МЕТРИЧЕСКИЕ ХАРАКТЕРИСТИКИ ОБНАРУЖЕНИЯ АНОМАЛЬНОГО ТРАФИКА В СЕТЯХ ИНТЕРНЕТА ВЕЩЕЙ

DOI: 10.36724/2072-8735-2022-16-1-15-21

Manuscript received 24 November 2021;
Accepted 22 December 2021

Татарникова Татьяна Михайловна,
Санкт-Петербургский государственный университет аэрокосмического приборостроения, г. Санкт-Петербург, Россия, ***tm-tatarn@yandex.ru***

Богданов Павел Юрьевич,
Санкт-Петербургский государственный университет аэрокосмического приборостроения, г. Санкт-Петербург, Россия, ***45bogdanov@gmail.com***

Ключевые слова: *интернет вещей, беспроводная сенсорная сеть, энергия, аномальный трафик, сетевая атака, система обнаружения атак, метрика, сигнатура, штатное поведение*

Обсуждается актуальная задача своевременного обнаружения аномального трафика в сетях интернета вещей, расточающего энергию сенсорных устройств. Под аномальным подразумевается трафик, который содержит вредоносное программное обеспечение, реализующее атакующее воздействие на узлы интернета вещей. Своевременное обнаружение аномального трафика способствует сохранению срока службы и, соответственно, выполнения оказываемых интернетом вещей услуг. Предметом исследования является применение метрических характеристик для обнаружения аномального трафика в сетях интернета вещей. Цель работы заключается в предложении системы метрик, позволяющих регистрировать сигнатуры отдельных сенсорных устройств или паттернов их поведения и оценивать режим работы отдельных сетевых сегментов. Поскольку интернет вещей строится по иерархическому принципу – от беспроводной сенсорной сети до глобальной сети, то и система обнаружения атакующих воздействий охватывает все уровни – от сенсорного устройства до глобального облака. Обнаружение аномального трафика как в беспроводной сенсорной сети, так и на уровне проводных сетей – локальных и глобальных реализуется с помощью метрик. Метрика представляет собой качественный или количественный показатель, который отражает ту или иную характеристику функционирования инфокоммуникационной сети. Анализ источников показал отсутствие систематизации метрических характеристик для сетей интернета вещей. Результаты исследований включают: описание элементов, образующих экосистему интернета вещей; многоуровневую модель архитектуры интернета вещей; систему метрик обнаружения аномального трафика, содержащую широкий набор прогнозирующих, диагностических и ретроспективных метрик. Предложенная система метрик может быть использована при построении систем обнаружения атак в сетях интернета вещей.

Информация об авторах:
Татарникова Татьяна Михайловна, *Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра инфокоммуникационных систем, д.т.н., профессор, г. Санкт-Петербург, Россия*
Богданов Павел Юрьевич, *Санкт-Петербургский государственный университет аэрокосмического приборостроения, кафедра технологий защиты информации, старший преподаватель, г. Санкт-Петербург, Россия*

Для цитирования:
Татарникова Т.М., Богданов П.Ю. Метрические характеристики обнаружения аномального трафика в сетях интернета вещей // T-Comm: Телекоммуникации и транспорт. 2022. Том 16. №1. С. 15-21.

For citation:
Tatarnikova T.M., Bogdanov P.Yu. (2022). Metric characteristics of anomalous traffic detection in internet of things. *T-Comm*, vol. 16, no.1, pp. 15-21. (*in Russian*)

Введение

Одной из наиболее перспективных технологий по иерархическому принципу, то и проектирования систем автоматизации управления, мониторинга, контроля считаются беспроводные сенсорные сети (Wireless Sensor Networks, WSN) в силу следующих их достоинств: мобильность, самоорганизация, быстрое развертывание, создание временной сети на местности, где прокладка обычных кабелей затруднена [1].

Беспроводная сенсорная сеть (БСС) образуется множеством сенсорных устройств (СУ) и коммутационных узлов (КУ), объединенных между собой посредством радиоканала. Источниками данных в сенсорной сети являются датчики (сенсоры), регистрирующие данные (измерения) об окружающей среде – температуре, влажности, освещении и т.д. Датчики, взаимодействуя между собой и с КУ, например маршрутизаторами, образуют распределенную, самоорганизующуюся систему сбора, обработки и передачи зарегистрированных данных [2].

