УДК 004.056.53
DOI 10.33764/2618-981X-2022-8-2-118-125

Обнаружение вторжений в систему Интернета вещей

Д. Н. Титов[1]*

[1] Сибирский государственный университет геосистем и технологий, г. Новосибирск, Российская Федерация
* e-mail: titov200708@mail.ru

Аннотация. Интернет вещей (IoT) – это развивающаяся технология, в которой вычислительные устройства и датчики обмениваются данными по сети для решения различных задач и предоставления услуг. Медицинское обслуживание, удаленное управление устройствами, взаимодействие между машинами и т.д. – это услуги, предоставляемые сегодня для пользователей без участия человека. Несмотря на ряд преимуществ, у этой технологии есть и недостатки, одним из которых является безопасность. Существует множество методов, используемых для защиты Интернета вещей, одним из них является система обнаружения вторжений (IDS) – это один из самых оригинальных и хорошо организованных методов, который может защитить устройства Интернета вещей от злоумышленников и с высокой точностью обнаружить их атаку. В статье рассмотрены такие виды атак как DDoS / DoS, hello flood и Sybil attack и т.д., а также различные виды подходов к IDS, такие как машинное обучение, SDN и идентификаторы на основе автоматов, которые могут быть полезны для предотвращения и обнаружения атак на устройства Интернета вещей.

Ключевые слова: Интернет вещей, система обнаружения вторжений, машинное обучение

Detection of intrusions into the Internet of things system

D. N. Titov[1]*

[1] Siberian State University of Geosystems and Technologies, Novosibirsk, Russian Federation
* e-mail: titov200708@mail.ru

Abstract. The Internet of Things (IoT) is an evolving technology in which computing devices and sensors exchange data over a network to solve various tasks and provide services. Medical care, remote control of devices, interaction between machines, etc. are services provided today for users without human intervention. Despite a number of advantages, this technology also has disadvantages, one of which is security. There are many methods used to protect the Internet of Things, one of them is the Intrusion detection System (IDS) – this is one of the most original and well-organized methods that can protect Internet of Things devices from intruders and detect their attack with high accuracy. The article discusses such types of attacks as DDoS/DoS, hello flood and Sybil attack, etc., as well as various types of approaches to IDS, such as machine learning, SDN and machine-based identifiers, which can be useful for preventing and detecting attacks on Internet of Things devices.

Keywords: Internet of Things, intrusion detection system, machine learning

Введение

Интернет вещей (IoT) – это повсеместная сеть, в которой устройства взаимодействуют без участия человека. Датчик устройства играет ключевую роль в среде Интернета вещей, поскольку данные, воспринимающиеся этим датчиком,

в дальнейшем отправляются в центральный орган для обработки. Интеллектуальные устройства, такие как, smart TV, smart mobile, smart doors и smart heater, соединяются друг с другом через Интернет, чтобы передавать информацию для обеспечения комфорта людям. На рис. 1 показана архитектура сети Интернета вещей.

