УДК 004.056.5 Научная статья

https://doi.org/10.32603/2071-8985-2022-15-5/6-32-40

# Обнаружение атак типа Denial-of-Sleep в беспроводных сенсорных сетях на основе методов машинного обучения

**В. А. Десницкий**

Санкт-Петербургский Федеральный исследовательский центр
Российской академии наук, Санкт-Петербург, Россия
desnitsky@comsec.spb.ru

**Аннотация.** Рассматриваются вопросы обнаружения атак типа Denial-of-Sleep в беспроводных сенсорных сетях. Такие атаки применимы к устройствам интернета вещей, функционирующим автономно и переключающимся между двумя режимами работы, а именно общим и энергоэффективным (спящим) режимами, в зависимости от бизнес-правил устройств. Будучи в целом достаточно эффективными, такие атаки довольно скрытны и могут значительно сократить и даже полностью разрядить время автономной работы устройства, тем самым приводя его в отключенное состояние. Анализируются исходные данные и применяются методы искусственного интеллекта для обнаружения атак типа Denial-of-Sleep. Модель обнаружения строится с использованием конкретных методов машинного обучения. Модель проверена на реальных данных, собранных на испытательном стенде с беспроводными модулями ZigBee, представляющими как обычные беспроводные сенсорные узлы, так и атакующие. Показатели качества обнаружения подтверждают эффективность и применимость предложенных методов обнаружения на практике.

**Ключевые слова:** беспроводная сенсорная сеть, безопасность, детектирование атак

**Для цитирования:** Десницкий В. А. Обнаружение атак типа Denial-of-Sleep в беспроводных сенсорных сетях на основе методов машинного обучения // Изв. СПбГЭТУ «ЛЭТИ». 2022. Т. 15, № 5/6. С. 32–40. doi: 10.32603/2071-8985-2022-15-5-32-40.

Original article

# Machine learning-based detection of Denial-of-Sleep attacks in wireless sensor networks

**V. A. Desnitsky**✉

Petersburg Federal Research Center of the Russian Academy of Sciences,
Saint Petersburg, Russia
✉ desnitsky@comsec.spb.ru

**Abstract.** The paper comprises detection of Denial-of-Sleep attacks in wireless sensor networks. Such attacks are applicable to IoT devices that operate autonomously and switch between two modes of operation, namely general and power-efficient (sleep) modes, depending on the business rules of the devices. Although being quite effective in general, such attacks are quite stealthy and can significantly reduce and even completely drain the battery life of the device, thereby bringing it into a disabled state. The paper analyzes the source data and applies artificial intelligence methods to detect Denial-of-Sleep attacks. The detection model is built using specific machine learning techniques. The model is validated on real data collected on a test bench with ZigBee wireless modules representing both benign wireless sensor nodes and attackers. The detection quality indicators confirm the effectiveness and applicability of the proposed detection methods in practice.

**Keywords:** wireless sensor network, security, attack detection

**For citation:** Desnitsky V. A. Machine learning-based detection of Denial-of-Sleep attacks in wireless sensor networks // LETI Transactions on Electrical Engineering & Computer Science. 2022. Vol. 15, no. 5/6. P. 32–40. doi: 10.32603/2071-8985-2022-15-5/6-32-40.

**Введение.** В настоящее время все большее распространение получают беспроводные сенсорные сети (БСС) в различных областях приложения – для мониторинга физических характеристик окружающей среды, помещений, технических устройств и объектов, внутри транспортных средств и систем соединенных пилотируемых и беспилотных транспортных средств, для удаленного контроля жизненно важных характеристик здоровья человека, животных и пр. Ввиду динамического, часто спонтанного характера функционирования таких систем изменения местоположения узлов беспроводной сети и режимов коммуникации, зачастую узлы таких сетей функционируют от автономных источников энергоснабжения. В отличие от других видов воздействий прямая или опосредованная атака на батарею устройства, во-первых, трудно обнаружима, а во-вторых, может быть крайне эффективна. Сложность обнаружения таких атак связана с тем, что расход заряда зачастую нелинейный, многофакторный и слабо предсказуемый, со спецификой такой атаки, а также с нехваткой комбинированных средств мониторинга, объединяющих анализ расхода заряда и несанкционированных действий пользователей и поведения других устройств.

В зависимости от специфики целевого устройства и, в частности, от того, насколько сильно процесс энергопотребления оптимизирован разработчиками такого устройства, отмена или препятствование атакующего таким оптимизациям позволит до той или иной степени повысить расход батареи. В ряде сценариев выполнение Denial-of-Sleep-атаки может привести к необходимости более раннего технического обслуживания автономно функционирующего узла БСС, что может быть сопряжено со значительными финансовыми потерями. Кроме того, до тех пор, пока такое устройство не будет должным образом обслужено персоналом, оно, вероятно, будет выключено и не сможет обеспечивать свои целевые функции. В других сценариях, например в случае дрона, выполняющего полет, последствием Denial-of-Sleep-атаки может оказаться крушение дрона, его потеря или угон злоумышленником [1]. Все это определяет необходимость и практическую важность разработки средств детектирования Denial-of-Sleep-атак с высокими значениями показателей качества детектирования. К важнейшим показателям можно отнести точность и полноту, а также f1-меру, интегрально оценивающую качество детектирования. Разработать программные средства детектирования Denial-of-Sleep-атак целесообразно с максимизацией указанных показателей целесообразно в условиях различных частотно-временных характеристик Denial-of-Sleep-атаки и эффективности различных реализаций атаки.