Построение «умных» систем на базе БСС обусловило появление интернета вещей (Internet of Things, IoT). Интернет вещей – это экосистема, представляющее собой программно-аппаратное решение, обеспечивающее автономную реализацию информационных процессов сбора, обработки и передачи данных в интересах оказываемой пользователю услуги [3].

«Умные» функции интернета вещей во многом определяются прикладными задачами, но в целом IoT предоставляет широкий набор услуг: экологический контроль территорий, охрана объектов, технологический процесс, мониторинг пациентов, «умный дом» и многое другое [4].

В свою очередь появление интеллектуальных мобильных устройств, использующих батареи в качестве источника питания актуализировало задачу своевременного обнаружения аномального трафика, расточающего энергию IoT. Устройствам IoT с низкой вычислительной мощностью, ограниченным объемом памяти и ограниченной емкостью батареи сложно выполнять сложные алгоритмы безопасности, требующие интенсивных вычислений и коммуникационной нагрузки. Эти недостатки делают устройства интернета вещей уязвимыми к аномальному трафику – различным атакам, реализация которых может нанести серьезный ущерб эксплуатируемому оборудованию IoT и даже физический ущерб людям.

Однако решения безопасности, такие как системы обнаружения атак (СОА), которые не увеличивают нагрузку на сенсорные устройства, эффективны и считаются первой линией защиты сетей интернета вещей. Своевременное обнаружение аномального трафика способствует сохранению срока службы сети интернета вещей [5].

Многоуровневая организация интернета вещей

Экосистему IoT образуют [6]:

– сенсорные и исполнительные устройства с функциями измерений и приема-передачи данных,

– телекоммуникационная инфраструктура, обеспечивающая транспортировку данных,

– серверы, выполняющие функции обработки данных,

– программное обеспечение, реализующее протоколы приема-передачи, хранения данных, методы анализа полученных данных и алгоритмы принятия решений по результатам анализа.

Название «экосистема» говорит о том, что образующие ее элементы находятся в закономерной взаимосвязи друг с другом и созданы условия для их совместного сбалансированного и устойчивого функционирования.

Типичная структура СУ включает в себя датчик (датчики), обработчик измеренных данных и интерфейсы взаимодействия с другими СУ. Работа СУ обеспечивается питанием от батареи.

Организация телекоммуникационной инфраструктуры интернета вещей зависит от масштаба охватываемой территории и сложности решаемой задачи. Срок службы БСС в отличие от сетей WiFi или WiMAX обусловлен энергозатратами сенсорных устройств на сбор, обработку, передачу данных, вычисление маршрута и т.д. Поэтому в целях экономии энергии многошаговое взаимодействие является более распространенным вариантом передачи данных в интернете вещей и реализуется иерархической структурой (рис. 1) [7].

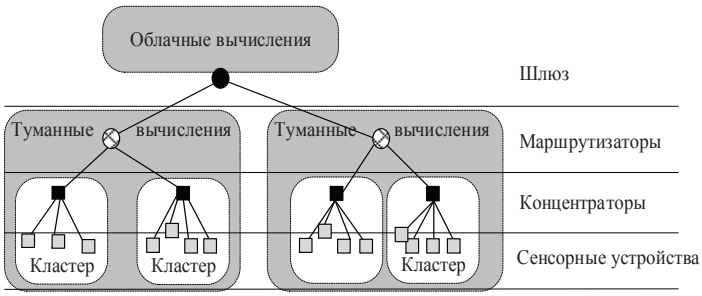

Рис. 1. Иерархическая структура организации сетей IoT

На нижнем уровне сети IoT пакеты данных от сенсорных устройств концентрируются в головном узле кластера, которые затем передаются ближайшему маршрутизатору. Далее пакеты транспортируются по коротким маршрутам и за несколько шагов (хопов) буду переданы на шлюз облачных вычислений.

Таким образом, на нижнем, физическом уровне из сенсорных устройств образуется беспроводная сенсорную сеть, которая строится как совокупность кластеров. Количество кластеров теоретически не ограничено, что позволяет масштабировать размер сети под требования задач контроля и/или мониторинга территорий.

Многоуровневая организация системы обнаружения атак интернета вещей

Безопасность должна охватывать все уровни архитектуры IoT: от датчика и до облака [8] (рис. 2).

