

# Rozpoznawanie urządzeń i wykrywanie nieautoryzowanego poboru energii elektrycznej na podstawie pomiaru napięcia

Zdzisław Kowalczyk, Marek Grzegorek

Politechnika Gdańska, Wydział Elektroniki, Telekomunikacji i Informatyki, Katedra Systemów Decyzyjnych i Robotyki, ul. Narutowicza 11/12, 80-233 Gdańsk, Polska

**Streszczenie:** W pracy rozpatrywany jest problem wykrywania nieautoryzowanego poboru energii z sieci elektrycznej przez identyfikację podłączonych urządzeń. Estymacja stanu sieci, rozumianej jako zbiór podpiętych układów, wraz z ustaloną listą urządzeń dopuszczonych, pozwala określić, czy w danej chwili ma miejsce pobór nieautoryzowany. W celu wykrywania urządzeń, proponuje się wykorzystać prostą metodę opartą na analizie wysokoczęstotliwościowego szumu elektromagnetycznego (EMI) indukowanego w sygnale napięcia zasilającego. Rozwiązanie to pozwala na centralny pomiar, w jednym miejscu – bez konieczności instalacji czujników w licznych punktach potencjalnego poboru prądu. Bazując na danych pomiarowych sygnału EMI, zrealizowano symulator syntezujący dane przypominające rzeczywiste spektrogramy. Dzięki zastosowaniu symulatora możliwe jest uzyskanie informacji o stanie sieci w różnych konfiguracjach w celu przeprowadzenia procedury projektowania detektora z użyciem uczenia pod nadzorem, co również jest prezentowane w pracy.

**Słowa kluczowe:** wykrywanie oszustw, nieinwazyjne monitorowanie obciążenia, wykrywanie urządzeń

## 1. Wprowadzenie

Problem wykrywania oraz rozpoznawania urządzeń podłączonych do sieci elektrycznej jest istotnym elementem takich zadań inżynierskich, jak bezinwazyjny pomiar prądu [4], rozpoznawanie aktywności, czy wykrywanie nadużyć. Aby przypisać zużycie energii do danego odbiornika, potrzebna jest informacja, kiedy urządzenie zostało włączone lub zmieniło tryb pracy. Zasadniczym zagadnieniem poruszonym w tej pracy jest wykrywanie nadużyć, jednak metody pomiaru i analizy danych mogą mieć zastosowanie również w innych wymienionych zadaniach.

Nieautoryzowany pobór energii elektrycznej powoduje straty finansowe właścicieli obiektu. Wykrycie kradzieży może istotnie ograniczyć wydatki, w szczególności w skali przemysłowej. Dodatkowo ze względu na przepisy przeciwpożarowe, w niektórych budynkach podłączanie urządzeń elektrycznych powinno być ograniczone. Przykładowo, w Schronisku "Murowaniec" znajdującym się w Tatrzańskim Parku Narodowym, podłącza-

nie urządzeń elektrycznych możliwe jest jedynie w wyznaczonym miejscu, a ponadto istnieją ograniczenia co do rodzaju sprzętu. Podłączanie urządzeń o wysokim ryzyku wywołania pożaru, takich jak grzałki, jest całkowicie zabronione.

W pracy zweryfikowano rozwiązanie oparte na pomiarze wysokoczęstotliwościowego szumu w sygnale napięcia wraz z systemem decyzyjnym wyuczonym na symulatorze. Symulator zaprojektowano na podstawie uzyskanych danych pomiarowych tak, aby wiernie oddawał wpływ pracy urządzenia elektrycznego na napięcie zasilania. System decyzyjny przetestowano zarówno na danych z symulacji, jak i na pomiarach rzeczywistych zebranych w lokalu mieszkalnym.

Zasadnicza część pracy podzielona została następująco: w rozdziale drugim opisano przedstawione w literaturze metody związane z wykrywaniem oraz rozpoznawaniem urządzeń podpiętych do sieci, w rozdziale trzecim przedstawiono zaproponowaną metodę wykrywania nadużyć, zaś w rozdziale czwartym przedstawiono uzyskane wyniki. W ostatnim rozdziale podsumowano efekty pracy oraz wskazano dalsze kierunki badań.

