Marta Rybczyńska
<marta@rybczynska.net>

Nowy atak na systemy anonimowości

Plan

- Teoria
  - Systemy anonimowości
  - Analiza ruchu
- Motywacja
- Atak
  - Zasada działania
  - Zasięg, zastosowanie, wnioski

Plan

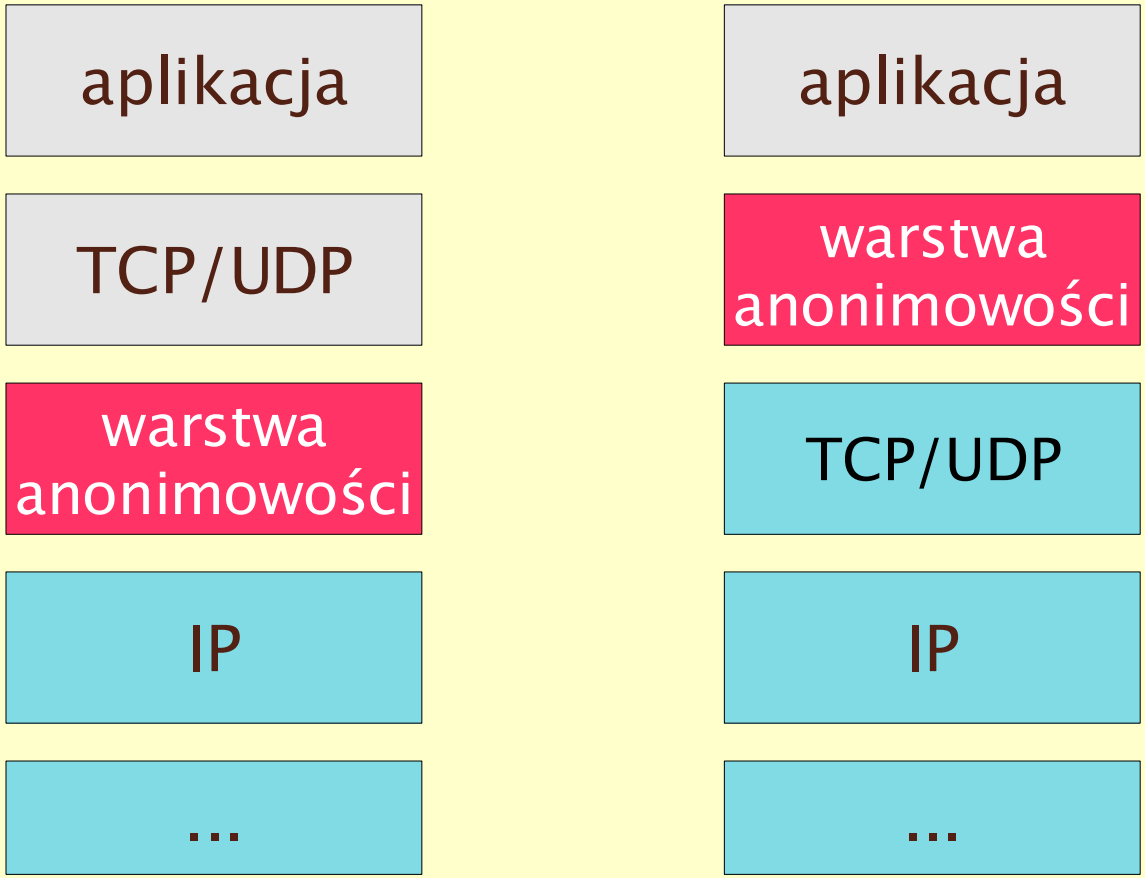
- Teoria
  - Systemy anonimowości
  - Analiza ruchu
- Motywacja
- Atak
  - Zasada działania
  - Zasięg, zastosowanie, wnioski

Wprowadzenie (1)

- Realizacje anonimowości
  - Dla konkretnego protokołu/usługi lub w takim protokole
  - Jako dodatkowa warstwa
    - Umożliwienie realizacji wielu usług
    - Przezroczystość
    - Wykorzystanie istniejących komponentów

Wprowadzenie (2)

- Fizyczna realizacja warstwy anonimowości



Wprowadzenie (3)

