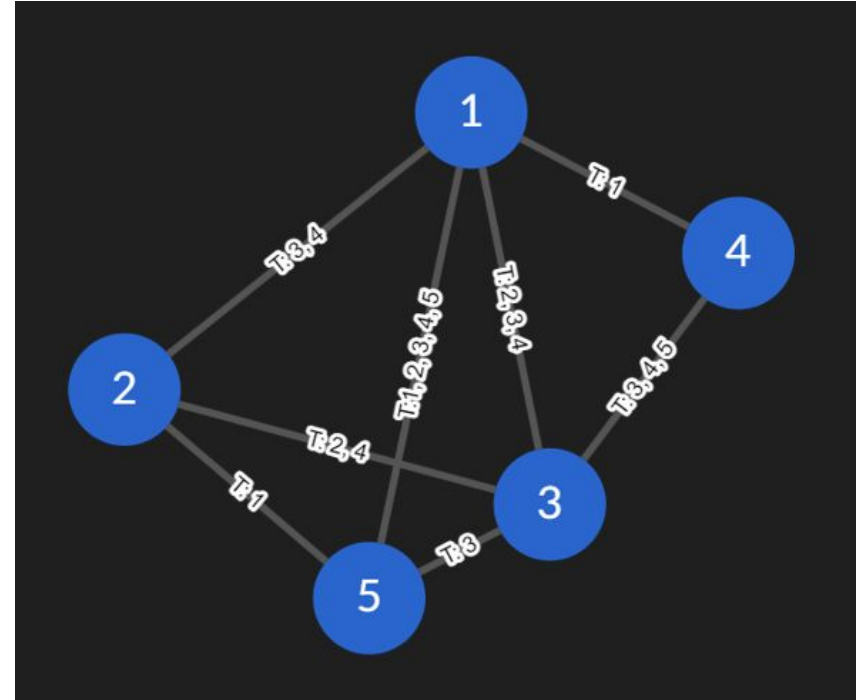


Sieci temporalne: ich struktura i podatność na błędy oraz ataki

Grzegorz Szumigaj

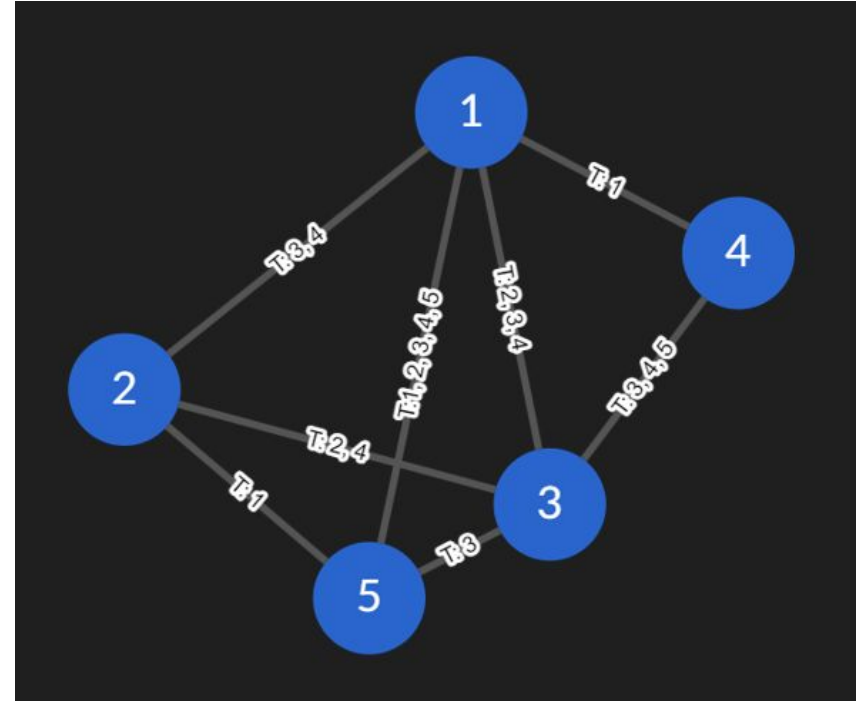
Czym jest sieć temporalna?

- $G(t) = (V, E(t))$
 - V - Stały zbiór wierzchołków
 - $E(t)$ - Zbiór krawędzi między wierzchołkami zależny od czasu t
- W czasie t jesteśmy w stanie wysłać informację z wierzchołka a do b w.t.w. gdy w czasie t istnieje krawędź z a do b



Odległości w sieci temporalnej

- Ścieżka z a do b to zbiór $d + 1$ wierzchołków $\{n_i\}$ takich, że w czasie $t_0 + i$ istnieje krawędź z n_i do n_{i+1}
 - $a = n_0$
 - $b = n_d$
 - d - długość ścieżki
- Najkrótszą ścieżką w sieci nazywamy $d_{ab}(t_1, t_2)$ - długość najkrótszej ścieżki między wierzchołkami a oraz b w przedziale czasowym $[t_1, t_2]$

