УДК 519.8 + 004.052 + 004.78

А.В. СКАТКОВ[1], Д.Ю. ВОРОНИН[1], С.А. ЧОРНОМЫЗ[2]

[1] *Севастопольский национальный технический университет, Украина*
[2] *Керченский колледж экономики и информационных технологий, Украина*

ИНФОРМАЦИОННЫЙ ПРОПОРЦИОНАЛЬНО-ИНТЕГРАЛЬНО-ДИФФЕРЕНЦИАЛЬНЫЙ РЕГУЛЯТОР КАК СРЕДСТВО КОМПЕНСАЦИИ ПОСЛЕДСТВИЙ АТАК

Рассмотрена проблема обеспечения высокой готовности вычислительных сервисов критического применения при воздействии информационных атак. Предлагаемое функциональное устройство – информационный пропорционально-интегрально-дифференциальный (ИПИД) регулятор – предназначено для компенсации последствий несанкционированных действий, нарушающих штатный режим функционирования вычислительных сервисов ИУС. Для обеспечения требуемого качества обслуживания реализуется децентрализованное управление распределенным вычислительным процессом в ИУС на основе ИПИД-регулятора при использовании мультиагентного подхода. Одним из возможных направлений дельнейшего исследования является использование предлагаемого ИПИД-регулятора при решении задачи детектирования скрытых атак в критических IT-системах на основе анализа информации об утечке вычислительных ресурсов.

Ключевые слова: *ИПИД-регулятор, информационная атака, компенсационное управление распределенными вычислительными сервисами, мультиагентный подход, QoS, утечка ресурсов, идентификация скрытых атак.*

Введение

Вследствие интенсификации процессов производства, бизнеса и оказания услуг расширились сферы внедрения информационных технологий. Они широко используются и в информационно-управляющих системах (ИУС) объектов критического применения (ОКП): в здравоохранении, энергетике, экономике, транспорте и многих других [1]. Повышенные требования к готовности вычислительных сервисов ИУС обусловлены особыми функциональными свойствами ОКП: наличием поглощающего состояния, критичностью, нестационарностью, режимом реального времени, наличием информационных атак [2].

Под информационной атакой в рамках данной статьи будем понимать любое несанкционированное действие, приводящее к нарушению штатного режима функционирования вычислительных сервисов (ВС) ИУС ОКП, направленного на обеспечение требуемого качества обслуживания. Сложность организации вычислительных процессов в ИУС обусловлена возможностью возникновения дефицита ресурсов при необходимости обеспечения весьма сжатых директивных сроков окончания обработки требуемого комплекса работ. Нарушение качества обслуживания ИУС может спровоцировать переход ОКП в невозвратное (поглощающее) состояние, сопровождающееся человеческими жертвами, техногенными катастрофами и существенным материальным ущербом [2].

На сегодняшний день одной из основных проблем организации вычислительного обслуживания ИУС является отсутствие эффективных инструментальных средств, способных скомпенсировать последствия информационных атак путем перераспределения существующих или привлечения дополнительных вычислительных ресурсов. Таким образом, задача синтеза функционального устройства компенсационного управления ВС ИУС, ориентированного на обеспечение высокой готовности, является актуальной.

1. Постановка задачи исследования

Целью ИУС является синтез управлений $u_i \in U$ на промежутке [0;T], которые компенсируют возмущающее воздействие ϑ и обеспечивают требуемую фазовую траекторию Ξ, связанную с пребыванием ОКП в работоспособных состояниях S: $S_1(t)$, $S_2(t+1)$, …, $S_n(t+n)$, при безусловном выполнении целевого ограничения $P_{i\Pi}(t) \equiv 0$, $\forall i = \overline{\{1, 2, \ldots, |S|\}}$, где $P_{i\Pi}(t)$ – вероятность перехода из состояния S_i в S_Π; $S_i \in S$, $S \cap S_\Pi = \varnothing$; S_Π – поглощающее состояние ОКП. Директивные требования TrD накладыва-

ют определенный регламентом срок $T_{ДИР}$, до которого следует выработать u_i.

Для решения задачи синтеза u_i необходимо при использовании ВС ИУС выполнить заданное множество информационно-вычислительных работ IVR(t) до наступления директивного срока $t_{ДИР}$. Каждая из этих работ имеет сложную структуру, которую в общем случае можно задать графом $G_b(t)$, множество дуг которого $\Gamma_b(t) = \bigcup_a g_{b,a}(t)$, где $g_{b,a}(t)$ – дуга, поставленная в соответствие a-ому заданию b-ой работы IVR(t). Таким образом, IVR(t) порождает множество $G(t) = \bigcup_b G_b(t)$.

