ИММУННЫЙ ПОДХОД К ОБНАРУЖЕНИЮ КОМПРОМЕТАЦИИ В МУЛЬТИАГЕНТНЫХ СИСТЕМАХ

Хаджинова Н. В., Сманцер Н. С., Соркин В. О.
Кафедра информационных технологий автоматизированных систем,
Белорусский государственный университет информатики и радиоэлектроники
Минск, Республика Беларусь
E-mail: khajynova@bsuir.by, {natalya.smantser, sorkindev}@gmail.com

Предложен подход к созданию саморегулируемой мультиагентной системы в целях обнаружения и изоляции скомпрометированных агентов с применением иммунных алгоритмов. В основе подхода лежат принципы искусственных иммунных систем – активно развивающейся области информатики и математического моделирования. Рассмотрены основные принципы работы и механизмы иммунной системы, роль Т-клеток и антигенов, описан алгоритм негативного отбора, предложена структура иммунной подсистемы управления инцидентами в мультиагентной системе.

Введение

Мультиагентные системы (МАС) дают возможность создавать сложные, распределенные и адаптивные решения для таких задач, как управление умными сетями, координация роботов и организация логистических цепочек. Их ключевое преимущество заключается в децентрализованной координации автономных агентов, способных к коллективному решению проблем. Однако эта же децентрализация является источником уязвимости: отказ или злонамеренная компрометация даже одного агента может дестабилизировать работу всей системы. Таким образом, критически важной задачей становится обеспечение саморегулирования МАС, одним из ключевых аспектов которой является своевременное обнаружение и изоляция скомпрометированных агентов.

Решение данной задачи может быть основано на принципе работы иммунной системы человека, которая эффективно решает проблему поиска и нейтрализации чужеродных организмов в распределенной и самоорганизующейся манере. Алгоритмы, основанные на этих принципах, – искусственные иммунные системы (ИИС) – уже успешно зарекомендовали себя в задачах информационной безопасности, таких как обнаружение сетевых вторжений и аномалий [1].

I. Саморегулируемые МАС и применение ИИС

Саморегулирование – это способность системы поддерживать свою работоспособность и целостность в изменяющихся условиях. Саморегулирование включает самодиагностику, адаптацию, самовосстановление. То есть постоянный мониторинг собственного состояния, изменение стратегии поведения при появлении угроз и возврат в стабильное состояние после атаки или сбоя.

Можно провести аналогию между саморегулируемой системой и адаптивной иммунной системой, которая также должна обеспечивать нормальное функционирование организма, одновременно вызывая иммунный ответ на аномальные объекты (антигены). Экспериментальные данные показывают, что толерантность, проявляемая иммунной системой, является результатом динамики и взаимодействия между специфическими регуляторными и эффекторными Т-клетками. Децентрализованный характер этих взаимодействий придает высокую степень устойчивости толерантности и обнаружению неисправностей, без необходимости генетически закрепленной записи о том, как должны выглядеть нормальные ткани [2].

Результаты исследования [1] подтверждают высокую эффективность применения ИИС в составе МАС для обнаружения неисправностей. Использование иммунных алгоритмов, таких как отрицательный отбор, теория опасности, клонирование и иммунная сеть, позволяет системам быстро адаптироваться к новым типам угроз, повышая точность обнаружения. Основные преимущества данного подхода включают способность к самонастройке, автономности и эффективной коммуникации агентов, что обеспечивает устойчивую работу в распределенных средах. Иммунный подход позволяет создавать надежные МАС для, например, управления умными электросетями, где агенты-производители и потребители автономно поддерживают баланс нагрузки и противодействуют кибератакам, или для координации роев дронов, обеспечивая их коллективное поведение и отказоустойчивость.

Данное исследование ограничивается рассмотрением основной способности иммунной системы: распознавать как своих или чужих большое количество антигенов с дальнейшей их классификацией и стимуляцией соответствующих защитных механизмов [3].

II. Алгоритм негативного отбора

В 1994 году Стефани Форрест предложила вычислительную модель способную распознавать «своих» и «чужих», получившую название алгоритм негативного отбора. Целью алгоритма негативного отбора является покрытие чужеродного пространства соответствующим множеством

детекторов. В работе алгоритма есть два этапа: «создание детекторов» и «распознавание чужеродного». На первом этапе создается множество детекторов с применением процесса, использующего в качестве входных данных множество «своих». Детекторы, которые определяют любой из «своих» образцов, исключаются из кандидатов. Правило соответствия обычно смоделировано с использованием модели аффинности (способность распознования) Т-клеток и антигенов. На этапе обнаружения сохраненные детекторы применяются для проверки новых входящих примеров на соответствие «своим» и чужеродным. Если поступивший пример совпадает с детектором, то он идентифицируется как чужеродный [4].