- Analiza ruchu (traffic analysis)
  - Odkrycie tożsamości (węzła) wysyłającego i odbierającego wiadomość
  - Bez ataku na mechanizmy kryptograficzne
  - Przykłady ataków:
    - brutalne (śledzenie całości systemu)
    - czasowe
    - oznaczanie wiadomości
    - przez powtórzenie
    - kontekstowe

Tor

- Niskie opóźnienia
- Wykorzystuje TCP
- Onion-routing
- Dynamiczne zestawianie ścieżek
- Popularny
  - 900-1000 routerów (maj/czerwiec 2007)
  - 'hundreds of thousands of users' (2007)
- http://tor.eff.org

Motywacja (1)

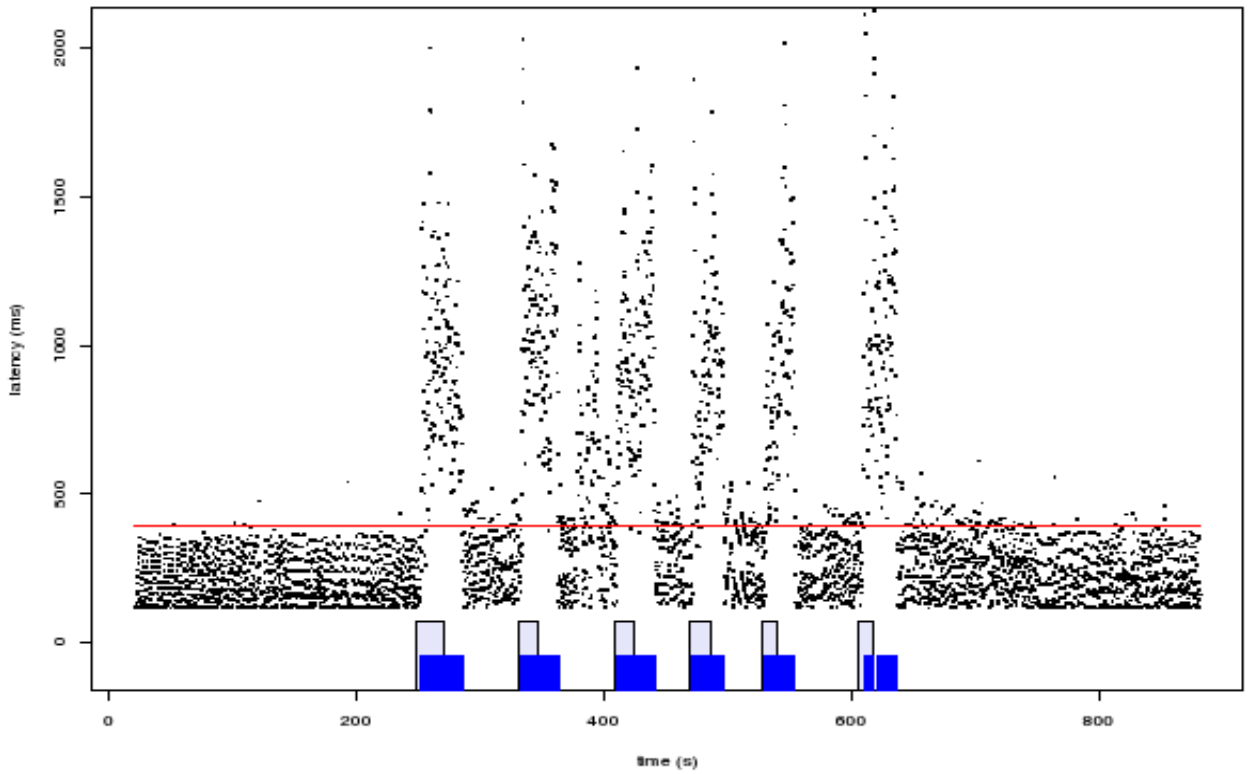


Figure 2. Probe results showing good correlation (Node K)

correlation quality varied, however for all but 2 nodes it correctly differentiated the case where the node was carrying the victim traffic and the case where the traffic flowed through other nodes.

