АНАЛИЗ МОДЕЛЕЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА ДЛЯ ОБНАРУЖЕНИЯ АТАК НА МАРШРУТИЗАТОРЫ БЕСПРОВОДНЫХ ЛОКАЛЬНЫХ СЕТЕЙ

Рейпназаров Ерназар[1[0000-0003-0100-3708]]***, Ешниязова Гоззал***[2[0009-0001-8424-2474]]*.*

[1]PhD, доцент кафедры Системы и сети передачи данных, Ташкентского университета информационных технологий имени Мухаммада ал-Хоразмий, E-mail: reypnazar0vernazar@gmail.com

[2]Ассистент кафедры Системы и сети передачи данных, Ташкентского университета информационных технологий имени Мухаммада ал-Хоразмий, E-mail: gozzal1115@gmail.com

Annotatsiya. Ushbu maqoladaWLAN marshrutizatorlariga qarshi hujumlarni aniqlash uchun zamonaviy sun'iy intellekt modellari o'rganilgan. Ayniqsa, «evil twin» hujumini RF-barmoq izi orqali aniqlash usuli tahlil qilingan. CNN modeli ishlab chiqilib, o'qitilgan va yuqori aniqlik ko'rsatgan.
Kalit so'zlar: CNN, RF barmoq izlari, marshrutizator, mashinani o'rganish, signal tasnifi, qurilma identifikatsiyasi, modelni o'qitish, RF signalini qayta ishlash, PHY-qatlamni aniqlash.

Аннотация. В данной статье рассматривается современные модели искусственного интеллекта для обнаружения атак на маршрутизаторы WLAN. Особое внимание уделено атаке типа «evil twin» и её выявлению с помощью анализа RF-отпечатков устройств. Разработана и обучена модель CNN, продемонстрировавшая высокую точность идентификации маршрутизаторов и обнаружения имитации.
Ключевые слова: CNN, RF-отпечатки, маршрутизатор, машинное обучение, классификация сигналов, идентификация устройств, обучение модели, обработка радиочастотных сигналов, распознавание по физическому уровню (PHY-layer).

Abstract: This article discusses explores modern artificial intelligence models for detecting attacks on WLAN routers. Special attention is given to the «evil twin» attack and its detection using RF fingerprint analysis. A convolutional neural network (CNN) model was developed and trained, demonstrating high accuracy in router identification and impersonation detection.
Key words: CNN, RF fingerprinting, router, machine learning, signal classification, device identification, model training, RF signal processing, PHY-layer recognition.

Введение

Современные вызовы информационной безопасности требуют применения интеллектуальных технологий, таких как искусственный интеллект и глубокое обучение. Сверточные нейронные сети (CNN), успешно используемые для систем распознавания образов, до недавнего времени привлекли беспокойство и кибербезопасности. Их возможность извлекать устойчивые признаки из радиосигналов позволяет эффективно определять и классифицировать беспроводные устройства, полностью соответствуя поставленным в вышеизложенных стратегических документах приоритетам. В этой статье будет изучение и сравнение наиболее актуальных для модели искусственного интеллекта моделей, которые будут использоваться наощупинь по выявлению атак на маршрутизаторы WLAN, и разрабатывать методологию распознавания атаки имитации маршрутизатора поинуленая по анализу RF-отпечатков посредством сверточной нейронной сети [1-4].

©Journal of Advances in Engineering Technology Vol.3(19), July — September, 2025
DOI 10.24412/2181-1431-2025-3-80-85

Методология

Атака типа «evil twin» (имитация маршрутизатора) заключается в том, что злоумышленник настраивает поддельную точку доступа с тем же MAC-адресом и SSID, что и у легитимного маршрутизатора, и побуждает пользователей подключиться к ней. Таким образом, атакующий может перехватывать трафик или осуществлять дальнейшие злоумышленные действия. Стандартные средства идентификации устройства по цифровым признакам (MAC-адрес, SSID и пр.) ненадежны, поскольку эти идентификаторы могут быть подделаны (спуфинг). Для надежного обнаружения «злого двойника» предлагается использовать физические особенности самого радиосигнала так называемый RF-отпечаток передатчика. RF-отпечаток представляет собой уникальную комбинацию характеристик радиотракта (неидеальности аппаратуры передатчика, а также специфический профиль радиоканала между передатчиком и приемником). При прочих равных условиях у каждого маршрутизатора в стационарной WLAN-сети формируется стабильный RF-отпечаток на стороне приемника. Сравнивая RF-отпечаток принятого сигнала с эталонными отпечатками известных маршрутизаторов, можно выявлять рассогласование между цифровой идентификацией (например, MAC-адресом) и физическим источником сигнала. Иными словами, если декодированный MAC-адрес кадра соответствует известному маршрутизатору, а RF-отпечаток нет, то источник определяется как имитатор (подделка). Такой подход был предложен в ряде работ, например, авторы в работе [5] разработали глубокую нейронную сеть, способную по сырым IQ-данным различать передатчики по их RF-следам.

