УДК 004.773:004.056.53

МЕТОДЫ ЗАЩИТЫ С ИСПОЛЬЗОВАНИЕМ ПОДВИЖНЫХ ЦЕЛЕЙ ДЛЯ МУЛЬТИАГЕНТНЫХ СИСТЕМ: ДИНАМИЧЕСКОЕ ИЗМЕНЕНИЕ ТОПОЛОГИИ СЕТИ ПРОТИВ ЦЕЛЕВЫХ АТАК

М.Ю. Шухман, В.Ю. Мишепуд, В.О. Соркин, К.А. Хаджинова

Учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», Минск, Беларусь

Аннотация. В статье рассматриваются методы защиты с использованием подвижных целей (Moving Target Defense, MTD), которые применяются для повышения безопасности многоагентных систем (MAS) за счет динамического изменения топологии сети. Основное внимание уделяется подходам, при которых агенты периодически меняют свои IP-адреса и маршруты передачи данных, что значительно усложняет задачу злоумышленников по идентификации узлов и отслеживанию их активности. Рассматриваются такие методы, как IP-перестановка, порт-хоппинг и рандомизация заголовков пакетов, которые делают поверхность атаки динамической и труднопредсказуемой. Особое внимание уделяется двум основным подходам MTD: хоппингу, требующему строгой синхронизации по времени, и мутации, которая

позволяет изменять параметры сети без жесткой привязки к временным рамкам. В статье анализируются преимущества и ограничения каждого из подходов в контексте децентрализованных и динамически изменяющихся многоагентных систем. Также обсуждаются перспективы применения MTD для защиты MAS от современных киберугроз, таких как внедрение поддельных агентов и атаки на сетевую инфраструктуру. В заключение делается вывод о необходимости дальнейшей разработки методов мутации, адаптированных для MAS, чтобы обеспечить максимальную гибкость и безопасность взаимодействия агентов в условиях постоянно меняющейся среды.
Ключевые слова: защита с использованием подвижных целей; динамическая сетевая топология; ротация IP-адресов; адаптивная маршрутизация; целевые атаки; мультиагентные системы; сетевая безопасность; кибербезопасность; интеллектуальный агент; взаимодействие агентов.

MOVING TARGET DEFENSE TECHNIQUES FOR MULTI-AGENT SYSTEMS: DYNAMIC NETWORK TOPOLOGY CHANGE AGAINST TARGETED ATTACKS

M.Y. Shuhman, V.Y. Mishepud, V.O. Sorkin, K.A. Khadzhynava
Educational Institution "Belarusian State University of Informatics and Radioelectronics", Minsk, Belarus

Abstract. The article discusses the methods of protection using Moving Target Defense (MTD), which are used to increase the security of multi-agent systems (MAS) by dynamically changing the network topology. The main focus is on approaches in which agents periodically change their IP addresses and data transmission routes, which significantly complicates the task of attackers to identify nodes and monitor their activity. Methods such as IP permutation, port hopping, and packet header randomization are considered, which make the attack surface dynamic and difficult to predict. Special attention is paid to two main MTD approaches: hopping, which requires strict time synchronization, and mutation, which allows changing network parameters without strict time constraints. The article analyzes the advantages and limitations of each approach in the context of decentralized and dynamically changing multi-agent systems. The prospects of using MTD to protect MAS from modern cyber threats, such as the introduction of fake agents and attacks on network infrastructure, are also discussed. In conclusion, it is concluded that it is necessary to further develop mutation methods adapted for MAS in order to ensure maximum flexibility and safety of agent interaction in an ever-changing environment.
Keywords: moving target defense, dynamic network topology, IP-address rotation, adaptive routing, targeted attacks; multi-agent systems; network security; cybersecurity; intelligent agent; agent interaction.

Введение

Сегодня многоагентные, или мультиагентные, системы (англ. Multi-agent system, MAS) представляют собой одно из наиболее перспективных направлений в области искусственного интеллекта. Эти системы используются для решения сложных задач, которые требуют координации множества независимых агентов, взаимодействующих между собой. Агент в данном контексте – это автономная сущность (программа, устройство или робот), способная воспринимать окружающую среду, принимать решения и действовать для достижения поставленных целей. Многоагентные системы находят применение в различных областях, таких как робототехника, управление умными сетями, логистика, кибербезопасность и многие другие [1].

Ключевой особенностью MAS является их распределенная и децентрализованная природа, что делает их гибкими и устойчивыми к сбоям. Однако эта же особенность создает значительные сложности в обеспечении безопасности, особенно в условиях постоянно растущих киберугроз ввиду большого объема передаваемой информации.

Одним из современных подходов к обеспечению безопасности в распределенных системах является защита с использованием подвижных целей (Moving Target Defense, MTD). Этот подход основан на идее динамического изменения параметров системы с целью затруднения сбора информации и проведения атак. MTD превращает статическую поверхность атаки в динамическую, что значительно увеличивает сложность анализа сети и снижает вероятность взлома [2].

Основная часть

Динамическая перестановка параметров системы реализуется за счет таких методов, как IP shuffling, порт-хоппинг и рандомизация заголовков пакетов, что позволяет периодически менять конфигурацию сети и усложнять отслеживание истинных характеристик агентов. При этом IP shuffling подразумевает регулярное изменение IP-адресов узлов, что затрудняет идентификацию и мониторинг их активности, а порт-хоппинг обеспечивает динамическую смену портов, через которые происходит обмен информацией, тем самым препятствуя злоумышленнику установить устойчивый канал связи. Рандомизация заголовков пакетов добавляет еще один уровень защиты, поскольку случайное формирование параметров пакетов делает анализ трафика и определение его источников крайне затруднительным.