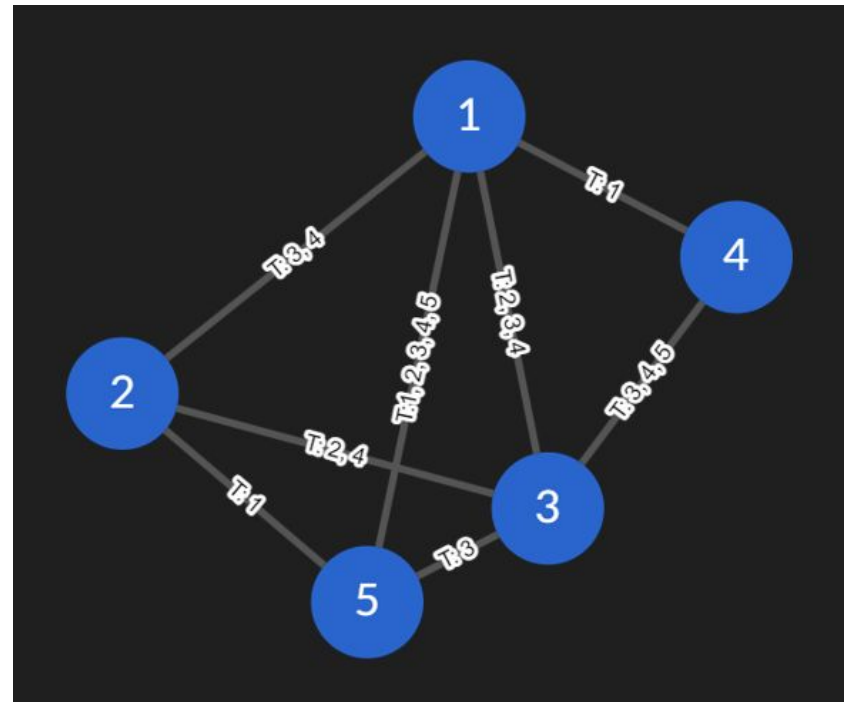


Efektywność sieci temporalnej

- Parametr E_G przyjmujący wartości od 0 do 1, określający efektywność tejże sieci
- Obliczany na podstawie sumy odwrotności odległości w sieci

$$E_G(t_1, t_2) = \frac{1}{N(N-1)} \sum_{i,j:i \neq j} \frac{1}{d_{ij}(t_1, t_2)}$$

- N - liczba wierzchołków
- $E = 0$ - w.t.w. gdy nie ma krawędzi w danym interwale
- $E = 1$ - w.t.w. gdy istniało w interwale bezpośrednie połączenie między każdym z wierzchołków

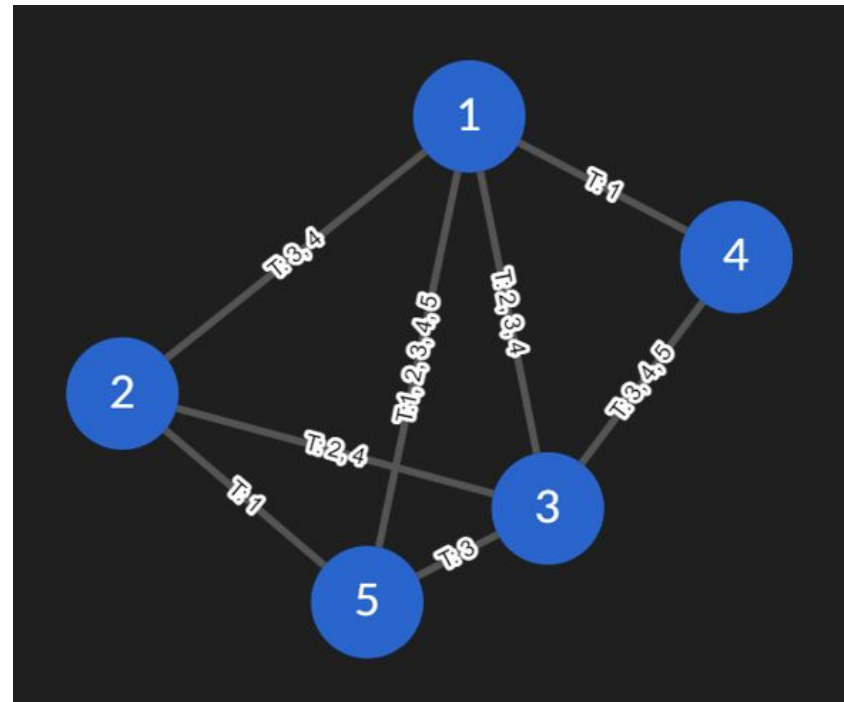


Odporność sieci temporalnej

- Parametr $R_G(D)$ zależny od “zniszczeń” w wyniku ataku na sieć
- Obliczany na podstawie efektywności przed i po ataku

$$R_G(D) = \frac{E_{G_D}}{E_G}$$

- D - Zniszczenie polegające na usunięciu krawędzi zawierających pewien podzbiór wierzchołków z grafu



Rodzaje ataków

Atak losowy

- Polega na wybraniu $P \cdot N$ losowych wierzchołków i usunięciu ich krawędzi z grafu
 - P - stałe prawdopodobieństwo ataku na konkretny wierzchołek
 - N - Liczba wierzchołków
- Liczbę zaatakowanych wierzchołków nazwijmy N_a

Atak oparty na “closeness”

- Polega na posortowaniu wierzchołków po parametrze “bliskości” i zaatakowaniu N_a pierwszych
- W sieciach tymczasowych parametr bliskości wierzchołka definiujemy jako średnią arytmetyczną odległości do pozostałych wierzchołków

$$C_i(t_1, t_2) = \sum_{j:j \neq i} \frac{1}{N-1} d_{ij}(t_1, t_2)$$

Atak oparty na stopniu wierzchołka

- Polega na wybraniu N_a wierzchołków o najwyższym stopniu w sieci temporalnej
- W sieciach temporalnych parametr ten możemy określić jako średnią arytmetyczną stopnia wierzchołka w każdym z czasów w zadanym przedziale czasowym

$$\deg_G(i, t_0, t_m) = \frac{1}{M} \sum_{k=0}^m \deg_{G(t_k)}(i)$$

Atak oparty na liczbie kontaktów między wierzchołkami

- Polega na wybraniu N_a wierzchołków, które przekazują najwięcej informacji w sieci temporalnej
- W sieciach temporalnych parametr ten możemy określić jako sumę przekazywanych wiadomości w momencie spotkania przez dwa wierzchołki
- Wiadomość z j do k jest przekazywana przez i , jeżeli $d_{ik}(t_1, t_2) < d_{jk}(t_1, t_2) + 1$