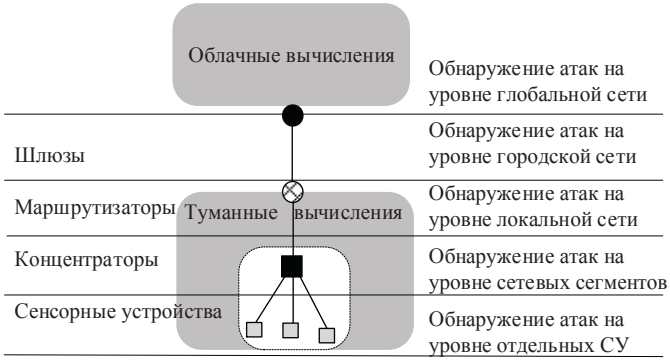

Рис. 2. Многоуровневая организация СОА в сетях IoT

Каждому компоненту в цепочке управления безопасностью данных предписан контрольный список процедур безопасности, которые рекомендуется предусмотреть при развертывании интернета вещей (табл. 1).

Базовым средством детектирования аномального трафика инфокоммуникационной сети является система обнаружения атак (СОА). Непосредственно обнаружению атаки предшествует процедура сбора статистик, обрабатываемых средствами СОА. Например, можно обрабатывать статистики, снимаемые с узлов сети во время приема, передачи и обработки пакетов данных [9]

Система обнаружения атак для сети интернета вещей, имеет иерархическую структуру, как и сама сеть – три компонентных уровня (рис. 3). На нижнем уровне иерархии находятся кластерные беспроводные сенсорные сети. Головной узел кластера отвечает за авторизацию других членов кластера, маршрутизатор отвечает за авторизацию головных узлов кластера, а шлюз за авторизацию маршрутизаторов.

На IoT-устройствах функционирует модуль обнаружения аномального поведения, на маршрутизаторах и шлюзах – интеллектуальная система обнаружения сетевых атак.

IoT-устройства оповещают о своем присутствии в конкретном кластере, направляя идентификатор (ID), например MAC-адрес в модуль мобильности. Модуль мобильности отвечает за регистрацию вновь прибывших в кластер устройств и удаление вышедших из кластера устройств. Любой вновь прибывший узел проходит процедуру аутентификации.

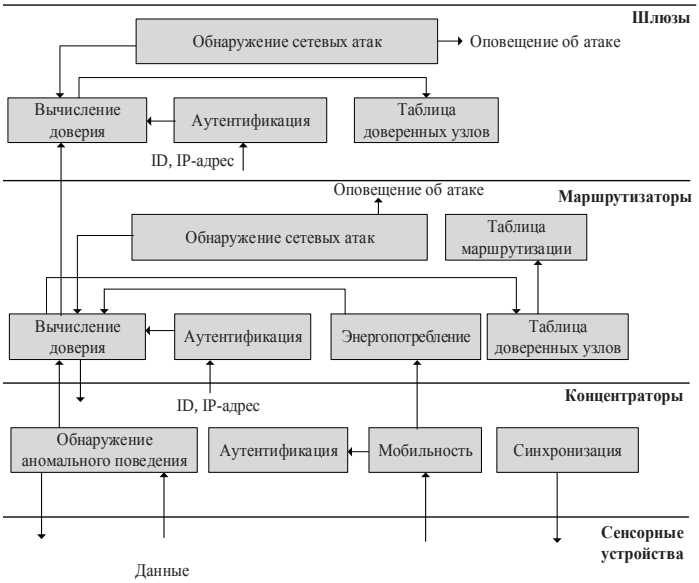

Рис. 3. Компоненты системы обнаружения атак

Модуль синхронизации представляет собой тактовый генератор – формирование временных окон (слотов) беспроводной сенсорной сети, во время которых происходит опрос IoT-устройств в кластере.

Модуль обнаружения (детектирования) аномального поведения реализуется путем профилирования каждого устройства – создания базы сигнатур для каждого сенсорного устройства при приеме и передаче данных. Под сигнатурой будем понимать последовательность зарегистрированных во времени значений характеристик, например загрузки процессора и/или памяти устройства, числа отправляемых пакетов, размеров пакетов, плотности распределения вероятностей временных задержек передачи/приема пакетов и других метрик [10].

На уровне сетей (локальных и глобальных) обнаружение сетевых атак реализуется контролем отклонения текущего режима работы сети от штатного. В основе такого подхода лежит модель поведения контролируемого участка сети [11].