Сложность обнаружения Denial-of-Sleep-атак заключается в том, что злоумышленник маскирует сообщения под сообщения других законных узлов. Более того, в общем случае внутренняя структура таких атакующих сообщений полностью такая же, как и у доброкачественных, поэтому единственная возможность их отлова заключается не в работе с отдельными атакующими сообщениями, а в выявлении последовательностей таких сообщений, составляющих атаку. Таким образом, основной научный вклад настоящих исследований включает подход, основанный на машинном обучении, для обнаружения атак типа Denial-of-Sleep с достаточно высокими значениями показателей качества детектирования. Исходные данные были получены в виде логов, извлеченных из сетевого трафика, как для нормальной работы сети, так и с пятью вариациями Denial-of-Sleep-атаки. Тестирование на независимых данных подтвердило достаточно высокое качество обнаружения построенного решения. Возможные усовершенствования подхода и реализованные модели раскрываются как будущие направления исследования. Элементы новизны полученных результатов выражаются в специализированном, подстроенном под особенности атак данного вида, интеллектуальном процессе анализа данных, ориентированном на доступные для такого анализа характеристики атак.

**Анализ работ в предметной области исследования.** В то время как проблематика анализа и моделирования Denial-of-Sleep-атак в беспроводных сенсорных сетях представлена в опубликованных работах довольно широко (например, [2]–[5]), вопросы детектирования таких атак служат предметом исследований в последние несколько лет.

В [6] внимание уделяется основанным на SYN flooding атакам типа «отказ в обслуживании» в беспроводных сенсорных сетях и их детектированию. При этом разработанное авторами средство детектирования ориентировано на применение в БСС в условиях критичности энергоресурсов, и оно, как утверждается в статье, не нарушает принципов периодического перехода узлов в режим сна. Данная работа позволяет под-

твердить необходимость средств детектирования различных видов атак в БСС, которые бы предполагали эффективное использование ресурсов и не имели бы в качестве своего побочного эффекта повышение энергозатрат. Необходимость достижения энергоэффективности средств обнаружения атак типов Denial-of-Sleep, forgery, replay и других в БСС также обосновывается в [7].

Опубликовано несколько работ по обнаружению Denial-of-Sleep-атак в контексте частных областей приложения БСС. В [8] предложен способ детектирования атак коллизии, атак типа Denial-of-Sleep и selfish-атак, связанных с эксплуатацией нарушителем процесса энергопотребления на MAC-уровне сетевого взаимодействия. В [7] представлен механизм кибербезопасности с низким энергопотреблением для приложений мониторинга интеллектуальных сетей на основе БСС для решения задач в области «умного города» – удаленный мониторинг, диагностика неисправностей оборудования, беспроводная измерительная инфраструктура, управление энергопотреблением в жилых помещениях и т. п.

В [2] предложено использовать подход на основе метафоры иммунной системы человека для детектирования некоторых видов Denial-of-Sleep в БСС с помощью мониторинга соседних узлов и коллаборативного выявления нарушителя. В [9] предложен подход к детектированию Denial-of-Sleep-атак в БСС на основе вероятностных поглощающих цепей Маркова. При этом такое детектирование основывается на оценке ожидаемого времени отключения сенсорной сети при нормальном сценарии. Факт обнаружения атаки выводится по факту отключения узла на основе сравнения его времени жизни и ожидаемого времени жизни в условиях его нормального функционирования. В [10] исследуется подход к обнаружению Denial-of-Sleep-атак с использованием метода опорных векторов и средства имитационного моделирования OPNET, который использовался для генерации исходных данных.

К отличительным особенностям настоящих исследований можно отнести ориентированность построенной модели детектирования Denial-of-Sleep-атак на возможность обнаружения таких атак на ранних стадиях их осуществления. Основываясь на текущих коммуникационных ресурсах, оказывается возможным выявить Denial-of-Sleep-атаку с высокой точностью еще до момента полного ее выполнения. Тем самым становится выполнимой минимизация негативных последствий Denial-of-Sleep-атаки как путем возможного предотвращения ее успешного завершения, так и в результате снижения инфраструктурного и финансового ущерба от нее. Кроме того, в рамках экспериментальной части на базе построенного программно-аппаратного стенда проведен перебор ряда моделей машинного обучения с учителем и определены средства, позволяющие детектировать атаки с наилучшим качеством в условиях ограниченности исходных данных.

