УДК 004.056.2

Одноклассовый SVM для обнаружения бот-сетей в устройствах IoT

Авторы: К.В Лисецкая., Е.А. Безверхняя, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Россия, Санкт-Петербург.
email: kristinasev62@gmail.com; kate.bezverkhnyaya@gmail.com
тел.: +7(978)769-54-81; +7(999)216-98-62
Научный руководитель: А.И. Спивак, Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики, Россия, Санкт-Петербург.

Устройства Интернета вещей (IoT) встречаются в нашей повседневной жизни довольно часто. Это могут быть камеры видеонаблюдения, медицинские мониторы, службы мониторинга трафика и многие другие. Система IoT позволяет упростить взаимодействие большого количества активных устройств, находящихся в одной сети. Системы IoT обычно включают в себя множество разноплановых недорогих устройств, которые обеспечены низким уровнем безопасности, а в некоторых вовсе может отсутствовать защита. Всвязи с этим возникает возможность потери огромного количества информации.

Несмотря на существующие способы защиты данных проблема остается актуальной, т.к. количество устройств, соединенных сетью растет из года в год, что делает данную область привлекательной для взломов.

Злоумышленники могут выполнять хакерские атаки на систему с целью ее отказа в обслуживании (DDoS) путем создания крупномасштабных ботнетов на основе IoT. Более того, скомпрометированные устройства могут не демонстрировать каких-либо явных симптомов заражения и могут продолжать выполнение своих обычных действий. Поэтому обнаружение взломанных устройств является сложной задачей и требует использование специальных методов.

Как было упомянуто выше: одной из многих угроз, с которыми сталкиваются устройства IoT, являются ботнеты. Ботнет – это совокупность скомпрометированных устройств, называемых ботами, управляемыми одним или несколькими пользователями, которые взаимодействуют с ботами для выполнения вредоносных действий. Использование ботнетов в системах IoT уже оказали огромное влияние на множество устройств, одним из ярких примеров стала атака Mirai в 2016 году. В этой атаке ботнет под названием Mirai заразил камеры видеонаблюдения, воспользовавшись настройками безопасности, которые были выставлены по умолчанию и не были изменены пользователями. Благодаря этому была осуществлена широкомасштабная DdoS-атака на крупного DNS-провайдера Dyn.

Одноклассовый SVM – это метод обнаружения аномалий в выборке, который пытается отделить обучающую выборку от начала координат с помощью гиперплоскости. Другими словами – это тип техники машинного обучения, которая вместо классификации экземпляра в одном из нескольких предопределенных шаблонов моделирует один и использует его, чтобы понять, принадлежит ли новый экземпляр шаблону или нет. Этот подход полезен, например, при обнаружении аномалий в данных. Устройства IoT выполняют конкретные задачи с определенным использованием вычислительных ресурсов. Моделирование использования ресурсов устройства с помощью одноклассового SVM может помочь обнаружить заражение ботнетом и аномалию в поведении IoT.

В предложенном подходе используется одноклассовый SVM, который является адаптацией метода опорных векторов для сценария с одним классом.

Модель потребления ресурсов строится на удаленном сервере. После этого построенная модель развёртывается в устройстве IoT, и система начинает анализировать потребление ресурсов для обнаружения отклонений в поведении. В тестах данный подход демонстрирует высокую производительность при обнаружении бот-сетей, при этом сохраняется низкое потребление ресурсов.

Заключение:

Основные результаты данной работы можно резюмировать следующим образом:

• Предложен упрощенный подход, который использует метод опорных векторов для обнаружения бот-сетей IoT с использованием данных о ресурсах устройства;

• Одноклассовый SVM имеет отличную прогнозирующую производительность;

• Подход способен защитить устройства IoT от ботнетов, не влияя на функциональность устройств;

• Данный подход опробован на реальном устройстве IoT, используя несколько разных ботнетов.