Modele syntetyczne

Model Erdősza–Rényiego

- Każda z krawędzi w grafie w danym momencie jest wybrana ze stałym prawdopodobieństwem, niezależnym od innych krawędzi
- Przypadek szczególny w modelu Markov

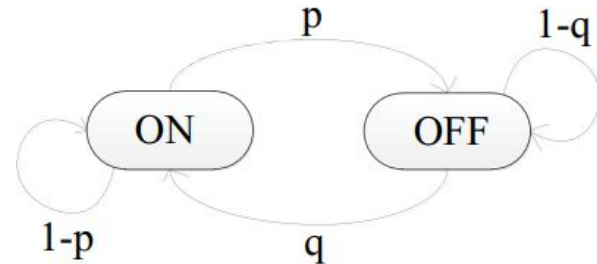
Model Markova

- Prawdopodobieństwo pojawienia się połączenia między wierzchołkami jest zależne od obecności krawędzi w poprzednim stanie
- q - prawdopodobieństwo, że między wierzchołkami powstanie nowa krawędź w jednej jednostce czasu
- p - prawdopodobieństwo, że między wierzchołkami zniknie istniejąca krawędź w jednej jednostce czasu

$$\Pr[\text{ON}] = \frac{q}{p + q}$$

$$\Pr[\text{OFF}] = \frac{p}{p + q}$$

- Jeżeli $p + q = 1$ to otrzymujemy model Erdősza–Rényiego



Model sieci mobilnych

Random WayPoint Model

- Wierzchołki są początkowo ustawiane losowo na planszy
- Każdy wierzchołek porusza się z pewną prędkością do losowo wybranego celu
- Po dotarciu do celu wierzchołek odczekuje chwilę po czym wybiera nowy cel
- Połączenie między wierzchołkami istnieje, jeżeli odległość między nimi jest mniejsza niż ustalone r

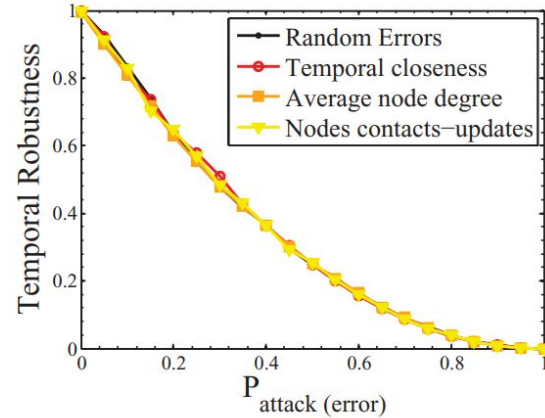
Random WayPoint Group Model

- Wybieranych jest M liderów
- pozostałe wierzchołki są przydzielane równomiernie pomiędzy liderów
- Liderzy poruszają się zgodnie ze schematem z modelu RWP
- Grupy poruszają się wokół liderów zachowując odpowiedni dystans
- Połączenia są ustalane w ten sam sposób co w RWP

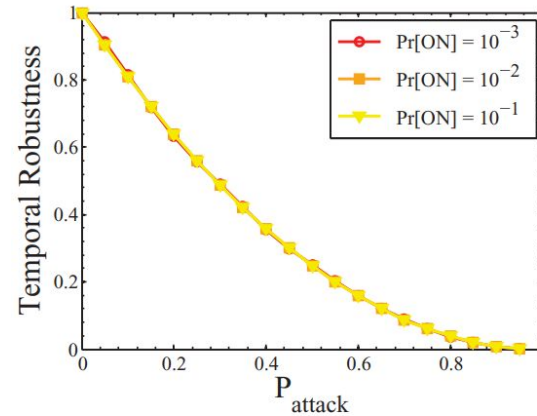
Wyniki symulacji ataków na modelach

Erdős–Rényi i Markov

- $N = 100$
- $\tau = 150$
- Wyniki dla obu rodzajów sieci zbliżone
- Brak znaczących różnic między różnymi sposobami ataków
- (a)
 - $\text{Pr}[\text{ON}] = 1/1000$
- (b)
 - Atak biorący pod uwagę średni stopień wierzchołka



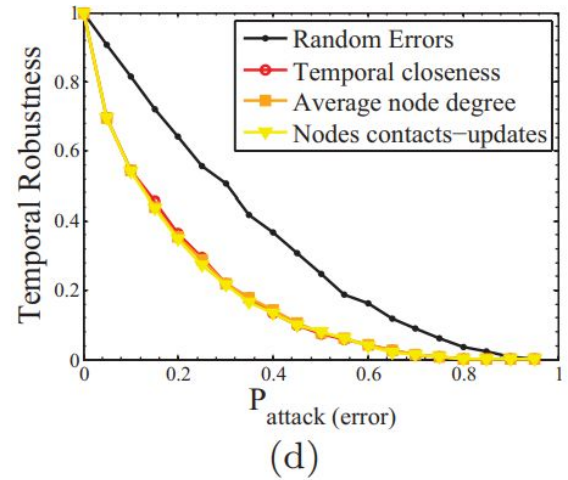
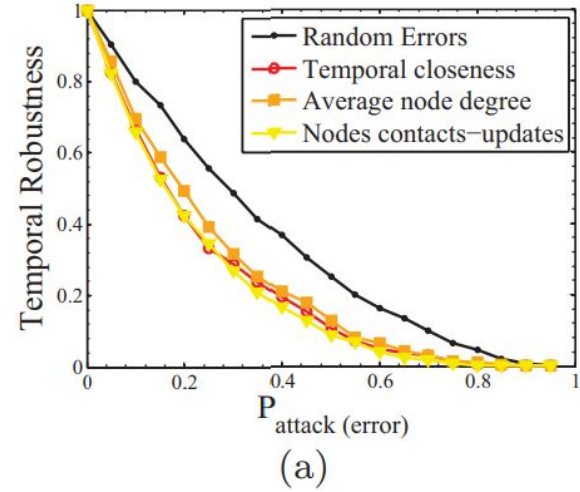
(a)