С точки зрения структурно-функциональной организации ВС ИУС реализованы в качестве распределенной вычислительной системы (параметры заданы множеством VS), способной при необходимости использовать дополнительные ресурсы, арендованные при помощи облачных технологий. Режим функционирования ВС ИУС, гарантирующий завершение обработки IVR(t) к $t_{ДИР}$, назовем штатным (ШРФ), то есть обеспечивающим необходимое качество обслуживание (QoS). К сожалению, ШРФ может быть нарушен в результате воздействия информационных атак на ИУС. Для компенсации их последствий необходимо эффективно управлять процессом вычислительного обслуживания IVR(t), то есть при необходимости эффективно перераспределять имеющиеся или привлекать дополнительные вычислительные ресурсы.

Пусть в соответствии с системой предпочтений $E=(e_1, e_2\ldots, e_l)$ получено множество оценок $Q_j(t_i)=(q_{1j}(t_i), q_{2j}(t_i),\ldots, q_{lj}(t_i))$, характеризующих $vr_j(t_i)$ – решение по управлению j-м узлом ВС ИУС, принятое в момент времени $t_i \in [0; T]$. Необходимо сконструировать систему правил формирования вектора $vr(t_i)=(vr_1(t_i), vr_2(t_i),\ldots, vr_{\overline{|VS|}}(t_i))$, $vr \in VR$ таким образом, чтобы вариант, выбранный из множества доступных альтернатив обеспечивал $\sum_j \Phi(Q_j, t_i, vr) \to \underset{vr \in VR}{extr}$, где VR – область допустимых управлений ВС ИУС, $j = \{1, 2, \ldots, \overline{|VS|}\}$, Φ – оператор свертки критериев, I – число элементов системы предпочтений.

2. Методика решения задачи при использовании ИПИД-регулятора

Далее для упрощения будем рассматривать частный случай поставленной задачи. Пусть в ИУС имеется всего один вычислительный сервис – $Q(t_i) = \left(K_{t_{ДИР}}(t_i, vr(t_i)), R_П(t_i, vr(t_i))\right)$, причем $vr(t_i)$ – уже скаляр, а не вектор. Системная характеристика $K_{t_{ДИР}}(t_i, vr(t_i))$, рассчитанная в момент времени $t_i \in [0; T]$, может быть использована качестве прогнозной количественной оценки степени нарушения ШРФ ВС при vr-ом варианте управления ВС ИУС.

$$K_{t_{ДИР}}(t_i, vr(t_i)) = t_i + \max_{j \in J}\left(ov_j(t_i, vr(t_i))\right) - t_{ДИР},$$

где $ov(t_i, vr(t_i))$ – вектор прогнозных значений остаточных длительностей выполнения информационно-вычислительных работ при выбранном $vr(t_i) \in VR$; VR – множество допустимых вариантов управления ВС ИУС, $J = \{1, 2, \ldots, \overline{|IVR|}\}$.

Ресурсные ограничения в момент времени $t_i \in T_y$ задаются кортежем $R = \langle R_Д, R_П(t_i, vr(t_i))\rangle$, где $R_Д$ – матрица, задающая максимальный объем доступных ресурсов в момент $t_i \in T_y$,. Ее столбцы соответствуют типам ресурсов, а строки – ресурсным ограничениям для соответствующего узла ВС ИУС. $R_П(t_i, vr(t_i))$ – функционал, характеризующий условия привлечения дополнительных ресурсов в момент времени $t_i \in T_y$ для реализации $vr(t_i)$.

Необходимо $\forall t_i \in T_y$ при соблюдении ресурсных ограничений R найти такое $vr(t_i)$, что

$$\begin{cases} K_{t_{ДИР}}(t_i, vr(t_i)) \to \min\limits_{vr(t_i) \in VR}, \\ R_П(t_i, vr(t_i)) \to \min\limits_{vr(t_i) \in VR}. \end{cases}$$

T_y – множество моментов принятия решений об управлении ВС ИУС (необходимость обусловлена последствиями информационных атак).

$$w(t_i) = M\left(K_{t_{ДИР}}(t_i, vr(t_i)), R_П(t_i, vr(t_i)), X\right),$$

где $w_i \in W$ – тип сложившейся вычислительной ситуации, M – модель классификации ситуации, X – классификационные критерии.