Выбранный в данной работе метод основывается на использовании CNN для классификации источников беспроводных сигналов по их RF-отпечаткам. Сеть обучается распознавать несколько известных маршрутизаторов по их индивидуальным RF-признакам, и также узнавать класс «Unknown» для всех остальных сигналов, не принадлежащих известным устройствам. При развертывании системы предполагается наличие наблюдателя – приемника, расположенного стационарно во внутренней сети, который принимает широковещательные сигналы Wi-Fi от ближайших точек доступа. Наблю-датель знает список доверенных (известных) маршрутизаторов и их MAC-адресов. Все прочие передатчики трактуются как неизвестные. Таким образом, задача сводится к отнесению каждого принятого кадра либо к одному из классов известных устройств, либо к классу Unknown. После классификации RF-отпечатка проверяется соответствие полученного класса с объявленным в кадре MAC-адресом. Если полученный RF-отпечаток не соответствует MAC-адресу (например, MAC известен, а RF-отпечаток классифицирован как Unknown, либо классифицирован не как тот самый маршрутизатор), то делается вывод об обнаружении имитатора маршрутизатора. В противном случае, источник распознается как легитимный. Благодаря этому совмещенному критерию появляется возможность выявлять атаки «злого двойника» даже при спуфинге MAC-адреса.

Зеленые лучи RF1, RF2, RF3 – стабильные RF-отпечатки от известных устройств. «Unknown Router Data» – совокупность сигнатур от неизвестных передатчиков. В условиях фиксированного положения маршрутизаторов и приемника эти RF-отпечатки остаются постоянными во времени, тогда как у неизвестных устройств сигнатуры произвольны и не совпадают с RF1–RF3.

На рисунке 3.1 схематично показан принцип использующегося подхода. Наблюдатель принимает от нескольких фиксированных доверенных маршрутизаторов специальные обучающие сигналы – в данном случае beacon-

©Journal of Advances in Engineering Technology Vol.3(19), July — September, 2025
DOI 10.24412/2181-1431-2025-3-80-85

кадры WLAN, содержащие Legacy Long Training Field (L-LTF). L-LTF представляет собой известную перестамбульную последовательность, которая передается всеми устройствами одинаково (в стандартах 802.11a/g/n/ac), поэтому на ней удобно базировать сравнение физических отпечатков без влияния различий в передаваемых данных. Предполагается, что маршрутизаторы и приемник неподвижны, и каждый известный маршрутизатор создает уникальный, неизменный во времени RF-отпечаток (обозначены как RF1, RF2, RF3 на рис. 1).

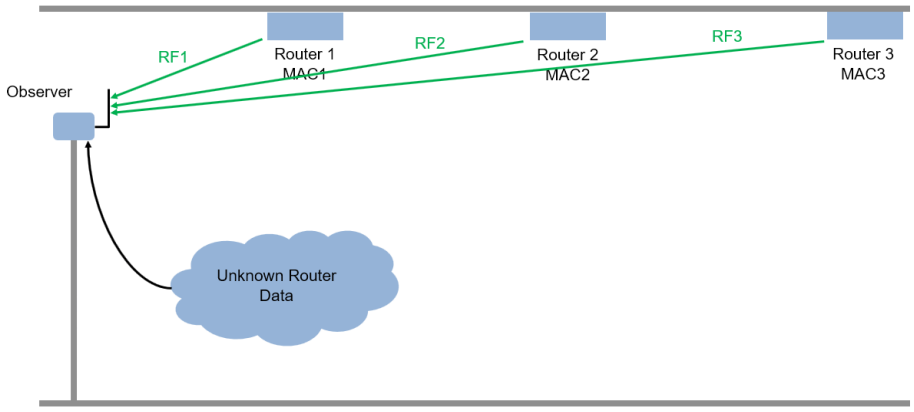

Рис.-1. Сценарий с тремя известными маршрутизаторами (Router 1–3) и стационарным наблюдателем.