(b)

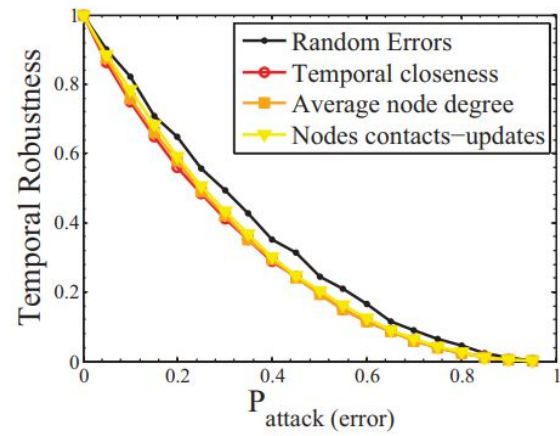
RWP i RWPG

- $\Pr[\text{ON}] = 10^{-4}$
- $\tau = 3600$
- (a) - RWP
- (d) - RWPG

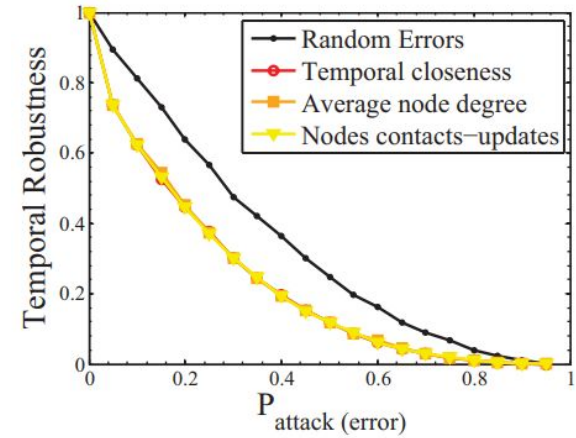


RWP i RWPG

- $\Pr[\text{ON}] = 10^{-3}$
- $\tau = 3600$
- (b) - RWP
- (e) - RWPG



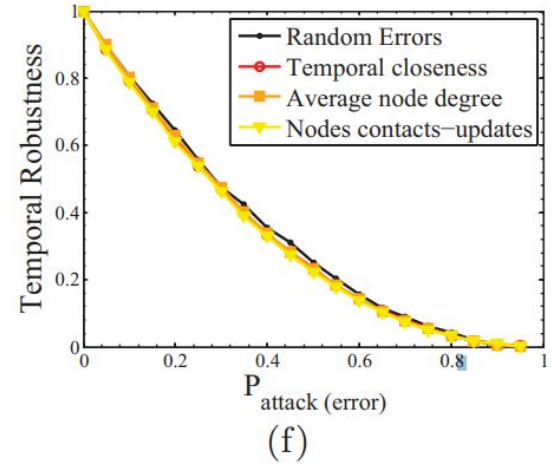
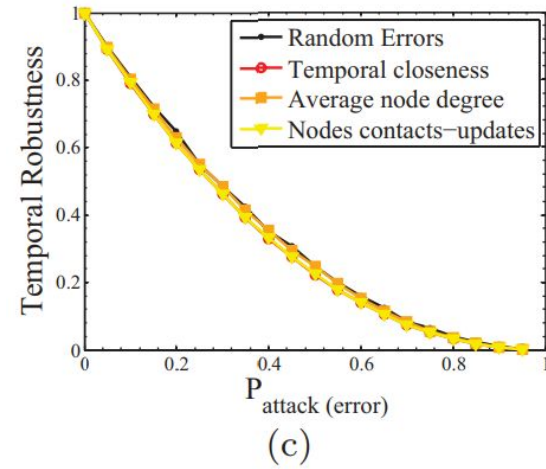
(b)



(e)

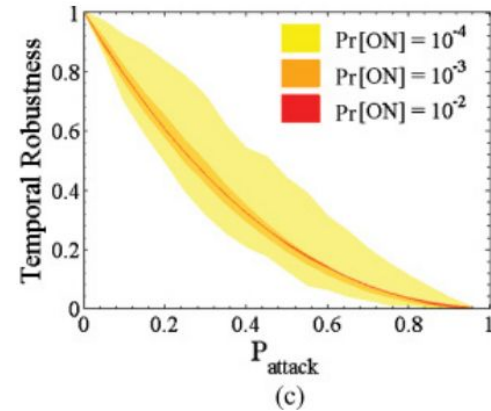
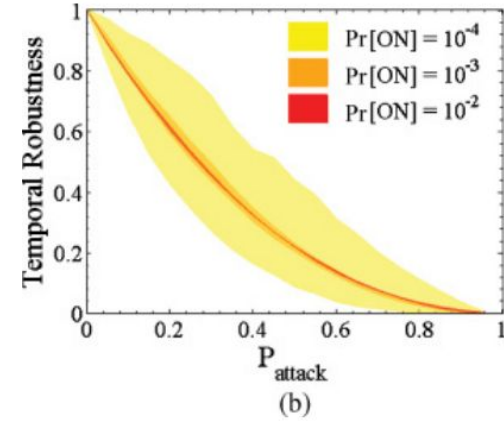
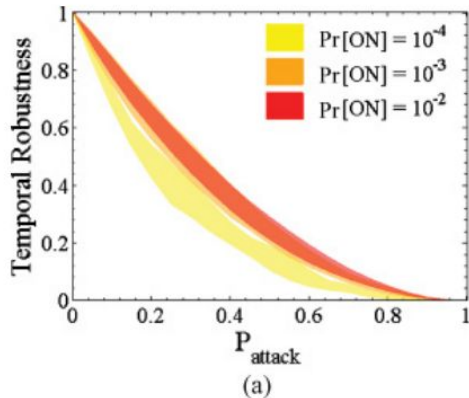
RWP i RWPG

