

POLITECHNIKA WROCŁAWSKA  
WYDZIAŁ INFORMATYKI I TELEKOMUNIKACJI



---

# Sieci złożone

---

Sprawozdanie z laboratorium

AUTOR

**Mikołaj Kaźmierczak**

nr albumu: **254287**

kierunek: **Inżynieria systemów**

*28 stycznia 2022*

### Streszczenie

Celem pracy jest sprawdzenie wpływu parametrów sieci komputerowej peer-to-peer na szybkość i zakres rozprzestrzeniania się wirusa komputerowego. Sieć została wygenerowana losowo.

## 1 Wstęp – sformułowanie problemu

W ramach tej pracy zostanie przeprowadzona analiza sieci złożonej peer-to-peer wygenerowanej losowo. Będzie ona polegać na sprawdzeniu jak szybko i w jakim zakresie wirus rozprzestrzeni się w sieci w zależności od określonych właściwości.

## 2 Opis rozwiązania

### 2.1 Sieć ogólnie

Generacja polega na wylosowaniu tysiąca węzłów, a następnie połączeniu ich ze sobą na podstawie najbliższej odległości z węzłami sąsiednimi - zestawia się z określonym węzłem wszystkie pozostałe węzły i wybiera 3 najbliższe. Na koniec sprawdza się czy graf jest spójny: jeśli nie - podgrafy łączy się ze sobą dwoma wierzchołkami które są najbliżej siebie pomiędzy rozłącznymi podgrafami.

### 2.2 Wierzchołki

Każdy wierzchołek ma określoną podatność na wirusa - tak lub nie.

### 2.3 Przebieg symulacji

Istnieją dwa scenariusze rozprzestrzeniania się wirusa:

- Zarażone węzły próbują zarazić wszystkich swoich sąsiadów.
- Węzeł który nie jest podatny na wirusa, po próbie zarażenia zaczyna "rozpowiadać" swoim sąsiadom o zagrożeniu. Następnie powiadomione węzły zaczynają zabezpieczać swoich sąsiadów działając w podobny sposób jak wirus, z tym że z odwrotnym skutkiem.

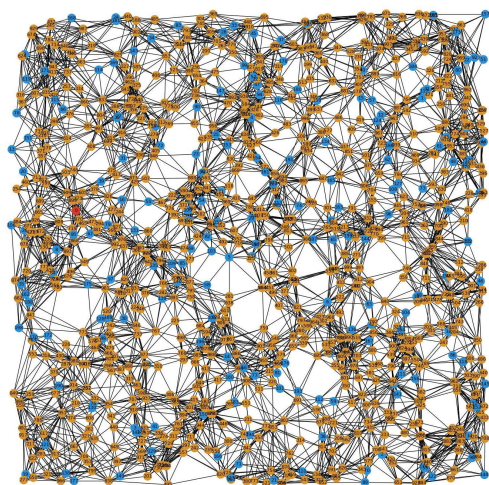
Te dwa scenariusze rozwijają się równolegle i reagują na siebie.

Istotna jest także podjęta decyzja o tym, że jeśli w danej epoce symulacji dochodzi jednocześnie do próby zarażenia i zabezpieczenia węzła, to zostaje on zarażony.

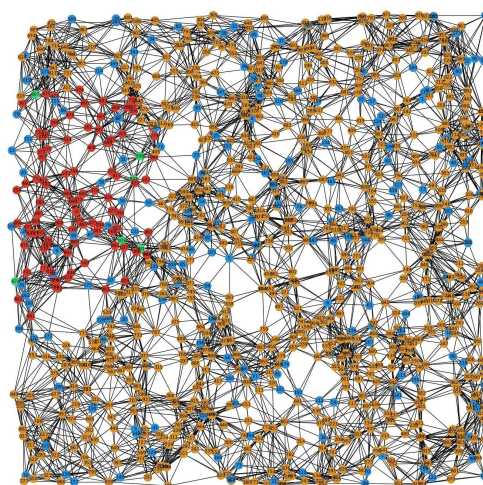
Na rysunku (1.) pokazano przykładowy przebieg symulacji dla sieci w której 20% węzłów jest zabezpieczonych przed zarażeniem wirusem oraz minimalny stopień wierzchołka wynosi 8. Więcej klatek oraz animacji z przebiegu symulacji dla 4 ciekawych kombinacji parametrów sieci znajduje się w załączonym do tego sprawozdania folderze zip (folder */frames*).

