УДК 004.056:004.942

ИСПОЛЬЗОВАНИЕ МЕХАНИЗМОВ АКТИВНОЙ ЗАЩИТЫ В РАСПРЕДЕЛЕННЫХ МУЛЬТИАГЕНТНЫХ СИСТЕМАХ УПРАВЛЕНИЯ

Н.В. Хаджинова
Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», г. Минск, Республика Беларусь

Аннотация. Предложена многоуровневая схема активной защиты распределенных мультиагентных систем управления, объединяющая контроль целостности кода, мониторинг контекста агентов и детектирование аномалий. Схема базируется на объектно-ориентированных полиморфных сетях Петри (*PPN*), позволяющих встраивать процедуры защиты в архитектуру интерпретаторов без нарушения требований реального времени. Экспериментальная оценка показала накладные расходы 8–12 % при точности обнаружения аномалий до 96 %, что соответствует требованиям систем мягкого реального времени.

Ключевые слова: активная защита; мультиагентные системы; распределенные системы управления; целостность; контроль контекста; детектирование аномалий; сети Петри; полиморфизм; безопасность в реальном времени; киберфизические системы.

USING ACTIVE PROTECTION MECHANISMS IN DISTRIBUTED MULTI-AGENT CONTROL SYSTEMS

N.V. Khajynava
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Republic of Belarus

Abstract. A multi-level active protection scheme for distributed multi-agent control systems is proposed, combining code integrity control, agent context monitoring, and anomaly detection. The scheme is based on object-oriented polymorphic Petri nets (*PPN*), which allow embedding protection procedures into the interpreter architecture without violating real-time requirements. Experimental evaluation showed an overhead of 8–12 % with an anomaly detection accuracy of up to 96 %, meeting the requirements of soft real-time systems.

Keywords: active protection; multi-agent systems; distributed control systems; integrity; context control; anomaly detection; Petri nets; polymorphism; real-time security; cyber-physical systems.

Введение

Распределенные мультиагентные системы (МАС) широко применяются в киберфизических системах и промышленном интернете вещей (*IIoT*). Децентрализация создает дополнительные векторы угроз: состязательные атаки, компрометация кода, подмена сообщений [1]. Традиционные методы защиты (антивирусы, статический анализ) недостаточно эффективны в реальном времени, где критична предсказуемость реакции. Предлагается встраиваемая в интерпретаторы

архитектура активной защиты на основе полиморфных расширений сетей Петри [2].

Основная часть

Схема включает четыре уровня контроля, встроенных в интерпретатор PPN:

Code-time – верификация кода (*SHA*-256, цифровые подписи). Эталонные хеши хранятся в *TPM*; при модификации модуль не исполняется.

Load-time – доверенная загрузка (*Trusted Boot*): каждый этап инициализации расширяет *PCR TPM*, гарантируя старт из доверенного состояния.

Runtime – мониторинг контекста агента (процесс, права, файлы, сеть) и контроль потока управления (*CFI*). Изоляция через песочницу (seccomp).

Anomaly Detection – по профилям нормального поведения выявляются отклонения; при обнаружении агент изолируется.

Защита встраивается через класс *SecureTransition*, наследующий базовый полиморфный переход *Transition<Time>*. Виртуальные методы *E, C, D, F* дополнены вызовами процедур безопасности. Метод *E* отвечает за проверку возможности срабатывания перехода, *C* – за изъятие токенов из входных позиций, *D* – за вычисление задержки, *F* – за генерацию выходных токенов.

```
template <class Time>
struct SecureTransition : public Transition<Time> {
    MultilevelSecurityProtection<Time> securityStack;
    ExecutionContextMonitor<Time> contextMonitor;
    virtual int E(int index) override {
        if (!securityStack.verifyFullSecurityStack()) return 0;
        if (!contextMonitor.E(index)) return 0;
        return 1;
    }
    virtual void C(int index) override {
        contextMonitor.C(index);   // фиксация контекста перед выполнением
        consumeTokens();
    }
    virtual Time D(int index) override {
        return estimateExecutionTime() + securityStack.getOverhead() + contextMonitor.D(index);
    }
    virtual void F(int index) override {
        if (!contextMonitor.validateContextIntegrity(index)) {
            recordSecurityEvent("CONTEXT_COMPROMISE");
            isolateAgent();
            return;
        }
        generateTokens();
    }
};
```

Такой подход обеспечивает встраивание проверок в декларативную структуру модели, сохраняя ее формальную семантику. Для минимизации накладных расходов захват контекста выполняется легковесными системными вызовами с кэшированием; для критических переходов допускается выборочный контроль.

Эксперименты проведены на стенде: процессор Intel Core i5-10600KF, 16 ГБ оперативной памяти, модуль TPM 2.0, ОС на базе ядра Linux (kernel 5.x). МАС включала от 10 до 100 агентов, взаимодействующих по протоколам аукциона и консенсуса. Моделировались атаки: модификация кода, подмена сообщений, переполнение буфера. Результаты (50 запусков) приведены в таблице. Архитектура Intel Core i5 обеспечивает детектирование аномалий в пределах 15 мс, что делает схему применимой в системах с циклом управления менее 20 мс.

Накладные расходы и эффективность защиты
Overhead and Protection Efficiency

Уровень защиты	Накладные расходы (% CPU)	Точность обнаружения	Время детектирования (мс)
Без защиты	0	–	–
Верификация кода (Code-time)	2–3	100%	–
Контроль контекста (Runtime)	3–5	92%	5
Полная защита + детектирование	8–12	96%	15

Заключение

Предложенная архитектура, интегрированная в полиморфные сетевые модели, обеспечивает комплексный контроль целостности на этапах загрузки, выполнения и обнаружения аномалий. Экспериментально подтверждены приемлемые накладные расходы (8–12 %) и высокая эффективность обнаружения аномалий (96 %), что допустимо для систем мягкого реального времени.

Список использованных источников

1. Dong J., Li S., Wang Y., Zhang L., Chen W., Liu X. (2022) Multi-Agent Adversarial Attacks for Multi-Channel Communications. Proceedings of AAMAS, 3, 1580–1582.

2. Ревотюк М. П., Хаджинова Н. В. (2006) Полиморфные сетевые модели дискретных процессов. В кн.: Идентификация систем и задачи управления (SICPRO'06): материалы Пятой международной конференции. Москва, Институт проблем управления им. В.А. Трапезникова РАН, с. 2042–2158.

References

1. Dong J., Li S., Wang Y., Zhang L., Chen W., Liu X. (2022) Multi-Agent Adversarial Attacks for Multi-Channel Communications. Proceedings of AAMAS, 3, 1580–1582.

2. Revotyuk M. P., Khajynava N. V. (2006) Polymorphic Network Models of Discrete Processes. In: Identification of Systems and Control Problems (SICPRO'06): Proceedings of the Fifth International Conference. Moscow, Institute of Control Sciences, pp. 2042–2158 (in Russian).

Сведения об авторах

Хаджинова Н.В., старший преподаватель кафедры ИТАС, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», khajynova@bsuir.by.

Information about the authors

Khajynava N.V., Senior Lecturer at the Department of Information Technologies of Automated Systems, Educational Institution "Belarusian State University of Informatics and Radioelectronics", khajynova@bsuir.by.