- $\Pr[\text{ON}] = 10^{-1}$
- $\tau = 3600$
- (c) - RWP
- (f) - RWPG



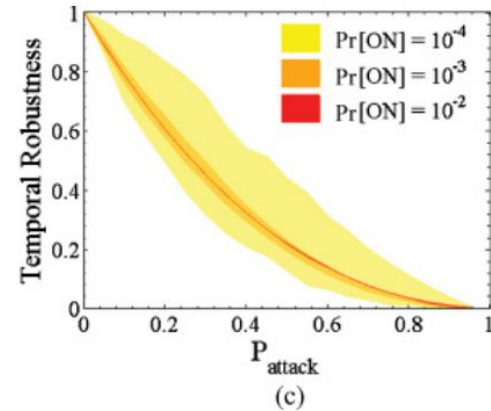
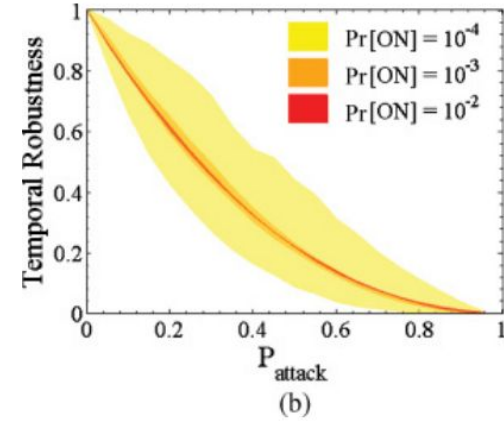
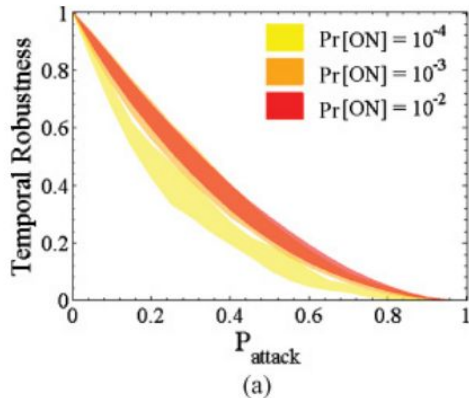
RWP - zakres odporności

- $\tau = 3600$
- Opisuje zakres wytrzymałości przy wybieraniu najlepszych i najgorszych wierzchołków
- (a) - closeness
- (b) - degree
- (c) - betweenness

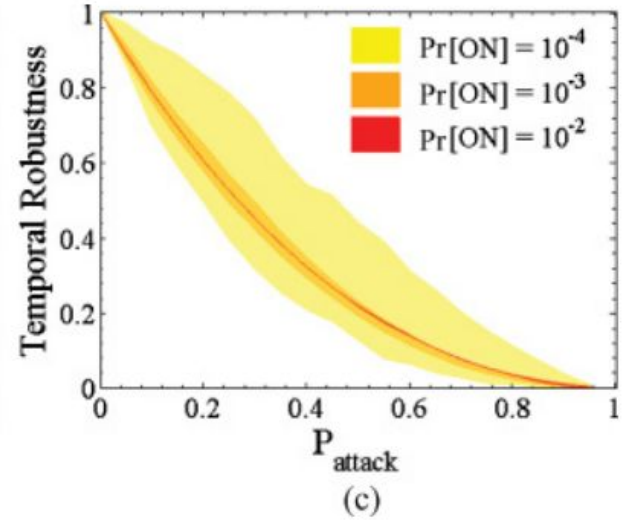
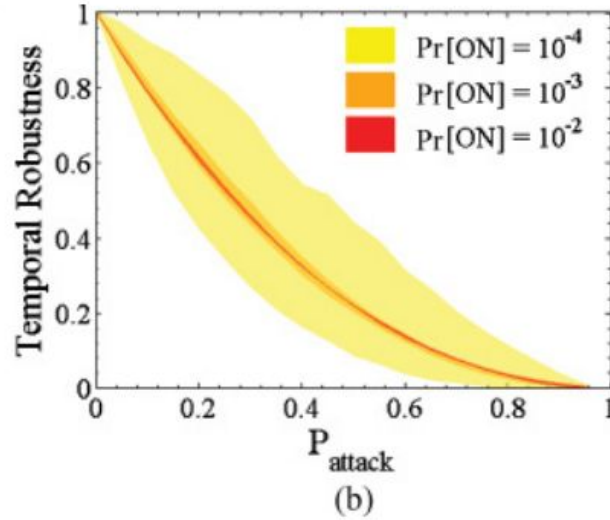
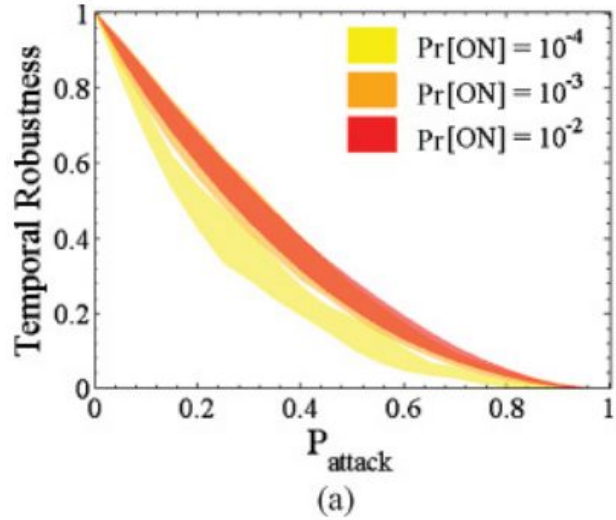


