УДК 004.056.53

ПРИМЕНЕНИЕ ИСКУССТВЕННЫХ ИММУННЫХ СИСТЕМ ДЛЯ ОБНАРУЖЕНИЯ СЕТЕВЫХ ВТОРЖЕНИЙ

И. В. Ребро, Е. В. Шарлаев

Алтайский государственный технический университет им. И.И. Ползунова,
г. Барнаул

В статье рассматривается решение задачи обнаружения сетевых вторжений с использованием искусственных иммунных систем, основанных на базовых принципах и механизмах биологической иммунной системы. Благодаря своим особенностям и характеристикам, иммунная система представляет большой интерес в области обработки массивов данных и защиты информации.

Ключевые слова: информационная безопасность, система обнаружения вторжений, искусственная иммунная система.

Проблема защиты информационных ресурсов сети от несанкционированной деятельности хакеров, воздействий вирусов, обеспечения конфиденциальности, целостности и доступности данных является одной из актуальнейших и в то же время наиболее сложных проблем нашего времени [1].

При решении задач, связанных с диагностикой и защитой сетевых ресурсов, центральным вопросом является оперативное обнаружение состояний сети.

Раннее обнаружение состояний, приводящих к потере работоспособности сети, уничтожению искажению или утечке информации, являющихся следствием отказов, сбоев случайного характера или результатом получения злоумышленником доступа к сетевым ресурсам, проникновения сетевых червей, вирусов и других угроз информационной безопасности, может позволить своевременно устранить их причину, а так же предотвратить возможные катастрофические последствия [2].

Для обнаружения используется большой спектр специализированных систем: средства систем управления, анализаторы сетевых протоколов, системы нагрузочного тестирования, системы сетевого мониторинга.

Проблемы защиты информационных ресурсов сетей решаются с помощью межсетевых экранов (firewall), антивирусов, систем обнаружения вторжений, систем контроля целостности, криптографических средств защиты.

Характерными особенностями использования этих систем является либо их периодическое и кратковременное применение для решения определенной проблемы, либо постоянное использование, но со статическими настройками. В результате методы анализа, используемые в современных системах, направлены на обнаружение известных и точно описанных типов воздействий, но зачастую оказываются не в состоянии обнаружить их модификации или новые типы, что делает их использование малоэффективным.

На сегодняшний день очень актуальной задачей является поиск более эффективных методов выявления недопустимых событий (аномалий) в работе сети, являющихся следствием технических сбоев или несанкционированных воздействий. Основным требованием к этим методам является возможность обнаружения произвольных типов аномалий, в том числе новых, а также воздействий распределенных во времени.

Общий подход решения этой задачи, заключается в поиске методов анализа, позволяющих выявить аномальные состояния информационных ресурсов в виде отклонений от обычного («нормального») состояния. Эти отклонения могут являться результатами сбоев в работе аппаратного и программного обеспечения, а также следствиями сетевых атак хакеров. Такой подход теоретически позволит обнаруживать как известные, так и новые типы проблем. От эффективности и точности аппарата, определяющего «нормальное» состояние и фиксирующего отклонение, зависит в целом эффективность решения вопросов диагностики и защиты сетевых ресурсов.[4]

Особую важность на текущий момент представляет проблема обнаружения аномальных состояний в работе сети, имеющих распределенный во времени характер. Такие состояния могут являться следствиями специально маскируемых сетевых атак злоумышленников, скрытых программно-аппаратных сбоев, новых вирусов и т.д.

Системами обнаружения вторжений называют множество различных программных и аппаратных средств, объединенных одним общим свойством – они занимаются анализом использования ресурсов и, в случае обнаружения каких-либо подозрительных или просто нетипичных событий, способны предпринимать некоторые самостоятельные действия по обнаружению, идентификации и устранению их причин [2].

