Prof. Piotr Gajewski DSc, PhD, Eng.
Military University of Technology
piotr.gajewski@wat.edu.pl

7.04.2025

Reviewer's opinion

on Ph.D. dissertation authored by

mgr eng. Malgorzata Wasilewska

entitled:

New Machine Learning Methods for Spectrum Sensing in Wireless Communication Systems

1. Problem and its impact

The rapid growth of wireless transmission services and applications in global mobile wireless networks causes an avalanche increase in the requirements for the use of resources concerning both transmission medium and computing. Scarcity of available frequency spectrum need to continuous search for solutions to increase the efficiency of the use of spectral resources. Here, the Cognitive Radio technique is promising technology, which enables opportunistic spectrum sharing by licensed users (Primary User -PU) and unlicensed ones (Secondary User – SU). The Spectrum Sensing SS mechanisms are utilized to detect PU transmissions in shared bands and to determine whether they are busy or free for SU transmission.

In order to ensure high efficiency of licensed band usage, sharing mechanisms (SS and SM) used by SU should be adapted to the signals transmitted in the PU system. In particular, in 4G (LTEa) and 5G (eLTE) networks, this applies to detecting resource blocks (RB) free in the sense of their potential use by SU. Solving the question of interference avoiding in a complex and rapidly changing EM environment requires the search for sensing methods that are more effective than the currently existing ones. This is the basic scientific problem discussed in the reviewed dissertation, which thesis is included in its thesis cit.: "*There exist new methods for spectrum sensing in wireless communication systems that are based on machine learning and that are more reliable than the existing ones.*"

In the reviewer's opinion, such a formulated thesis, repeated in the conclusions, contains a logical error, because if something exists, it cannot be better than something that already exists. This error can be easily fixed by changing "The existing new methods" to "Advanced new methods". This becomes obvious after analysing the research goals formulated in the dissertation.

Besides, Artificial Intelligence (AI) is an another trend in this area. It is confirmed by the recently growing number of publications on the use of Machine Learning (ML) methods (including Deep Learning - DL) in solving various problems for more effective wireless networks, including efficient use of physical and computational network resources. Intelligent sensing SS and spectrum management SM methods are suitable to support the radio-environment awareness development and using in situation of rapidly changing conditions of the wireless systems environment. Spectrum sensing can be carried out individually by the CR node, but much more effective is cooperative sensing, in which the decision on spectrum occupancy is made on the basis of information collected by groups of sensors. Context awareness modelling and Federated Learning FL are very promising methods that can be used in cognitive solutions.

As a consequence of new radio technologies deployment, cognitive skills using awareness formation, sensing, contextual modelling, machine learning, and federated learning increase the system's vulnerability to security threats and require the identification of threats and the use of countermeasures.

Security is closely related to the development of communication technology, but very often treated as a separate problem to be solved.

Presented dissertation is undoubtedly of a scientific nature, falling within the scope of broad scientific research to increase the wireless systems capabilities. It is therefore very important to provide in this dissertation a comprehensive solution for new sensing techniques and methods of counteracting threats related to their implementation.

2. Contribution

The original Author's contributions are strictly connected with her research goals focussed as follow:

- to analyse the state of the art in the field of reliable SS in radio communication channels, and project the knowledge gaps against her original solutions;
- to develop the effective, low-cost algorithm for the autonomous ML-supported SS, that takes advantage of the measured PU's signal energy and the time- and frequency dependencies of the sensed signal spectrum;
- to develop the effective, DL algorithms for SS and spectrum occupancy prediction that take into the wireless channel variations into account;
- to develop an efficient FL-based SS algorithm, suitable for varying radio propagation conditions;
- to evaluate the impact of coordinated and random poisoning attacks on FL based SS, and to design an efficient algorithm to detect and mitigate such attacks.

Below, an analysis of the content of individual chapters from the point of view of the Author's contribution is presented.