Figure 2 shows a good correlation between probe data in victim traffic. The dots indicate the latency of the probes and the pattern of the victim stream sent is shown at the bottom. The victim stream received is overlaid to show how the pattern is distorted by the network. Finally, the horizontal line indicates the mean latency during the sample period. In contrast, Figure 3(a) shows the same node being monitored

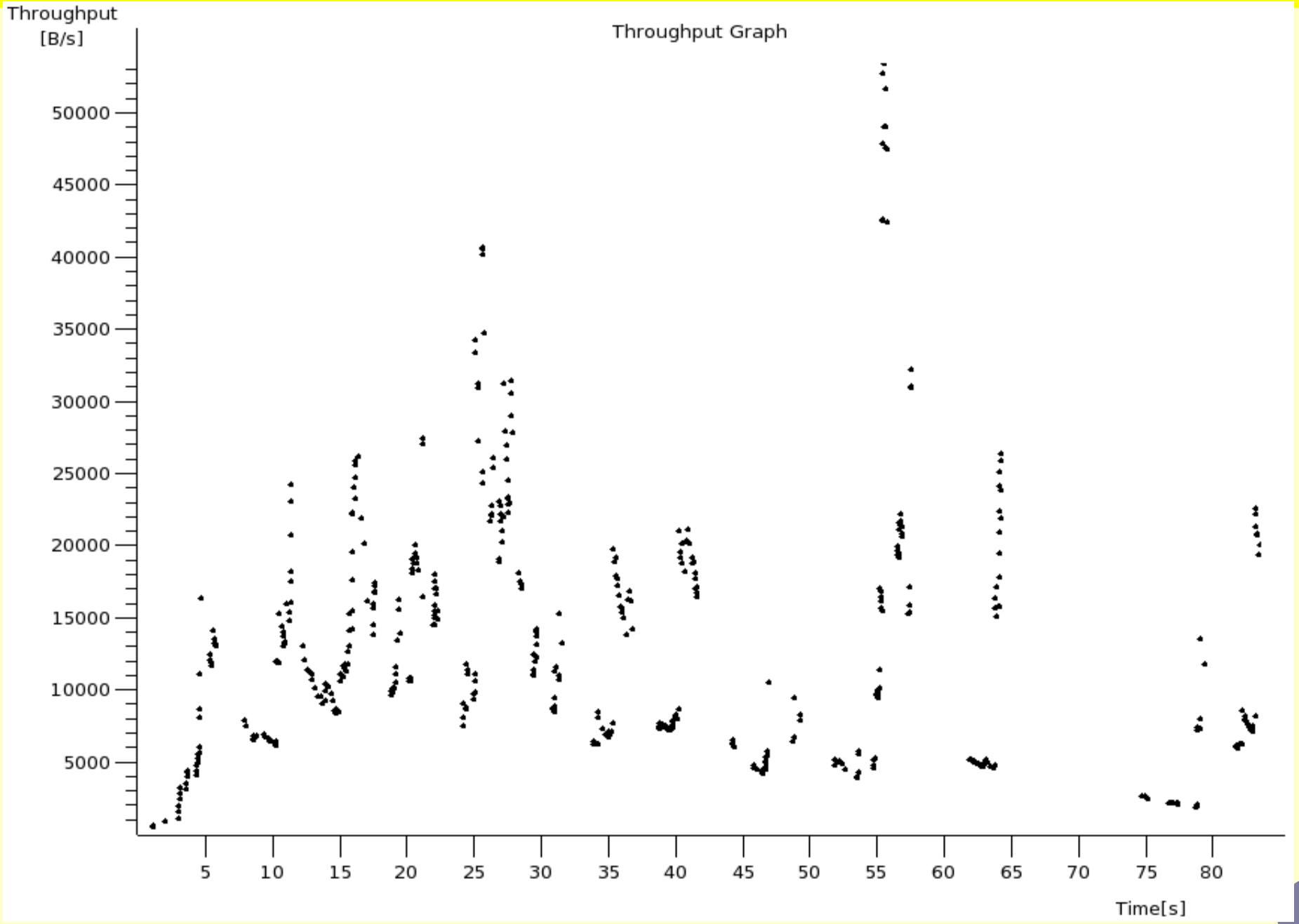
or to improve the correlation function as suggested in Section 3.3. There appears to be significant room for improvement, as shown in Figure 3(b) which was not correctly identified as being correlated, despite showing visible similarity to the traffic pattern.