Objaśnienie znaczenia kolorów:

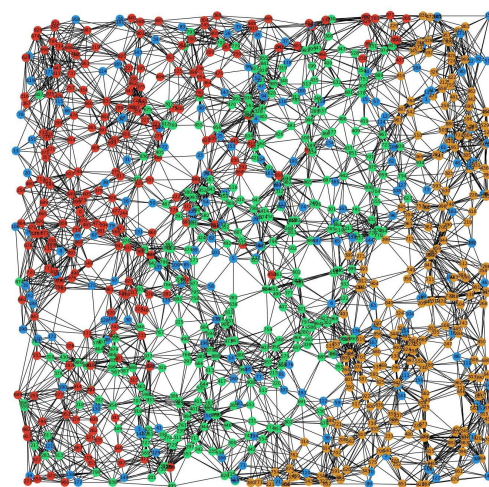
- pomarańczowy - wrażliwość na wirusa
- niebieski - zabezpieczony przed wirusem
- czerwony - zainfekowany
- zielony - poinformowany o zagrożeniu



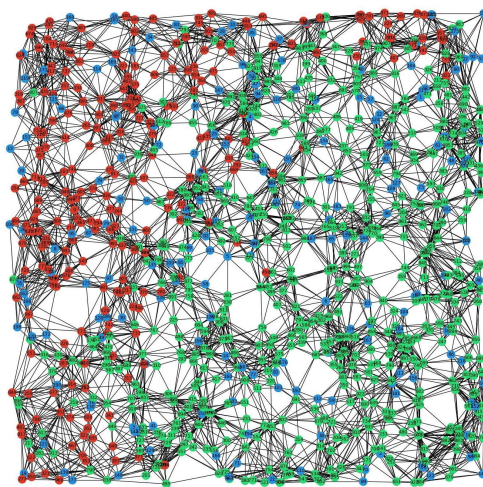
(a) epoka 0 (początek)



(b) epoka 3



(c) epoka 9



(d) epoka 14 (koniec)

Rysunek 1: Przykładowy przebieg symulacji

## 3 Rezultaty obliczeń

### 3.1 Plan badań

Badania wykonano z użyciem metody **Monte Carlo**. Polegały one na sprawdzeniu właściwości sieci przy określonych dla niej wartości parametrów. **Dla każdej kombinacji parametrów wykonano tysiąc powtórzeń.** Wszystkich kombinacji było łącznie 49, co oznaczało 49000 łącznych uruchomień symulacji. Wykorzystany został multiprocessing, dzięki czemu korzystano ze 100% mocy CPU (Ryzen 9 5900X). Czas trwania obliczeń wyniósł około 5h.

Parametry:

- $s$  : ilość zabezpieczonych węzłów wyrażona w procentach  
 $s = (20, 30, 40, 50, 60, 70, 80)$
- $p$  : minimalna ilość połączeń z sąsiednimi węzłami (minimalny stopień)  
 $p = (2, 3, 4, 5, 6, 7, 8)$

### 3.2 Wyniki obliczeń

Zmierzone właściwości:

- ilość zainfekowanych węzłów
- ilość zabezpieczonych węzłów
- długość trwania symulacji w liczbie epok
- ilość krawędzi
- średnią długość najkrótszej ścieżki pomiędzy węzłami

Uśrednione dla każdej kombinacji parametrów wyniki przedstawiono w tabeli (1.).

### 3.3 Analiza wyników

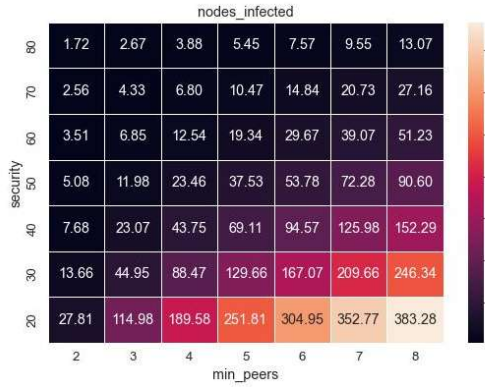
Wyniki wszystkich właściwości dla danej kombinacji parametrów zostały uśrednione dla tysiąca iteracji i przedstawione w tabeli (1.). Zestawiono je na wykresach wraz z wartościami parametrów  $s$  i  $p$  dla danej kombinacji. Rysunek (2.) przedstawia wszystkie zależności.

Wykres (a) przedstawia *promił zainfekowanych węzłów* (wykres (b) jest jego przeciwieństwem). Największy wpływ na zwiększenie ilości zainfekowanych węzłów miała *minimalna ilość połączeń z innymi węzłami*. *Procentowa ilość zabezpieczonych* węzłów miała mniejszy wpływ na wyniki, natomiast największe spadki zakończyły się na 50%. To sugeruje że jest to minimalna wartość w jaką należy celować przy projektowaniu takiej sieci, by minimalizować zagrożenie. Bardzo efektywnym ustawieniem wydaje się być **50% zabezpieczonych węzłów i minimalny stopień węzła o wartości 5**. Ta konfiguracja najbardziej redukuje ilość zainfekowanych węzłów, jednocześnie utrzymując wysoki stopień łączności, oraz realną w praktycznej implementacji ilość węzłów zabezpieczonych.