Five main chapters (1-5) are preceded by Introduction that shows Author's motivation for undertaking research on the application of ML in SS procedures, thesis and main goals, dissertation outline, and Author's published contributions. Final chapter 6 contains general conclusions.

The Author's original achievements being included in chapters 2-5. Each of this chapters is preceded by an introductory commentary, and ends with conclusions.

Chapter 1 presents a review of the literature, identifying the State of the Art (SOTA) research in the Author's scientific area, that are:

a- The significance of Context Awareness in Wireless Communications; Question 1: "What is the role of context information, its availability, and representation in contemporary and future radio communication networks?"

b- Machine Learning Methods for Context Awareness; Question 2: "What are the suitable AI/ML methods to enrich context awareness in these networks?"

c- Machine Learning for Spectrum Sensing; Question 3: "What kind of ML algorithms and framework are considered for autonomous and cooperative SS?"

d- Resource occupation pattern recognition; Question 4: "How the ML-based pattern recognition methods can be used for SS and prediction in time-, frequency-, and spatial dimension?"

e- Context-Awareness Design Trade-offs, and Recommendations: Question 5: "What are the design trade-offs and recommendations for intelligent context-aware radio communication?"

The content of each sub-sections gives completely answer to above questions and justifies the logical order of the analyses carried out in the following chapters.

Ad a- Based on the general definition of context, reference literature for wireless communication, the Author specifies in detail the information including the Context Awareness model, generic cycle model for radio context management, context information gathering and its using (e.g. in cited Content

Awareness Radio Access Technology – CRAT). The conclusion from this analysis is the need to use AI/ML in the context of information gathering and utilization.

Ad b- In order to answer to the Question 2, the Author presents a general classification of ML methods along with a description of the essence of these methods and examples of their application in relation to Context Awareness presented in the literature.

Ad c- The next subsection concerns the analysis of knowledge regarding the use of ML to improve individual sensing performed by node, ML algorithms enhancing the properties of cooperative sensing with particular emphasis on the issues of using neural networks, and reducing the complexity of AI/ML algorithms. The main conclusion from these considerations is: ML can significantly increase SS efficiency.

Ad d- The use of ML enables not only the determination of the current occupation of radio resources, using SS, but also make it possible prediction of the status of radio channels in subsequent reference to time, frequency and spatial dependencies. This is discussed in terms of graphical interpretation of the signal in these domains and the use of pattern recognition.

Ad e- Design trade-offs and Recommendations are identified versus Reliability, Power Consumption, Incomplete Information, and Quality Database.

In Chapter 2, the possibilities of improving the quality of autonomous sensing through the use of ML are presented. Firstly some standard methods are discussed, like Energy Detection, and two algorithms were selected: kNN and RF (Random Forest). The Author proposes new detection algorithm for the 5G-downlink signal presence using above ML methods and Energy Value – based decision making, where the energy of subsequent blocks of N received samples is determined, forming the EV vector for a given data set. To compare the properties (detection probability and false alarm probability) of ED-based ML and EV-based ML and both classes of algorithms, an experiment was conducted where MATLAB was used for signal, channel, detector and calculation simulations, and ML algorithms were implemented using Python scikit-learn library. Additionally, in the decision-making phase, implementations of SVM and Gaussian NB algorithms were modelled. In the simulation scenario, a channel model with AWGN, fading and shadowing effect was used.

Based on the research, the following conclusions were drawn:

- EV-based ML performs better than ED- based ML for higher SNR,
- Application both ML methods increases the probability of detection.

Chapter 3 concerns improvement of autonomous SS by application Neural Network-based DL methods. The chapter presents the following: DL concept for spectrum occupancy detection and prediction (SS & SP), new DL algorithms for SS and SP, new DL algorithm for spectrum occupancy prediction combined with fading level occupation.