5 Discussion

Our experiments clearly show that Tor streams retain their timing characteristics as they travel through the anonymising network. Furthermore, these characteristics

Murdoch, Denezis – Low-Cost Traffic Analysis of Tor, 2005

Motywacja (2)


Throughput
[B/s]
Throughput Graph
50000
45000
40000
35000
30000
25000
20000
15000
10000
5000
5
10
15
20
25
30
35
40
45
50
55
60
65
70
75
80
Time[s]

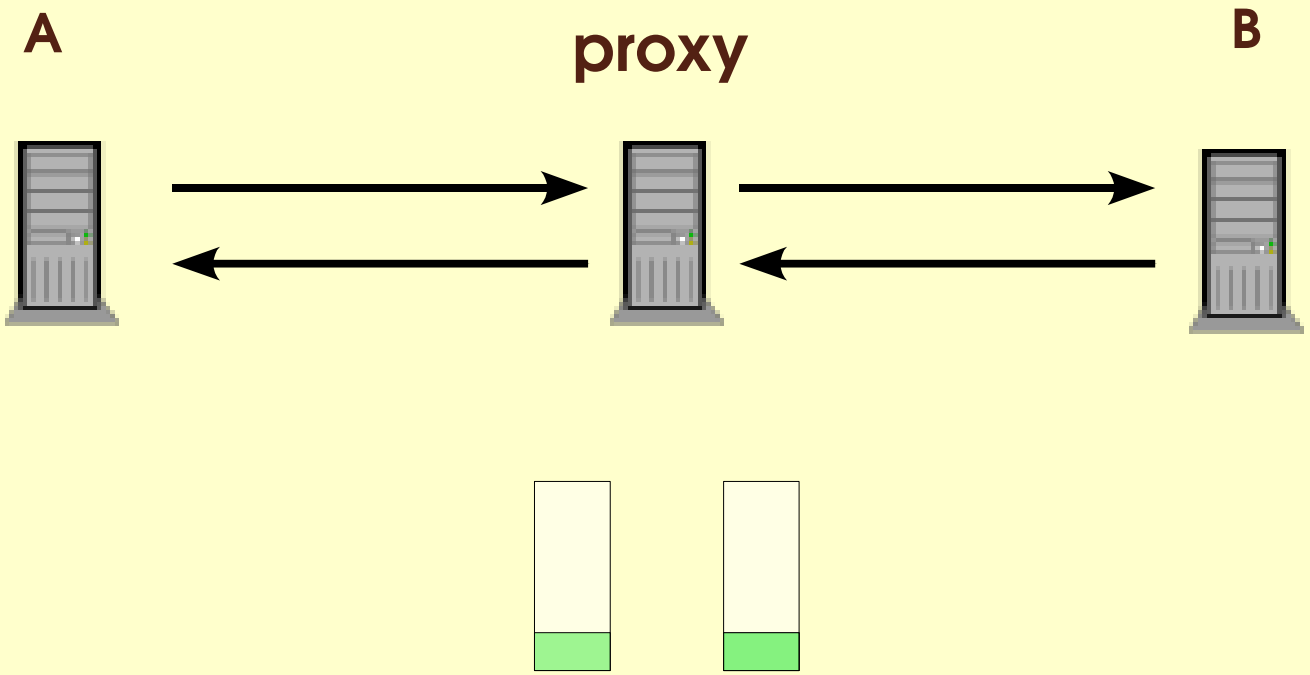
Plan

- Teoria
  - Systemy anonimowości
  - Analiza ruchu
- Motywacja
- Atak
  - Zasada działania
  - Zasięg, zastosowanie, wnioski

