Т. М. ТАТАРНИКОВА, Ф. БИМБЕТОВ
Санкт-Петербургский государственный электротехнический университет «ЛЭТИ»
им. В.И. Ульянова (Ленина), Санкт-Петербург

МОДЕЛЬ МОНИТОРИНГА РАСХОДА ТРАФИКА УСТРОЙСТВОМ ИНТЕРНЕТА ВЕЩЕЙ

Обсуждается проблема обнаружения аномального трафика на устройстве интернета вещей – умном устройстве. Разработано приложение, представляющее собой информационную систему анализа статистических характеристик трафика, исходящего от умного устройства. Приложение устанавливается на умное устройство. Предложены характеристики, применяемые для идентификации аномалии сетевого трафика. Приведено описаний типов аномалий и характеристики, свидетельствующие о наличии аномалии в сетевом трафике.

Введение. Устройства интернета вещей (IoT-устройства) подвержены киберугрозам, способным привести к выводу устройства из работы, перехвату управления и другим. Самые популярные из киберугроз – это DDos-атаки и кража личных данных [1]. В первом случае, атаки становятся возможными благодаря цепочке подключенных устройств к интернету и заражении каждого из них вредоносной программой, которая позволяет удерживать полный контроль над устройством без согласия владельца. Во втором случае, речь идет о данных, получаемых с различных датчиков и гаджетов пользователя, которые в случае кражи могут дать похитителю информацию личного характера. Например, датчик движения, установленный в системе умного дома, может быть использован для получения информации о присутствии или отсутствии в доме людей [2].

Большинство современных гаджетов не способны противостоять атакам и краже данных по ряду причин [3]:

- Круглосуточная работа устройств позволяет даже в случаях частичного внешнего контроля обойти систему защиты.
- Полный контроль со стороны пользователя отсутствует.
- Сами владельцы редко замечают, что их устройства подвержены атаке или краже данных.

Очевидно, что все причины связаны с тем, что внешний контроль пользователя отсутствует или очень слаб.

Система контроля за расходом трафика. Для усиления контроля за расходом трафика предлагается приложение, интегрированное в интернет-устройство. Приложение представляет собой информационную систему с функциями учета расхода трафика, контроля потребляемых ресурсов и прогнозирования объемов трафика и ресурсов, которая укажет пользователю на аномальные случаи. Таким образом, пользователь будет предупрежден о возможных угрозах и краже.

В приложении анализируются несколько характеристик трафика, полученного от интернет-устройства, такие как частота пакетов, передаваемых по определенному типу протокола, количество пакетов трафика за установленное время и т. д. [4].

Для идентификации сетевой аномалии используются следующие характеристики:

- x_1 – интенсивность отправки пакетов;
- x_2 – интенсивность отправки пакетов с портом, указанным протоколом используемого IoT-устройства;
- x_3 – интенсивность отправки пакетов с адресом, в котором отправителем числится IoT-устройство;
- x_4 – интенсивность отправки пакетов с адресом, в котором получателем числится сервер с системой контроля.
- x_5 – интенсивность получения пакетов с неправильной контрольной суммой.
- x_6 – интенсивность отправки пакетов по определенному протоколу (UDP/TCP/MQTT).

После обнаружения аномалий система способна распознать угрозы. Для этого предложен трехуровневый идентификационный алгоритм, в котором анализируются характеристики, приведенные в таблице.

