Обнаружение атак Denial-of-Sleep в беспроводных сетях кризисного управления на основе машинного обучения

В. А. Десницкий[1], И. В. Котенко[2]
Санкт-Петербургский институт информатики и автоматизации Российской академии наук (СПИИРАН)
Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО)
[1]desnitsky@comsec.spb.ru, [2]ivkote@comsec.spb.ru

***Аннотация*. В работе исследуются атаки истощения энергоресурсов, направленные на узлы оперативно разворачиваемой на местности проводной сети, организующей функции кризисного управления. Моделирование атак Denial-of-Sleep осуществляется на терминальные устройства сети на базе платформы Arduino и коммуникационных интерфейсов Digi XBee s2. Построенное на основе машинного обучения обнаружение атак Denial-of-Sleep базируется на выделении набора характерных признаков нормального и атакующего трафика, полученного в рамках экспериментального стенда моделирования. Точность обнаружения подтверждается проверкой работы предложенного механизма на контрольном трафике.**

Ключевые слова: атака типа Denial-of-Sleep; обнаружение атак; киберфизическая безопасность

I. Введение

Широкое распространение автономно работающих киберфизических устройств обуславливает их подверженность атакам типа Denial-of-Sleep, являющихся разновидностью атак истощения энергоресурсов [1]. Таким атакам подвержен широкий спектр устройств – мобильные коммуникаторы, узлы сенсорных сетей, переносные сканеры, мультимедиа-камеры и др.

Эффективность таких атак подтверждается возможностью злоумышленника путем воздействия на атакуемое устройства по беспроводным каналам связи сократить время его жизни в десятки, сотни и даже тысячи раз. Сложность обнаружения данного вида атак связана, в первую очередь, с отсутствием и сложностью встраивания средств мониторинга энергопотребления киберфизических устройств, а также сложностью дифференциации атакующих воздействий от легитимных операций [2].

Условием для осуществления атаки Denial-of-Sleep является возможность перехода атакуемого устройства в режим пониженного энергопотребления (режим сна).

Работа выполнена в СПИИРАН при поддержке Гранта Президента Российской Федерации № МК-5848.2018.9.

Воздействуя на устройство и вынуждая его реагировать на входящие запросы, нарушитель препятствует переходу устройства в режим сна, тем самым сокращая время жизни устройства, что для устройств критически важной инфраструктуры может оказаться фатальным.

В работе предложен подход к обнаружению атак Denial-of-Sleep на основе применения машинного обучения. Подход реализуется на тестовом сценарии беспроводной сети кризисного управления. При этом обучение базируется на предложенном наборе признаков нормального и аномального трафика специфичных данному сценарию.

II. Релевантные работы

Анализ и оценка показателей некоторых видов атак Denial-of-Sleep, в частности, показателей эффективности, представлены в работах [2–5].

Опубликован ряд статей, раскрывающих частные механизмы обнаружения атак Denial-of-Sleep в беспроводных сенсорных сетях [6–8]. К отличительным особенностям предложенного в настоящей работе подхода можно отнести выбранный специфичный набор частотных признаков трафика, значения которых, также как и точность процесса обнаружения зависят от бизнес-функций целевой сети.

III. Сценарий кризисного управления

Обнаружение атак Denial-of-Sleep базируется на дифференциации атакующего и нормального трафика сети. Структура и интенсивность трафика во многом определяется спецификой конкретной сети и особенностями коммуникации между ее узлами. Поэтому возникает необходимость построения типового сценария, который, во-первых, мог бы использоваться как основа и источник исходных данных для формирования средств обнаружения и, во-вторых, для обоснования корректности полученных в работе решений.

Моделируемый сценарий представляет беспроводную оперативно разворачиваемую на местности сеть,

организующую функции кризисного управления на базе модулей Arduino и беспроводных интерфейсов Digi XBee s2. Сеть предоставляет коммуникационную среду обмена данными между устройствами служб реагирования. Коммуникационные сервисы включают передачу показаний сенсоров, служебных команд и различных мультимедиа данных.

Типовой узел сети схематично представлен на рис. 1. Узел включает модуль XBee, способный работать в режиме цикличного сна, микроконтроллер Arduino, поддерживающий энергосберегающий режим *Power-down Mode*, а также цифровые или аналоговые сенсоры и элементы пользовательского интерфейса.