The NN-based algorithm can perform only single Resource Block (RB) classification, while RNN classifies several following blocks but for single frequency only. The most complex CNN algorithm can classify multiple RBs in time and frequency domains. Additionally, Primitive Algorithm is proposed for evaluation of prediction improvement. In simulations, plots of P_d and P_{fa} vs SNR have been obtained.

In the first part of chapter, the author examines different DL methods, namely Neural Network (NN), Recurrent Neural Network (RNN), and Convolutional Neural Network (CNN) algorithms. Their application and performance in SS and SP are compared and advantages and disadvantages are noted. A simple baseline method, used for results comparison of SP is proposed.

In the second part of this chapter the author focuses on one chosen DL method, namely CNN applied for both SS and SP. Here, a fading level estimation at the receiver is proposed CNN-based algorithm designed by the Author. Optimization of the fading level threshold for the spectrum occupancy decision making is discussed, and its impact on the SS and SP results is analysed. The obtained results show the high effectiveness of the proposed solution, preventing the hidden node phenomenon.

Chapter 4 consists of the design and application of Federated Learning (FL) to SS. The Author's proposed FL-based SS offers advantages over alternative schemes, including higher decision quality, better spectrum prediction, data privacy, and the ability to build an universal model for all SUs, making it suitable for new users.

In Chapter 5, Author explored the effects of label-flipping random and coordinated attacks on FL-based SS. A new method for continuous monitoring, detection, and elimination of attacked models is proposed, using statistical tests for the SUs' models similarity, as well as clustering of these tests results. The author concluded that extremely aggressive attacks increasing the FL-based SS false alarm rate and very mild attacks were hard to detect decreasing the true-positive detection rate. Proposed solution ensures the attack detection and mitigation is very effective (nearly 100% detection for moderately aggressive attacks). Moreover, the complexity of the author's proposed method is not particularly high. Next she then indicates further research in terms of the heterogeneity of attacks.

The conclusions in Chapter 6 are clearly. In the reviewer's opinion, the Author's generalized final conclusions are very accurate, and should be cited:

"ML can improve the performance of spectrum detection implemented in autonomous sensors. This is especially true for DL methods designed by the author for 5G communication systems based on CNNs. These new methods are also capable of RBs occupancy prediction, which allows to better protect the PU transmission or better utilize the resources by SUs. The new cooperative SS methods based on CNNs in each sensor and FL algorithm proposed by the author can perform even better than the autonomous ones. Furthermore, in such a scenario, new incoming SUs can take advantage of the global FL model without the need for extensive data collection and training of the local model. Although FL assures data privacy by design, it is still prone to poisoning attacks. The new proposed anomaly detection method based on the application of statistical tests for model similarity and clustering for genuine and attacked models is capable of detecting attackers and compensating for their harmful effects on FL-based SS."

It should therefore be stated that the set goals have been fully achieved. All of Author's solutions are her scientific achievements (confirmed by simulation experiments). They show a great practical importance and can be used in future network implementations.

The assessment of correctness and the list of shortcomings are included in point 4 of review.

3. Knowledge of the candidate

Whole dissertation confirm very good general knowledge of the candidate in the discipline of Information and Communication Technology. Introduction and first chapter demonstrate extensive knowledge of wireless communications, next-generation network standards, AI/ML solutions and their practical applications in these networks, allowing for the identification of gaps and the formulation of the scope and solution of the dissertation is confirmed in Introduction and Chapter 1. Chapters 2-5 contain the author's solutions to problems related to these objectives, including an explanation of the scientific and research context, a description of the solution and its simulation tests, an interpretation of their results, and conclusions. Chapter 6 contains overall conclusions.

The dissertation is characterized by very high quality of both substantive content from the point of view both scientific and practical significance of solutions, their novelty, but also substantive and linguistic correctness. Also noteworthy is the diligence and exceptional care for the editorial side. Overall, the presented dissertation is a complete work on very high level, and bears the marks of an outstanding work.