RWPG - zakres odporności

- $\tau = 3600$
- Opisuje zakres wytrzymałości przy wybieraniu najlepszych i najgorszych wierzchołków
- (a) - closeness
- (b) - degree
- (c) - betweenness

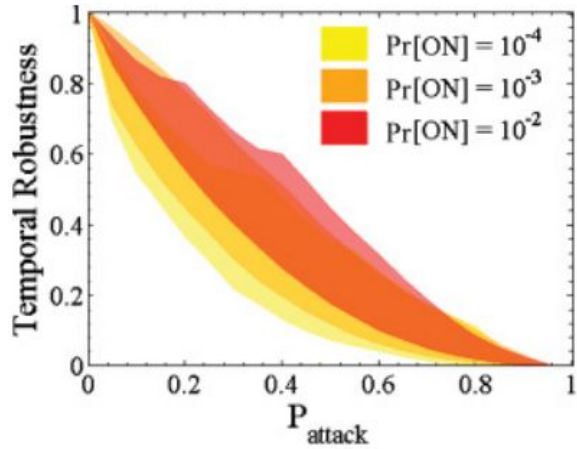


RWP - zakres odporności

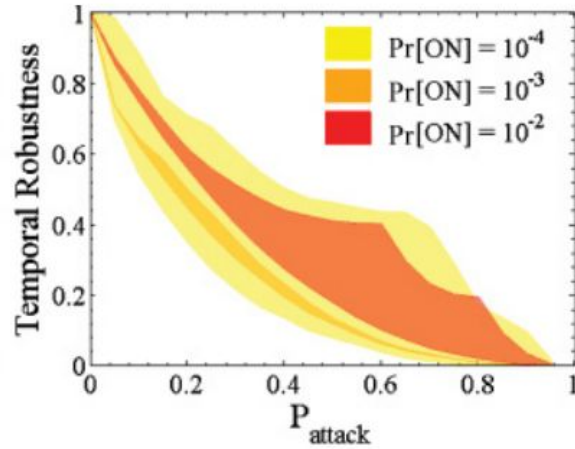


- $\tau = 3600$
- (a) - closeness (b) - degree (c) - betweenness

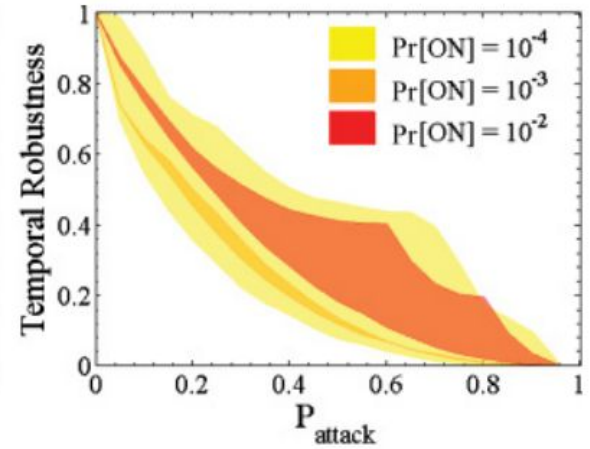
RWPG - zakres odporności



(a)



(b)



(c)

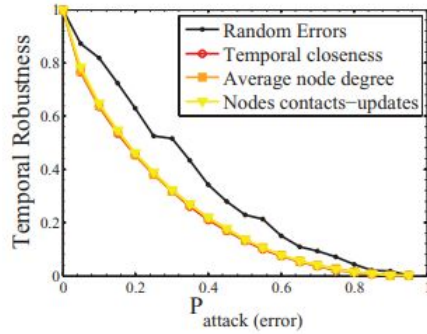
- $\tau = 3600$
- (a) - closeness (b) - degree (c) - betweenness

Prawdziwe sieci temporalne

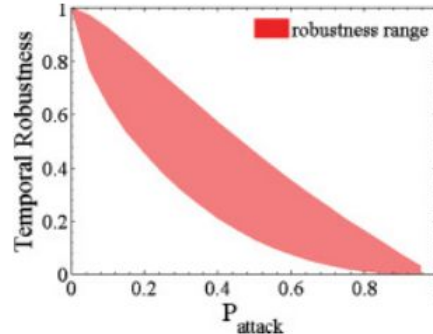
Taksówki w San Francisco

- $N = 488$
- odstępy czasu - $1s$
- $\tau = 86400$ (1 dzień)
- odległość potrzebna do stworzenia połączenia - $200m$

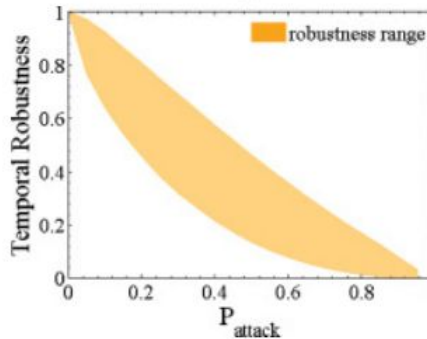
Taksówki w San Francisco



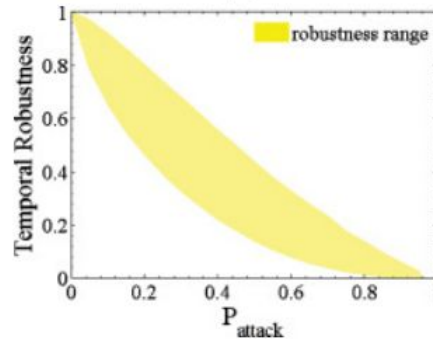
(a)



(b)