III. Структура ИИС управления инцидентами

Можно предложить структуру подсистемы обнаружения и изоляции аномалий саморегулируемой МАС на основе иммунного алгоритма (см. рис. 1).

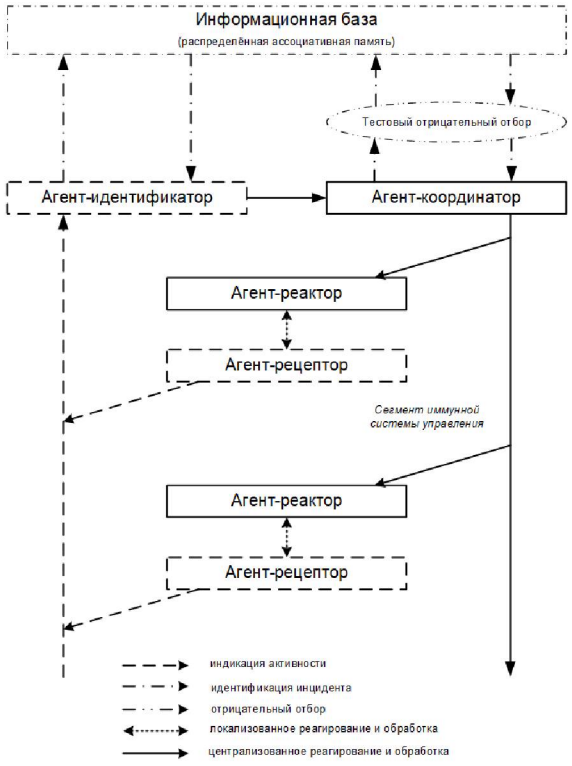

Рис. 1 – Структура ИИС управления инцидентами

Структура включает в себя четыре класса агентов: агенты-рецепторы; агенты-идентификаторы; агенты-координаторы; агенты-реакторы. Агенты-рецепторы соответствуют макрофагам и другим антиген-презентирующим клеткам, которые выставляют частицы антигена на своей поверхности, привлекая внимание В-лимфоцитов для распознавания. Агенты-идентификаторы (детекторы) соответствуют В-лимфоцитам, которые распознают антиген и заранее подвергались «отрицательному отбору» в тимусе. Агенты-координаторы соответствуют лимфокинам, выделяемым Т-лимфоцитами для активации В-лимфоцитов. Агенты-реакторы соответствуют фагоцитам, имеющим антитела для уничтожения антигена.

Заключение

В результате исследования методов построения ИИС предложен вариант структуры иммунной подсистемы управления инцидентами в МАС. В основе предложенной структуры лежат основные принципы работы и механизмы иммунной системы, использована роль Т-клеток и антигенов, механизм отрицательного отбора для генерации агентов-идентификаторов, которые отвечают за распознавание аномалий, «пойманных» агентами-рецепторами.

Таким образом, предложенная иммуноинспирированная архитектура может стать отправной точкой к дальнейшему созданию саморегулируемых МАС для управления сложными объектами, такими как интеллектуальные энергосети или автономные логистические системы. Внедрение таких систем позволит достичь качественно нового уровня отказоустойчивости и автономности, обеспечивая проактивное обнаружение и локализацию аномалий, а также минимизацию каскадных сбоев, что критически важно для функционирования систем в условиях неопределённости и динамически меняющейся среды.

1. Seresht, N. A. MAIS-IDS: A distributed intrusion detection system using multi-agent AIS approach / N. A. Seresht, R. Azmi // Engineering Applications of Artificial Intelligence. – 2014. – Vol. 35. – P. 286–298.
2. Tarapore, D. Abnormality detection in multiagent systems inspired by the adaptive immune system / D. Tarapore [and et al] // Proceedings of the 2013 international conference on Autonomous agents and multi-agent systems. – 2013. – P. 23–30.
3. Гладыш, С. В. Иммунокомпьютинг в управлении инцидентами информационной безопасности / С. В. Гладыш // Штучний інтелект. – 2008. – №1. – С. 12–129.
4. Частикова, В. А. Искусственные иммунные системы: основные подходы и особенности их реализации / В. А. Частикова, Д. А. Картамышев // Научные труды КубГТУ. – 2016. – № 8. – С. 193–208.