**Детектирование и эксперименты.** Атаки типа Denial-of-Sleep, а также нормальное функционирование устройств моделировались на программно-аппаратном стенде, включающем 3 узла сети. В каждый узел входят микроконтроллер Arduino Uno, беспроводной коммуникационный интерфейс Digi XBee серии 2, а также связующие электронные компоненты. На рис. 1 приведена общая схема использованных процессов детектирования атак типа Denial-of-Sleep в БСС, состоящая из следующих семи основных шагов.

1. Анализ имеющихся логов, включающих записи нормального функционирования автономно работающего узла сети и узла, находящегося под различными вариациями атаки типа Denial-of-Sleep.

2. Формирование признакового пространства и извлечение конкретных значений признаков атакующих воздействий. Выделение обучающих и тестовых выборок.

3. Формирование нескольких наборов данных – датасетов и контроль их сбалансированности. Используется двуклассовая классификация на предмет проверки наличия или отсутствия атак типа Denial-of-Sleep с использованием всех исходных данных. Также применяется классификация для каждого из пяти рассматриваемых видов атакующих, отличающихся друг от друга по степени эффективности атаки и ее скрытности. Таким образом формируются 6 датасетов.

4. Формирование классификаторов на основе ряда методов машинного обучения, а именно метода k-ближайших соседей, метода опорных векторов, логистической регрессии, AdaBoost-классификатора, наивного байесовского классификатора [11].

5. Обучение классификаторов на обучающих выборках имеющихся шести наборов данных. В качестве значений гиперпараметров методов обучения заданы значения по умолчанию. Тестирование классификаторов, вычисление показателей качества детектирования атак.


*Рис. 1.* Стадии исследования процессов детектирования атак типа Denial-of-Sleep
*Fig. 1.* Research stages of Denial-of-Sleep attack detection process

6. Выбор наилучших методов классификации для каждого набора данных при помощи сравнения значений показателей качества детектирования.

7. Интегральная классификация и оценка на суммарном объеме данных, учитывающая атакующие воздействия всех пяти разновидностей.

Итак, были проанализированы имеющиеся логи, включающие записи нормального функционирования автономно работающего узла сети и узла, находящегося под пятью различными вариациями атаки типа Denial-of-Sleep. Продолжительность записи логов для каждой из атак и логов нормального функционирования составляет ~10 мин с разным количеством сообщений в каждом из логов. Для логов нормального функционирования число сообщений варьирует от 115 до 826 штук в зависимости от конкретных значений 3 установленных параметров моделирования. Для логов, описывающих смешанный трафик, данное значение варьирует от 96 до 1980 сообщений. Метки времени для каждой записи были нормализованы относительно нулевого момента времени.

Для детектирования атак с использованием интеллектуальных методов было выделено признаковое пространство, состоящее из $N = 50$ признаков. Каждая конкретная запись данных (семпл) представляет собой цепочку временных меток, отражающих время прихода очередных 50 сообщений, последовательно поступивших на узел-жертву. Выборки разбивались на обучающие и тестовые в соотношении 0.75 к 0.25 соответственно. В качестве разметки использованы метки двух классов, 0 – для нормального трафика, 1 – для трафика, содержащего атакующие сообщения.

Фрагмент датасета, построенного для смешенного трафика для простой Denial-of-Sleep-атаки, приведен на рис. 2. Для универсальности и удобства использования названия признаков, указанные в верхней строке, условно обозначены целыми неотрицательными числами. В частности, на рисунке видно, что первые 8 семплов были получены простым разбиением входной последовательности меток времени на $N$ векторов. Также можно увидеть, что начиная с образца данных под номером 8 временные метки идут в следующем порядке.

Для разработки интеллектуальных методов детектирования Denial-of-Sleep-атак были использованы программные реализации методов машинного обучения из библиотеки Scikit-learn. Использованы следующие классы: KNeighborsClassifier, SVC, LogisticRegression, AdaBoost, GaussianNB. Их выбор обусловлен тем, что они достаточно хорошо зарекомендовали себя в качестве простых и перспективных средств решения

