УДК 004.4

ВИЯВЛЕННЯ СИГНАЛІВ БПЛА ЗА ДОПОМОГОЮ НЕЙРОМЕРЕЖ (НА ПРИКЛАДІ НАБОРІВ ДАНИХ КОМЕРЦІЙНИХ ДРОНІВ)

Чубай Д. Р.,, Ігнатова С.С.
Київська інженерна гімназія, Комунальний заклад позашкільної освіти «Київська Мала академія наук учнівської молоді»
E-mail: daniil.chubay@gmail.com

DETECTION OF UAV SIGNALS USING NEURAL NETWORKS (USING THE DATA SETS OF COMMERCIAL DRONES)

The article describes the features of communication protocols in different UAVs and proposes to use neural networks to detect and classify UAV signals. During the research, it was found that CNN models score the best at the detection/classification of UAVs. RNN and Transformer models showed abnormal results.

З розвитком застосування БПЛА у військовій та цивільній сферах зростає потреба у засобах виявлення безпілотників. Ефективні засоби виявлення БПЛА допомагають військовослужбовцям мати краще уявлення про стан справ у повітряному просторі, тому дослідження з цієї теми можуть спасти життя наших воїнів та загалом покращити безпеку людей.

У різних БПЛА використовують різні види протоколів зв’язку. В них, зокрема, використовуються різні види модуляції. В залежності від типу інформації, яка передається, модуляції поділяються на цифрові та аналогові.

У цифрових модуляціях в БПЛА переважно використовуються технології псевдовипадкового перелаштування робочої частоти та ортогонального частотного поділу каналів. Ортогональний частотний поділ каналів (ОЧПК; англ. Orthogonal Frequency-Division Multiplexing — OFDM) – це різновид частотного поділу каналів, який модулює цифрові дані різними близькими несучими хвилями. До протоколів ОЧПК, які використовуються в БПЛА, належить WI-FI стандартів 802.11n або 802.11ac, Enhanced WI-FI, розроблений компанією DJI. ОЧПК використовується у дронах Yuneec Mantis Q, Parrot ANAFI, DJI Mavic Air. Іншою технологією, яка поширена в БПЛА, є псевдовипадкове перелаштування робочої частоти (ППРЧ; англ. Frequency-Hopping Spread Spectrum) – метод передачі радіосигналів шляхом швидкої зміни несучої сигнала. DJI має свої протоколи, засновані на ППРЧ, зокрема Lightbridge, Ocusync. У популярному приймачі FrSky теж використовується FHSS [5, с. 12]. Окрім того, до цифрових протоколів належать сімейство DSM (зокрема, DSMX, DSM2, DSSS), ACCESS/FRSKY, A-FHSS, AFHDS та AFHDS2, HiSky, DEVO [3, с. 177–178]. В БПЛА може використовуватися стільниковий зв’язок 3/4G. Для навігації використовують зв’язок GPS (GNSS), зокрема за допомогою протоколу NMEA [8, с. 35-37]. Окрім цифрової, використовується аналогова модуляція. Зокрема, в стандартах PAL, NTSC. Для контролю БПЛА може використовуватися FM модуляція [3, с. 176]. БПЛА/дрони можуть використовувати частоти 27, 28, 35, 40, 220–400, 433, 725–770, 790–830, 850-916, 935–960, 950–1200 МГц, 1.4–1.85, 2.1–

2.7, 4.4–5.85, 14.4–14.83, 15.15–15.35, 17.1–18.8, 21.1–21.7 ГГц, [2, с. 32–33][1, с. 18–19][3, с. 179–180]. Сюди входять частоти, на яких здійснюється контроль БПЛА, навігація, передача телеметрії, передача відео тощо. Отже, в технологіях комунікації у БПЛА маємо досить велике різноманіття.

Машинне навчання в останні роки стало популярним та ефективним інструментом для автоматизації складних задач. На відміну від класичних алгоритмів, нейронні мережі здатні за допомогою проб і помилок виявляти комплексні структури, комбінації різних параметрів. Зокрема, вони здатні вирішувати задачі, пов'язані з класифікацією сигналів [6, с. 451–460]. Отже за допомогою нейромереж можна й виявляти різні види БПЛА за їх радіосигналами. Як вже було зазначено, різні види та моделі БПЛА мають різні технології та протоколи комунікації, через що вручну описувати алгоритм виявлення кожного окремого пристрою є неефективним способом. Натомість нейромережі можуть самі виокремлювати параметри, за якими треба визначати присутність сигналів БПЛА. Наприклад, присутність БПЛА може бути виявлена нейромережами внаслідок відстеження того, наскільки часто передаються пакети даних на певних частотах. Тому ми вирішили дослідити які моделі нейромереж найбільш ефективні у виявленні/класифікації БПЛА.

Для цього ми використовували набори даних з записами радіосигналів дронів, доступні у вільному доступі. Спочатку нами було обрано набор даних «DroneRF». Втім через велику кількість відліків (2 млн на кожному сегменті) тренування моделей нейромереж на цьому наборі даних займало забагато часу. Тому ми вирішили звернутися набору даних «Noisy Drone RF signals classification».