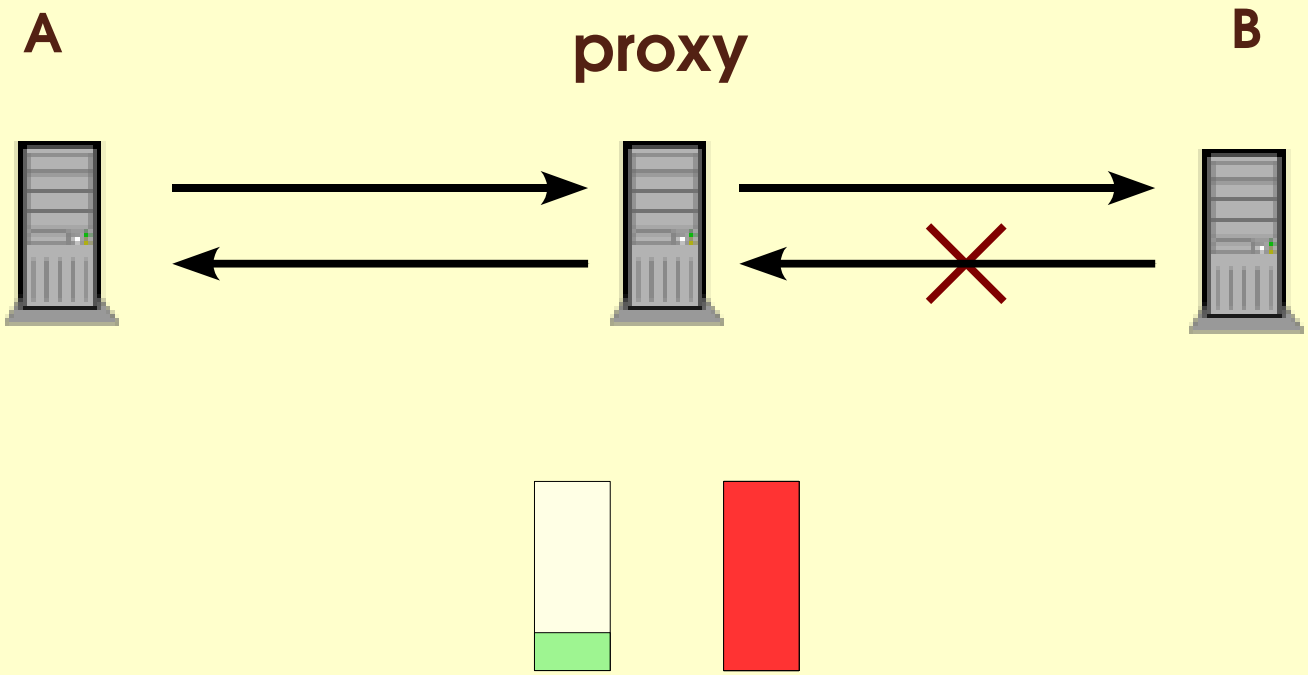
Atak: założenia

- System anonimowości
  - wykorzystuje serwery pośredniczące (proxy)
  - używa protokołu niższej warstwy zapewniającego dostarczenie danych (np. TCP)
- Możliwości atakującego
  - blokowanie transmisji od wybranego węzła
  - monitorowanie ruchu w wybranym punkcie