Эти отпечатки определяются характеристиками аппаратуры конкретного маршрутизатора и профилем радиоканала между ним и приемником. Любой другой (незнакомый системе) передатчик с большой вероятностью будет обладать иным RF-отпечатком. Таким образом, все «чужие» сигналы будут классифицироваться как Unknown. Наблюдатель, помимо RF-анализа, также декодирует MAC-адрес отправителя из поля Address2 заголовка beacon-кадра. Если MAC-адрес присутствует в белом списке и RF-отпечаток равен отпечатку подходящего маршрутизатора (например, фрейм от Router 2 и маркирован как Router 2) – то источник считается легитимным. И если MAC-адрес фрейма известный, а RF-отпечаток не был равен (класс «Unknown» или другой) – то зафиксировано событие олицетворения маршрутизатора (имитации).

Для обучения сети использовался алгоритм градиентной оптимизации Adam (Adaptive Moment Estimation) – он показал себя высококачественным при обучении нейронных сетей на выбор User-like данных и обеспечивает более стремительное достижение плато ошибки, чем используемый.std. SGD. В качестве функции потерь использовалась категориальная кроссэнтропия (она используем в автоматическом режиме слоем classificationLayer в MATLAB). Гиперпараметры обучения приведены в таблице 1.

Таблица 1.

Гиперпараметры и условия обучения CNN-модели.

Гиперпараметр	**Значение в эксперименте**	**Примечания**
Оптимизатор	Adam	β_1=0.9, β_2=0.999 (по умолчанию)
Мини-батч (batch size)	256 кадров	Обновление градиентов каждые 256 примеров
Начальная скорость обучения	0.0001 (1×10^(-4))	Постепенное уменьшение приPlateau

©Journal of Advances in Engineering Technology Vol.3(19), July — September, 2025
DOI 10.24412/2181-1431-2025-3-80-85

L2-регуляризация весов	0.0001	Во всех слоях (WeightDecay)
Максимум эпох	100	Остановка раньше приEarlyStopping
Критерий Early Stopping	validation patience = 3	Прерывание, если 3 эпохи нет улучшения на валидации
Перемешивание данных	каждая эпоха (shuffle every-epoch)	Для разграничения эпох
Разбиение на выборки	80% обуч., 10% валид., 10% тест	Как описано в разд. 3.2.2

Результаты, описанные выше, показали, что натравка обучения модели очень натуральна. В первой эпохе точность классификации на тренировочных данных достигла ~98%, а во второй эпохе — 100%, как показано на графике построения обучения (рис.2). Точность увеличивалась только на несколько процентов с помощью дополнительного натяжения. При этом критические ошибки (потери) медленно снижались и наталкивались на плато, что демонстрирует отсутствие заметного переобучения. Кроме того, валидационная точность быстро выросла до сто процентов, уравнявшись с тренировочной, и в соответствии с методом раннего остановки он автоматически завершал процесс обучения ранее, на десятой эпохе. При использовании CPU обучение заняло примерно 6 минут.