### Autor korespondujący:

Zdzisław Kowalczyk, [zdzislaw.kowalczyk@eti.pg.edu.pl](mailto:zdzislaw.kowalczyk@eti.pg.edu.pl)

### Artykuł recenzowany

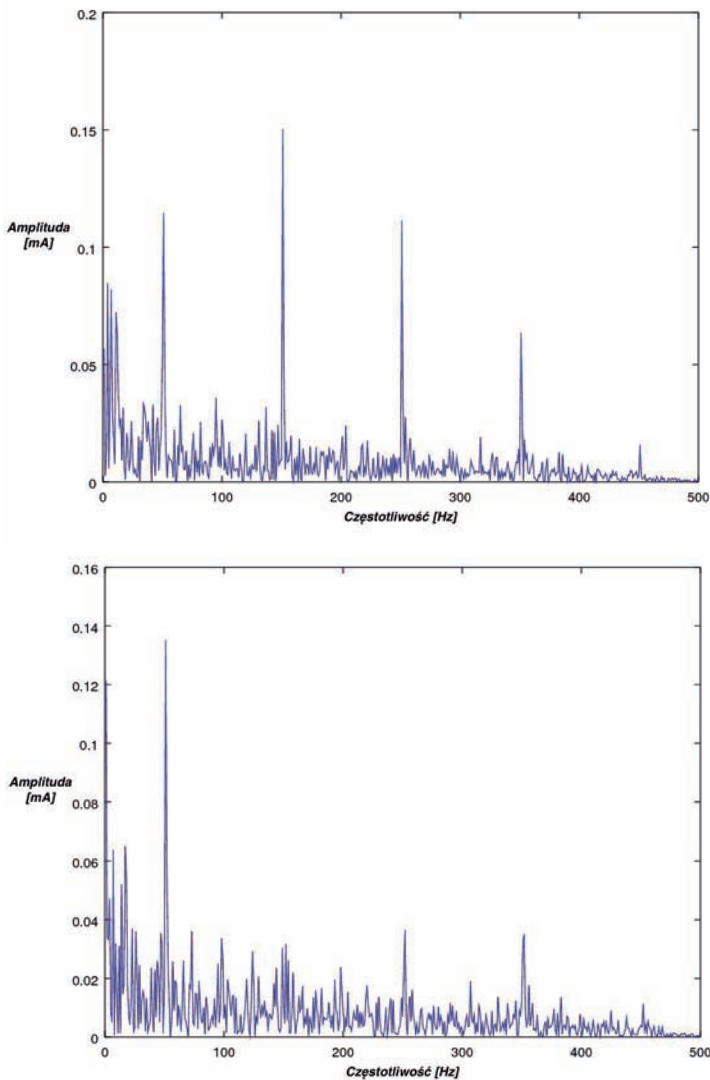
nadesłany 09.09.2020 r., przyjęty do druku 25.11.2020 r.



Zezwala się na korzystanie z artykułu na warunkach licencji Creative Commons Uznanie autorstwa 3.0

## 2. Stan wiedzy

Metody wykrywania i rozpoznawania podpiętych do sieci urządzeń elektrycznych, można podzielić ze względu na sposób pomiaru oraz rodzaj mierzonych sygnałów. Rozróżnia się metody oparte na pomiarze rozproszonym lub jednopunktowym. Pomiar rozproszony polega na instalacji czujników



Rys. 1. Widmo szumu przejściowego monitora LCD (górną) oraz telewizora (dół). Duża różnica w szumie przejściowym pozwala na określenie, które urządzenie zostało włączone

Fig. 1. Spectrum of the transient noise of the LCD monitor (top) and the TV set (bottom). The big difference in the transient noise allows determining which device was switched on

przy każdym odbiorniku z osobną lub przy listwie łączącej niewielką liczbę urządzeń. Rozwiązanie to pozwala na określenie stanu sieci z dużą dokładnością, jednak wymaga dużej liczby czujników i znacznej ingerencji w instalację elektryczną. Z tego powodu rozwinięto metody wykorzystujące pomiar jednopunktowy, które pozwalają na pomiar bezinwazyjny, tj. bez istotnej modyfikacji instalacji elektrycznej.