Stan normalny



B przestaje odbierać



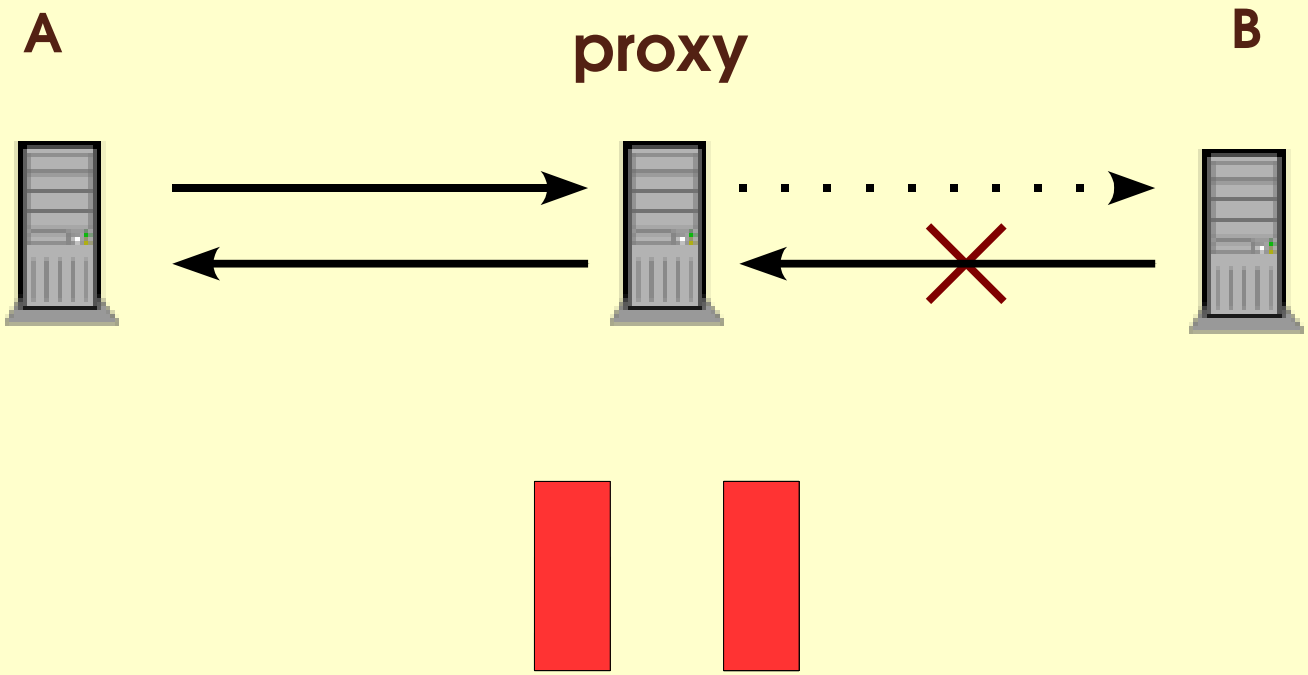
Reakcja na przepełnienie bufora

- **Nie odbierać nowych danych**
- Odbierać i odrzucać
- Odrzucić zawartość bufora nadawczego; napełniać od nowa

} giną dane

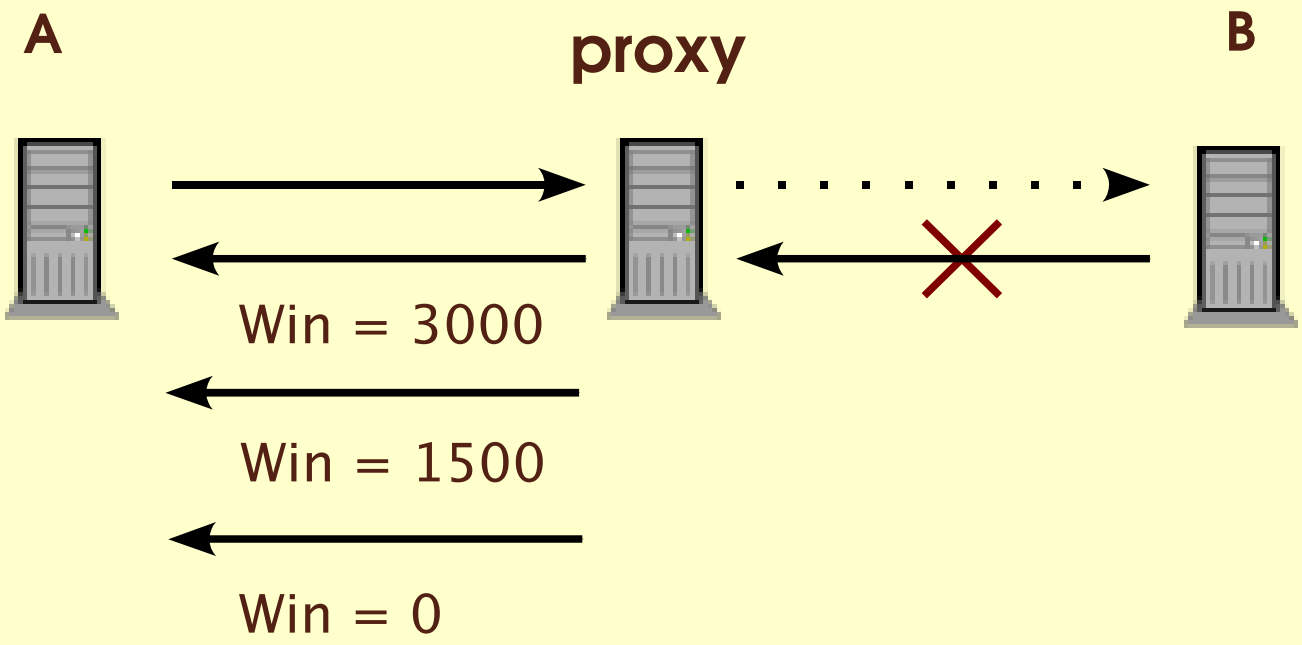
- Zgłosić błąd, rozłączyć itp.
- Próbować zestawić nowe połączenie (np. inną drogą)

