Wyniki:

Eksperymenty zostały przeprowadzone dla 3 metod uczenia modelu ML:

- analizy całości ruchu sieciowego z ekstrakcją prostego zestawu cech: entropia, średnia, odchylenie standardowe
- analizy całości ruchu sieciowego z ekstrakcją pełnego zestawu cech: wariancja, współczynnik skośności, współczynnik Kurtoza, wskaźnik punktów zwrotnych (turning points rate)
- przesuwnego okna  z ekstrakcją pełnego zestawu cech

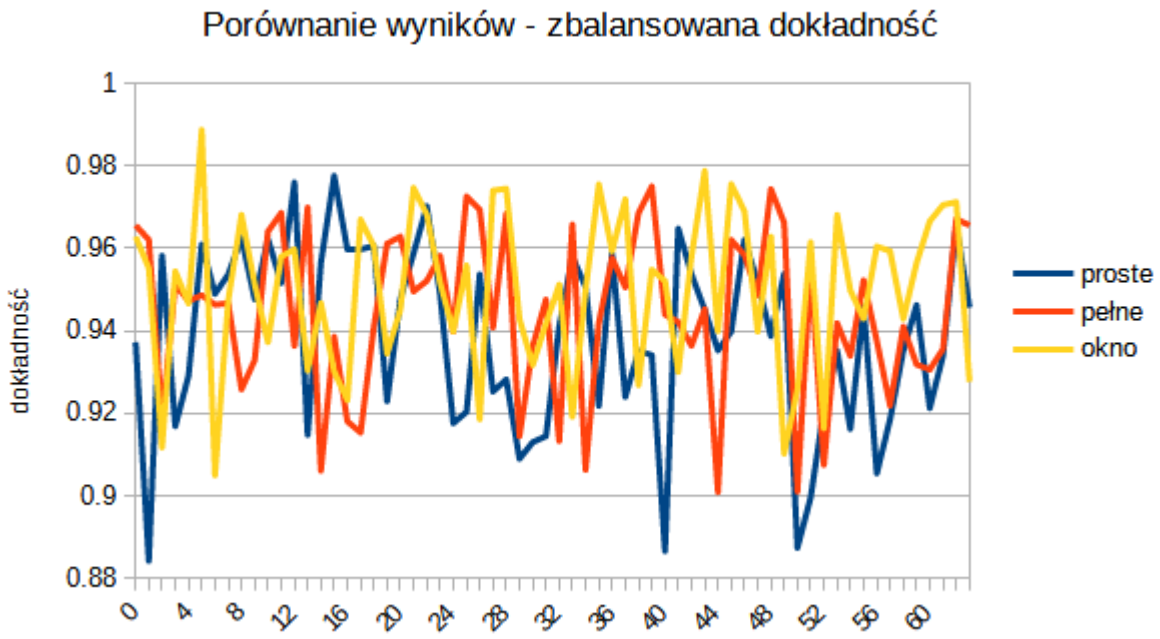
Dla każdej metody predykcję powtórzono 64 razy z podziałem 70%/30% danych treningowych i testowych oraz wyliczona została zwykła i zbalansowana dokładność wykrywania anomalii.