Для класифікації сигналів нами було обрано протестувати згорткові нейронні мережі, рекурентні нейронні мережі і моделі-трансформери, оскільки ці моделі непогано себе показали у схожих галузях. Згорткові нейронні мережі (ЗНН; англ. Convolutional neural network – CNN) різняться від інших нейронних мереж наявністю згорткових шарів, які мають ядро-фільтр, що проходиться по масиву вхідних даних. Ми використали модель нейромережі, запропоновану в [10], додавши до неї шар виключення. В результаті було отримано точність класи на перевірочних даних 86% (див. рис. 1).

Рис. 1. Точність моделі ЗНН.

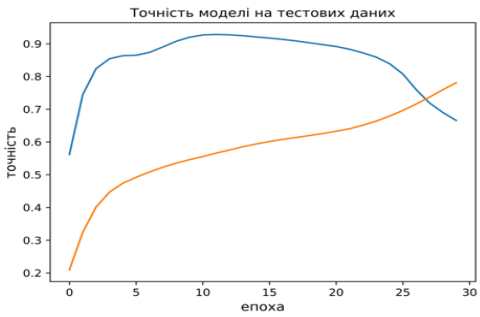

Рис. 2. Точність моделі РНН.

Класифікація спектрограм не дала помітних кращих результатів: було отримано точність лише 62%. Наступним видом нейронних мереж, який ми спробували застосувати, були рекурентні нейронні мережі (РНН; англ. recurrent neural network — RNN). Їх особливість полягає в тому, що вони оброблюють послідовності даних з зберіганням внутрішньої пам'яті. У більшості випадків РНН вже в першій епосі досягала точності на перевірочних даних близько 95%, але

згодом точність дуже різко падала. Найбільш реалістичні результати були отримані, коли коефіцієнт навчання (параметр learning_rate) був понижений до значення 10^{-6} (див. рис. 2). Були також розглянуті трансформери – нові моделі нейромереж, описані в 2017 р. у статті „Attention is All You Need". Для нашої задачі ми використали імплементацію, запропоновану в [7] для класифікації часових рядів, але змінювали там коефіцієнт навчання та значення параметру dropout. Трансформер вів себе подібно до рекурентних нейронних мереж.

Отже, найкраще у виявленні/класифікації дронів себе показали згорткові нейронні мережі з точністю 86%. Навчання рекурентних нейронних мереж та трансформерів дало аномальні результати. Можливо проблема полягає у поганій сумісності цих моделей нейромереж з обраними наборами даних.

Напрямками нашої подальшої роботи буде: написання кращої попередньої обробки та виділення ознак у наборах даних; імплементація нейронної мережі з підкріпленням (для динамічного корегування ваг нейронної мережі на основі нових записів); розробка пристрою, який аналізуватиме спектр на наявність БПЛА у режимі реального часу. Останнє може здійснюватися за допомогою SDR приймача. Для вивантаження нейромережі на пристрої з обмеженими обчислювальними можливостями існує бібліотека Tensorflow Lite Micro (TFLM). Прикладом імплементації зв'язки SDR (HackRF), TFLM і Keras є система для аналізу радіосигналу криптогаманця Ledger Blue, яку розробили T. Рот та ін. [9].

Література

1. Боротьба з безпілотними літальними апаратами (за досвідом проведення ООС (раніше АТО). К.: «Центр учбової літератури», 2022. 43 с.
2. Макаренко С. И. Противодействие беспилотным летательным аппаратам. СПб.: Наукоемкие технологии, 2020. 204 с.
3. Communication, Remote Control and Autonomous Flights. *Unmanned electrical vehicles and autonomous system simulation* / Editors: Sell R., Czekalski P., Ņikitenko A. Riga: RTU Press, 2021. pp. 175-181.
4. Noisy Drone RF Signal Classification. Kaggle. URL: https://www.kaggle.com/datasets/sgluege/noisy-drone-rf-signal-classification
5. Rozenbeek D. J. Evaluation of Drone Neutralization Methods using Radio Jamming and Spoofing Techniques. 2020. URL: https://www.diva-portal.org/smash/get/diva2:1460807/FULLTEXT01.pdf.
6. Steven W. S. The Scientist & Engineer's Guide to Digital Signal Processing. California: California Technical Pub, 1999. 640 p.
7. Timeseries classification with a Transformer model. Keras. URL: https://keras.io/examples/timeseries/timeseries_classification_transformer/
8. UAV Networks and Communications / Edited by Kamesh Namuduri, Serge Chaumette, Jae H. Kim, James P. G. Sterbenz. Cambridge University Press, 2018. 242 p.
9. Using TensorFlow / machine learning for automated RF side-channel attack classification. *Leveldown security*. URL: https://leveldown.de/blog/tensorflow-sidechannel-analysis/.
10. Zhiguang Wang, Weizhong Yan, Tim Oates. Time Series Classification from Scratch with Deep Neural Networks: A Strong Baseline. arXiv. URL: https://arxiv.org/abs/1611.06455.