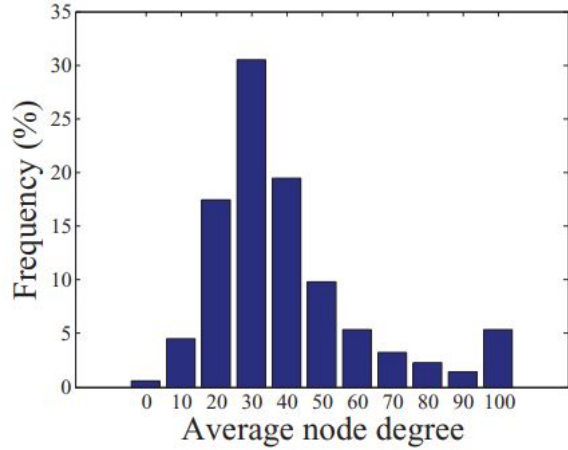
(c)



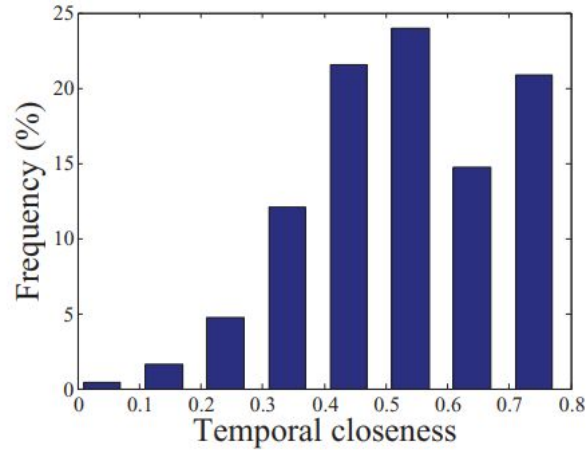
(d)

- (a) - różne strategie ataku
- (b) - closeness
- (c) - degree
- (d) - betweenness
- a - randomowy atak mniej wpływa na odporność sieci
- b, c, d - pokazują istotność niektórych hubów sieci komunikacji

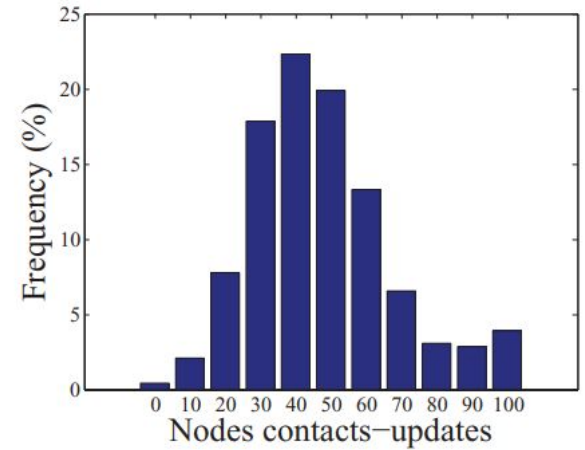
Taksówki w San Francisco



(a)



(b)



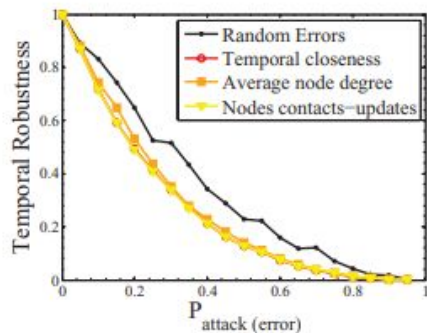
(c)

- Właściwości wierzchołków (taksówek)

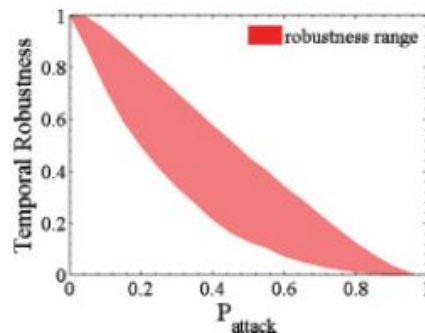
Konferencja INFOCOM w Barcelonie

- $N = 78 + 20$
- odstępy czasu - $1s$
- $\tau = 345\,600$ (4 dni)
- odległość potrzebna do stworzenia połączenia:
 - uczestnik - $30m$
 - statyczne urządzenia - $100m$

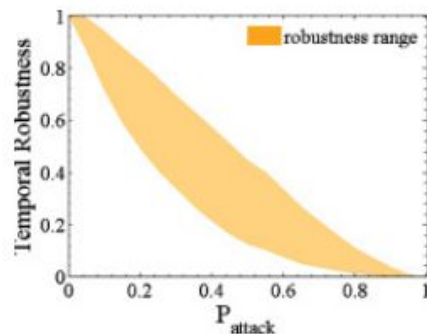
Konferencja INFOCOM w Barcelonie



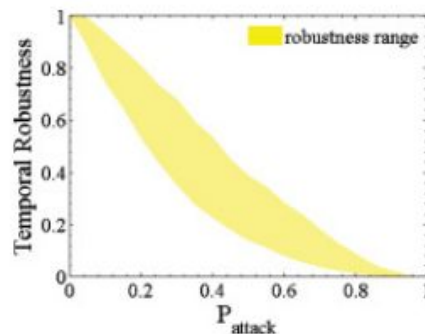
(a)



(b)