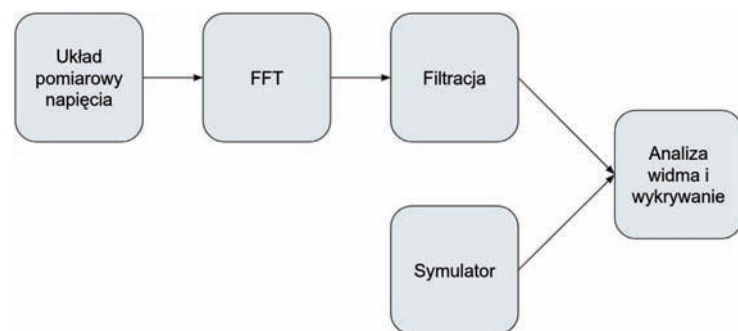
Klasyfikacja ze względu na rodzaj mierzonego sygnału uwzględnia metody oparte na pomiarze napięcia lub prądu, a także rozwiązania, w których analizowane są szumy przejściowe [3] (rys. 1) lub ciągłe [1] (rys. 4). Wykonywany równoległe pomiar napięcia może być dokonany bezinwazyjnie, natomiast (szeregowy) pomiar prądu wymaga ingerencji w sieć lub zastosowanie czujników opartych na efekcie Halla. W zależności od typu, podłączane urządzenia generują szum przejściowy, związany na przykład z przełącznikami mechanicznymi, lub szum ciągły, pochodzący na przykład z pracy silników AC lub zasilaczy pulsacyjnych. Należy zaznaczyć, że rozwiązania oparte na analizie szumu przejściowego oraz ciągłego są raczej metodami komplementarnymi, a nie konkurencyjnymi, ponieważ z góry trudno ocenić, która z nich lepiej

nadaje się do wykrywania momentów włączenia lub wyłączenia określonego typu urządzenia.

Blisko związana z omawianą problematyką jest metoda zaproponowana przez UbiComp Labs [1], polegająca na pomiarze i analizie wysokoczęstotliwościowego szumu elektromagnetycznego w sygnale napięcia. Wykorzystuje się tu fakt, że wiele nowoczesnych odbiorników ma energooszczędne zasilacze pulsacyjne. Zasilacze te z uwagi na swoją specyficzną zasadę pracy, wprowadzają do sieci elektrycznej mocno charakterystyczny szum wysokoczęstotliwościowy. Dwa różne urządzenia, nawet tego samego typu, wprowadzają na tyle odmienny szum, że możliwe jest ich rozróżnienie po przeanalizowaniu widma sygnału napięcia, a także trybu pracy konkretnego urządzenia [2]. Podobnie jak zasilacze pulsacyjne, także silniki prądu zmiennego wprowadzają unikatowy dla danego urządzenia szum. Zatem odbiorniki tego rodzaju można wykrywać przy użyciu tej samej metody. Wnoszony szum można wykryć nawet bez dedykowanego układu pomiarowego, jeżeli tylko dostępny jest wzmacniacz i głośniki o dużej mocy. Po odpowiednim zwiększeniu wzmocnienia takiego sygnału, łatwo można usłyszeć szum trwający w czasie podłączenia (podpięcia) ładowarki do laptopa lub innego aparatu z zasilaczem impulsowym do gniazdka sieci. Po odłączeniu urządzenia, szum się wyraźnie zmniejsza. Takie właśnie rozwiązanie będzie zastosowane w dalszej części pracy jako podstawowe przy wykrywaniu nieautoryzowanego poboru energii elektrycznej.