Современные системы обнаружения вторжений используют методы интеллектуального анализа данных, позволяющие выявить значимые корреляции в больших объемах данных, применяя алгоритмы:

– экспертных систем;
– искусственных нейронных сетей;
– искусственных иммунных систем;
– нечетких систем;
– генетических алгоритмов.

Анализ данных может состоять из трех стадий:

1) выявление закономерностей (поиск скрытых закономерностей и их валидация);

2) использование выявленных закономерностей для предсказания неизвестных значений (решаются задачи классификации и прогнозирования);

3) анализ исключений (выявление и объяснение аномалий в выявленных закономерностях).

Искусственные иммунные системы строятся по аналогии с иммунной системой живого организма [3].

Искусственные иммунные системы представляют собой сложную адаптивную структуру, эффективно использующую различные механизмы обучения, памяти и ассоциативного поиска для решения задач распознавания и классификации.

Идея создания искусственных иммунных систем появилась в результате изучения процессов биологического иммунитета, который защищает организм от болезнетворных бактерий и вирусов, обнаруживая и уничтожая их.

При построении искусственной иммунной системы для обнаружения и классификации сетевых атак на компьютерные системы используются базовые принципы и механизмы биологической иммунной системы.

Искусственная иммунная система моделирует основные процессы биологической иммунной системы, а так же их взаимодействие. Отличие заключается в способе представления информации и структуре иммунного детектора.

Жизненный цикл детекторов иммунной системы представлен на рисунке 1.

Рисунок 1 – Жизненный цикл детекторов искусственной иммунной системы

Иммунные детекторы генерируются по случайному алгоритму, что дает возможность создания большого количества разнообразных по своей структуре детекторов, которые способны реагировать на любую аномалию. Далее детекторы проходят стадию обучения, на которой они приобретают способность корректно реагировать на чужеродные объекты или явления. Для того чтобы детекторы не генерировали ложные срабатывания, они тщательно отбираются. Те из них, которые не обучились корректно классифицировать объекты, удаляются. Отобранные детекторы допускаются к выполнению функций классификации объектов.

Каждому детектору выделяется некоторое лимитированное количество времени (время жизни), на протяжении которого он может существовать.

Если на протяжении этого времени детектор не обнаруживает аномалий, то он удаляется, а на его место приходит новый, структурированный отличный детектор. Если детектор обнаружил аномалию, происходит так называемая стадия активации. На этой стадии происходит информирование об обнаруженной аномалии и её уничтожение. Детектор, обнаруживший аномалию, трансфор-

мируется в детектор иммунной памяти. Детекторы иммунной памяти характеризуются большим временем жизни и уровнем доверия.

Заключение. В ходе исследования рассмотрена задача реализации алгоритмов иммунной системы для обнаружения вторжения в сеть. Особенностью подхода является автоматическое создание обучающих данных, представляющих вредоносный трафик. Предложенный подход может быть использован в реальной вычислительной среде, поскольку нет необходимости генерировать трафик, содержащий атаки, который необходим в других подходах.

СПИСОК ЛИТЕРАТУРЫ

1. Аграновский, А.В. «Обучаемые системы обнаружения и защиты от вторжений» / А.В. Аграновский // Искусственный интеллект. – 2001. – № 3. – с. 440-444.

2. Шелухин, О.И. «Обнаружение вторжений в компьютерные сети (сетевые аномалии): учеб. пособие» / Д.Ж. Сакалема, А.С. Филинова, О.И. Шелухин. – М.: Горячая линия – Телеком, 2013.

3. Дасгупта, Д. «Искусственные иммунные системы и их применение» / Д. Дасгупта. – М.: Физматлит, 2006. – 344 с.

4. Лукацкий, А.В. «Обнаружение атак» / А.В. Лукацкий. – СПб: БХВ-Петербург, 2001. – 624 с.

Ребро И.В. – студент, АлтГТУ им. И.И. Ползунова.
Шарлаев Е.В. – к.т.н., доцент АлтГТУ им. И.И. Ползунова.