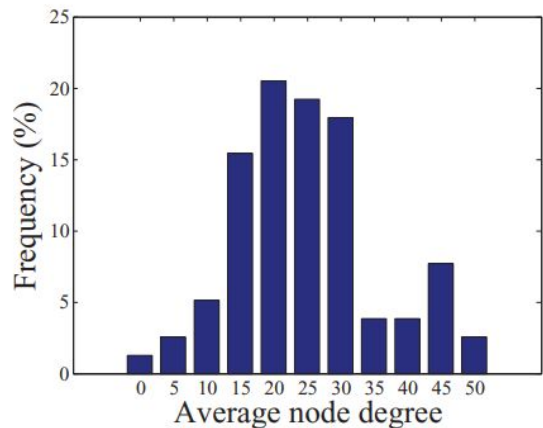
(c)



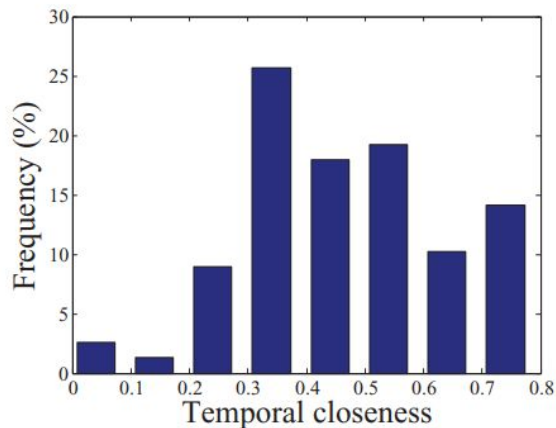
(d)

- (a) - różne strategie ataku
- (b) - closeness
- (c) - degree
- (d) - betweenness
- a - randomowy atak mniej wpływa na odporność sieci
- b, c, d - pokazują istotność niektórych hubów sieci komunikacji

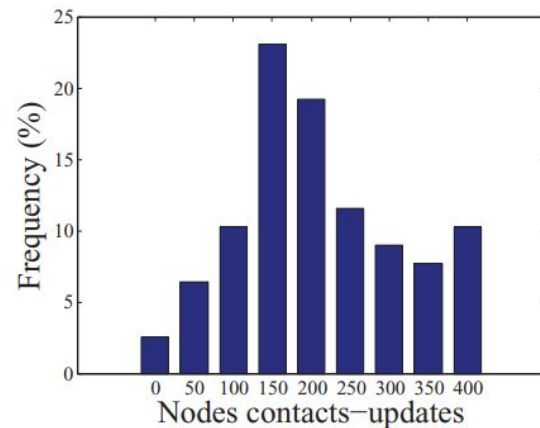
Konferencja INFOCOM w Barcelonie



(a)



(b)

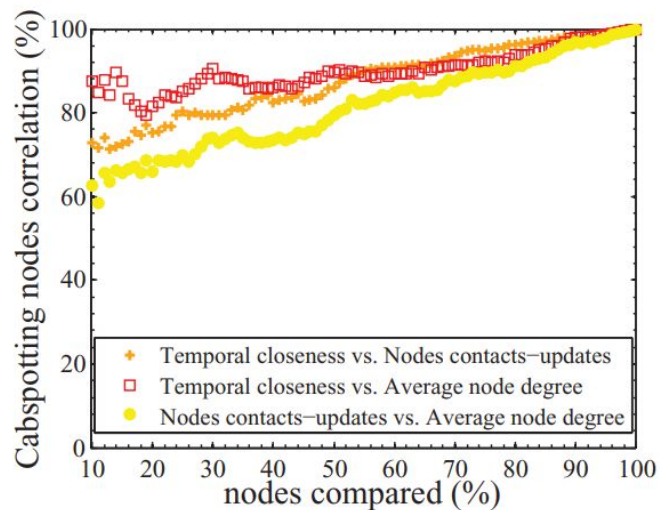


(c)

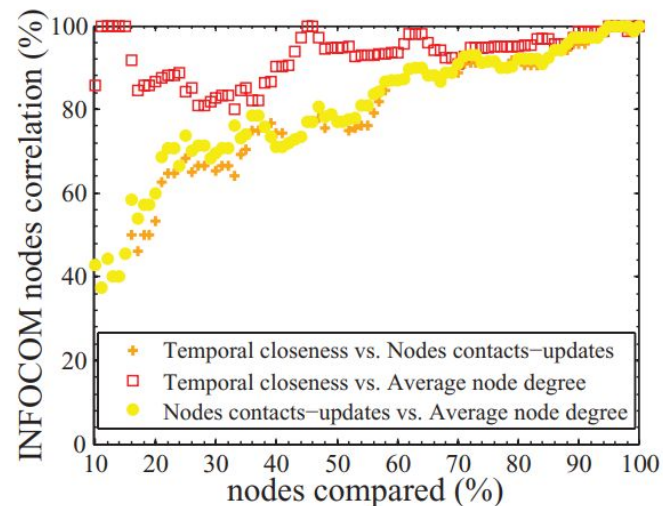
- Właściwości wierzchołków (przebieżników telefonicznych)

Pokrywanie się wierzchołków w zależności od strategii

- (a) - taksówki (b) - konferencja



(a)



(b)

Podsumowanie

- Możemy użyć metryki odporności sieci temporalnej do określenia przepustowości sieci po ataku o określonej skali
- Ataki możemy przeprowadzać losowo, lub korzystając z miar centralności
- W sieciach jednorodnych ataki losowe mają podobny wpływ jak ataki inteligentne
- W prawdziwych sieciach ataki inteligentne wpływają na wydajność sieci średnio 50% - 75% bardziej niż ataki losowe

Koniec

Bibliografia

- **Error and attack vulnerability of temporal networks** - *S Trajanovski, S Scellato, I Leontiadis* - Physical Review E, 2012 • APS
- **Temporal networks** - *P Holme, J Saramäki* - Physics reports, 2012 - Elsevier
- **Applications of temporal graph metrics to real-world networks** - *J Tang, I Leontiadis, S Scellato, V Nicosia, C Mascolo, M Musolesi, V Latora* - Temporal Networks, 2013 • Springer