### 3. Przyjęta metoda

Oczywiście trudno jest zapewnić warunki badań, w których nie następuje włączenie urządzenia bez wiedzy eksperymentatora. Z tego względu, na tym etapie badań zdecydowano, aby mierzyć szum generowany przez zestaw urządzeń testowych, z pełną wiedzą odnośnie czasu ich pracy, zaś następnie przygotować symulację umożliwiającą uwzględnienie rozmaitych scenariuszy. Umożliwiono między innymi dobór zakresu częstotliwości, w którym mieszczą się szumy urządzenia, oraz zmianę tego zakresu w trakcie pracy – ciągłą, jak w przypadku urządzeń z silnikami prądu zmiennego, lub skokową, co jest typowe dla niektórych urządzeń elektronicznych. W ten sposób można dowolnie zmieniać charakterystykę wirtualnych urządzeń, które można też swobodnie włączać i wyłączać. Dzięki temu uzyskano w pełni oznaczone dane, zbliżające warunki badania do sytuacji rzeczywistej i pozwalające na szerszą ocenę jakości proponowanej metody analizy diagnostycznej, której ogólny schemat przedstawiono na rys. 2.



Rys. 2. Schemat badania oraz weryfikacji metody wykrywania urządzeń elektrycznych (na podstawie pomiarów)

Fig. 2. Scheme of testing and verification of the method of detecting electrical devices (based on measurements)

### 3.1. Układ pomiarowo-diagnostyczny

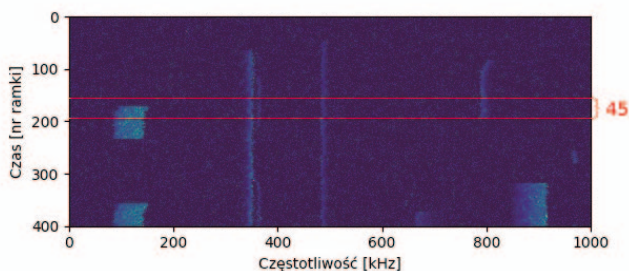
Według polskich standardów, napięcie sygnału elektrycznego sieci cechuje amplituda 230 V i częstotliwość 50 Hz. Dopuszczalny zakres mierzonego sygnału napięcia powszechnie dostępnych przetworników analogowo-cyfrowych (ADC) mieści się w granicy od kilku do kilkudziesięciu woltów. Z tego względu zastosowano analogowy filtr górnoprzepustowy przepuszczający składowe powyżej około 1 kHz, usuwając główną składową sygnału napięcia i jej harmoniczne oraz otrzymując na wyjściu sygnał o amplitudzie dopasowanej do zakresu przetwornika ADC. Odfiltrowanie wszystkich składowych sygnału poniżej 1 kHz nie zmniejsza skuteczności przyjętego rozwiązania, gdyż zasilacze impulsowe oraz silniki prądu zmiennego wprowadzają charakterystyczny szum na wyższych częstotliwościach. W prezentowanej implementacji, tak zmodyfikowany sygnał napięciowy podawany jest na wejście 12-bitowego przetwornika ADC, działającego z częstotliwością 2 milionów próbek na sekundę. Następnie skonwertowany i przesłany do komputera sygnał podlega analizie FFT odcinkami o szerokości 2048 próbek, prowadząc do wygenerowania kolejnych ramek widma. Odcinki tworzone były z 2% nakładaniem się, tj. ze skokiem co 1536 próbek. Zbierany spektrogram sygnału jest dalej wygładzany w czasie na każdej z częstotliwości z osobna (filtracja na rys. 2). Wygładzanie spektrogramu oparto na filtracji medianowej z oknem 20 ramek widmowych. Schemat takiego przetwarzania przedstawiono na rys. 3.



Rys. 3. Schemat systemu pomiarowo-diagnostycznego  
Fig. 3. Diagram of the measurement and diagnostic system

### 3.2. Symulacja

Po zmontowaniu urządzenia pomiarowo-diagnostycznego i zebraniu pomiarów przy kontrolowanym włączaniu i wyłączeniu urządzeń testowych, uzyskano obserwacje dotyczące charakterystyki szumu EMI. W zależności od rodzaju urządzenia, generowany szum może zajmować to samo pasmo częstotliwości przez cały czas pracy urządzenia. Może też – w pewnych trybach pracy – podlegać ciągłym i powolnym zmianom (jak w przypadku odkurzacza i innych urządzeń z silnikami AC), albo zmianom skokowym (jak to się dzieje w przypadku konsoli PlayStation 3). Mając na uwadze powyższe obserwacje, zrealizowano symulator przebiegu widma sygnału zasilania analizowanego układu (przykładowy wynik zilustrowano na rys. 4).