********** DATASET EXTRACTED AND MERGED FROM THE TRAFFIC:

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0.0 | 349.0 | 883.0 | 1259.0 | 1757.0 | 7076.0 | 7418.0 | 7947.0 | 8308.0 | 8838.0 | 9198.0 |
| 1 | 66186.0 | 66715.0 | 67075.0 | 67416.0 | 67929.0 | 68273.0 | 74062.0 | 74407.0 | 74906.0 | 75278.0 | 75764.0 |
| 2 | 134964.0 | 135313.0 | 135826.0 | 141687.0 | 142032.0 | 142411.0 | 142953.0 | 143311.0 | 148692.0 | 149052.0 | 149397.0 |
| 3 | 206896.0 | 207257.0 | 207771.0 | 208146.0 | 213900.0 | 214244.0 | 214760.0 | 215116.0 | 215477.0 | 216005.0 | 221325.0 |
| 4 | 276112.0 | 276472.0 | 276971.0 | 282308.0 | 282837.0 | 283183.0 | 283680.0 | 284037.0 | 289357.0 | 290061.0 | 290418.0 |
| 5 | 343845.0 | 344191.0 | 349263.0 | 349791.0 | 350137.0 | 350635.0 | 350997.0 | 351350.0 | 351884.0 | 356985.0 | 357342.0 |
| 6 | 410773.0 | 416139.0 | 416483.0 | 416999.0 | 417355.0 | 422895.0 | 423256.0 | 423798.0 | 424158.0 | 429679.0 | 430023.0 |
| 7 | 482112.0 | 482455.0 | 482984.0 | 488336.0 | 488868.0 | 489225.0 | 489757.0 | 490117.0 | 490583.0 | 495982.0 | 496338.0 |
| 8 | 0.0 | 1371.0 | 2895.0 | 4256.0 | 5803.0 | 7173.0 | 14023.0 | 15393.0 | 16892.0 | 18263.0 | 25236.0 |
| 9 | 121835.0 | 123193.0 | 124828.0 | 126186.0 | 133017.0 | 134388.0 | 135889.0 | 137246.0 | 138804.0 | 145874.0 | 147228.0 |
| 10 | 255887.0 | 258225.0 | 258831.0 | 260207.0 | 267134.0 | 268662.0 | 270017.0 | 271377.0 | 272886.0 | 274243.0 | 281157.0 |
| 11 | 377272.0 | 378892.0 | 380233.0 | 387143.0 | 388749.0 | 390111.0 | 391608.0 | 398378.0 | 399903.0 | 401262.0 | 402836.0 |
| 12 | 0.0 | 357.0 | 858.0 | 1217.0 | 1728.0 | 2075.0 | 2432.0 | 7925.0 | 8280.0 | 8813.0 | 9171.0 |
| 13 | 36830.0 | 37173.0 | 37672.0 | 38017.0 | 38373.0 | 43320.0 | 44410.0 | 44926.0 | 45287.0 | 45800.0 | 46159.0 |
| 14 | 72274.0 | 72789.0 | 73147.0 | 73692.0 | 74035.0 | 74380.0 | 80186.0 | 80695.0 | 81040.0 | 81400.0 | 81899.0 |
| 15 | 108964.0 | 109310.0 | 109837.0 | 114927.0 | 115284.0 | 115795.0 | 116141.0 | 116643.0 | 117004.0 | 117355.0 | 117889.0 |

*Рис. 2.* Фрагмент датасета, построенного для смешанного трафика для простой Denial-of-Sleep-атаки
*Fig. 2.* A fragment of a dataset constructed for mixed traffic for simple Denial-of-Sleep attack

задач классификации в различных областях приложения. При этом их разнообразие и отличающиеся принципы, на основе которых они построены, позволяют рассчитывать на нахождение среди них достаточно эффективных, которые способны выдать приемлемые значения показателей качества классификации.

Для каждой из 5 разновидностей Denial-of-Sleep-атаки указанные методы машинного обучения были запущены на обучающих выборках. При проверке построенных классификаторов на тестовых выборках были посчитаны показатели правильности, точности, полноты и f1-меры. В табл. 1–5 приведены значения этих показателей для каждой разновидности атаки. Для показателей точности, полноты и f1-меры значения приведены поклассово [*значение для нормы*, *значение для атаки*]. Значения показателей приведены в формате до 2 цифр после запятой. В рамках проведенных экспериментов оптимизация включала выяснение, перебор и сравнения на независимых тестовых данных наилучших значений показателей качества детектирования для каждой разновидности атаки.

Кроме того, была проведена интегральная классификация в целом – выполнена на объединенном датасете. Результаты итоговой классификации приведены в табл. 6.

*Табл. 1.* Показатели качества детектирования простой Denial-of-Sleep-атаки
*Tab. 1.* Quality indicators of detection of Simple Denial-of-Sleep attacks

| Метод машинного обучения | Правильность | Точность | Полнота | f1-мера |
|---|---|---|---|---|
| KNeighborsClassifier | 0.96 | [0.89, 0.98] | [0.89, 0.98] | [0.89, 0.98] |
| SVC | 0.89 | [1.0, 0.88] | [0.33, 1.0] | [0.5, 0.93] |
| LogisticRegression | 0.84 | [0.5,0.91] | [0.56, 0.89] | [0.53, 0.9] |
| AdaBoostClassifier | **0.98** | [**1.0**, **0.98**] | [**0.89**, **1.0**] | [**0.94**, **0.99**] |
| GaussianNB | 0.85 | [0.56, 0.91] | [0.56, 0.91] | [0.56, 0.91] |