Рис. 1. Терминальное устройство сети

Анализ возможных операций между узлами сети показывает, что атака Denial-of-Sleep может быть осуществлена путем эксплуатации трех следующих групп коммуникационных функций узлов сети: *ping*, которая проверяет доступность некоторого узла сети; *sendHelloData* – отправка широковещательного инициирующего сообщения; *get*-функции – запрашивающие показания сенсоров или метаданные узлов сети; *send*-функции – отправляющие ответ на get-функции и функция *sendHelloData*. В рамках данного сценария скомпрометированный нарушителем или ложный узел XBee [9] осуществляет атаку Denial-of-Sleep путем эксплуатации приведенных функций. Чтобы сделать атаку более скрытной нарушитель может комбинировать данные функции, имитируя легитимный трафик.

IV. Обнаружение Denial-of-Sleep атак

Обнаружение Denial-of-Sleep атак базируется на классификации поступающего на узел беспроводного трафика. В процессе классификации учитываются следующие признаки (характеристики) трафика:

F – частота запросов определенного вида к узлу за заданный период времени *t*;

C – общее число запросов определенного вида за все время измерения;

D – количество необоснованно дефрагментированных пакетов, полученных за определенный промежуток времени;

R – распределение поступающих запросов за определенный период *t* по адресам источников пакетов в процентном выражении и в абсолютном измерении.

В совокупности данные характеристики с заданными параметрами и частотными значениями позволяют характеризовать конкретную цепочку беспроводных пакетов как атакующую или нормальную. При этом точные числовые значения определяются спецификой и бизнес-логикой конкретной беспроводной сети.

Первоначально значения характеристик заданы эвристически, исходя из некоторого типового сценария работы сети. Примеры правил с граничными значениями характеристик для классификации нормального и атакующего трафика приведены в таблице. При этом обучение на предварительно классифицированном трафике позволяет уточнить эти значения.

ТАБЛИЦА I Примеры граничных значений ха-рактеристик для классификации трафика

Правила	Описание
$F_{SendHelloData,Mission}(node_0) <= 1$	отправка широковещательного инициирующего сообщения при подключении узла $node_0$ к сети может осуществляться не чаще 1-го раза в течение миссии
$F_{ping}(node_0,node_1,1\ m) <= 10$	проверка доступности узла $node_1$ не должна включать более 10-ти запросов в минуту
$F_{ping}(node_0,node_1,1\ h) <= 50$	проверка доступности узла $node_1$ не должна включать более 50 запросов в час
$D_{sendSensorReadings}(node_0,node_1, 3\ par, 5\ s) <= 5\%$	ответ на запрос показаний более чем 3-х сенсоров должен осуществляться в рамках одного пакета данных
$F_{send}(node_0,node_1,1\ h) <= 1$	число ошибочных ответов на запросы данных не должно превышать 1 шт. за 1 час

Отметим, что в общем случае каждая характеристика по отдельности не позволяет установить, является ли некоторый образец трафика атакующим или нет, тогда как полученная посредством обучения область в многомерном пространстве характеристик и принадлежность трафика данной области позволит определить его в качестве атакующего. Обнаружение атаки Denial-of-Sleep включает два программных компонента, располагающихся на микроконтроллере Arduino узла сети: (1) компонент сбора, предобработки и накопления данных о поступающих пакетах; (2) компонент классификации поступающего трафика на основе обученного классификатора.

В качестве метода для проведения обучения выбран метод *k* ближайших соседей. Обучающая и тестовые выборки были сформированы эмпирически в соотношении 75% и 25%, соответственно, путем моделирования нормального и атакующего трафика в рамках разработанного программно-аппаратного прототипа беспроводной ZigBee-сети.

V. Реализация и дискуссия

Алгоритм классификации данных трафика разработан на языке Python 3 с использованием библиотеки scikit-learn. На рис. 2 показан фрагмент интерфейса построенного программного прототипа средства моделирования Denial-of-Sleep атак. В частности, показан экземпляр атакующего пакета на основе инициирующей функции *SendHelloData*.

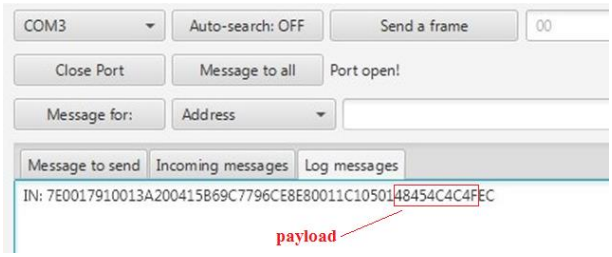

Рис. 2. Пример атакующей команды на XBee-модуль

Полученные на обучающей выборке значения частотных характеристик трафика позволили корректно классифицировать атаки Denial-of-Sleep на тестовой выборке с отсутствием ошибок 1 и 2 рода в 78% случаев. Помимо выбора обучающего метода на точность построенного классификатора влияют также качество исходных данных нормального и атакующего трафика и заданная система признаков.