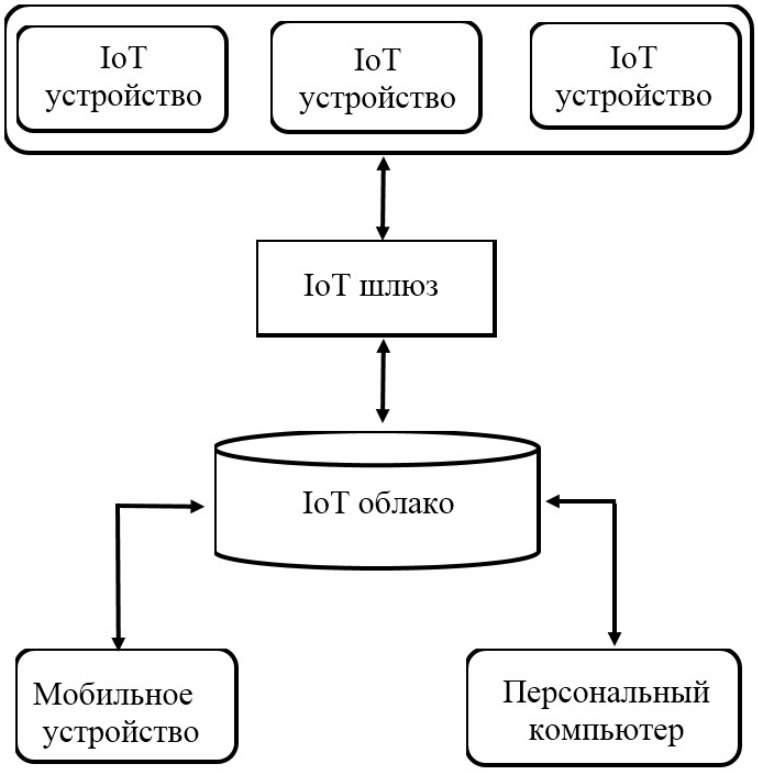

Рис. 1. Архитектура сети интернета вещей

Шлюз действует как пороговое значение между устройствами Интернета вещей и устройства управления (ноутбуки и мобильные телефоны пользователей). Из-за несовместимой архитектуры устройств среда Интернета вещей становится неоднородной. В результате созданной неоднородности эти устройства уязвимы для атак злоумышленников. Злоумышленник может получить удаленный контроль над смарт-устройствами и использовать его в своих злонамеренных целях. Как обсуждалось в [1], в 2016 году каждое устройство Интернета вещей подвергалось атаке раз в две минуты. Согласно недавнему исследованию HP, в настоящее время почти 70% интеллектуальных устройств уязвимы для угроз безопасности. Другое исследование HP показывает, что 90% устройств собирают личную информацию на этапе тестирования. Эти данные могут быть использованы в недобросовестных целях из-за взлома устройства или в результате кибератаки [2].

В реализации Интернета вещей задействованы многочисленные технологии. Например, радиочастотная идентификация (RFID), связь в ближнем поле (NFC), связь между машинами (M2M) и связь между транспортными средствами (V2V). В RFID информация передается через радиочастоту. RFID-система состоит из нескольких считывателей и метки. Данные хранятся на бирке в элек-

тронном виде. Эта система работает в режиме реального времени для мониторинга объектов. NFC также является своего рода средством связи, при котором информация передается по беспроводной сети. Небольшой объем информации передается только в том случае, если оба устройства поддерживают технологию NFC. В отличие от технологии Bluetooth, она не требует предварительного подключения. Связь M2M происходит в основном в компьютерах, встроенных процессорах, мобильных телефонах и датчиках.

Система обнаружения вторжений (IDS) используется для мониторинга сети. Она работает как сигнализация, которая только идентифицирует инциденты. Обладая множеством преимуществ, она также имеет некоторые проблемы, например, если сигнал тревоги не прослушивается должным образом, это может нанести вред системе. У нее также есть проблемы, которые могут возникнуть из-за самого IDS. Информация, которую она считывает из IP-пакета, также может быть подделана, что также является проблемой. Чтобы снизить проблемы сетевой безопасности, пользователи используют множество методов; IDS – один из них. Это помогает обнаруживать вторжения в сеть и информировать пользователя об угрозах. Раннее обнаружение атак защищает сеть от взлома.

Система обнаружения вторжений (IDS)

IDS нацелена на мониторинг сети, обнаружение скомпрометированных узлов и вторжений в сеть, а также на оповещение пользователя об обнаруженных вторжениях [3]. Она также отлично работает как для внешних, так и для внутренних атак. Эта технология постепенно развивается, чтобы смягчить последствия компьютерных преступлений. Обычно идентификаторы состоят из трех основных компонентов: Мониторинг, Анализ и обнаружение, Сигнализация.