*Табл. 2.* Показатели качества детектирования рандомизированной Denial-of-Sleep-атаки
*Tab. 2.* Quality indicators of Randomized Denial-of-Sleep attack detection

| Метод машинного обучения | Правильность | Precision | Полнота | f1-мера |
|---|---|---|---|---|
| KNeighborsClassifier | 0.92 | [0.78, 0.96] | [0.78, 0.96] | [0.78, 0.96] |
| SVC | 0.9 | [1.0, 0.9] | [0.44, 1.0] | [0.62, 0.95] |
| LogisticRegression | 0.78 | [0.38, 0.9] | [0.56, 0.82] | [0.45, 0.86] |
| AdaBoostClassifier | **1.0** | **[1.0, 1.0]** | **[1.0, 1.0]** | **[1.0, 1.0]** |
| GaussianNB | 0.85 | [0.56, 0.91] | [0.56, 0.91] | [0.56, 0.91] |

*Табл. 3.* Показатели качества детектирования усиленной Denial-of-Sleep-атаки (вариант 1)
*Tab. 3.* Quality indicators for detecting Smart Denial-of-Sleep attack (option 1)

| Метод машинного обучения | Правильность | Точность | Полнота | f1-мера |
|---|---|---|---|---|
| KNeighborsClassifier | 0.77 | [0.73, 0.78] | [0.53, 0.89] | [0.62, 0.83] |
| SVC | 0.65 | [0.50, 0.76] | [0.60, 0.68] | [0.55, 0.72] |
| LogisticRegression | 0.79 | [0.88, 0.77] | [0.47, 0.96] | [0.61, 0.86] |
| AdaBoostClassifier | **0.93** | **[0.93, 0.93]** | **[0.87, 0.96]** | **[0.90, 0.95]** |
| GaussianNB | 0.63 | [0.47, 0.73] | [0.53, 0.68] | [0.5, 0.7] |

*Табл. 4.* Показатели качества детектирования усиленной Denial-of-Sleep-атаки (вариант 2)
*Tab. 4.* Quality indicators for detecting Smart Denial-of-Sleep attack (option 2)

| Метод машинного обучения | Правильность | Точность | Полнота | f1-мера |
|---|---|---|---|---|
| KNeighborsClassifier | 0.87 | [1.0, 0.84] | [0.58, 1.00] | [0.74, 0.92] |
| SVC | 0.77 | [0.80, 0.76] | [0.33, 0.96] | [0.47, 0.85] |
| LogisticRegression | 0.79 | [0.83, 0.79] | [0.42, 0.96] | [0.56, 0.87] |
| AdaBoostClassifier | **0.97** | **[0.92, 1.0]** | **[1.00, 0.96]** | **[0.96, 0.98]** |
| GaussianNB | 0.79 | [0.75, 0.81] | [0.5, 0.93] | [0.6, 0.86] |

*Табл. 5.* Показатели качества детектирования усиленной Denial-of-Sleep-атаки (вариант 3)
*Tab. 5.* Quality indicators for detecting Smart Denial-of-Sleep attack (option 3)

| Метод машинного обучения | Правильность | Точность | Полнота | f1-мера |
|---|---|---|---|---|
| KNeighborsClassifier | 0.74 | [0.79, 0.67] | [0.79, 0.67] | [0.79, 0.67] |
| SVC | 0.61 | [0.62, 0.5] | [0.93, 0.11] | [0.74, 0.18] |
| LogisticRegression | 0.39 | [0.5, 0.31] | [0.36, 0.44] | [0.42, 0.36] |
| AdaBoostClassifier | **1.0** | **[1.0, 1.0]** | **[1.0, 1.0]** | **[1.0, 1.0]** |
| GaussianNB | 0.61 | [0.63, 0.50] | [0.86, 0.22] | [0.73, 0.31] |

*Табл. 6.* Показатели качества детектирования Denial-of-Sleep-атак (интегральный классификатор)
*Tab. 6.* Quality indicators for detecting Smart Denial-of-Sleep attacks (integral classifier)

| Метод машинного обучения | Правильность | Точность | Полнота | f1-мера |
|---|---|---|---|---|
| KNeighborsClassifier | 0.91 | [0.2, 0.93] | [0.08, 0.97] | [0.12, 0.95] |
| SVC | 0.91 | [0.0, 0.93] | [0.0, 0.99] | [0.0, 0.96] |
| LogisticRegression | 0.92 | [0.4, 0.94] | [0.17, 0.98] | [0.24, 0.96] |
| AdaBoostClassifier | **0.97** | **[0.89, 0.97]** | **[0.67, 0.99]** | **[0.76, 0.98]** |
| GaussianNB | 0.87 | [0.31, 0.97] | [0.67, 0.88] | [0.42, 0.92] |

По всем 5 разновидностям атак и их объединению среди использованных методов обучения метод AdaBoostClassifier был определен в качестве наилучшего. В табл. 7 приведены итоговые усредненные по классам средневзвешенные значения показателя f1-меры для оценки качества детектирования, и этот показатель целесообразно рассматривать в качестве целевого.