В данной парадигме защиты большое значение имеет синхронизация между агентами, так как в традиционных схемах, основанных на методах типа hop-ping, изменение конфигураций происходит в строго определенном временном интервале, что требует высокой точности и согласованности всех участников системы [3]. Однако, учитывая динамичный характер многоагентных систем, требующих возможности беспрепятственного добавления новых узлов и изменения сетевой топологии, традиционные подходы, основанные на строгой временной синхронизации, зачастую оказываются недостаточно гибкими.

Альтернативой таким методам являются подходы, основанные на принципе мутации, когда ответственность за изменение параметров сети переносится на внешние механизмы, позволяющие агентам свободно изменять свою организацию без жестких ограничений. В таких системах используются технологии, позволяющие динамически обновлять конфигурацию, не требуя постоянного обмена синхронизирующей информацией между всеми участниками сети.

Примером таких технологий являются системы NASR и MOTAG, которые обеспечивают динамическую смену параметров через использование таймеров, DHCP-серверов или группы прокси-узлов, что позволяет минимизировать возможность получить достоверную информацию о структуре сети. При этом, если традиционные методы типа DYNAT или APOD, основанные на криптографическом преобразовании идентификационной информации, успешно применимы для стационарных сетевых инфраструктур, их использование в условиях постоянно меняющейся топологии многоагентных систем нередко приводит к сложностям в поддержании единого протокола синхронизации и совместимости между различными узлами [4].

Заключение

Подводя итоги, можно сделать вывод, что применение методов защиты с использованием движущихся целей (MTD) в многоагентных системах является перспективным направлением. MTD позволяет значительно повысить безопасность MAS за счет динамического изменения параметров сети, что затрудняет злоумышленникам проведение атак. Однако для успешного применения MTD в контексте MAS необходимо учитывать особенности этих систем, такие как их распределенная и децентрализованная природа, а также динамически изменяющаяся конфигурация.

Особое внимание следует уделить разработке методов мутации, которые более подходят для MAS, чем методы хоппинга. Мутационные подходы, такие как NASR и MOTAG, позволяют агентам свободно изменять свою организацию, не нарушая работу системы. Однако для их успешного применения необходимо решить такие проблемы,

как защита от внедрения поддельных агентов и обеспечение безопасности механизмов перетасовки.

В будущем исследования в этой области должны быть направлены на разработку более совершенных механизмов мутации, которые будут учитывать специфику многоагентных систем и обеспечивать максимальную децентрализацию. Это позволит агентам сохранять гибкость и свободу в организации своей структуры взаимодействия, одновременно обеспечивая высокий уровень безопасности. Таким образом, MTD открывает новые возможности для повышения устойчивости многоагентных систем к киберугрозам, но требует дальнейшей проработки и адаптации существующих методов к специфике MAS.

Список использованных источников

1. Мультиагентные системы искусственного интеллекта : научные труды КубГТУ / М. П. Малыхина, Д. А. Герасимов ; Кубан. гос. технологический ун-т. – Краснодар : КубГТУ, 2018. – 9 с. – URL: https://ntk.kubstu.ru/data/mc/0051/2074.pdf (дата обращения: 04.03.2025).

2. Реализация механизма защиты движущейся цели без потерь : монография / М. Зал, М. Михальский, П. Звежыковский ; под общ. ред. Х. Дж. Бурас. – Познань : Познань. тех. ун-т. 2024. – 24 с. – URL: https://doi.org/10.3390/electronics13050918 (дата обращения: [04.03.2025]).

3. Корнелльский университет : [сайт]. – Нью-Йорк, 2019. – URL: https://arxiv.org/pdf/1909.08092 (дата обращения 04.03.2025).

4. Введение в перетасовку сетевых адресов : монография / Г. Цай, Б. Ван, С. Ван [и др.] : Колледж компьютерных наук. – Чанша, Китай : Нац. ун-т оборонных технологий. 2016. – 6 с. – URL: https://icact.org/upload/2016/0109/20160109_finalpaper.pdf (дата обращения: 04.03.2025).

Сведения об авторах

Шухман М.Ю., студент группы 220601 факультета информационных технологий и управления, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», mjshuhman@gmail.com.
Мишепуд В.Ю., студент группы 220601 факультета информационных технологий и управления, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», vladislavmishepud@gmail.com.
Соркин В.О., студент группы 220601 факультета информационных технологий и управления, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», sorkindev@gmail.com.
Хаджинова К.А., студент группы 320604 факультета информационных технологий и управления, учреждение образования «Белорусский государственный университет информатики и радиоэлектроники», xju2005@gmail.com.

Information about the authors

Shuhman M., student of group 220601, Faculty of information Technology and Management, Educational Institution "Belarusian State University of Informatics and Radioelectronics", mjshuhman@gmail.com.
Mishepud V., student of group 220601, Faculty of Information Technology and Management, Educational Institution "Belarusian State University of Informatics and Radioelectronics", vladislavmishepud@gmail.com.
Sorkin V., student of group 220601, Faculty of Information Technology and Management, Educational Institution "Belarusian State University of Informatics and Radioelectronics", sorkindev@gmail.com.
Khadzhynava K., student of group 320604, Faculty of Information Technology and Management, Educational Institution "Belarusian State University of Informatics and Radioelectronics", xju2005@gmail.com.