УДК 004

Методы и алгоритмы по обнаружению распределенных низкоинтенсивных DoS-атак на информационную систему

Авторы: Нагуськин В.В. (v.naguskin@yandex.ru), Левкович С.С., Мельничук П.Ф., Исаева А.В. Соловьев Д.В., Бондаренко И.Б., Гатчин Ю.А.
Научный руководитель: Соловьев Денис Викторович, Университет ИТМО, Санкт-Петербург

На данный момент в мире растет количество возможных угроз информационной безопасности. Актуальной задачей является создание современных методов и алгоритмов по обнаружению угроз и их устранению. Данные методы должны работать на опережение.

В настоящие время при создании современных методов, работающих на опережение и чаще всего, используют такие математические подходы как: вероятностно-статистические методы, методы теории конфликтов (теории игр), методы теории искусственного интеллекта.

Однако, одним из перспективных математических подходов является применение методов теории искусственного интеллекта. К этим методам относятся: искусственные нейронные сети (ИНС) и генетические алгоритмы (ГА).

Из большого числа различных конфигураций ИНС наиболее распространенной является многослойная нейронная сеть, широко используемая для поиска закономерностей и классификации. Сеть состоит из нескольких слоев: входного слоя, скрытых слоев и выходного слоя, связанных между собой прямыми однонаправленными связями. Нейронную сеть можно разрабатывать под любую задачу и степень сложности этой задачи. Главой особенностью ИНС является ее способность к обучаемости.

Генетические алгоритмы относятся к числу универсальных методов оптимизации, позволяющих решать задачи различных типов таких как, комбинаторные, общие задачи с ограничениями и без ограничений, и различной степени сложности.

С применением ИНС и ГА методов могут быть решены задачи требующие обработки разноплановой информации, извлечения знаний, проведения интеллектуального анализа и нахождения оптимального решения. По сравнению с традиционными математическими методами методы ИНС и ГА обеспечивают достаточно высокое качество решений при меньших затратах. Они позволяют выявлять нелинейные закономерности в неоднородных данных, дают лучшие результаты при большом числе входных параметров по сравнению с классическими методами.

Данные методы являются одними из перспективных в области обеспечения информационной безопасности. Использование этих методов связано с их ключевыми особенностями, с помощью которых можно обнаружить атаки на доступность информации. Данные атаки образуют класс атак называемых атаки на «отказ в обслуживании» (DoS-атаки).

В современном мире роль ИНС и ГА трудно переоценить. По мнению специалистов, данные технологии войдут в десятку важнейших информационных технологий. Однако нужно заметить, что ИНС и ГА не является единственным средством для решения любых неформальных задач, они продолжают развиваться и совершенствоваться. В настоящей работе будут рассмотрены методы и алгоритмы по обнаружению распределенных низкоинтенсивных DoS-атак на информационную систему на основе технологий ИНС и ГА.

Автор Нагуськин В.В.

Научный руководитель Соловьев Д.В.