*Табл. 7.* Средневзвешенные значения показателя f1-меры для AdaBoostClassifier
*Tab. 7.* AdaBoostClassifier f1-measure weighted averages

| Вариант эксперимента | Средневзвешенная f1-мера |
|---|---|
| Простой вариант атаки типа Denial-of-Sleep | 0.98 |
| Рандомизированная атака типа Denial-of-Sleep | 1.00 |
| Усиленная атака типа Denial-of-Sleep, вариант 1 | 0.98 |
| Усиленная атака типа Denial-of-Sleep, вариант 2 | 0.95 |
| Усиленная атака типа Denial-of-Sleep, вариант 3 | 1.00 |
| Интегральная классификация | 0.97 |

**Анализ результатов.** В качестве анализа результатов, полученных экспериментально, отметим, что итоговые значения качества детектирования представляются достаточно высокими – для всех 5 разновидностей Denial-of-Sleep-атаки и случая интегральной классификации средневзвешенные значения f1-меры превышают 0.95. При этом полученные данные в текущем их виде не позволяют сделать однозначные выводы о зависимостях между качеством детектирования атаки и степенью ее скрытности.

Несмотря на достаточно высокие значения вычисленных показателей, в качестве возможных путей дальнейшего повышения качества детектирования Denial-of-Sleep-атак имеет смысл применять следующее. В качестве базовых способов целесообразно расширить перечень методов классификации, а также применить методы автоматического перебора гиперпараметров и тестирования качества на них с использованием механизма GridSearch [11].

Кроме того, возможно воспроизведение процесса обучения на расширенных наборах исходных данных. В частности, для повышения сбалансированности данных между классами, которая особенно важна для некоторых методов машинного обучения, можно применять семплирование. Оно может быть основано на частичном смещении вектора признаков ближе к началу вектора на $k$ штук с заполнением оставшихся в конце вектора $k$ признаков значениями из начала следующего по времени семпла. При таком семплинге первый и последний векторы будут отбрасываться. В условиях преобразований временных последовательностей событий из логов в используемую систему признаков необходимо контролировать отсутствие наложений одних и тех же фрагментов данных, которые могут попадать и в

обучающую, и в тестовую выборки. Проверка и недопущение подобных пересечений позволит не получить излишне оптимистичные оценки классификатора из-за недостаточной независимости тестируемых данных от обучающих данных. В частности, это будет направлено на то, чтобы не достигнуть эффекта переобучения. Предварительные данные экспериментов по применению подобного семплинга для детектирования атаки типа Denial-of-Sleep с использованием AdaBoostClassifier позволяют сделать вывод о небольшом повышении значений показателей качества детектирования. Возможны также и другие методики семплинга, позволяющие более точно подобрать нужные семплы, в том числе относящиеся к определенным классам. При недостаточности имеющихся объемов исходных данных наряду с семплингом разумно также применять кроссвалидацию.

К возможностям увеличения числа семплов в исходных данных, которые еще необходимо будет проверить на практике, можно отнести уменьшение значения параметра *N*, отвечающего за нарезку логов на семплы. Отметим, что суммарный объем исходных данных от этого не возрастет, и нет гарантии, что качество детектирования возрастет или не уменьшится. При применении определенных методов – метода ближайших соседей или логистической регрессии, возможно также некоторое повышение качества детектирования за счет дополнительных преобразований и нормализации признаков, например с приведением данных к некоторому единому масштабу при помощи механизмов MinMaxScaler, StandardScaler и др.

Помимо этого повышение качества детектирования может достигаться также за счет комбинирования классификаторов с использованием методик голосования и стекинга. Такие методики могут применяться как для обнаружения конкретных разновидностей Denial-of-Sleep-атак, так и для интегральной классификации.

Построенные в рамках данной работы механизмы детектирования Denial-of-Sleep-атаки были обучены и протестированы на 8 режимах интенсивности каждой из проанализированных 5 разновидностей атак. Несмотря на то, что в процессе экспериментов строго соблюдался принцип независимости данных из тестовых выборок от данных из обучающих выборок, тем не менее, в общем случае семплы каждого из режимов попадали как в обучающие, так и в тестовые выборки. Это обстоятельство позволяет установить тот факт, что на практике построенные классификаторы будут гарантированно работать с установленным качеством лишь в случае их применения для детектирования Denial-of-Sleep-атаки с одним из приведенных ранее 8 режимов работы (или в режиме, близком к одному из установленных). В режимах, отличных от указанных, классификаторы, скорее всего, также будут выдавать неплохие результаты, но качество детектирования может несколько снизиться.