Сетевой трафик, шаблоны и ресурсы отслеживаются с помощью модуля мониторинга. Модуль анализа и обнаружения играет важную роль в обнаружении вторжений в соответствии с определенным алгоритмом. Модуль сигнализации запускает сигналы тревоги при обнаружении вторжения. На рис. 2 изображена архитектура IDS.

Система предотвращения отслеживает многочисленные виды угроз, которые могут возникнуть в отношении данных передаваемых по сети. При мониторинге вторжений вы можете отслеживать данные и трафик. На этапе обнаружения вторжения атака обнаруживается, если она соответствует шаблонам. Затем, после идентификации атаки, в разделе ответа она выдаст уведомление, чтобы система обнаружила атаку. А затем, она используется для восстановления данных, поврежденных или уничтоженных в результате атак. Существует две категории, в которые классифицируется IDS: Сетевая система обнаружения вторжений (NIDS) и Система обнаружения вторжений на основе хоста (HIDS).

Сетевая Система Обнаружения Вторжений (NIDS) используется для обнаружения сетевых угроз путем мониторинга и анализа сетевого трафика. NIDS охватывает те места, где процент возникновения атаки больше. Обычно она размещается во всех подсетях.

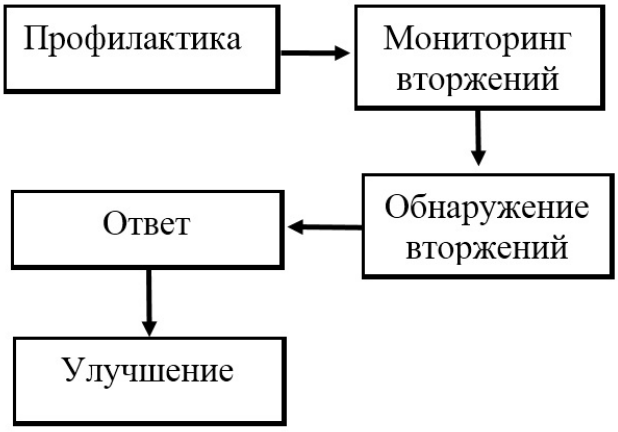

Рис. 2. Архитектура IDS

Система обнаружения вторжений на базе хоста (HIDS) обычно используется в одной системе. При подключении к Интернету она работает на всех устройствах, подключенных к сети. Она сравнивает предыдущий образ набора файлов к набору файлов всей системы. Затем предупреждает администратора, если происходит изменение.

Методы идентификации

Машинное обучение – это детище искусственного интеллекта, которое может извлекать результаты из анализируемых данных и принимать решения с минимальным человеческим взаимодействием. На рис. 3 показан обзор структуры машинного обучения.