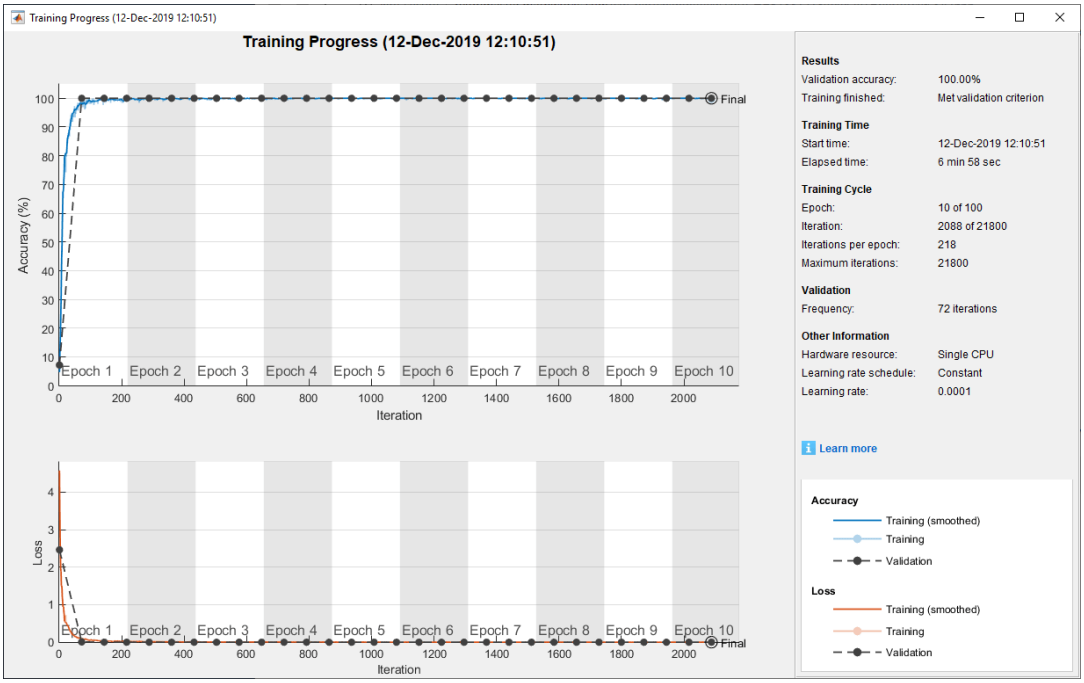

Рис.-2. График обучения CNN на синтетических данных: точность (Accuracy) и функция потерь (Loss) в процентах от итерации.

Видно, что в ~2 эпохи ~100% классификация точности на обучение и валидация наборах достигается дополнительно после чего тренировка оказывается выполнена досрочно (Validation Patience 3) из-за знаков ошибок на валидации.

После завершения обучения и проверки реализованная CNN-модель показала возможность ошибок-ноль при классификации сигналов Wi-Fi маршрутизаторов в контролируемом режиме эксперимента. На выборке для

©Journal of Advances in Engineering Technology Vol.3(19), July — September, 2025
DOI 10.24412/2181-1431-2025-3-80-85

проверки достигла точности– 100%. Это означает, что во всех проверках нейросеть правильно определила, является ли принятый кадр одному из известных маршрутизаторов или отнесла его в класс Unknown, если отпечаток не совпадает ни с одним из эталонов. Таким образом, метод классификации по RF-отпечаткам обеспечил возможность гарантировать эффективное различие «своих» устройств от «чужих».

Следовательно, например, при наблюдении в рассматриваемом эксперименте над наблюдателем, получившим видеоролики с MAC-адреса Router 2, но RF-отпечатка не RF2, а неизвестный (RF-X), алгоритм отдал сигнал о несовпадении (имитации). Это uyguno согласуется с схемой на рис. 3.