Rys. 4. Przykładowy spektrogram wygenerowany w symulatorze. Na rysunku zaznaczono przykładową paczkę pomiarową, na podstawie której wykrywane i rozpoznawane są urządzenia

Fig. 4. Sample spectrogram generated in the simulator. The figure shows an example of a measuring package based on which devices are detected and recognised

Proces generowania przebiegu widma polega na losowaniu urządzeń oraz ich parametrów. Następnie w każdym kroku losowane są zdarzenia włączenia i wyłączenia poszczególnych urządzeń oraz zmiany trybu pracy. W celu przybliżenia warunków rzeczywistych, każde z urządzeń działa z nałożonym z góry, minimalnym czasem pracy w danym trybie. Użytkownik przed rozpoczęciem syntezy spektrogramu może określić liczbę i typ urządzeń oraz czas trwania. Historia zmian stanów urządzeń jest przechowywana w pamięci systemu, co ułatwia automatyczny pomiar skuteczności metod detekcji oraz rozpoznawania urządzeń.

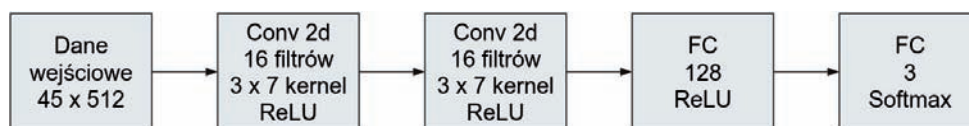
### 3.3. Wykrywanie

W projekcie założono brak informacji o zestawie podłączanych urządzeń. Z tego względu, w przyjętym rozwiązaniu najpierw wykrywane jest podpięcie, bądź odłączenie urządzenia a następnie analiza zmiany w celu ustalenia tożsamości urządzenia. Wykrywanie urządzeń polega na przetworzeniu widmowej paczki pomiarowej (rys. 4), złożonej z 45 kolejnych ramek widma (odpowiadające mniej więcej 0,1 sekundy mierzonego sygnału napięcia), przez zaprojektowaną splotową sieć neuronową. Rozpoznanie urządzenia polega na (komparatywnym) wykrywaniu częstotliwości, na których nastąpiła istotna zmiana. Należy zauważyć, że żadne dotrenowanie sieci neuronowej dla nowych urządzeń nie jest wymagane, gdyż jej wyjście determinuje włączenie lub wyłączenie określonego urządzenia (zaś klasyfikacja przeprowadzona jest bez nadzoru).

Zastosowana w procesie wykrywania sieć neuronowa zbudowana jest z dwóch warstw splotowych z 16 filtrami i wymiarem filtra  $3 \times 7$  (odpowiednio dla wymiaru czasu i częstotliwości) oraz warstwy w pełni połączonej o 128 neuronach. Wyjście sieci służy klasyfikacji obecnego okna pomiarowego do jednej z trzech kategorii: (1) włączenia bądź (2) wyłączenia urządzenia lub (3) braku zmiany stanu sieci elektrycznej. Z uwagi na zastosowanie przesuwającego się okna pomiarowego, zachodzi niebezpieczeństwo wielokrotnego wykrywania tego samego zdarzenia. Z tego względu, włączenie i wyłączenie urządzenia jest sygnalizowane jedynie w sytuacji, gdy zachodzi w chwili odpowiadającej środkowej ramce widma z okna pomiarowego (dla 45 ramek w paczce pomiarowej, jest to 23 ramka widma, przypadająca na połowę czasu potrzebnego do zebrania pełnego okna). Przy minimalnym przesunięciu, nie nastąpi wykrycie zmiany. Jako alternatywne rozwiązanie można zastosować również inne metody, np. typu non-maximum suppression [8]. We wszystkich warstwach wykorzystano funkcję aktywacji *Relu*. Schemat architektury, zaimplementowanej z użyciem biblioteki Jax, przedstawiono na rys. 5. Do optymalizacji parametrów sieci zastosowano algorytm ADAM [5] z domyślnymi ustawieniami. W celu wyuczenia sieci neuronowej, ze zbioru wygenerowanych w symulatorze spektrogramów, wyodrębniono okna pomiarów, każde złożone z 45 kolejnych ramek widma, przypadające na każde z trzech możliwych zdarzeń. Uczenie sieci trwało 10 tysięcy iteracji, przy czym w każdej z nich parametry sieci uaktualniano na podstawie 32 przypadków, podzielonych na poszczególne kategorie<sup>1</sup>.