Модуль вычисления доверия позволяет в онлайн режиме удалять скомпрометированные узлы из списка доверенных узлов. Таблица маршрутизации строится на основе этого списка.

Список доверенных узлов формируется независимо на каждом машрутизаторе, алгоритм формирования списка включает следующие шаги:

1. Инициализация. Каждым узлом формируется список доверенных узлов, в который на момент инициализации включаются все узлы-соседи. Инициализация выполняется один раз перед началом функционирования IoT.

2. Контроль. Каждый узел оценивает поведение своих соседей по специальным характеристикам (метрикам) и вычисляет свой уровень доверия к ним. Собственное доверие узла p к узлу-соседу q оценивается как

$$C_{p,q} = \sum_{i=0}^{n} m_i w_i, \qquad (1)$$

где n – число метрик, участвующих в оценке доверия; m_i – величина i-й метрики; w_i – вес i-й метрики.

3. Оценка репутации узла p к соседнему узлу q на основе сведений полученных со стороны других узлов

$$R_{p,q} = \frac{\sum_{i=1}^{L} C_{p,i} C_{i,q}}{\sum_{i=1}^{L} C_{p,i}}, \qquad (2)$$

где L – количество узлов, обменивающихся оценками доверия.

Оценка репутации требуется тем узлам, которые не могут получить ее от соседей. С этой целью узлы периодически рассылают оценки доверия всем узлам из своего списка доверенных узлов.

4. Вычисление доверия узла p к узлу-соседу q как суммы оценки собственного доверия и оценки репутации

$$D = C_{p,q} \frac{z}{r} + R_{p,q} \left(1 - \frac{z}{r}\right), \qquad (3)$$

где r – число взаимодействий с узлом за раунд; z – количество обменов репутацией с узлом за раунд.

1. Принятие решения на основе значения D о взаимодействии с узлом-соседом или исключения его из списка доверенных узлов согласно логическому правилу $D > P?$, где P – пороговый уровень доверия.

2. Формирование списка доверенных узлов БСС с учетом 5-го шага алгоритма. На основе списка доверенных узлов строятся маршруты доставки данных до шлюза облачных вычислений.

Система метрик

Для своевременного обнаружения аномального трафика сетей интернета вещей необходима система метрик, позволяющая в реальном времени оценить наличие угроз, направленных на безопасность функционирования IoT [12].

Метрика – это качественный или количественный показатель, характеризующий функционирование IoT и уровень эффективности обнаружения аномального трафика.

Количественные показатели проще отслеживать, поэтому они используются чаще. На основании значений этих показателей можно делать выводы о состоянии сети: статус узлов, их производительность, объем передаваемого трафика, время доставки, состояние доставки и т.п.

Метрики могут объединяться в систему (иерархию) метрик.

Иерархия метрик – это древовидная структура или схема, во главе которой находится основная метрика. Чтобы ее построить, нужно анализировать данные и понять реальные зависимости между метриками.

Система метрик проектируются под конкретную задачу.

Различаю несколько типов метрик: прогнозирующие, диагностические, ретроспективные. Прогнозирующие определяют будущий результат и позволяют диагностировать будущие проблемы. Диагностические характеризуют мониторинг текущего состояния. Ретроспективные дают анализ полученного результата.

Обозначим множество метрик позволяющие оценить статус узлов IoT-сети – доверенный или скомпрометированный как $M=\{m_1, m_2, \ldots, m_n\}$.

К прогнозирующим метрикам будут относиться все требуемые или допустимые значения диагностических метрик – значения, которые устанавливают порог, за пределами которого требуется принятие решения.

К диагностическим метрикам отнесем следующие:

m_1 – интенсивность передачи пакетов: $m_1=1/N$, где N – количество переданных узлом пакетов за один раунд;

Понятие раунда соответствует интервалам времени, в течение которых определенные IoT-устройства выполняют функции головных узлов соответствующих кластеров.

m_2 – продолжительность передачи пакета данных, с; Если по время передачи пакета не произошло сбоев, то продолжительность передачи пакета данных оценивается как $m_2=L/v$, где L – длина пакета данных, v – скорость канала связи.

m_3 – доля ретранслированных пакетов $m_3=r^*/r$, где r^* – количество пакетов, переданных через узел в раунде; r – количество взаимодействий с узлом за раунд;