В рамках дальнейшего изложения материала будем считать, что $vr(t_i)$ – параметр, характеризующий приращение вычислительной мощности. Тогда цель функционирования ИПИД-регулятора (структурная схема представлена на рис.1) можно сформулировать следующим образом: $\forall k$ найти такое приращение мощности вычислительного сервиса ИУС $\Delta\mu(t_{k+1})$, чтобы при сложившейся $w(t_k)$ и текущей длине очереди не обслуженных информационно-вычислительных работ $l(t_k)$ обеспечить выполнение (1).

$$\begin{cases} K_{t_{ДИР}}(t_{k+1}, \Delta\mu(t_{k+1})) \to \min\limits_{vr \in VR}, \\ R_{П}(t_{k+1}, \Delta\mu(t_{k+1})) \to \min\limits_{vr \in VR}. \end{cases} \quad (1)$$

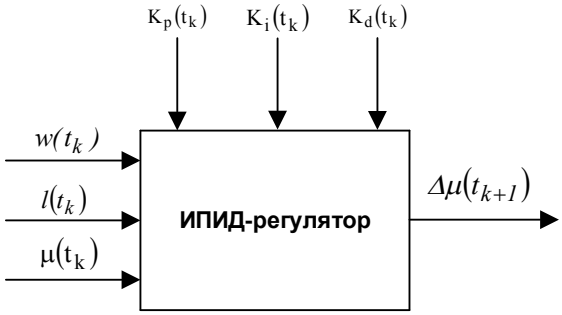

Рис. 1. Структурная схема ИПИД-регулятора

Предлагаемая методика включает следующие этапы.

1. При помощи системы мониторинга ВС УИС получаем информацию о значениях $l(t_k)$ и $\mu(t_k)$.

2. При использовании модели M (в соответствии с выбранными критериями X) определяем тип складывающейся вычислительной ситуации $w(t_k)$.

3. На основе технологий, описанных в [3], определяем коэффициенты усиления пропорциональной, интегральной и дифференциальной составляющих регулятора $K_p(t_k)$, $K_i(t_k)$, $K_d(t_k)$, обусловленные $w(t_k)$.

4. По аналогии с классическим ПИД-регулятором [9, 10] имеем:

$$\Delta\mu(t_{k+1}) = K_p(t_k) \cdot K_{t_{ДИР}}(t_k, \mu(t_k)) + $$
$$+ K_i(t_k) \cdot \int_0^{t_k} K_{t_{ДИР}}(t, \mu(t)) \partial t + $$
$$+ K_d(t_k) \cdot \frac{\partial K_{t_{ДИР}}(t, \mu(t))}{\partial t}.$$

Результаты вычислительного эксперимента подтверждают эффективность предлагаемого подхода. Для вычислительных ситуаций 1-3 использование ИПИД-регулятора не дало ощутимого уменьшения $R_{П}$, однако $K_{t_{ДИР}}$ удалось уменьшить на 30%. Наибольшую эффективность использования предлагаемого функционального устройства можно наблюдать для $w(t_k) = 4, \ldots, 7$ (уменьшение $R_{П}$ до 50%, а $K_{t_{ДИР}}$ – до 68%). Дефицит ресурсов, характерный для вычислительных ситуаций 8-10, не был эффективным образом парирован ввиду недостатка времени на принятие решений и привлечения дополнительных ресурсов. Для более аргументированных утверждений планируется расширить функциональность предлагаемого ИПИД-регулятора, а также реализовать ряд имитационных экспериментов при помощи гибридной имитационной модели с применением системной динамики, дискретно-событийного и агентного подхода [4 – 6].

Заключение

Рассмотрена проблема обеспечения высокой готовности вычислительных сервисов критического применения при воздействии информационных атак. Рассматриваемая задача относится к классу многокритериальных задач параметрической оптимизации. Предложен подход к решению поставленной задачи путем синтеза ИПИД-регулятора, предназначеного для компенсации последствий несанкционированных действий, нарушающих штатный режим функционирования вычислительных сервисов ИУС. Для обеспечения требуемого качества обслуживания реализуется децентрализованное управление распределенным вычислительным процессом в ИУС на основе ИПИД-регулятора при использовании мультиагентного подхода. Приводятся результаты вычислительного эксперимента, демонстрирующие эффективность предложенного подхода. Одним из возможных направлений дельнейшего исследования является использование предлагаемого ИПИД-регулятора при решении задачи детектирования скрытых атак в критических IT-системах на основе анализа информации об утечке вычислительных ресурсов.

Литература

1. Харченко, В.С. Безопасность критических инфраструктур: математические и инженерные методы анализа и обеспечения [Текст] / В.С. Харченко. – Министерство образования и науки Украины, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», 2011. – 641 с.

2. Информационные технологии для критических инфраструктур: монография [Текст] / А.В. Скатков [и др.] — Севастополь: Изд-во «СевНТУ», 2012. — 306 с.

3. Рутковская, Д. Нейронные сети, генетические алгоритмы и нечеткие системы [Текст] / Д. Рутковская, М. Пилиньский, Л. Рутковский. – М.: Горячая линия – Телеком, 2004. – 452 с.

