**Введение**

- введение в предметную область (взаимодействие устройств интернета вещей);

Угрозы, производящие к атакам на большие сети, такие как Интернет, требуют эффективных методов их выявления и реагирования. Наибольшую проблему вызывают атаки имеющие аномальное поведение в характеристиках выбранного пакета атрибутов сетевого трафика. Обнаружение атаки должно быть таким точным, насколько это возможно. Ложные срабатывания могут привести к нежелательным реакциям. Метод обнаружения должен быть эффективным против самых разнообразных атак, существующих на сегодняшний день, а также быть надежным против будущих попыток злоумышленников уклониться от обнаружения. Разработка эффективных методов выявления недопустимых событий (аномалий) в работе сети, являющихся следствием технических сбоев или несанкционированных воздействий, является актуальной задачей. Основным требованием, предъявляемым к этим методам, является возможность обнаружения в реальном масштабе времени произвольных типов аномалий, в том числе неизвестных ранее.

Одними из современных способов решения данной проблемы являются классификаторы - систематизированный перечень наименованных объектов, каждому из которых в соответствие дан уникальный код. Классификация объектов производится согласно правилам распределения заданного множества объектов на подмножества (классификационные группировки) в соответствии с установленными признаками их различия или сходства. Существует множество различных видов классификаторов. Но среди всего перечня было принято решение провести исследование на основе базовых классических классификаторов. (Метод наивного Байеса, Метод логистической регрессии, Метод пассивно-агрессивного классификатора, Метод KNN (k ближайших соседей), Метод “k средних”, Метод "дерево решений")

Цель данной работы можно сформулировать следующим образом - исследование эффективности многоклассовой классификации сетевых атак на устройства Интернета вещей (IoT) с помощью наиболее распространенных классических алгоритмов машинного обучения.

В качестве языка программирования был выбран Python. Это оптимальный выбор для поставленной перед нами задачи. Python один из самых популярных языков для анализа данных и машинного обучения. Его сильными сторонами является простота написания кода, простая и понятная структура. Именно для данного языка программирования разработано множество библиотек для анализа данных и машинного обучения. Почти все эти библиотеки реализованы на C/C++, что существенно ускоряет работу.

**1. Описание и первичная обработка исходных данных**

**поиск источников данных**

Для работы нам нужны данные. Причем к данным выдвигаются конкретные требования:

* “свежесть”
* объемность
* интерпретируемость признаков
* удобный формат
* высокое качество проработки классов
* предобработка человеком

Данные должны быть новыми, чем новее тем лучше. Методы злоумышленников меняются очень быстро. Из за чего черты присущие определенным атакам еще год назад могут измениться или вовсе исчезнуть. Оптимально, если данные за прошлый год, так как на их сбор и качественную предобработку нужно много времени, более новые данные хорошо качества достать не видиться возможным.

Данные должны быть большие как по числу объектов (замеры трафика) так и по числу замеряемых признаков. Нужно будет выделять из данных объекты на обучение, на проверку моделей, на итоговую проверку. Большое количество данных также дает возможность использовать больше методов в обучении (например кросс валидация) и уменьшает вероятность переобучения моделей. Большое количество признаков в принципе дает больше данных для обучения моделям. Также в данных с большой вероятностью будут сильно коррелирующие и вредные признаки, которые придется выкидывать. Оптимально число объектов должно быть не менее 10 миллионов с 20 или более признаками.

В бизнес задачах не всегда требуется интерпретируемость, главное чтобы модель улучшала необходимую метрику. Нам же для анализа и исследования нужно понимать на что именно реагирует конкретная модель и чем этот раздражитель является в реальном мире. Это дает возможность лучше понять что мешает а что помогает правильной классификации.

Данные должны быть представлены в стандартном удобном формате (.csv , .raw , .xls/.xlsx , .mat). Это обеспечивает удобность и простоту чтения данных, а также независимость от платформы (UNIX/Windows).

В исследуемых данных должно быть выделено как можно больше классов. Это делает задачу классификации более сложной, но повышает простор исследований и ценность самой данной работы. Оптимально классов должно быть не меньше 8.

Лучше если в классификации данных использовали ручные методы специалистов, а не только автоматические методы. Это улучшает качество классификации, а также начинают лучше фиксироваться выбросы и аномалии в данных.