Отметим, что построенный в работе классификатор и полученные экспериментальные данные имеют относительный характер в виду того, что механизм обнаружения атак Denial-of-Sleep должен адаптироваться с учетом особенностей и сценариев работы конкретной сети. При изменении регламентов работы сети должно производиться переобучение с учетом измененных режимов работы, типов и структуры пакетов данных, различных их статистических характеристик и образцов трафика. К полученным в работе результатам можно отнести подтверждение применимости и работоспособности предложенного подхода к выявлению атак Denial-of-Sleep в беспроводных сетях на основе машинного обучения.

Предложенный классификатор может использоваться для анализа трафика беспроводных сетей индустриального уровня с учетом сопутствующих технологических ограничений беспроводных протоколов RFID, IR, Wi-Fi и др. При обнаружении атакующего трафика должны активироваться средства противодействия, в том числе уведомления легитимных участников информационного обмена и возможная приостановка или корректировка функционирования критически важных устройств во избежание их аварийного завершения.

В общем случае функции сбора, предобработки и проверки поступающего трафика на уже обученном классификаторе ложатся на микроконтроллер каждого конкретного узла беспроводной сети, имеющего определенные вычислительные ограничения, а также ограничения энергопотребления. Это обуславливает дополнительные нефункциональные требования к компонентам защиты [10], в том числе к компонентам фильтрации данных и к вычислительной сложности алгоритмов классификации.

VI. Заключение

В работе представлен предложенный авторами подход к обнаружению атак Denial-of-Sleep на узлы беспроводной самоорганизующейся ZigBee-сети на примере мобильной сети кризисного управления. Для выявления данного вида атак применен метод *k* ближайших соседей, позволяющий на основе заданного набора признаков классифицировать трафик, полученный на прототипе сети в рамках разработанного сценария.

В качестве будущих исследований планируется повышение точности обнаружения за счет сравнения и использования альтернативных классификаторов, а также учета в процессе обучения правил, основанных не только на частотных характеристиках, но также и на особенностях структуры беспроводных пакетов.

Список литературы

[1] Hsueh C.T., Wen C.Y., Ouyang Y.C. A Secure Scheme Against Power Exhausting Attacks in Hierarchical Wireless Sensor Networks // IEEE Sensors Journal. 2015. Vol. 15. № 6. P. 3590-3602.

[2] Desnitsky V., Kotenko I. Modeling and Analysis of Energy Resource Exhaustion Attacks in IoT // Intelligent Distributed Computing XI. Studies in Computational Intelligence. Springer-Verlag. 2017. Vol. 737. P. 263-270.

[3] Uher J., Mennecke R.G., Farroha B.S. Denial of Sleep attacks in Bluetooth Low Energy wireless sensor networks // 2016 IEEE Military Communications Conference (MILCOM). Baltimore. MD. 2016. P. 1231-1236.

[4] Capossele A.T., Cervo V., Petrioli C., Spenza D. Counteracting Denial-of-Sleep Attacks in Wake-Up-Radio-Based Sensing Systems // 2016 13th Annual IEEE International Conference on Sensing. Communication, and Networking (SECON). London. 2016, P. 1-9.

[5] Brownfield M., Gupta Y., Davis N. Wireless sensor network denial of sleep attack // Proceedings from the Sixth Annual IEEE SMC Information Assurance Workshop. West Point. NY. USA. 2005. P. 356-364.

[6] Manju V.C., Senthil Lekha S.L., Sasi Kumar M. Mechanisms for detecting and preventing denial of sleep attacks on wireless sensor networks // 2013 IEEE Conference on Information & Communication Technologies. JeJu Island. 2013. P. 74-77.

[7] Chen C., Hui L., Pei Q., Ning L., Qingquan P. An Effective Scheme for Defending Denial-of-Sleep Attack in Wireless Sensor Networks // 2009 Fifth International Conference on Information Assurance and Security. Xi'an. 2009. P. 446-449.

[8] Dhunna G.S., Al-Anbagi I. A Low Power Cyber-Attack Detection and Isolation Mechanism for Wireless Sensor Network // 2017 IEEE 86th Vehicular Technology Conference (VTC-Fall). Toronto. ON. 2017. P. 1-5.

[9] Десницкий В.А., Чечулин А.А., Котенко И.В., Левшун Д.С., Коломеец М.В. Комбинированная методика проектирования защищенных встроенных устройств на примере системы охраны периметра // Труды СПИИРАН. 2016. Вып. 5(48). С. 5-31.

[10] Desnitsky V., Kotenko I. Expert Knowledge based Design and Verification of Secure Systems with Embedded Devices // Lecture Notes in Computer Science (LNCS). Vol. 8708. Springer-Verlag. 2014. P. 194-210.