B ciągle nie odbiera

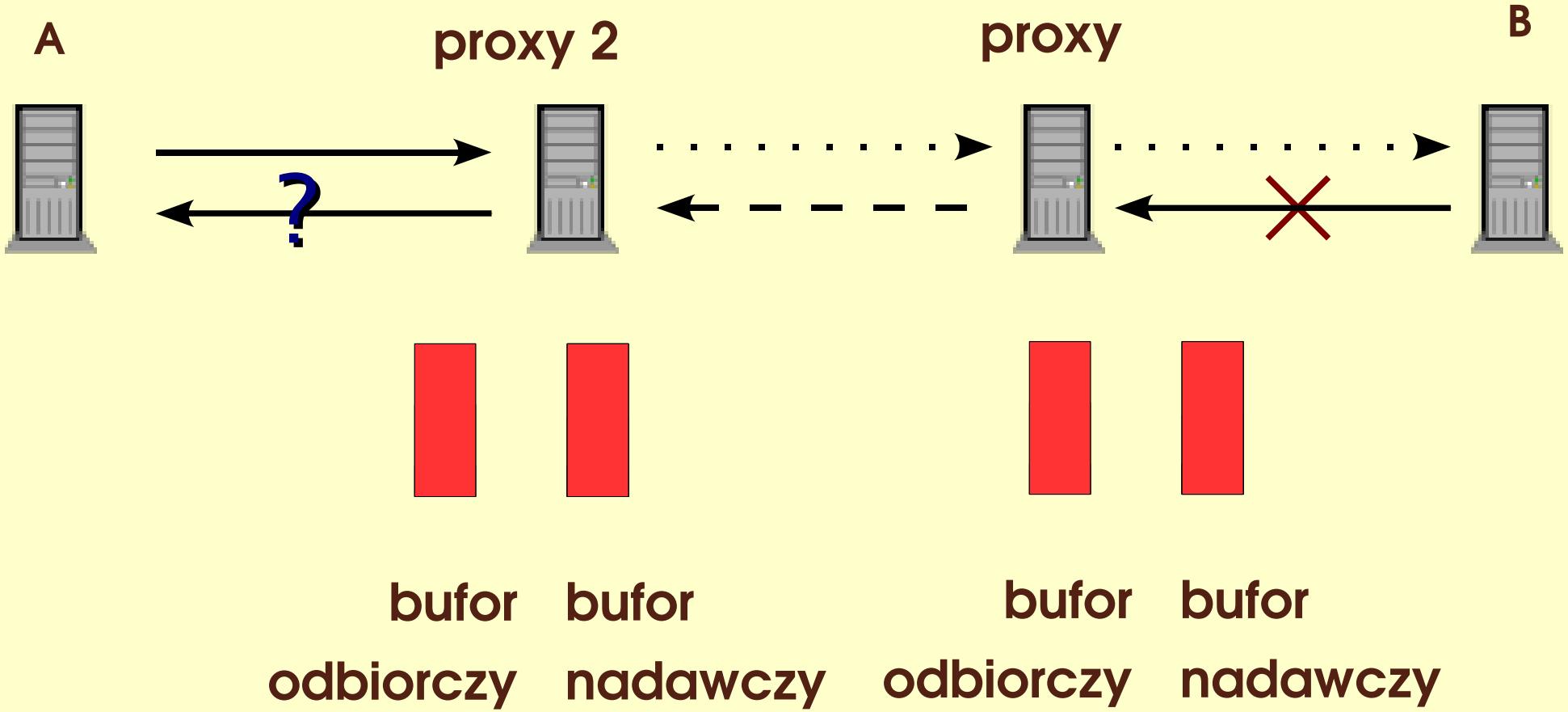


Mechanizm okna

- Powiadomienie: ile możemy jeszcze przyjąć?
- Wartość okna zależy od stanu bufora



Więcej serwerów



Zasada działania

- Zablokowanie ruchu z węzła B
- Przepełnienie buforów w kolejnych serwerach pośredniczących
- Na kolejnych połączeniach:
  - wielkość okna spada do 0
  - brak potwierdzeń pakietów z danymi
- Zaburzenia dotrą do węzła A