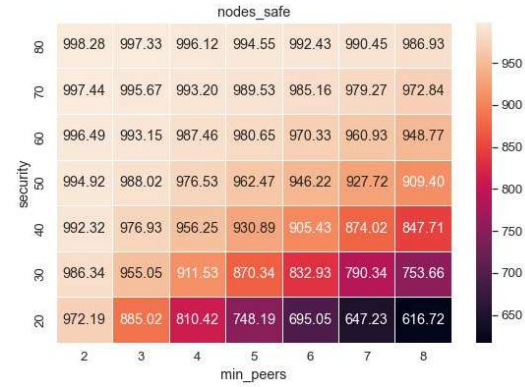
Wykresy (c) i (d) wykazują że największy spadek *ilości epok potrzebnych do ukończenia symulacji* oraz *średniej najkrótszej długości ścieżki* (które to własności mają bezpośredni wpływ na prędkość rozprzestrzeniania się informacji, a zatem też zagrożeń w sieci) następuje po zwiększeniu *minimalnego stopnia wierzchołka* z 2 na 3. Przy kolejnych przejściach ten wpływ znacznie spada. Wydaje

Tabela 1: Zmierzone wartości.

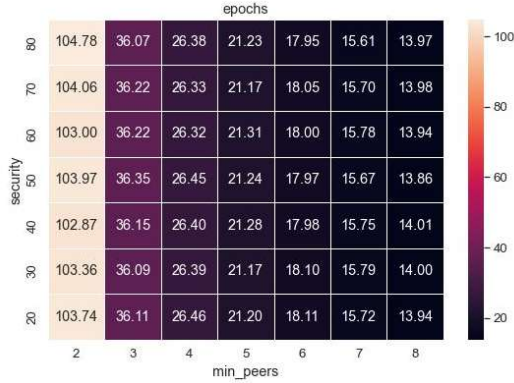
s	p	zainfekowane	zabezpieczone	epoki	krawędzie	śr.najk.dłg.śc.
80	2	1.722	998.278	104.784	1438.177	51.560864
80	3	2.667	997.333	36.067	2210.753	18.497737
80	4	3.885	996.115	26.377	3038.997	13.334797
80	5	5.452	994.548	21.232	3894.600	10.747133
80	6	7.566	992.434	17.947	4770.087	9.090586
80	7	9.549	990.451	15.606	5660.701	7.908291
80	8	13.070	986.930	13.972	6561.811	7.022169
70	2	2.561	997.439	104.062	1437.968	51.259483
70	3	4.334	995.666	36.218	2210.038	18.512081
70	4	6.802	993.198	26.326	3038.613	13.344238
70	5	10.470	989.530	21.170	3894.482	10.756841
70	6	14.836	985.164	18.049	4770.674	9.086617
70	7	20.733	979.267	15.696	5659.988	7.907234
70	8	27.163	972.837	13.980	6560.793	7.020544
60	2	3.510	996.490	103.001	1438.464	50.892062
60	3	6.853	993.147	36.218	2210.119	18.503059
60	4	12.539	987.461	26.325	3039.748	13.342314
60	5	19.345	980.655	21.313	3894.470	10.748352
60	6	29.672	970.328	17.998	4770.587	9.090314
60	7	39.074	960.926	15.780	5661.005	7.906785
60	8	51.228	948.772	13.937	6560.595	7.020063
50	2	5.075	994.925	103.973	1438.202	51.399659
50	3	11.977	988.023	36.354	2210.905	18.494181
50	4	23.465	976.535	26.446	3038.285	13.343574
50	5	37.531	962.469	21.237	3894.966	10.750997
50	6	53.784	946.216	17.969	4770.021	9.085959
50	7	72.280	927.720	15.674	5659.864	7.905302
50	8	90.599	909.401	13.863	6561.161	7.019253
40	2	7.681	992.319	102.869	1438.131	51.160025
40	3	23.065	976.935	36.154	2210.157	18.496959
40	4	43.750	956.250	26.397	3039.573	13.339345
40	5	69.106	930.894	21.281	3895.706	10.749248
40	6	94.570	905.430	17.979	4770.697	9.082308
40	7	125.982	874.018	15.746	5660.214	7.903483
40	8	152.288	847.712	14.005	6561.989	7.019072
30	2	13.660	986.340	103.359	1438.410	51.012495
30	3	44.954	955.046	36.091	2210.457	18.502268
30	4	88.466	911.534	26.394	3039.487	13.345194
30	5	129.665	870.335	21.172	3893.991	10.752458
30	6	167.069	832.931	18.097	4770.067	9.091517
30	7	209.657	790.343	15.785	5660.062	7.905358
30	8	246.343	753.657	13.996	6560.658	7.021163
20	2	27.808	972.192	103.743	1438.099	50.994377
20	3	114.978	885.022	36.113	2210.430	18.506363
20	4	189.578	810.422	26.458	3038.787	13.347298
20	5	251.810	748.190	21.197	3895.709	10.747893
20	6	304.949	695.051 <sup>4</sup>	18.109	4769.588	9.089119
20	7	352.767	647.233	15.718	5660.050	7.908031
20	8	383.283	616.717	13.937	6561.336	7.018734