Таблица

Типы сетевых атак

Название типа аномалии	Описание аномалии	Изменения в трафике	Свидетельствующая характеристика
DoS-, DDoS-атака	Распределённая атака типа отказ в обслуживании на одну жертву	Выброс в представлении трафика пакеты/с, потоки/с, от множества источников к одному адресу назначения. Высокая заметность	Увеличение пакетов с одним адресом назначения. В случае IoT-устройств, подключенных к одному получателю, то это просто резкое увеличение количества отправки пакетов
Перегрузка	Необычно высокий спрос на один сетевой ресурс или сервис	Скачок в трафике по потокам/с к одному доминирующему ИБ-адресу и доминирующему порту. Обычно кратковременная аномалия.	Кратковременное увеличение пакетов с одним адресом назначения и одним портом. Отличие от DoS- и DDos-атак заключается в кратковременности и воздействии на один порт
Сканирование сети/портов	Сканирование сети по определённым открытым портам или сканирование одного хоста по всем портам с целью поиска уязвимостей	Скачок в трафике по потокам/с, с несколькими пакетами в потоках от одного доминирующего IP-адреса	Кратковременное увеличение пакетов с одним адресом отправления
Деятельность червей	Вредоносная программа, которая самостоятельно распространяется по сети и использует уязвимости ОС	Выброс в трафике без доминирующего адреса назначения, но всегда с одним или несколькими доминирующими портами назначения	Увеличение пакетов с одним портом назначения от разных источников
Точка-мультиточка	Распространение контента от одного сервера многим пользователям	Выброс в пакетах, байтах от доминирующего источника к нескольким назначениям, все к одному хорошо известному порту	Увеличение пакетов с одним портом назначения от одного источника
Отключения	Сетевые неполадки, которые вызывают падение в трафике между одной парой источник-назначение	Падение трафика по пакетам, потокам и байтам обычно до нуля. Может быть долговременным и включать все потоки источник-назначение от или к одному маршрутизатору	Сильное уменьшение количества пакетов от IoT-устройства
Переключения потока	Необычное переключение потоков трафика с одного входящего маршрутизатора на другой	Падение в байтах или пакетах в одном потоке трафика и выброс в другом. Может затрагивать несколько потоков трафика	Сильное уменьшение количества пакетов в одном потоке и резкое увеличение в другом
Пакеты с ошибками	Неполадки, которые вызывают повреждение пакетов	Выброс в трафике повреждённых пакетов	Увеличение пакетов, в которых контрольная сумма не подтверждает содержимое пакета

В работе реализован статистический метод в режиме Semi-Supervised anomaly detection (режим распознавания частично с учителем). В качестве самого метода выбран критерий согласия χ^2. В качестве аппроксимации выбран метод среднеквадратичного приближения. Непосредственно коэффициенты для аппроксимирующей функции можно получить с помощью функции scipy.optimize.curve_fit() из библиотеки SciPy языка Python, на котором реализовано приложение. Функция основана на выбранном ранее методе среднеквадратичного приближения.

Основными параметрами, передаваемыми в функцию scipy.optimize.curve_fit(), являются:

1) Функция *f*, которая отвечает за то, какую функцию нужно приближать к исходным данным. В параметры самой функции f передаются: дискретная выборка аргументов и коэффициенты. Сама функция *f* определяется отдельным методом.

2) Дискретные значения, для которых ищутся коэффициенты аппроксимации.

На выходе функция scipy.optimize.curve_fit() на первом месте выдаст искомый массив коэффициентов.

На последнем этапе с помощью функции *f* и полученных коэффициентов находятся интересующие дискретные значения от аппроксимирующей функции.

Графики этапов работы функции изображены на рис. 1–4.