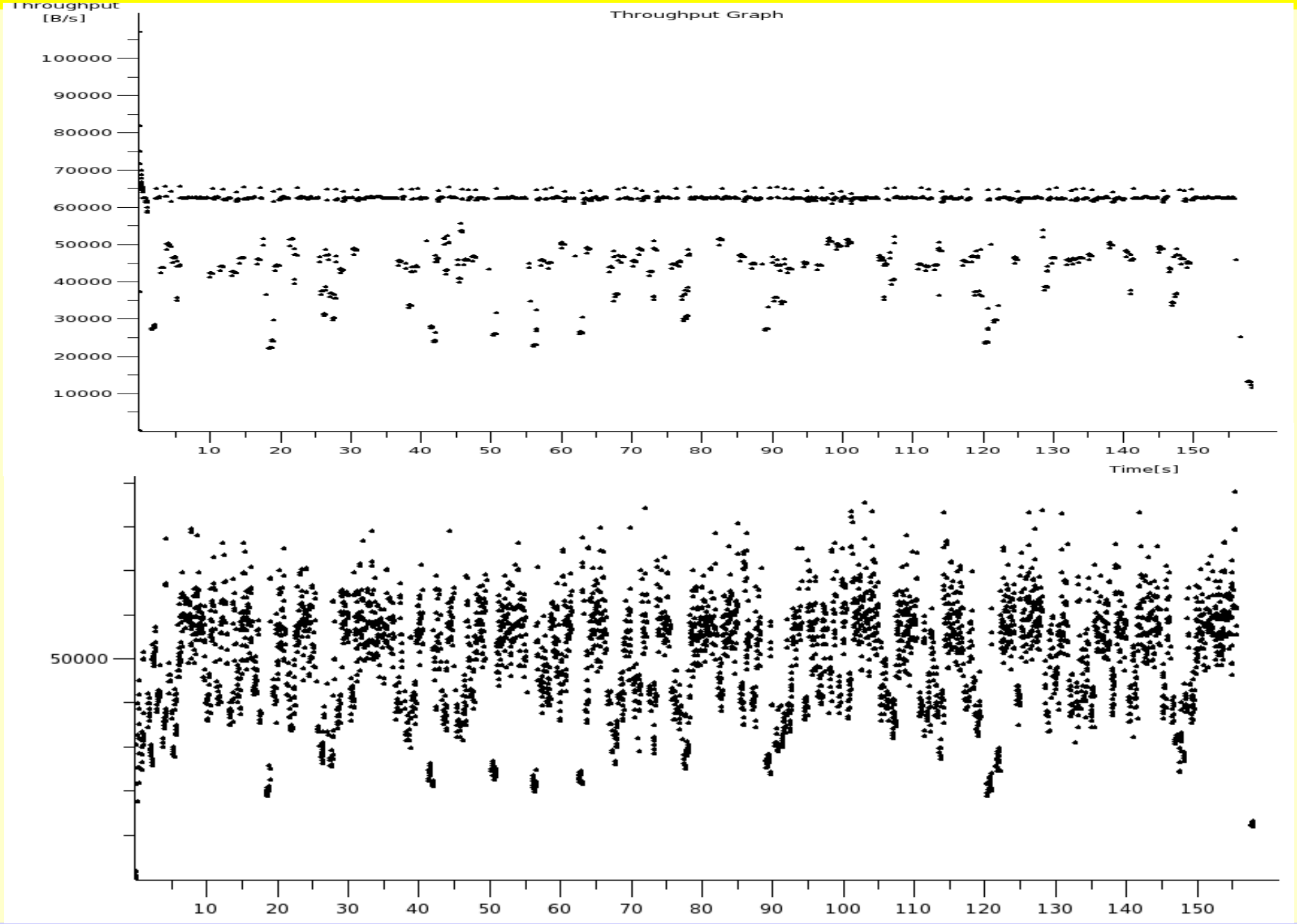
Zastosowanie ataku

- Potwierdzenie faktu komunikacji (czy B komunikuje się z A)
- Śledzenie połączeń wybranego węzła
- Nie jest potrzebne przejęcie części infrastruktury

Zasięg ataku

- Systemy anonimowości o niskich opóźnieniach
  - Tor
  - wszystkie używające TCP (?)
- Konieczność transferu dość dużej ilości danych
- Wpływ innych zjawisk sieciowych
  - ograniczenia przepływności
  - duże obciążenie
  - straty

W praktyce...


Throughput [B/s]
Throughput Graph
100000
90000
80000
70000
60000
50000
40000
30000
20000
10000
10
20
30
40
50
60
70
80
90
100
110
120
130
140
150
Time[s]
50000

Ciąg dalszy...

- Jak tanio (i skutecznie) zaatakować?
- Czas trwania ataku
- False positives
- Agregacja ruchu
  - co się dzieje, kiedy połączenie między serwerami proxy agreguje dane z kilku połączeń między użytkownikami?

Marta Rybczyńska
<marta@rybczynska.net>

Nowy atak na systemy anonimowości