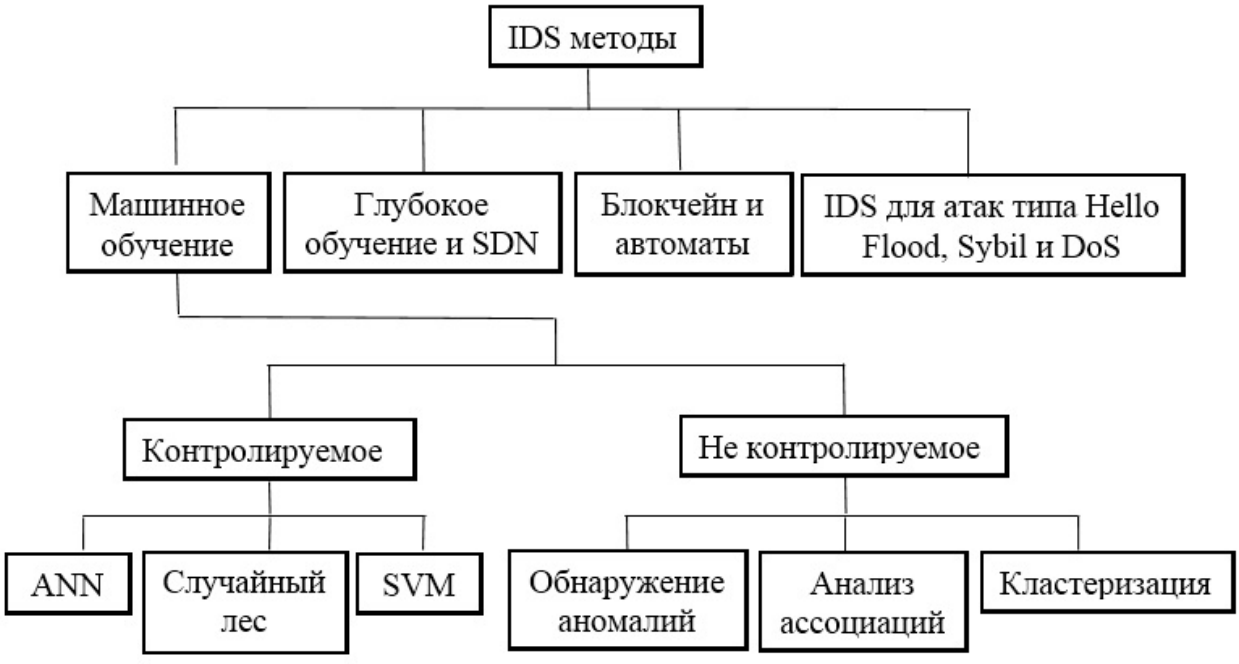

Рис. 3. Структура обучения методов IS

В алгоритмах контролируемого машинного обучения пользователи имеют предварительные знания о выходных данных для данной выборки. Основная цель контролируемого обучения – обучить машины проводить анализ трафика на основе уже имеющихся данных с достоверным результатом. Контролируемое обучение обычно происходит при классификации результатов сопоставления входных данных с меткой вывода. Некоторые хорошо известные контролируемые алгоритмы – это Случайный лес, машина на опорных векторах (SVM) и Искусственная нейронная сеть (ANN).

Случайный лес является гибким и одним из наиболее часто используемых алгоритмов из-за его простоты. Простая работа Случайного леса заключается в том, что он строит деревья решений, а затем объединяет их для получения оптимальных решений или прогнозов. Наиболее заметным преимуществом алгоритма случайного леса является то, что он используется как для регрессии, так и для классификации. Обычно производители не обращают внимания на безопасность устройств Интернета вещей. Их беспокоит только маломощное аппаратное оборудование [5]. Следовательно, устройства Интернета вещей не имеют вычислительных возможностей для выполнения задачи шифрования.

Основная концепция Машины опорных векторов (SVM) – это плоскость принятия решений. Она подобна разделителю, который разделяет членов разных классов. В этом IDS алгоритмы машинного обучения, такие как SVM, первичный классификатор Байеса, дерево решений J48 и таблица решений, используются в модели обнаружения аномалий в качестве алгоритмов контроля. Набор данных KDD99 используется для установки целей обучения и оценки. Сегодня большинство IDS предназначены либо для традиционной сетевой архитектуры Интернета вещей, либо для беспроводных сенсорных сетей (WSN). Но ни одна из них не подходит для IPV6. Известные традиционные IDS, такие как Snort и Bro, работают с системой на основе IP, но они не могут управлять гетерогенной средой. Поэтому новые компоненты должны обладать способностью справляться с таким огромным трафиком.

Неконтролируемое обучение. При обучении без контроля нам не нужно обучать модель. Она выдает результаты для непредвиденных данных на основе своего предыдущего опыта. Следовательно, она может находить всевозможные неизвестные закономерности.