Головной узел, в течение раунда выполняет роль транзита – ретранслятора пакетов данных от оконечных сенсорных устройств – членов кластера.

m_4 – целостность данных:

$$m_4=\begin{cases}1, \text{ если } CRC=CRC^*,\\ 0, \text{ если } CRC\neq CRC^*,\end{cases}$$

где CRC – контрольная сумма поля данных, записанная в формате пакета; CRC^* – контрольная сумма, вычисленная узлом на основе поля данных пакета.

m_5 – доля корректно ретранслированных пакетов $m_5=r^{**}/r^*$, где r^{**} – количество пакетов, верно ретранслированных через узел за раунд.

Под верно ретранслированными пакетами будем понимать пакеты, которые прошли проверку целостности данных согласно метрике m_4.

m_6 – обмен репутацией: $m_6=z/r$, где z – количество обменов репутацией с узлом за раунд;

m_7 – корректность репутации узла:

$$m_7=\begin{cases}1, \text{ если } C_{pq}-\dfrac{\sum_{i=1}^{L}R_{iq}}{L}\geq R_{\text{доп}},\\ 0, \text{ если если } C_{pq}-\dfrac{\sum_{i=1}^{L}R_{iq}}{L}< R_{\text{доп}},\end{cases}$$

где $R_{\text{доп}}$ – установленный порог нормированного количества не совпавших уровней доверия с уровнями доверия, полученными от других узлов; m_8 – корректность обмена репутацией: $m_8=z^*/z$, где z^* – количество корректных обменов репутацией с узлом за раунд.

Корректным обменом репутацией сичтаются случаи, при которых $m_7=1$.

m_9 – уровень остаточной энергии: $m_9=E_j/E_0$, где E_j – энергия СУ в текущем *j-м* раунде БСС; E_0 – энергия того же СУ на начало функционирования БСС.

m_{10} – доля подтвержденных пакетов: $m_{11}=r^+/r^*$, где r^+ – количество полученных в раунде подтверждений о получении пакетов.

m_{11} – доля срочных пакетов $m_{12}=r^{**}/r$, где r^{**} – количество срочных пакетов, ретранслированных узлом за раунд;

m_{12} – доля управляющих пакетов $m_{12}=p^*/r$, где p^* – количество управляющих пакетов, ретранслированных узлом за раунд;

m_{13} – доля пакетов с полезными данными $m_{12}=p^{**}/r$, где p^{**} – количество пакетов с полем данных, переданных через узел за раунд;

m_{14} – продолжительность «спящего» режима узла сенсорной сети, с. Очевидно, что если во время «спящего» режима зафиксирована передачи данных от соответствующего узла сенсорной сети, то высока вероятность, что узел скомпрометирован.

m_{15} – метка начала момента активации сенсорного устройства.

m_{16} – метка момента окончания активации сенсорного устройства

Очевидно, что если вне периода $[m_{17};m_{16}]$ зафиксированы передачи данных от соответствующего узла сенсорной сети, то высока вероятность, что узел скомпрометирован.

К ретроспективным метрикам отнесем статистические (накопленные) показатели отправляемого и принимаемого IoT-устройствами трафика и значения диагностических метрик предыдущего раунда сети:

m_{17} – среднее арифметическое плотности распределения (математическое ожидание) диагностической метрики распределенной во времени, например, объема передан-

ных/принятых данных, временной задержки доставки пакетов и т.п.

m_{18} – медиана плотности распределения диагностической метрики.

m_{19} – стандартное отклонение плотности распределения диагностической метрики.

m_{20} – среднеквадратичное отклонение плотности распределения диагностической метрики.

m_{21} – коэффициент корреляции между диагностическими метриками.

m_{22} – ковариационный момент между диагностическими метриками.

m_{23} – историческое доверие: $m_{21}=T(i\text{-}1)$, где $T(i\text{-}1)$ – значение уровня доверия к узлу на предыдущем раунде функционирования сенсорной сети.

Список метрик не ограничивается перечисленными. Содержание этого списка может дополняться специалистами в области информационной безопасности и сетевыми администраторами.