Jeśli dana paczka pomiarowa zostanie pozytywnie sklasyfikowana przez sieć neuronową (jako jeden ze zdefiniowanych przypadków określających zmianę stanu urządzenia), obliczana jest różnica między drugą a pierwszą połową analizowanego

<sup>1</sup> Realizowane jest tu wsadowe przetwarzanie danych w postaci 32 przykładów, równoległe przepuszczanych przez sieć, zaś na ich podstawie obliczany jest gradient funkcji kosztu względem parametrów sieci, który jest niezbędny do aktualizacji parametrów.



Rys. 5. Architektura wykorzystanej sieci neuronowej: Conv 2d oznacza dwuwymiarową warstwę spłotową, zaś FC – warstwę w pełni połączoną o podanej liczbie neuronów

Fig. 5. Architecture of the neural network used: Conv 2d means a two-dimensional convolution layer, and FC – a fully connected layer with a given number of neurons

spektrum (dla każdej częstotliwości z osobna). Następnie przez progowanie, wyodrębniany jest zbiór częstotliwości (na których zachodzi istotna zmiana), charakteryzujących dane urządzenie. Zatem albo zbiór ten przypisywany jest do nowego urządzenia, albo pozwala zidentyfikować urządzenie istniejące w bazie danych systemu. W przypadku zebranych danych dla sześciu urządzeń, metoda ta pozwoliła bezbłędnie zidentyfikować wszystkie urządzenia.

W celu wykrycia nieautoryzowanego poboru, wydaje się, że istnieją co najmniej dwie możliwości. Pierwsza wymagałaby rejestracji każdego autoryzowanego urządzenia i wpisywania do bazy. Druga metoda polegałaby na rejestracji urządzeń przez pewien okres testowy, w którym zakładamy, że nie ma poboru nieautoryzowanego. Gdy podłączy się „obce” urządzenie, które nie zostało zarejestrowane w okresie testowym, zasygnalizowany zostanie nieautoryzowany pobór.

## 4. Wyniki

Wycuczony model przetestowano na innych zsyntezowanych w symulatorze przebiegach (nieznajdujących się w zbiorze uczącym), jak również danych pomiarowych. Dokładność wykrywania momentu włączenia i wyłączenia wyniosła odpowiednio 91% oraz 72% dla danych syntetycznych i rzeczywistych. W trakcie pomiarów użyto sześciu urządzeń testowych, tj. obwodów światła w pokoju i w korytarzu, telewizora, monitora, konsoli PlayStation 3 oraz odkurzacza. Oznaczono 40 zmian stanu włączenia urządzenia (ON/włączenie bądź OFF/wyłączenie) i na podstawie tych danych sprawdzono skuteczność działania sieci neuronowej. Wyniki symulacyjne można było uśrednić korzystając z wygenerowanych 1000 przypadków. Należy zaznaczyć, że architekturę sieci opracowano i proces jej uczenia przeprowadzono na podstawie danych z symulatora, bez użycia danych rzeczywistych – zgodnie z zasadą uczenia maszynowego, która sugeruje, aby testować model na innym zbiorze danych niż zbiór danych uczących (kształtujących model). Dlatego należy oczekiwać, że otrzymany wynik powinien się potwierdzić w nowych eksperymentach rzeczywistych (również będących spoza zbioru testowego). Jednakowoż gorsze wyniki predykcji przy danych rzeczywistych świadczą o potrzebie kontynuacji prac dotyczących lepszego dopasowania syntetycznych charakterystyk szumowych do urządzeń i pomiarów rzeczywistych.

