {
         mu += mu_delta;
     }
     narusheniyaA++;
} else if (F_v < -eps) {
   PH0H0 = Math.min(0.95, PH0H0 + 0.10);
   PH1H1 = Math.max(0.05, PH1H1 - 0.10);
```

```
    PH1H0 = Math.min(0.95, PH1H0 + 0.05);
    PH0H1 = Math.max(0.05, PH0H1 - 0.05);
      if (mu > mu_min + eps) {
          mu -= mu_delta;
      }
}
if (queue1.size() > l_porog) {
   narusheniyaB++;
}
```

Семейство параметрически заданных функций текущих потерь для системы G/G/1 с управлением приводится на рис. 1, причем для наглядности было оставлено два ряда данных.

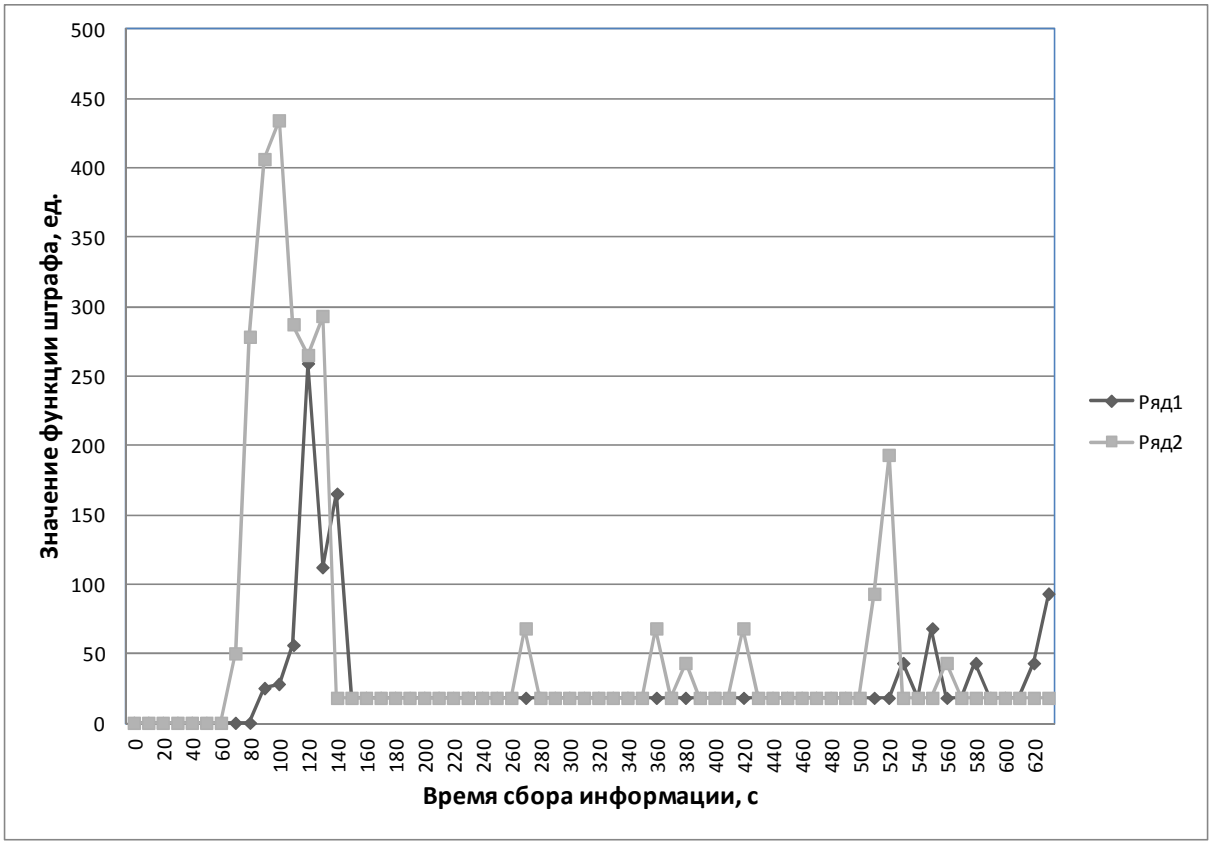

Рис. 1. Семейство параметрически заданных функций текущих потерь для системы G/G/1 с управлением

При использовании простого критерия знаков [4] для оценки значимости и направления сдвига проверяется гипотеза H_0=«нет различия в параметре положения, нет сдвига при сравнении количества превышений заранее заданной пороговой величины значениями функции штрафа системы G/G/1 с управлением по отношению к системе G/G/1 без управления». Рассчитанное значение значимости, равное 0,1334, мало. Из этого следует, что гипотеза H_0 от-

вергается, эффект управления статистически достоверен, управление в G/G/1 является полезным.

Вывод. В работе описаны методы, позволяющие выполнять управление процессами в однородных сетях критического применения при использовании непараметрических критериев и рандомизированных стратегий. Перспективой дальнейших изысканий по данной тематике станет детализация аддитивной функции значений текущих потерь.

Литература

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

2. 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.

3. Топорков В.В. Модели распределенных вычислений / В.В. Топорков. — М.: Физматлит, 2004. — 320 с.

4. Хиценко В.Е. Непараметрическая статистика в задачах защиты информации: конспект лекций / В.Е. Хиценко. — Новосибирск: Изд-во НГТУ, 2012. — 196 с.

5. Ткаченко К.С. Стохастические автоматы и имитационные модели для поддержки решения задач динамической реструктуризации распределенных сред / К.С. Ткаченко // Информатика и информационные технологии в образовании, науке и производстве: сборник научных статей. Ч. I. — Волжский: Изд-во «Нобель Пресс», 2014. — ISBN 978-5-519-01758-9 — 170 с. — С.44—47.

6. Ткаченко К.С. Модель и инструментальное средство принятия решений для открытых GRID-архитектур / К.С. Ткаченко, Н.Л. Корепанова // Збірник наукових праць Академії військово-морських сил імені П.С. Нахімова. — Севастополь: АВМС імені П.С. Нахімова, 2013. — Вип. 4(16). — 186 с. — С.105—112.

7. Ткаченко К.С. Программная система адаптивного принятия решений при априорной неопределенности входных данных / К.С. Ткаченко // Вісник СевНТУ: зб. наук. пр. Вип. 131/2012. Серія: Інформатика, електроніка, зв'язок. — Севастополь, 2012. — С.78—81.

TKACHENKOKIRILLSTANISLAVOVICH@MAIL.RU,
TKACHENKOKIRILLSTANISLAVOVICH@GMAIL.COM