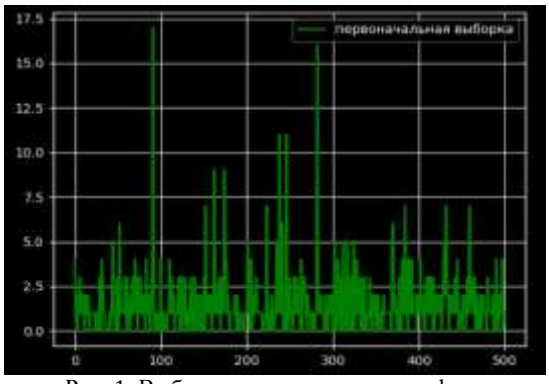

Рис. 1. Выборка не аномального трафика IoT-устройства

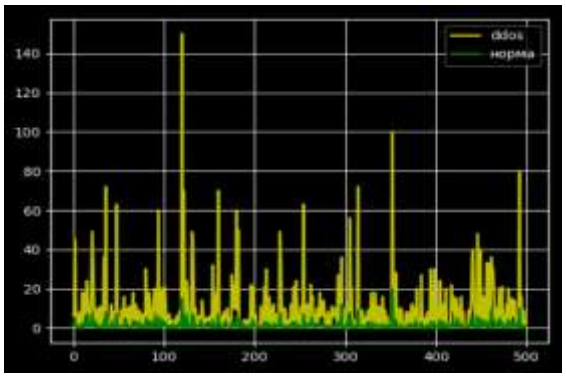

Рис. 2. Аномальный и не аномальный трафик в одном окне

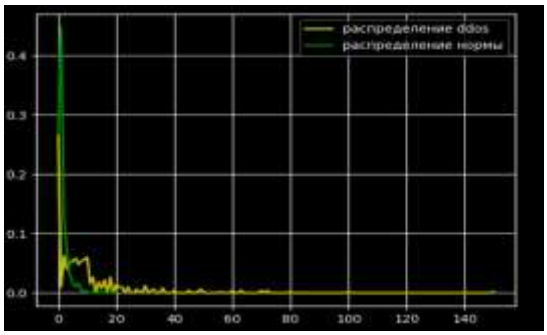

Рис. 3. Функция распределения аномального и не аномального трафика

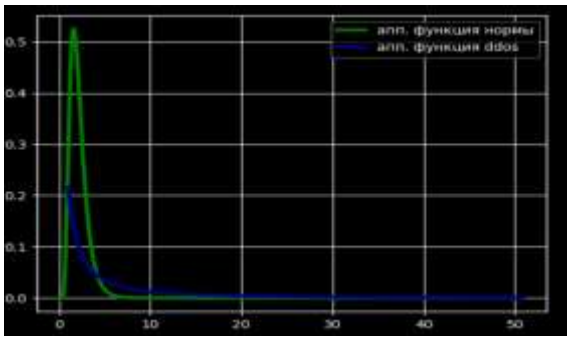

Рис. 4. Аппроксимирующие функции распределений аномального и не аномального трафика

Разработанный метод chi_square() принимает две выборки и возвращает сумму квадратов разности от этих двух выборок. Далее остается только сравнить значение.

Заключение. Эффективными способами борьбы с киберугрозами является постоянный мониторинг и анализ трафика. Поскольку сфера применения устройств интернета вещей постоянно расширяется, то периодически появляется новое вредоносное программное обеспечение, характеристики которого могут стать известными уже после реализации атаки. Поэтому важно отслеживать именно аномалии в трафике, а не делать упор на идентификацию угрозы.

В работе предложено приложение, которое устанавливается в устройство интернета вещей, способствующее предупреждению атаки на устройство и кражу личных данных.

ЛИТЕРАТУРА

1. **Tatarnikova T.M.** Restricting data leakage through non-obvious features of Android 5 smartphone. *Informatsionno-Upravliaiushchie Sistemy*. 2019. Vol. 5. P. 24–29. doi: 10.31799/1684-8853-2019-5-30-37.
2. **Sovetov B.Y., Tatarnikova T.M., Cehanovsky V.V.** Detection System for Threats of the Presence of Hazardous Substance in the Environment. *2019 XXII International Conference on Soft Computing and Measurements (SCM)*, St. Petersburg, Russia, 2019. P. 121-124. doi: 10.1109/SCM.2019.8903771.

3. **Bogatyrev V.A., Vinokurova M.S.** Control and Safety of Operation of Duplicated Computer Systems. *Communications in Computer and Information Science, IET – 2017*. 2017. Vol. 700. P. 331-342.
4. **Татарникова Т.М., Бимбетов Ф., Богданов П.Ю.** Выявление аномалий сетевого трафика методом глубокого обучения. *Известия СПбГЭТУ ЛЭТИ*. 2021. № 4. С. 36-41.

T.M.Tatarnikova, F.Bimbetov (Saint Petersburg Electrotechnical University “LETI”, St. Petersburg)
Monitoring model of traffic consumption by the internet of things device

The problem of detecting anomalous traffic on an Internet of Things device, a smart device, is discussed. An application has been developed, which is an information system for analyzing the statistical characteristics of traffic coming from a smart device. The application is installed on a smart device. The characteristics used to identify network traffic anomalies are proposed. Descriptions of the types of anomalies and characteristics indicating the presence of an anomaly in network traffic are given.

Авторы готовы представить текст на английском языке для сборника материалов мультиконференции, который будет подан для индексирования в Scopus