Обнаружение аномалий. При обнаружении аномалий в наборе принимаемых данных обнаруживаются аномальные точки. Это полезно для выявления поддельных операций, поиска поврежденных частей оборудования или точного определения ошибок, возникших во время работы по вводу данных. Однако, когда обнаружение аномалий включено постоянно, устройство обнаружения вторжений может потреблять больше энергии. Применение модели на основе первичного классификатора Байеса обеспечивает низкие вычислительные затраты, благодаря выбору характеристик и оптимальному сокращению измерений, что позволит снизить энергозатраты.

Анализ ассоциаций. Интеллектуальный анализ ассоциаций классифицирует наборы элементов, которые обычно одновременно передаются в вашем наборе

данных. Он направлен на выработку правил, которые помогают в получении новых знаний. Правила ассоциации основаны исключительно на отношениях между элементами. Эти правила основываются на связи предсказания и следствия. Механизм анализа состоит из двух основных частей. Во-первых, поиск набора элементов в базе данных. Вторая часть заключается в выявлении последствий.

Кластеризация – это лучшая модель для анализа данных, если они содержат несколько больших двоичных объектов. Условие построения такой модели – это то, что определение как указатель данных относится к двоичному объекту. Из указателей создаются большие двоичные объекты. Эти объекты известны как кластеры, а метод, используемый в этом процессе, называется кластеризацией. Сегодня кластеризация данных рассматривается как эффективный метод для правильного выполнения категоризации данных в реалистичных группах.

Глубокое обучение и программно-определяемая сеть (SDN) – основа IDS

Глубокое обучение – это функция искусственного интеллекта, которая, как правило, заставляет компьютер принимать решения подобно человеческому мозгу. SDN делает сеть программируемой. Вместо маршрутизаторов и коммутаторов в SDN для целей управления используется централизованный контроллер. Маршрутизаторы и коммутаторы используются только в качестве устройств пересылки. Контроллер SDN имеет полое представление о сети, и благодаря этому структура сети становится легко понятной.

В [6] предлагается решение для обеспечения безопасности путем реализации нового IDS. В предлагаемой работе анализируется фаза сетевого подключения и сетевые протоколы хост-сети, а затем по каналам виртуальной сети устанавливается соединение. Но найти разницу между вредоносным трафиком и обычным трафиком – это очень сложное задание, и именно IDS на основе SDN является хорошим решением этой проблемы, и программируемая сеть – лучшее решение для контроля за трафиком в Интернете вещей.

Технология блокчейн (BC) основана на топологии P2P. Это технология распределенного реестра, которая, потенциально, может хранить данные на тысячах серверов по всему миру. Существует множество успешных реализаций технологии блокчейн, но первой из них является сеть Биткойн [4]. Устройства Интернета вещей эффективно работают благодаря распределенному, легкому и масштабируемому подходу к обеспечению безопасности и конфиденциальности. Системой, обладающей вышеупомянутыми характеристиками (распределенный, безопасный и частный характер), является технология блокчейн, которая является первой криптовалютой [7]. В [8] предложено решение, основанное на инновационном экземпляре Биткойна, устраняющем необходимость в монетах и идее доказательства ее работы (POW). Эта модель основана на многоуровневой композиции и распределении уровней для обеспечения безопасности биткойна. Сегодня оптимальным решением будет использование умного дома совместно с облачным хранилищем. Уязвимость встроенных функций, физических компонен-

тов, сетевых устройств и прикладного уровня, расположенных на разных уровнях, является проблемой для безопасности. Пользователи используют различные протоколы для взаимодействия с этими компонентами, которые могут быть подвержены атакам.