С учетом поставленной задачи диссертационного исследования основной в системе метрик будет метрика m_9 – уровень остаточной энергии узла. На втором уровне – все метрики, оказывающие влияние на расход энергии: m_1, m_2, m_3, m_6, m_{10}, m_{14}, на третьем уровне – метрики безопасности: m_4, m_5, m_7, m_8, m_{15}, m_{16}, на четвертом уровне – метрики, требующие накопления своих значений для последующего анализа состояний IoT-узлов и сети: m_{11}, m_{12}, m_{17}, m_{18}, m_{19}, m_{20}, m_{21}, m_{22}, m_{23}.

Организация сбора метрических характеристик.

Метрические характеристики собираются с помощью специализированных узловых и сетевых программных агентов СОА. Узловые агенты интегрируются в системное программное обеспечение сетевых узлов и собирают метрические характеристики о событиях, связанных с приемом, обработкой и передачей пакетов данных. При этом на одном и том же сетевом узле могут работать несколько разных узловых агентов, собирающих определенные метрики. Сетевые агенты интегрируются в сетевое программное обеспечение и собирают метрические характеристики о процессах приема-передачи пакетов данных в контролируемых сегментах сети [13].

Собранные узловыми и сетевыми агентами метрики анализируются средствами СОА. При этом в зависимости от этапа реализации атаки собранные метрики участвуют в оценке отклонения от профиля (сигнатурный метод) и/или оценке отклонения от штатного режима функционирования сети (поведенческий метод).

На этапе сбора информации применяются только сигнатурные методы обнаружения атак, направленные на сбор статистик (метрик) о функционировании сенсорных устройств и сетевых сегментов. Вредоносные действия от атак пока не очевидны. Используются узловые и сетевые агенты.

Обнаружение атак на этапе вторжения выполняется с применением сигнатурных и поведенческих методов. Поскольку вторжением можно считать с одной стороны отклонение от профиля сенсорного устройства, а с другой как отклонение от штатного режима функционирования сети, то эффективным считается сочетание обоих методов. Для сбора метрик, участвующих в оценке отклонения от профиля и от штатного поведения применимы как узловые, так и сетевые агенты.

Для обнаружения атак на этапах воздействия и развития применяются только поведенческие методы, т.к. результаты от действий атак проявляются в виде отклонений от штатного режима функционирования сети. Соответствующие метрики собираются узловыми агентами.

В таблице 1 приведены применяемые на разных стадиях развития атаки методы, агенты и метрики.

Таблица 1

Методы, агенты и метрики, применяемые на разных стадиях атаки

Стадия атаки	Метод	Тип агента	Метрики
Сбор данных	Сигнатурный	Сетевой, Узловой	
Вторжение	Сигнатурный, поведенческий	Сетевой, Узловой	
Реализация	Поведенческий	Узловой	
Развитие	Поведенческий	Узловой	

Вместе с тем, как показывает анализ, применение только сигнатурных и/или поведенческих методов для обнаружения распределенных сетевых атак недостаточно. На этапе реализации и развития сетевой атаки применяются только поведенческий метод с привлечением узловых агентов, собирающими значения метрик, в то время как распределенные атаки являются атаками, реального времени и для их распознавания и дальнейшего развития также необходимы методы, работающие «на лету». В связи с этим популярность приобретают методы, основанные на глубоком анализе [14,15].

Глубокий анализ – это методы, в которых при обработке в режиме реального времени решения о возникновении событий принимаются «на лету» – пока новые события создаются в режиме реального времени, старые передаются в движок глубокой обработки.

Заключение

Показано, что к интернету вещей, как и к любой другой инфокоммуникационной системе применим многоуровневый подход к обнаружению аномального трафика. Система обнаружения атакующих воздействий на устройства и узлы интернета вещей охватывает все уровни архитектуры IoT: от датчика и до облака. Приведена общая схема многоуровневой системы защиты, рекомендуемая при развертывании интернета вещей.

Обнаружение аномального трафика подразумевает сбор метрических характеристик узловыми и сетевыми агентами, а затем анализ метрических величин сигнатурными и поведенческими методами системы обнаружения атак.

Предложена система метрик, позволяющие оценить статус узла – доверенный или скомпрометированный. Метрики используются при построении системы обнаружения атак и бывают прогнозируемыми, диагностическими и ретроспективными.

В дальнейшем планируется на основе метрических характеристик реализовать сигнатурную модель сенсорных устройств и поведенческую модель коммутационных узлов интернета вещей с проведением натурного эксперимента.