## 5. Podsumowanie

W pracy przedstawiono rozwiązanie umożliwiające wykrywanie nieautoryzowanego poboru energii elektrycznej. Wpływ urządzeń na wysokoczęstotliwościowy szum w sygnale napięcia został zamodelowany, po czym zrealizowany został symulator, na podstawie którego można było dobrać metody wykrywania i rozpoznawania urządzeń. Rozwiązanie zostało przetestowane na danych z symulacji jak i rzeczywistych, pomierzonych w sieci elektrycznej mieszkania.

Przyjęte rozwiązanie wykorzystuje szumową charakterystykę wysokoczęstotliwościową, której źródłem są zasilacze

urządzeń elektrycznych działających w analizowanej sieci. W sytuacji, kiedy miejsce pomiaru napięcia będzie oddzielone transformatorem od punktu podpięcia urządzenia, szum wysokoczęstotliwościowy może być znacznie wytłumiony – co z kolei może utrudnić lub uniemożliwić wykrycie (podłączenia/odłączenia) urządzeń w przyjętej metodzie. Z tego względu, pożądanym kierunkiem dalszych badań powinno być uwrażliwienie metody na sygnały o stosunkowo niskiej częstotliwości (do kilkudziesięciu kHz). Architektura sieci została tak dobrana, aby umożliwić pracę w czasie rzeczywistym na standardowym mikroprocesorze.

Należy zaznaczyć, że istnieje możliwość zastosowania bardziej złożonej architektury sieci neuronowej. Mogłoby to przełożyć się na poprawę dokładności detekcji zdarzeń nieautoryzowanego poboru energii elektrycznej. Odpowiednią wydajność wnioskowania sieci można by też uzyskać innymi metodami proponowanymi w literaturze na temat uczenia maszynowego, takimi jak restrukturalizacja przez usuwanie niepotrzebnych wag (ang. *pruning*) [6] lub wnioskowanie z użyciem uproszczonych/skwantowanych reprezentacji danych [7], na przykład *float 16* albo *int 8*, zamiast formatu domyślnego, jakim jest *float 32*.

## Bibliografia

1. Gupta S., Reynolds M.S., Patel S.N., *ElectriSense: Single-Point Sensing Using EMI for Electrical Event Detection and Classification in the Home*. [in:] Proceedings of the 12th ACM International Conference on Ubiquitous Computing, 2010, 139–148.
2. Chen K.Y., Gupta S., Larson E.C., Patel S., *DOSE: Detecting user-driven operating states of electronic devices from a single sensing point*. [in:] Proceedings of the IEEE International Conference on Pervasive Computing and Communications, 2015, 46–54, DOI: 10.1109/PERCOM.2015.7146508.
3. Patel S.N., Robertson T., Kientz J.A., Reynolds M.S., Abowd G.D., *At the Flick of a Switch: Detecting and Classifying Unique Electrical Events on the Residential Power Line*. [in:] Proceedings of the 9th International Conference on Ubiquitous Computing, 2007, 271–278, DOI: 10.1007/978-3-540-74853-3\_16.
4. Zeifman M., Roth K., *Non-Intrusive Appliance Load Monitoring: Review and Outlook*. [in:] IEEE Transactions on Consumer Electronics, Vol. 57, No. 1, 2011, 76–84, DOI: 10.1109/TCE.2011.5735484.
5. Kingma D.P., Ba J., *Adam: A Method for Stochastic Optimization*. [in:] arXiv e-prints, 2014.
6. Molchanov P., Tyree S., Karras T., Aila T., Kautz J., *Pruning Convolutional Neural Networks for Resource Efficient Inference*. [in:] arXiv e-prints, 2016.
7. Guo Y., *A Survey on Methods and Theories of Quantized Neural Networks*. [in:] arXiv e-prints, 2018.
8. Neuback A., Van Gool L., *Efficient Non-Maximum Suppression*. [in:] Proceedings of the 18th International Conference on Pattern Recognition, 2006, DOI: 10.1109/ICPR.2006.479.