Поэтому возможным совершенствованием процесса обучения станет модификация разбиений исходных данных на обучающую и тестовую выборки. В частности, целесообразно будет выделять под тестирование один или несколько режимов моделирования атаки целиком. И в процессе обучения семплы, составляющие атакующие данные этих тестовых режимов не должны входить в обучающие выборки. Другими словами, предлагается не только изолировать между собой семплы обучающей и тестовой выборок, но также и разграничить режимы, часть которых уйдет целиком в обучающую выборку, а оставшиеся – в тестовую. На первых порах данная модификация может привести к снижению качества детектирования за счет того, что тестовые и обучающие данные будут в большей степени иметь отличные друг от друга структуры. Тем не менее, применение описанных способов повышения качества детектирования будет способствовать нивелированию данного эффекта.

В целом, отметим, что за основу для экспериментов были взяты записи логов, извлеченных из трафика устройств БСС, осуществляющих коммуникации по протоколу ZigBee, имеющему ряд технологических ограничений и специфичных особенностей. К ним можно отнести, в частности, довольно низкую дальность действия беспроводного сигнала, использование динамической маршрутизации на основе статической адресации узлов, а также фактически отсутствующие во второй версии протокола какие-либо средства защиты. Несмотря на все это, моделирование Denial-of-Sleep-атак и возможности по обобщению полученных результатов на другие протоколы коммуникации БСС – LoRaWAN, LPWAN, Sigfox и др. – представляются вполне обоснованными. Это справедливо ввиду того, что основные принципы организации подобных Denial-of-Sleep-атак остаются достаточно универсальными и справедливы по отношению к широ-

кому спектру устройств интернета вещей, функционирующих от автономных источников питания и поддерживающих динамическую смену режимов энергоэффективности [1].

**Заключение.** В настоящей статье обнаружение Denial-of-Sleep-атак проводилось при использовании методов машинного обучения с применением серии признаков, значения которых были нормализованы. В качестве основных показателей качества обнаружения для выбора конкретных обучающих моделей были выбраны точность, полнота и f1-мера, а также показатель средневзвешенного значения f1-меры. Эксперименты проводились на нормальном трафике и пяти разновидностях атакующего трафика, отличающихся простотой реализации атаки, ее эффектом и скрытностью. Среди выбранных обучающих моделей наилучшие значения показателей качества обнаружения всех рассмотренных разновидностей Denial-of-Sleep-атак были получены с использованием модели AdaBoostClassifier. В среднем значение f1-меры составляет ~0.97, что подтверждает обоснованность использования такой модели для эффективного обнаружения данного вида атак. В рамках дальнейшей работы по этому направлению планируются исследования альтернативных методов интеллектуального анализа данных и их оценка.

## Список литературы

1. Desnitsky V., Kotenko I. Simulation and assessment of battery depletion attacks on unmanned aerial vehicles for crisis management infrastructures // Simulation Modelling Practice and Theory. 2021. Vol. 107. P. 102244. doi: 10.1016/j.simpat.2020.102244.

2. Intrusion detection system for wireless sensor networks using danger theory immune-inspired techniques / H. M. Salmon, C. M. Farias, P. Loureiro, L. Pirmez, S. Rossetto, P. H. Rodrigues, R. Pirmez, F. C. Delicato, L. F. Carmo // Intern. J. of Wireless Information Networks. 2013. Vol. 20. P. 39–66. doi: 10.1007/s10776-012-0179-z.

3. Uher J., Mennecke R. G., Farroha B. S. Denial of Sleep attacks in Bluetooth Low Energy wireless sensor networks // 2016 IEEE Military Communications Conf. Baltimore: MD, 2016. P. 1231–1236. doi: 10.1109/MILCOM.2016.7795499.

4. Counteracting Denial-of-Sleep attacks in wake-up-radio-based sensing systems / A. T. Capossele, V. Cervo, C. Petrioli, D. Spenza // Proc. of 13th Annual IEEE Intern. Conf. on Sensing, Communication, and Networking (SECON). IEEE. 2016. P. 1–9. doi: 10.1109/SAHCN.2016.7732978.

5. Udoh E., Getov V. Performance analysis of denial-of-sleep attack-prone mac protocols in wireless sensor networks // Proc. of 20th Intern. Conf. on Computer Modelling and Simulation (UKSim). IEEE. 2018. P. 151–156. doi: 10.1109/UKSim.2018.00038.

6. Nishanth N., Mujeeb A. Modeling and detection of flooding-based Denial-of-Service attack in wireless Ad Hoc network using bayesian inference // IEEE Systems J. 2021. Vol. 15, no. 1. P. 17–26, doi: 10.1109/JSYST.2020.2984797.

7. Dhunna G. S., Al-Anbagi I. A Low Power WSNs attack detection and isolation mechanism for critical smart grid applications // IEEE Sensors J. 2019. Vol. 19, no. 13. P. 5315–5324. doi: 10.1109/JSEN.2019.2902357.

8. Razaque A., Abdulghafour M., Khan M. J. Detection of selfish attack over wireless body area networks // Proc. of IEEE Conf. on Open Systems (ICOS). IEEE. 2017. P. 48–52. doi: 10.1109/ICOS.2017.8280273.