Решение против DOS-атак предложено в [9]. Архитектура системы выглядит следующим образом: датчик, анализатор пакетов, обнаружение атак, правила генерации и правила IP таблиц для вывода, которые являются правилами, созданными брандмауэром. Он также имеет модули захвата IP-адресов и захвата пакетов. Модуль IP Capture захватывает IP-адреса всех активных устройств в сети. Выходные данные IP Capture являются входными данными для захвата пакетов для обнаружения атак. Как только пакеты собраны, их функции извлекаются и загружаются в базу данных пакетов DB. Анализатор пакетов использует эти функции для определения того, поступает ли трафик с зарегистрированных сетевых устройств. Анализатор пакетов использует эти функции для определения того, поступает ли трафик с зарегистрированных сетевых устройств. Затем он обменивается информацией с модулем обнаружения атак. Модуль обнаружения атак отвечает за классификацию атаки на основе функций, предоставляемых анализатором пакетов. Наконец, запись об атаке вставляется в базу данных. Модуль правил генерации создает функцию блокировки атак на основе истории атак, хранящейся в базе данных. Этот подход позволяет обнаруживать распределенные атаки типа "Отказ в обслуживании", атаки Hello Flood и атаки Sybil.

Результаты

Устройства Интернета вещей обладают меньшими вычислительными возможностями для выполнения громоздких задач обработки. Тем не менее, безопасность устройств Интернета вещей не может быть поставлена под угрозу. Для преодоления вышеупомянутого дефекта предложено решение, основанное на алгоритмах машинного обучения. Предлагаемая работа состоит из трех модулей сбора данных, модуля обработки данных и модуля обнаружения. Случайный лес и Нейронные сети используются для обнаружения и категоризации вторжений соответственно. В [4] для защиты от DoS-атак предлагается решение, основанное на машинном обучении и подходе, основанном на правилах, для мониторинга аномального поведения сети. Подход машинного обучения помогает в обучении модели для нормальной работы сети. Эта модель может обнаружить аномалию, даже если она возникает впервые.

Заключение

Технологии Интернета вещей развиваются, но производители не уделяют серьезного внимания мерам безопасности. Они, в основном, фокусируется на устройствах с меньшим объемом вычислений и низким энергопотреблением, поэтому н развиваются подходы к обеспечению безопасности изготавливаемых устройств. Для устранения образовавшихся уязвимостей в системе безопасности

используются различные методы защиты, IDS – один из них. Был проведен отбор различных методов, реализуемые в IDS, затем собрана информация по каждому из них на основе технологии и техники применения. В статье были исследованы идентификаторы с использованием машинного обучения, глубокого обучения, блокчейна, теории автоматов и SDN.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Collen, A., et al., "Ghost-safe-guarding home IoT environments with personalised real-time risk control". in International ISCIS Security Workshop. 2018. Springer.

2. Kanuparthi, A., R. Karri, and S. Addepalli, "Hardware and embedded security in the context of internet of things". in Proceedings of the 2013 ACM workshop on Security, privacy & dependability for cyber vehicles. 2013.

3. Ganapathy, S., et al., "Intelligent feature selection and classification techniques for intrusion detection in networks: a survey". EURASIP Journal on Wireless Communications and Networking, 2013. 2013(1): p. 271.

4. Pandey, P. and A. Barve, "An Energy-Efficient Intrusion Detection System for MANET", in Data, Engineering and Applications. 2019, Springer. P. 103–117.

5. Pacheco, J. and S. Hariri, "IoT security framework for smart cyber infrastructures". in 2016 IEEE 1st International Workshops on Foundations and Applications of Self* Systems (FAS* W). 2016. IEEE.

6. Chawla, S. and G. Thamilarasu, "Security as a service: real-time intrusion detection in internet of things". in Proceedings of the Fifth Cybersecurity Symposium. 2018.

7. Nakamoto, S., "A peer-to-peer electronic cash system". Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf, 2008.

8. Dorri, A., et al., "Blockchain for IoT security and privacy: The case study of a smart home". in 2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops). 2017. IEEE.

9. Sousa, B.F.L.M., et al., "An intrusion detection system for denial of service attack detection in internet of things". in Proceedings of the Second International Conference on Internet of things, Data and Cloud Computing. 2017.