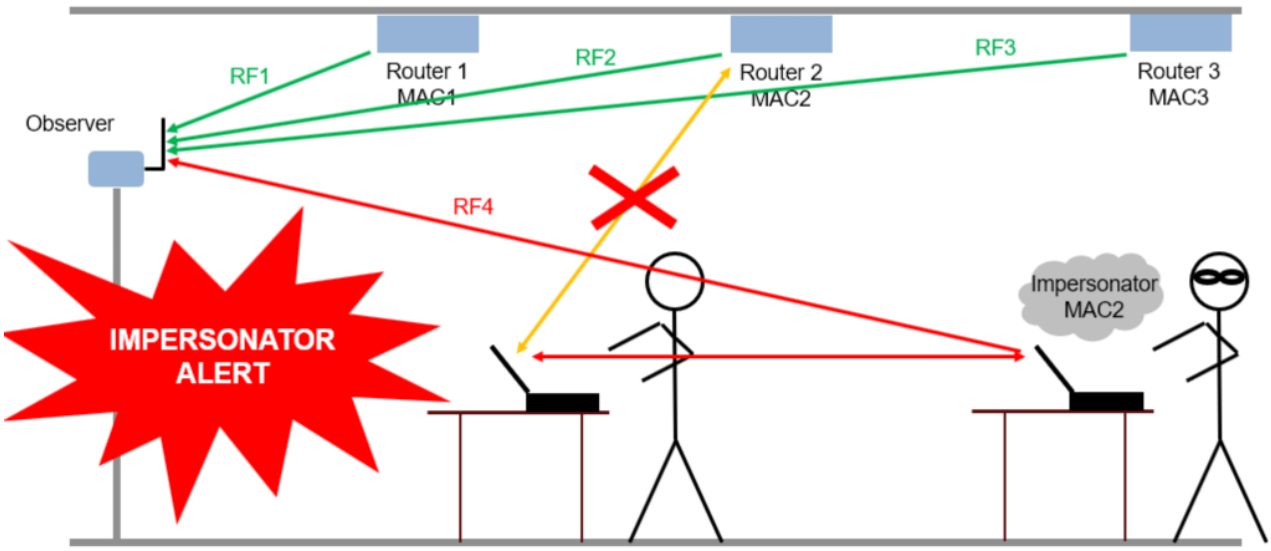

Рис.-3. Схема обнаружения имитации маршрутизатора

Злоумышленник (справа) копирует MAC-адрес доверенного Router 2 (на потолке), формируя поддельную точку доступа. Пользовательская станция подключается к более сильному сигналу (к злоумышленнику). Приемник (Observer) принимает beacon-кадры с MAC Router 2, но их RF-отпечаток (красный луч RF4) не совпадает с ожидаемым RF2 от легитимного маршрутизатора. Система фиксирует «имитатор обнаружен!» и выдает тревогу. На рисунке 3.6 зеленым цветом показаны легитимные сигналы известных роутеров (RF1, RF2, RF3), а красным – сигнал злоумышленника, который «притворяется» Router 2. Несмотря на одинаковый MAC-адрес, различие в RF-отпечатках позволяет надежно определить подлог. В эксперименте нейросеть присвоила всем таким кадрам класс Unknown, тем самым пометив их как угрозу. Данный пример демонстрирует, что разработанный метод способен укрепить защиту WLAN-сети, дополняя традиционные механизмы аутентификации физическим уровнем идентификации передатчика [7-13].

Заключение

Разработанная в этой статье модель и эксперименты демонстрировали эффективность использования метода RF-фингерпринтинга для повышения безопасности WLAN. Поставленный метод также может быть использован как часть комплексной системы защиты Wi-Fi, дополняя ее физическим слоем аутентификации точек доступа и разрешающим останавливать атаки типа «злой двойник» при успехе спуфингов сетевых идентификаторов.

©Journal of Advances in Engineering Technology Vol.3(19), July — September, 2025
DOI 10.24412/2181-1431-2025-3-80-85

Список использованной литературы:

[1]. Stallings W. Wireless Communications & Networks. – Pearson Education, 2013. – 608 p..
[2]. Hasan M., Islam M., Zarif M.I.I., Hashem M.M.A. Attack and anomaly detection in IoT sensors in IoT sites using machine learning approaches. – Internet of Things, 2020, Vol. 7, 100059.
[3]. Xiao Y., Shen C., Du X., Zhang J. A survey on deep learning-based anomaly detection in network security. – IEEE Access, 2021, Vol. 9, pp. 120412–120430.
[4]. MathWorks. Design a Deep Neural Network with Simulated Data to Detect WLAN Router Impersonation. – MATLAB Documentation. URL: https://www.mathworks.com/help/comm/ug/detect-router-impersonation-using-deep-learning.htmlsed anomaly detection in network security. – IEEE Access, 2021, Vol. 9, pp. 120412–120430.
[5]. D'Oro S., Restuccia F., Melodia T. Detection of Evil Twin Attacks in 802.11 Networks with Machine Learning and Physical Layer Analysis. – Proceedings of IEEE INFOCOM, 2019
[6] Nguyen T.T., Armitage G. A survey of techniques for internet traffic classification using machine learning. – IEEE Communications Surveys & Tutorials, 2008.
[7] Koziarski M., Woźniak M. Evaluation of machine learning algorithms for anomaly detection in wireless networks. – Expert Systems with Applications, 2020.
[8] Tang T.A., Mhamdi L., McLernon D., Zaidi S.A.R., Ghogho M. Deep Learning Approach for Network Intrusion Detection in Software Defined Networking. – IEEE Network, 2018, Vol. 32(2), pp. 118–126.
[9] Bahl P., Padmanabhan V.N. RADAR: An in-building RF-based user location and tracking system. – Proceedings of IEEE INFOCOM, 2000, Vol. 2, pp. 775–784.
[10] Daei M., Jadidoleslamy H. A Survey on Machine Learning-based Intrusion Detection Systems for Wireless Networks. – Journal of Computer Science and Technology, 2021.
[11] Soltani R., Li J., Zhang H. Deep Learning-Based Physical Layer Authentication for Wireless Security: A Review. – IEEE Access, 2020, Vol. 8, pp. 132650–132666.
[12] Sagduyu Y.E., Shi Y., Li J., Li W. Adversarial Deep Learning for Over-the-Air Spectrum Poisoning Attacks. – IEEE Transactions on Mobile Computing, 2020.
[13] Ali M.U., Ghani A., Khan A. A Review of Wireless Security Protocols in the Context of IEEE 802.11 WLAN. – Journal of Communications, 2019, Vol. 14(3), pp. 232–240

©Journal of Advances in Engineering Technology Vol.3(19), July — September, 2025
DOI 10.24412/2181-1431-2025-3-80-85