# Device Recognition and Detection of Unauthorized Electricity Consumption Based on Voltage Measurement

**Abstract:** The paper examines the problem of detecting unauthorized energy consumption from the electric network by identifying connected devices. The estimation of the network condition, understood as a set of connected systems, together with a set list of approved devices, allows to determine whether an unauthorized consumption is taking place at a given moment. In order to detect devices, it is proposed to use a simple method based on the analysis of high-frequency electromagnetic noise (EMI) induced in the supply voltage signal. This solution allows for central measurement in one place – without the need to install sensors in numerous points of potential current consumption. Based on the measurement data of the EMI signal, a simulator was implemented that synthesized data resembling actual spectrograms. Thanks to the use of the simulator, it is possible to obtain information about the state of the network in various configurations in order to carry out the detector design procedure using supervised learning, which is also presented in the paper.

**Keywords:** Fraud detection, non-intrusive load monitoring, appliance detection

## prof. dr hab. inż. Zdzisław Kowalczyk

zdzislaw.kowalczyk@eti.pg.edu.pl  
ORCID: 0000-0001-9174-546X

Prof. dr hab. inż. (2003, 1993, 1986, 1978). Od 1978 r. pracuje na Wydziale Elektroniki, Telekomunikacji i Informatyki Politechniki Gdańskiej, gdzie jest profesorem zwyczajnym automatyki i robotyki oraz Kierownikiem Katedry Systemów Decyzyjnych i Robotyki. Odbił naukowe wizyty na Uniwersytecie Oulu (1985), Australijskim Uniwersytecie Narodowym (1987), Technische Hochschule Darmstadt (1989) oraz na Uniwersytecie George'a Masona (1990-1991). Główne zainteresowania naukowe to automatyka i robotyka, teoria sterowania, adaptacja, modelowanie systemów, identyfikacja i estymacja, diagnostyka, wykrywanie usterek, przetwarzanie sygnałów, sztuczna inteligencja, komputerowe systemy sterowania i informatyka. Jest autorem i współautorem ponad 20 książek (m.in. WNT 2002, Springer 2004-2016, PWNT 2007-2019), około 120 artykułów w czasopiśmie (45 na JCR) oraz ponad 300 publikacji konferencyjnych i rozdziałów książkowych. Liczba cytowań w Google Scholar przekroczyła 25 setek, zaś na JCR – ponad 750 cytowań. Jest prezesem Polskiego Towarzystwa Konsultacyjnego (TKP) i Polskiego Towarzystwa Pomiarów, Automatyki i Robotyki (POLSPAR, NMO IFAC), a także przewodniczący Komitetu Technicznego IFAC ds. Inteligentnych Pojazdów Autonomicznych (TC 7.5). Jest on także członkiem Komitetu Automatyki i Robotyki Polskiej Akademii Nauk. Profesor Kowalczyk od 2003 roku jest założycielem i redaktorem naczelnym wydawnictwa PWNT – Pomorskiego Wydawnictwa Naukowo-Technologicznego. Wśród innych licznych funkcji naukowych jest obecnie redaktorem m.in. magazynów International Journal of Applied Mathematics and Computer Science oraz IEEE Transactions on Cognitive and Developmental Systems. Jest również laureatem nagród Ministerstwa Edukacji Narodowej za 1990 i 2003 r., Nagrody Polskiej Fundacji Nauki Polskiej w 1999 r. w dziedzinie automatyki oraz Medalu Stowarzyszenia Elektryków Polskich SEP w 2014 r. im. Profesora Pawła Jana Nowackiego.



## mgr inż. Marek Grzegorek

marek.grzegorek@pg.edu.pl  
ORCID: 0000-0002-6708-6756

Absolwent Wydziału Elektroniki, Telekomunikacji i Informatyki Politechniki Gdańskiej. Studia magisterskie ukończył w lipcu 2017 r. w dyscyplinie Automatyka i Robotyka w Katedrze Systemów Decyzyjnych i Robotyki Wydziału ETI. Obecnie pracownik tej katedry i uczestnik Studium Doktoranckiego na Wydziale Elektroniki, Telekomunikacji i Informatyki Politechniki Gdańskiej. W przeszłości pracował w firmach Opera Software oraz Amazon realizując projekty, w których wykorzystywał modele uczenia maszynowego do porównywania obrazów oraz syntezy mowy.