**выбор подходящих данных**

Для проведения дальнейшей работы мы выбрали набор данных [IoT - 23](https://www.stratosphereips.org/datasets-iot23) созданный в лаборатории Avast AIC laboratory. Он подошел по всем выдвинутым к данным требованиям:

* опубликован 22 янваля 2020 года
* включает в себя более 325 миллионов объектов и более 20 признаков
* признаки понятны и интерпретируемые
* данные представлены в формате легко преобразуемом в .csv
* включает в себя более 10 классов
* была выполнена тщательная предобработка специалистами

**Описание набора данных**

Исследование проводилось на наборе данных IoT-23 от "Stratosphere Laboratory" опубликованные 22 янваля 2020 года (<https://www.stratosphereips.org/datasets-iot23>). Данный набор данных имеет 23 захвата сетевого трафика в диапазоне от 2018 до 2019 года, выполненных на устройствах IoT, 20 вредоносных захватов и 3 захвата для безопасного трафика устройств IoT. Этот сетевой трафик IoT был захвачен в "Stratosphere Laboratory", AIC group, FEL, CTU University, Чешская Республика.

Каждая запись в наборе представляет собой образ сетевого соединения и включает 23 информационных признака – индивидуальное измеряемое свойство или характеристику наблюдаемого явления – и промаркирована как «атака» или «не атака».

В исследуемом наборе атаки делятся на девять основные категории:

**Attack:** эта метка указывает на то, что был некоторый тип атаки от зараженного устройства к другому хосту. Здесь мы обозначаем как атаку на любой поток, который, анализируя его полезную нагрузку и поведение, пытается воспользоваться некоторыми уязвимыми услугами. Например, грубая сила к некоторому логину telnet, инъекция команды в заголовок запроса GET и т. д.

**C&C:** эта метка указывает, что зараженное устройство было подключено к серверу CC. Эта активность была обнаружена при анализе захвата вредоносных программ в сети, потому что соединения с подозрительным сервером являются периодическими, или наше зараженное устройство загружает с него некоторые двоичные файлы, или некоторые IRC-подобные или декодированные заказы приходят и уходят с него.

**DDoS:** эта метка указывает, что зараженное устройство выполняет распределенную атаку отказа в обслуживании. Эти потоки трафика обнаруживаются как часть DDoS-атаки из-за количества потоков, направленных на один и тот же IP-адрес.

**FileDownload:** эта метка указывает, что файл загружается на наше зараженное устройство. Это обнаруживается путем фильтрации соединений с байтами ответа более 3 КБ или 5 КБ, обычно это сочетается с некоторым известным подозрительным портом назначения или IP-адресом назначения, известным как сервер C&C.

**HeartBeat:** эта метка указывает, что пакеты, отправленные по этому соединению, используются для отслеживания зараженного хоста сервером C&C. Это было обнаружено путем фильтрации соединений с байтами ответа ниже 1B и с периодическими аналогичными соединениями, обычно это сочетается с некоторым известным подозрительным портом назначения или IP-адресом назначения, известным как сервер C&C.

**Mirai:** эта метка указывает, что соединения имеют характеристики ботнета Mirai. Эта метка добавляется, когда потоки имеют аналогичные шаблоны, как наиболее распространенные известные атаки Mirai.

**Okiru:** эта метка указывает, что соединения имеют характеристики ботнета Okiru. Это решение о маркировке было сделано с теми же параметрами, что и с Mirai, но с той разницей, что это семейство ботнетов менее распространено.

**PartOfAHorizontalPortScan:** эта метка указывает, что соединения используются для выполнения горизонтального сканирования портов для сбора информации для выполнения дальнейших атак. Для размещения этих меток мы полагаемся на шаблон, в котором соединения совместно используют один и тот же порт, одинаковое количество передаваемых байтов и несколько различных IP-адресов назначения.

**Torii:** эта метка указывает, что соединения имеют характеристики ботнета Torii. Это решение о маркировке было сделано с теми же параметрами, что и с Mirai, но с той разницей, что это семейство ботнетов менее распространено.

Метка указывающая на то, что в соединениях не было обнаружено никаких подозрительных вредоносных действий: **Benign.**

Три наиболее распространенных вредоносных (недоброкачественных потоков) метки являются: PartOfAHorizontalPortScan (213 852 920 потоков), Okiru (60 990 707 потоков) и DDoS (19 472 910 потоков). В то время как три наименее распространенные вредоносные (недоброкачественные потоки) метки: C&C-Mirai (2 потока), Okiru-Attack (3 потока) и PartOfAHorizontalPortScan-Attack (5 потоков).