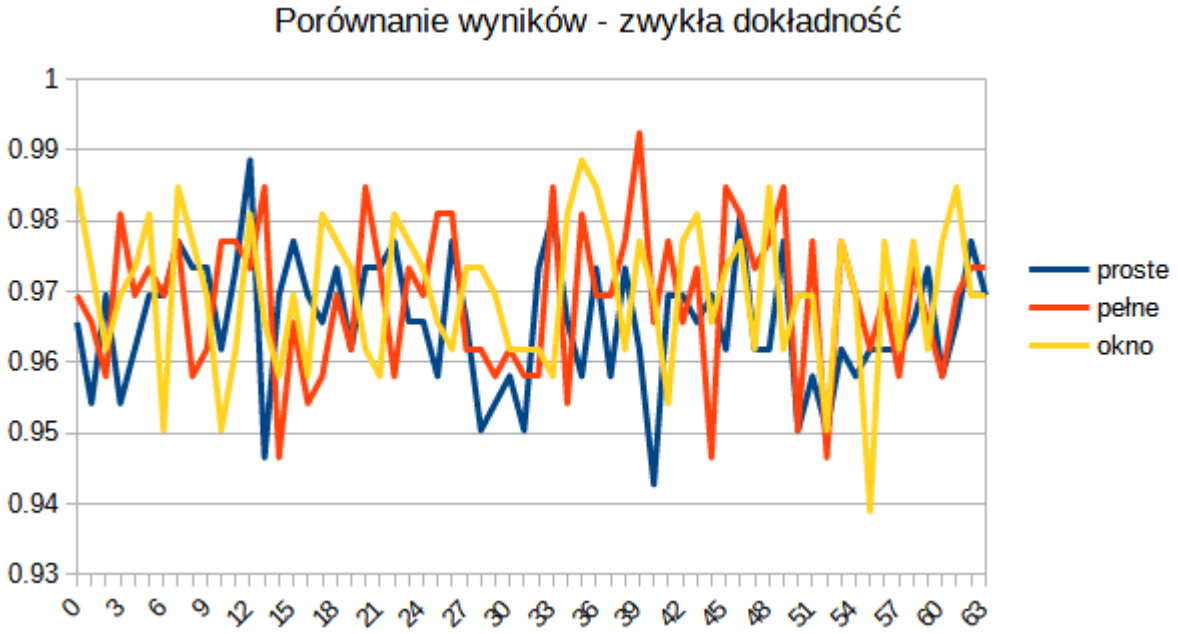
Wyniki eksperymentów zostały przedstawione na wykresach. Pierwsze dwa wykresy przedstawiają porównanie dokładności wykrywania anomalii poszczególnych metod odpowiednio dla zbalansowanej średniej (figura 1) i zwykłej średniej (figura 2). Pozostałe wykresy zawierają porównanie wyników dokładności zbalansowanej i zwykłej dla każdej z metod: analizy całościowej z ekstrakcją prostych cech (figura 3),  analizy całościowej z ekstrakcją pełnych cech (figura 4) oraz przesuwnego okna (figura 5). Dla każdej z metod wyliczono średnią wartość dokładności zbalansowanej i zwykłej, co zostało przedstawione w tabeli 1.

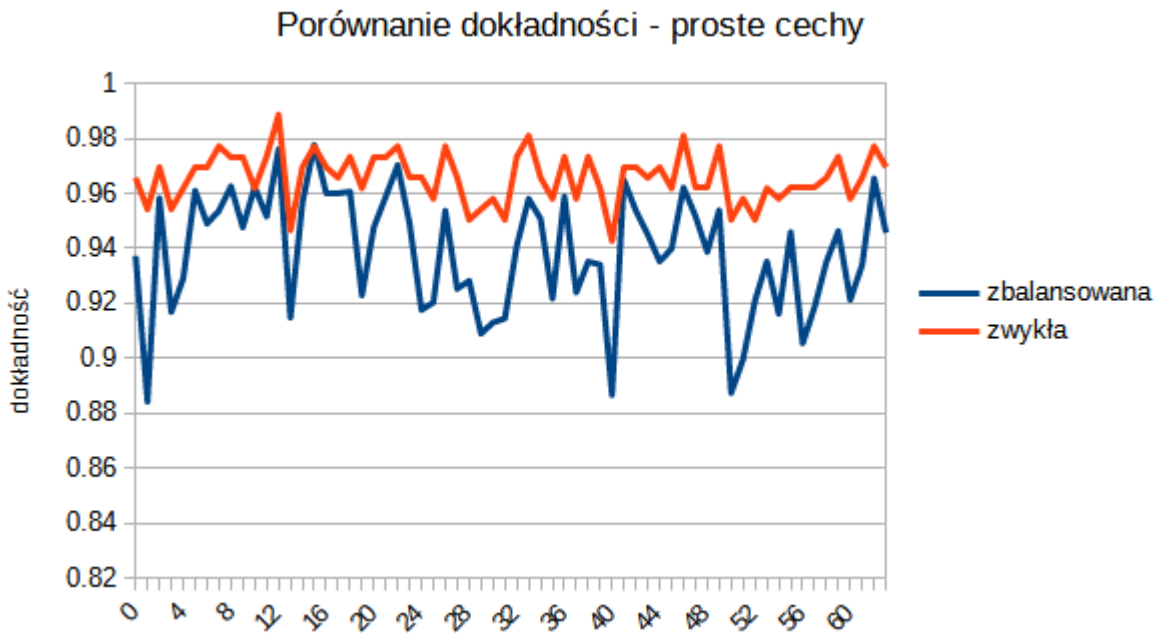
Wnioski:

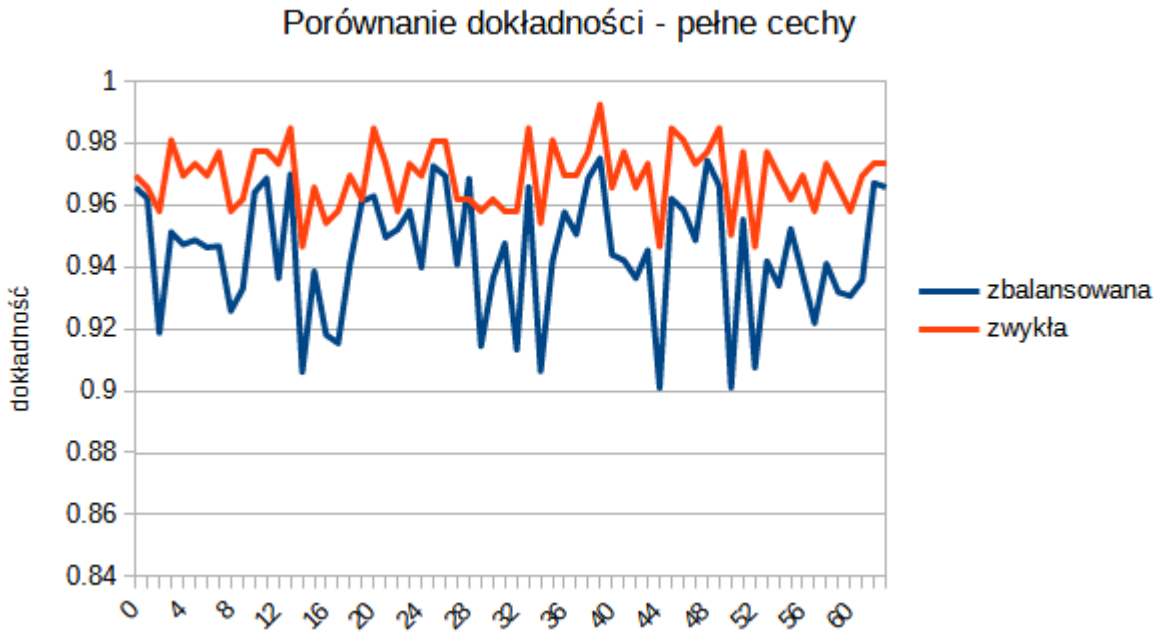
Analiza uzyskanych wyników i wyliczonych statystyk pozwala uzyskać następujące wnioski w zakresie wykrywania anomalii przez modele:

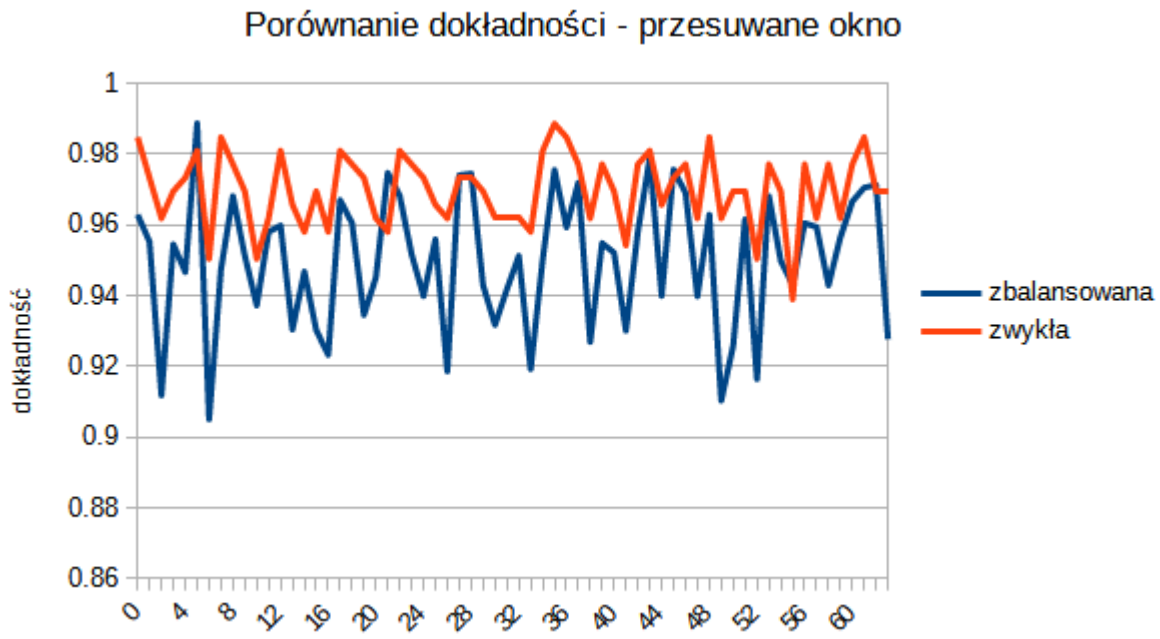
- Wszystkie modele uzyskały wysokie wartości dokładności w wykrywaniu anomalii (powyżej 90%), co oznacza, że wszystkie analizowane metody trenowania modeli pozwalają uzyskać akceptowalne wyniki.
- Całościowa analiza z ekstrakcją prostych cech uzyskała nieco gorsze wyniki dokładności od pozostałych, zarówno dla dokładności zbalansowanej (o ok. 1pp.) i zwykłej (o ok 0.5pp.)
- Metody analizy całościowej z pełnymi cechami i przesuwanego okna uzyskały niemal identyczne wyniki (ok. 95% zbalansowanej i ok 97% zwykłej dokładności)
- Żadna z metod nie uzyskiwała zawsze lepszych lub gorszych wyników od pozostałych dla eksperymentów (to, który algorytm uzyskał najlepszą dokładność, a który najgorszą, było zależne od konkretnego eksperymentu). Nieznaczna różnica w dokładności jest dobrze widoczna jedynie po wyliczeniu średnich z wyników.
- Dla wszystkich metod średnie wyniki dokładności zwykłej były o ok. 2-3pp. wyższe od średnich wyników dokładności zbalansowanej.
- Dla niektórych eksperymentów wyniki dokładności zbalansowanej były wyższe od wyników dokładności zwykłej.
- Ze względu na bardzo wysoką dokładność modelu i to, że kategorie danych nie były bardzo mocno niezbalansowane, do stwierdzenia skuteczności modelu nie jest konieczne wyliczenie dokładności zbalansowanej (można to ocenić już po wynikach zwykłej dokładności).


Porównanie wyników - zbalansowana dokładność
dokładność
1
0.98
0.96
0.94
0.92
0.9
0.88
0
4
8
12
16
20
24
28
32
36
40
44
48
52
56
60
proste
pełne
okno


Porównanie wyników - zwykła dokładność
1
0.99
0.98
0.97
0.96
0.95
0.94
0.93
0
3
6
9
12
15
18
21
24
27
30
33
36
39
42
45
48
51
54
57
60
63
proste
pełne
okno


Porównanie dokładności - proste cechy
dokładność
1
0.98
0.96
0.94
0.92
0.9
0.88
0.86
0.84
0.82
0
4
8
12
16
20
24
28
32
36
40
44
48
52
56
60
zbalansowana
zwykła


Porównanie dokładności - pełne cechy
dokładność
1
0.98
0.96
0.94
0.92
0.9
0.88
0.86
0.84
0
4
8
12
16
20
24
28
32
36
40
44
48
52
56
60
zbalansowana
zwykła




| Typ dokładności | Proste cechy | Pełne cechy | Przesuwane okno |
|---|---|---|---|
| zbalansowana | 93.88% | 94.97% | 95.00% |
| zwykła | 96.56% | 96.89% | 96.98% |