4. Schieritz, N. Modeling the Forest or Modeling the Trees [Text] / N. Schieritz, P. Milling // A Comparison of System Dynamics and Agent-Based Simulation. The 21st International Conference of the System Dynamics Society, New York, USA. 2003.

5. Borshchev, A. From System Dynamics and Discrete Event to Practical Agent Based Modeling [Text] / A. Borshchev, A. Filippov. // Reasons, Techniques,

Tools, The 22nd International Conference of the System Dynamics Society, Oxford, England. 2004.

6. Rahmandad, H. Heterogeneity and Network Structure in the Dynamics of Diffusion: Comparing Agent-Based and Differential Equation Models [Text] / H. Rahmandad, J. Sterman. MIT Sloan Working Paper No. 4512-04.

7. Бон, Я.В. ИТ Сервис-менеджмент, введение [Текст] / Я.В. Бон, Г. Кеммерлинг, Д. Пондаман. — М.: IT Expert, 2003. – 215 с.

8. Ястребенецкий, М.А. Безопасность атомных станций: Информационные и управляющие системы [Текст] / М.А. Ястребенецкий, В.Н. Васильченко, С.В. Виноградская. – К.: Техніка, 2004. – 472 с.

9. Ротач, В.Я. К расчету оптимальных параметров реальных ПИД-регуляторов по экспертным критериям [Текст] / В.Я. Ротач // Промышленные АСУ и контроллеры. – 2006. – № 2. – С. 22 – 29.

10. Энциклопедия АСУ ТП [Электронный ресурс]. – Режим доступа: http://bookasutp.ru. – 10.01.2013 г.

Поступила в редакцию 28.02.2013, рассмотрена на редколлегии 27.03.2013

Рецензент: д-р техн. наук, доцент, проф. каф. компьютерных систем и сетей А.В. Горбенко, Национальный аэрокосмический университет им. Н.Е. Жуковского «ХАИ», Харьков, Украина.

ІНФОРМАЦІЙНИЙ ПРОПОРЦІЙНО-ІНТЕГРАЛЬНО-ДИФЕРЕНЦІАЛЬНИЙ РЕГУЛЯТОР ЯК ЗАСІБ КОМПЕНСАЦІЇ НАСЛІДКІВ АТАК

О.В. Скатков, Д.Ю. Воронін, С.А. Чорномиз

Розглянуто проблему забезпечення високої готовності обчислювальних сервісів критичного застосування при впливі інформаційних атак. Запропонований функціональний пристрій – інформаційний пропорційно-інтегрально-диференціальний (ІПІД) регулятор – призначений для компенсації наслідків несанкціонованих дій, що порушують штатний режим функціонування обчислювальних сервісів ІУС. Для забезпечення необхідної якості обслуговування реалізується децентралізоване управління розподіленим обчислювальним процесом в ІУС на основі ІПІД-регулятора при використанні мультиагентного підходу. Одним з можливих напрямів дельнейшего дослідження є використання пропонованого ІПІД-регулятора при вирішенні задачі детектування прихованих атак в критичних ІТ-системах на основі аналізу інформації про витік обчислювальних ресурсів.

Ключові слова: ІПІД-регулятор, інформаційна атака, компенсаційне управління розподіленими обчислювальними сервісами, мультиагентний підхід, QoS, витік ресурсів, ідентифікація прихованих атак.

INFORMATIONAL PROPORTIONAL-INTEGRAL-DERIVATIVE CONTROLLER AS A DEVICE FOR ATTACK CONSEQUENCES COMPENSATION

A.V. Skatkov, D.Y. Voronin, S.A. Chornomyz

The problem of critical computing services high-availability ensuring in the impact of information attacks was considered. The proposed functional device (informational proportional-integral-derivative (IPID) controller) was designed to compensate the effects of unauthorized activities that violate the normal mode of functioning of computing services of information management system (IMS). To ensure the required quality of service it's suggested to use of decentralized management of distributed computing process in IMS. It was implemented based on IPID controller using multi-agent approach. One of the possible directions in the individual studies is the use of the proposed IPID controller for solving the hidden attack detection problem in critical IT-systems based on the analysis of information about the leak of computing resources.

Key words: IPID controller, information attack, compensation management lennymi distributed computing services, Multi-Agent Systems, QoS, resource leak, identify hidden attacks.

Скатков Александр Владимирович – д-р техн. наук, проф., проф. кафедры кибернетики и вычислительной техники Севастопольского национального технического университета, Севастополь, Украина.

Воронин Дмитрий Юрьевич – канд. техн. наук, ст. преп. кафедры кибернетики и вычислительной техники Севастопольского национального технического университета, Севастополь, Украина, e-mail: dima@voronins.com.

Чорномыз Сергей Анатольевич – директор Керченского колледжа экономики и информационных технологий, Керчь, Украина.