9. Bhattasali T., Chaki R. AMC model for Denial of Sleep attack detection // arXiv:1203.1777v1. 2012. doi: 10.48550/arXiv.1203.1777.

10. Mohd N., Singh A., Bhadauria H. S. A Novel SVM based IDS for distributed Denial of Sleep strike in wireless sensor networks // Wireless Personal Communications. 2019. Vol 111. P. 1999–2022. doi: 10.1007/s11277-019-06969-9.

11. Scikit-learn library. Machine Learning in Python. URL: https://scikit-learn.org (дата обращения 13.04.2022).

## Информация об авторе

**Десницкий Василий Алексеевич** – канд. техн. наук, доцент, старший научный сотрудник лаборатории проблем компьютерной безопасности СПб ФИЦ РАН. Санкт-Петербургский Федеральный исследовательский центр Российской академии наук, 14-я линия В. О., д. 39, Санкт-Петербург, 199178, Россия.
E-mail: desnitsky@comsec.spb.ru
https://orcid.org/0000-0002-3748-5414

## References

1. Desnitsky V., Kotenko I. Simulation and Assessment of Battery Depletion Attacks on Unmanned Aerial Vehicles for Crisis Management Infrastructures // Simulation Modelling Practice and Theory. 2021. Vol. 107. P. 102244. doi: 10.1016/j.simpat.2020.102244.

2. Salmon H. M., Farias C. M., Loureiro P., Pirmez L., Rossetto S., Rodrigues P. H., Pirmez R., Delicato F. C., Carmo L. F. Intrusion Detection System for Wireless Sensor Networks Using Danger Theory Immune-Inspired Techniques // Intern. J. of Wireless Information Networks. 2013. Vol. 20. P. 39–66. doi: 10.1007/s10776-012-0179-z.

3. Uher J., Mennecke R. G., Farroha B. S. Denial of Sleep Attacks in Bluetooth Low Energy Wireless Sensor Networks // 2016 IEEE Military Communications Conf. Baltimore: MD, 2016. P. 1231–1236. doi: 10.1109/MILCOM.2016.7795499.

4. Capossele A. T., Cervo V., Petrioli C., Spenza D. Counteracting Denial-of-Sleep Attacks in Wake-Up-Radio-Based Sensing Systems // Proc. of 13th Annual IEEE Intern. Conf. on Sensing, Communication, and Networking (SECON). IEEE. 2016. P. 1–9. doi: 10.1109/SAHCN.2016.7732978.

5. Udoh E., Getov V. Performance Analysis of Denial-of-Sleep Attack-Prone MAC Protocols in Wireless Sensor Networks // Proc. of 20th Intern. Conf. on Computer Modelling and Simulation (UKSim). IEEE, 2018. P. 151–156. doi: 10.1109/UKSim.2018.00038.

6. Nishanth N., Mujeeb A. Modeling and Detection of Flooding-Based Denial-of-Service Attack in Wireless Ad Hoc Network Using Bayesian Inference // IEEE Systems J. 2021. Vol. 15, no. 1. P. 17–26, doi: 10.1109/JSYST.2020.2984797.

7. Dhunna G. S., Al-Anbagi I. A Low Power WSNs Attack Detection and Isolation Mechanism for Critical Smart Grid Applications // IEEE Sensors J. 2019. Vol. 19, no. 13. P. 5315–5324. doi: 10.1109/JSEN.2019.2902357.

8. Razaque A., Abdulghafour M., Khan M. J. Detection of Selfish Attack Over Wireless Body Area Networks // Proc. of IEEE Conf. on Open Systems (ICOS). IEEE. 2017. P. 48–52. doi: 10.1109/ICOS.2017.8280273.

9. Bhattasali T., Chaki R. AMC Model for Denial of Sleep Attack Detection // arXiv:1203.1777v1. 2012. doi: 10.48550/arXiv.1203.1777.

10. Mohd N., Singh A., Bhadauria H. S. A Novel SVM Based IDS for Distributed Denial of Sleep Strike in Wireless Sensor Networks // Wireless Personal Communications. 2019. Vol 111. P. 1999–2022. doi: 10.1007/s11277-019-06969-9.

11. Scikit-learn library. Machine Learning in Python. URL: https://scikit-learn.org (дата обращения 13.04.2022).

## Information about the author

**Vasily A. Desnitsky** – Cand. Sci. (Eng.), Assistant Professor, Senior researcher of the Laboratory of Computer Security Problems of SPC RAS. St. Petersburg Federal Research Center of the Russian Academy of Sciences, 14th Liniya V. O., 39, Saint Petersburg, 199178, Russia.
E-mail: desnitsky@comsec.spb.ru
https://orcid.org/0000-0002-3748-5414

Статья поступила в редакцию 01.05.2022; принята к публикации после рецензирования 12.05.2022; опубликована онлайн 30.06.2022.

Submitted 01.05.2022; accepted 12.05.2022; published online 30.06.2022.