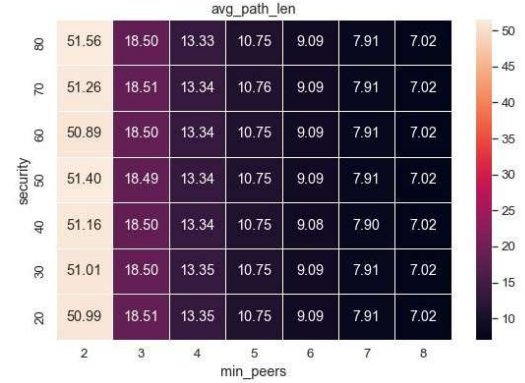
(a) promil zainfekowanych węzłów



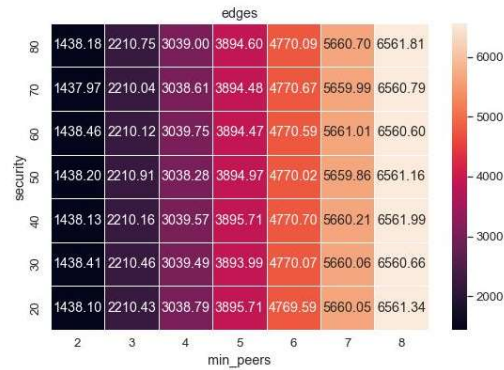
(b) promil zabezpieczonych węzłów



(c) ilość epok w symulacji



(d) średnia najkrótsza długość ścieżki



(e) ilość krawędzi

Rysunek 2: Przykładowy przebieg symulacji



się on mieć rozkład logarytmiczny, choć należałoby tę tezę potwierdzić. Co ważne, ten nagły spadek *średniej najkrótszej długości ścieżki* ma bezpośrednie odzwierciedlenie na wykresach (a) i (b), co oznacza że po przekroczeniu *minimalnego stopnia węzła* z 2 na większy znacznie zwiększa się zagrożenie sieci. Taka ilość połączeń może się jednak okazać niewystarczająca dla większości realnych implementacji tego typu rozwiązań.

Wykres (e) pokazuje, że *ilość krawędzi* wydaje się rosnąć mniej więcej liniowo wraz z *minimalnym stopniem węzła*.

## 4 Wnioski

Otrzymane wyniki wykazują, że największy wpływ na rozprzestrzenianie się zagrożenia w sieci ma wpływ *minimalna ilość połączeń między węzłami*. Także *ilość zabezpieczonych węzłów* ma duże znaczenie, choć stosunkowo mniejsze. Bardzo efektywną konfiguracją wydaje się być 50% zabezpieczonych węzłów oraz minimalna ilość połączeń między węzłami o wartości 5.

## A Dodatek

Do sprawozdania załączono dwa foldery zip.

Pierwszy (*frames.zip*) zawiera stopklatki dla epok oraz ich animacje (mp4) dla 4 ciekawych kombinacji parametrów, a drugi - kod (*code.zip*):

- main.ipynb - notatnik jupyter, w którym przeprowadzano obróbkę oraz analizę wyników
- model.py - plik python, gdzie zawarto model symulacyjny i kilka funkcji pomocniczych, między innymi do wczytywania i zapisywania modeli sieci
- utils.py - plik python ze zbiorem funkcji pomocniczych
- r.txt - plik requirements, który zawiera listę paczek potrzebnych do uruchomienia skryptów

Do przeprowadzenia badań korzystano z języka Python w wersji 3.10.2 oraz bibliotek PyPi:

```
https://www.python.org/  
https://pypi.org/project/numpy/  
https://pypi.org/project/pandas/  
https://pypi.org/project/networkx/  
https://pypi.org/project/matplotlib/  
https://pypi.org/project/seaborn/
```