Литература

1. *Киричек Р.В., Парамонов А.И., Прокопьев А.В., Кучерявый А.Е.* Эволюция исследований в области беспроводных сенсорных сетей // Информационные технологии и телекоммуникации. 2014. №4 (8). С. 29-41.

2. *Кнеллер В.Ю.* "Приборное облако" – концепция функционирования сенсорных систем на основе интернет-технологии // Датчики и системы. 2010. №8. С. 66-69.

3. Интернет вещей и межмашинные коммуникации. Обзор ситуации в России и мире // Мобильные телекоммуникации. 2013. №7. С. 26-28.

4. *Восков Л.С. Пилипенко Н.А.* Web вещей – новый этап развития интернета вещей// Качество. Инновации. Образование. 2013. № 2. С. 44-49.

5. *Татарникова Т.М., Богданов П.Ю., Краева Е.В.* Предложения по обеспечению безопасности системы умного дома, основанные на оценке потребляемых ресурсов//Проблемы информационной безопасности. Компьютерные системы. 2020. № 4. С. 88-94.

6. *Ли П.* Архитектура интернета вещей/ пер. с анг. М.А. Райтмана. М.: ДМК Пресс, 2019. 454 с.

7. *Татарникова Т.М.* Аналитико-статистическая модель оценки живучести сетей с топологией mesh // Информационно-управляющие системы.

8. *T & Bogdanov, P & Kraeva, E & Stepanov, S & Sidorenko, A.* Detection of network attacks by deep learning method. Journal of Physics: Conference Series. 1901 (1). 2021. P. 012051. DOI 10.1088/1742-6596/1901/1/01205.

9. *Татарникова Т.М., Бимбетов Ф., Богданов П.Ю.* Выявление аномалий сетевого трафика методом глубокого обучения // Известия СПбГЭТУ ЛЭТИ. 2021. № 4. С. 36-41.

10. *Jyothsna V., Prasad V.V.R.* A Review of Anomaly Based Intrusion Detection Systems // International Journal of Computer Applications. 2011. vol. 28, no. 7. P. 26-35.

11. *Gyanchandani M., Rana J.L., Yadav R.N.* Taxonomy of Anomal Based Intrusion Detection System: A Review // International Journal of Scientific and Research Publicctions. 2012. Vol. 2. Issue 12. P. 1-13.

12. Lee W., Xiang D. Information-theoretic measures for anomaly detection // Security and Privacy. 2001. P. 130-143.

13. *Татарникова Т.М., Журавлев А.М.* Нейросетевой метод обнаружения вредоносных программ на платформе Android // Программные продукты и системы. 2018. № 3. С. 543-547.

14. *Пальчевский Е.В., Христодуло О.И.* Разработка метода самообучения импульсной нейронной сети для защиты от DDoS-атак // Программные продукты и системы. 2019. Т. 32. № 3. С. 419-432. DOI: 10.15827/0236-235X.127.419-432.

15. *Сафронова Е.О., Жук Г.А.* Применение искусственных нейронных сетей для прогнозирования DoS атак // Молодой ученый. 2019. №23. С. 27-30.

METRIC CHARACTERISTICS OF ANOMALOUS TRAFFIC DETECTION IN INTERNET OF THINGS

Tatyana M. Tatarnikova, *St. Petersburg State University of Aerospace Instrumentation, St. Petersburg, Russia,* ***tm-tatarn@yandex.ru***

Pavel Yu. Bogdanov, *St. Petersburg State University of Aerospace Instrumentation, St. Petersburg, Russia,* ***45bogdanov@gmail.com***

Abstract

The urgent problem of timely detection of abnormal traffic in the Internet of Things networks, which wastes the energy of sensor devices, is discussed. Anomalous traffic means traffic that contains malicious software that implements an attacking effect on the nodes of the Internet of Things. Timely detection of abnormal traffic contributes to the preservation of the service life and, accordingly, the performance of the services provided by the Internet of Things. The subject of this research is the application of metric characteristics to detect abnormal traffic in the Internet of Things networks. The aim of the work is to propose a system of metrics that allow registering signatures of individual sensor devices or patterns of their behavior and assessing the mode of operation of individual network segments. Since the Internet of Things is built on a hierarchical basis - from a wireless sensor network to a global network, the attack detection system covers all levels - from a sensor device to a global cloud. Detection of abnormal traffic both in the wireless sensor network and at the level of wired networks - local and global - is implemented using metrics. A metric is a qualitative or quantitative indicator that reflects one or another characteristic of the functioning of an infocommunication network. Analysis of the sources showed the lack of systematization of metric characteristics for the Internet of Things networks. Research findings include: a description of the elements that make up the IoT ecosystem; layered model of the architecture of the Internet of things; an abnormal traffic detection metrics system containing a wide range of predictive, diagnostic and retrospective metrics. The proposed system of metrics can be used to build intrusion detection systems in IoT networks.