The reference analysis leads to the conclusion that list do not include publications from 2023-2024. Thus, the SOTA review can't take into account the latest achievements in the use of AI//ML techniques in the field of wireless communication. However, based on reviewer's knowledge, it can be stated that

the analysis carried out in the dissertation fully justifies the high value of the proposed solutions and obtained results. This is confirmed by the two most recent (not listed) Author's publications in IEEE Communications Magazine (2023) and IEEE JSAR (accepted for publication in 2025).

Moreover, the Author's publication record is significant and includes eight articles in foreign journals, one chapter in a book published by Springer, one paper at an international conference proceedings and four post-conference papers (in Polish *Przegląd Telekomunikacyjny* and *Wiadomości Telekomunikacyjne*).

Here, it can be assumed a significant Candidate's contribution (first on the list of authors apart from two titles) that concern research related to the topic of the dissertation. Particularly noteworthy are articles published (including those accepted for publication) in international journals published by IEEE (*Journal of Selected Areas in Communication, Communication Magazine, Wireless Communications Letters, Access*). It testifies to the Author's deep knowledge, broad understanding of the subject, and excellent ability to extract and generalize knowledge contained in the publications listed in the references.

4. Other remarks

Regardless of the very high assessment, the reviewer would like to point out several shortcomings of the dissertation.

These include:

- the aforementioned lack of foreign references from years 2023-2024,
- unclear way of adopting neural network structures and their parameters for each use case,
- incorrect text layout on page 63 where the reference to Figures 10 and 11 precedes the description of Figures 8 and 9,
- lack expression for FL global model creation (para 2 in 5.4) or explanation of "averaging weights γ_n " (it is also usen in last paragraph on p.112).

The reviewer also noticed a few minor errors:

- p. 12 "processing process" (paragraph before Fig.1.1)
- p.13 second para. should be "such as for example"
- p.15 no explanation of A2-A4 RSRQ
- p. 18 should be K-means (sentence 6 in "Clustering"),
- p.25 no explanation of PCA (para.3),
- p.37 should be "Radio Environment Map" as proper name,
- p. 59 should be "preceding" instead "preceded",
- para.1 in 3.2.2 second word "model" is unnecessary,
- missing variable in formula (3.3) e.g *thr*=
- p.112 last para.: is the reference to fig.5.1 correct or maybe it should be fig.4.1?
- p. 120 last para.: is the value 70% correct, maybe it should be 75% (as in Table 5.2)?

5. Conclusion

Taking into account what I have presented above and the requirements imposed by Article 13 of *the Act of 14 March 2003 of the Polish Parliament on the Academic Degrees and the Academic Title* (with amendments)[1], my evaluation of the dissertation according to the three basic criteria is the following:

[1] http://www.nauka.gov.pl/g2/oryginal/2013_05/b26ba540a5785d48bee41aec63403b2c.pdf

A. Does the dissertation present an original solution to a scientific problem? (the selected option is marked with **X**)

[X]	[ ]	[ ]	[ ]	[ ]
Definitely YES	*Rather yes*	*Hard to say*	*Rather no*	*Definitely NO*

B. After reading the dissertation, would you agree that the candidate has general theoretical knowledge and understanding of the discipline of **Information and Communication Technology**, and particularly the area of **AI/ML applications in CR-based communication**?

[X]	[ ]	[ ]	[ ]	[ ]
Definitely YES	*Rather yes*	*Hard to say*	*Rather no*	*Definitely NO*

C. Does the dissertation support the claim that the candidate is able to conduct scientific work?

[X]	[ ]	[ ]	[ ]	[ ]
Definitely YES	*Rather yes*	*Hard to say*	*Rather no*	*Definitely NO*

Taking into account general impression of the Author's contribution, the style of presenting the problems and the results obtained, the novelty of the proposed solutions, their quality and scientific value I **recommend to distinguish** the dissertation for its high quality.

Signature