Keywords: *internet of things, wireless sensor network, energy, abnormal traffic, network attack, attack detection system, metric, signature, regular behavior.*

References

1. R.V. Kirichek, A.I. Paramonov, A.V. Prokop'yev, A.Ye. Kucheryavyy (2014). Evolution of research in the field of wireless sensor networks. *Information technologies and telecommunications*, no. 4 (8), pp. 29-41. (In Russian)
2. V.Yu. Kneller (2010). "Instrument cloud" – the concept of functioning of sensor systems based on Internet technology. *Sensors and systems*, no. 8, pp. 66-69. (In Russian)
3. Internet of things and machine-to-machine communications. Overview of the situation in Russia and the world. *Mobile telecommunications,* no. 7, 2013, pp. 26-28. (In Russian)
4. L.S. Voskov, N.A. Pilipenko (2013). Web of things – a new stage in the development of the Internet of things. *Quality. Innovation. Education*, no. 2, pp. 44-49. (In Russian)
5. T.M. Tatarnikova, P.Yu. Bogdanov, E.V. Kraeva (2020). Smart home security proposals based on assessment of consumption resources. *Problems of information security. Computer systems*, no 4, pp. 88-94. (In Russian)
6. P. Lee (2018). Internet of Things for Architects. Packt Publ., Birmingham – Mumbai, 524 p.
7. T.M. Tatarnikova (2017). Analytical-Statistical Model of Mesh Network Survivability Evaluation. *Information and control systems*, vol. 1(86), pp. 17-22, DOI: 10.15217/issnl684-8853.2017.1.17
8. T. Tatarnikova, P. Bogdanov, E. Kraeva, S. Stepanov, A. Sidorenko (2021). Detection of network attacks by deep learning method. *Journal of Physics: Conference Series*, 1901(1), pp. 012051, DOI 10.1088/1742-6596/1901/1/01205
9. T.M.Tatarnikova, F. Bimbetov, P.Yu. Bogdanov (2021). Detection of network traffic anomalies by deep learning. *Izvestia SPbGETU LETI*, no. 4, pp. 36-41 (In Russian)
10. V. Jyothsna, V.V.R. Prasad (2011). A Review of Anomaly Based Intrusion Detection Systems. *International Journal of Computer Applications*, vol. 28, no. 7, pp. 26-35.
11. M. Gyanchandani, J.L. Rana, R.N. Yadav (2012). Taxonomy of Anomal Based Intrusion Detection System: A Review. *International Journal of Scientific and Research Publicctions,* vol., 2., issue 12, pp. 1-13.
12. W. Lee, D. Xiang (2001). Information-theoretic measures for anomaly detection. *Security and Privacy,* pp. 130-143.
13. T.M. Tatarnikova, A.M. Zhuravlev (2018). A neural network method for detecting malicious programs on the Android platform. *Software & Systems*, no. 3, pp. 543-547, DOI: 10.15827/0236-235X.031.3.543-547. (In Russian)
14. E.V. Palchevsky, O.I. Christodulo (2019). Development of a self-learning method for a pulsed neural network to protect against DDoS attacks. *Software & Systems*, vol. 32, no. 3, pp. 419-432. DOI: 10.15827 / 0236-235X.127.419-432 (In Russian)
15. E.O. Safronova, G.A. Zhuk (2019). Application of artificial neural networks for predicting DoS attacks. *Young Scientist*, no. 23, pp. 27-30. (In Russian)

Information about authors:

Tatyana M. Tatarnikova, *St. Petersburg State University of Aerospace Instrumentation, Department of Information and Communication Systems, Doctor of Technical Sciences, Professor, St. Petersburg, Russia*

Pavel Yu. Bogdanov, *St. Petersburg State University of Aerospace Instrumentation, Department of Information and Communication Systems, senior lecturer, St. Petersburg, Russia*