Marta Rybczyńska
<marta@rybczynska.net>

Analiza ruchu w systemach anonimowości: Tor i JAP

Plan

- Wstęp
  - Zasada działania, podobieństwa i różnice: Tor i JAP
  - Analiza ruchu
- Ataki
  - prezentacja
  - wyjaśnienie działania
- Wyniki

Anonimowość z niskimi opóźnieniami

- Po co?
  - pobieranie plików
  - przeglądanie stron WWW
  - komunikatory, rozmowy telefoniczne (VoIP)
- Jak?
  - serwery pośredniczące
  - mixy (czasu rzeczywistego)
  - ruch nadmiarowy

Tor

- http://tor.eff.org
- Onion routing
- Dynamiczne zestawianie ścieżek (circuits)
- Wysoka wydajność
- Nie ma:
  - miksowania
  - ruchu nadmiarowego

JAP (Java Anon Proxy)

- http://anon.inf.tu-dresden.de
- Podejście oparte na miksach
- Statyczne ścieżki
- Kaskady miksów
- Dobra wydajności
- Nie ma:
  - ruchu nadmiarowego

Tor i JAP: porównanie

- Metoda działania
  - Onion routing vs miksy
- Wydajność
  - W obu akceptowalna
  - JAP: ograniczenie do ~128kbit/s (?)
- Bezpieczeństwo

Analiza ruchu

- Dane
  - informacje o ruchu sieciowym
  - z określonych punktów
  - tradycyjnie: globalny atakujący
- Wynik
  - powiązanie nadającego z odbierającym
  - potwierdzenie istnienia transmisji (traffic confirmation)
  - ...

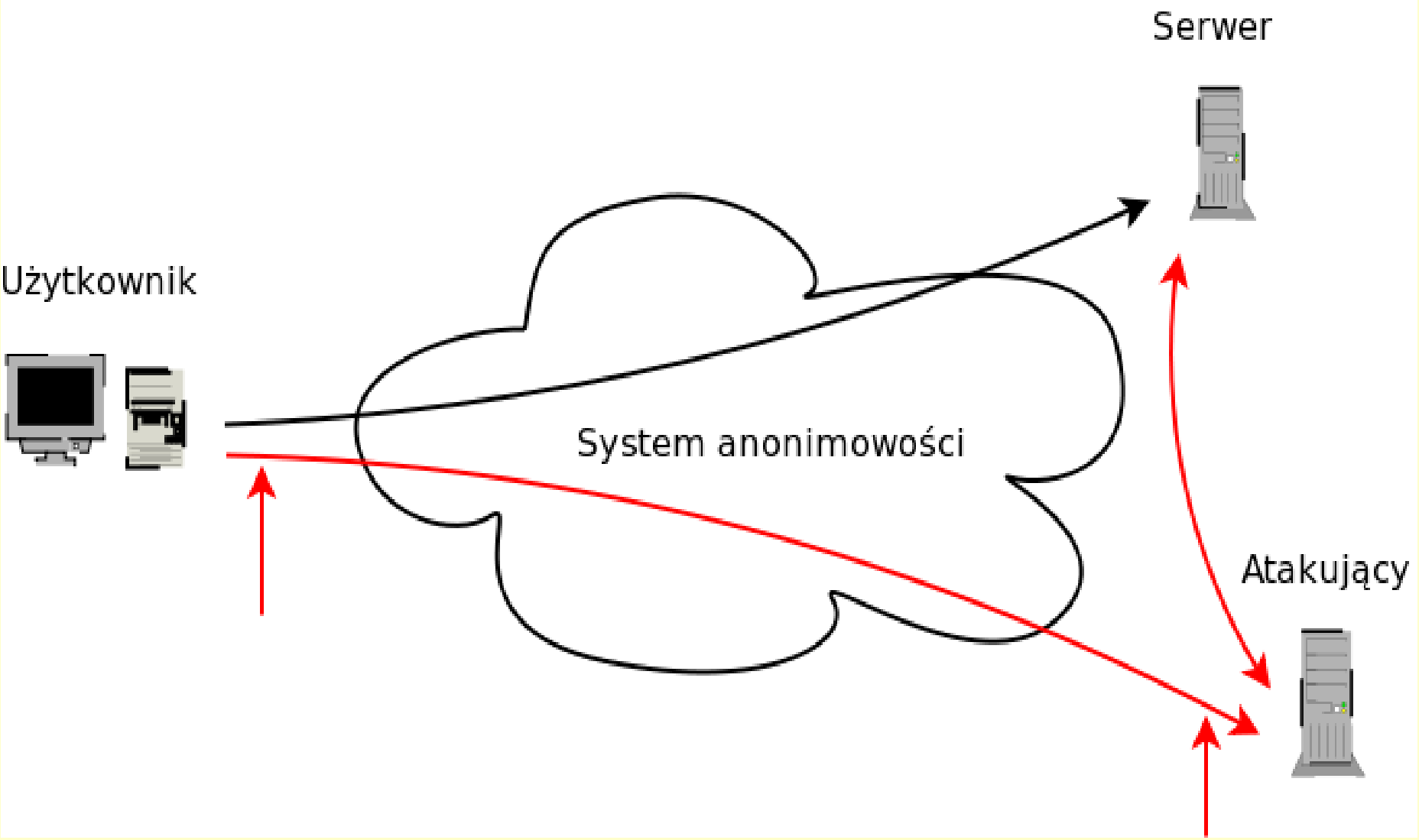
Model ataku: założenia

- Atakujący lokalny (małe możliwości)
- Dostęp do strumienia ruchu
  - jest (dla atakującego)
  - zwykły strumień ruchu użytkownika
- Cel
  - powiązanie stron
  - potwierdzenie istnienia komunikacji

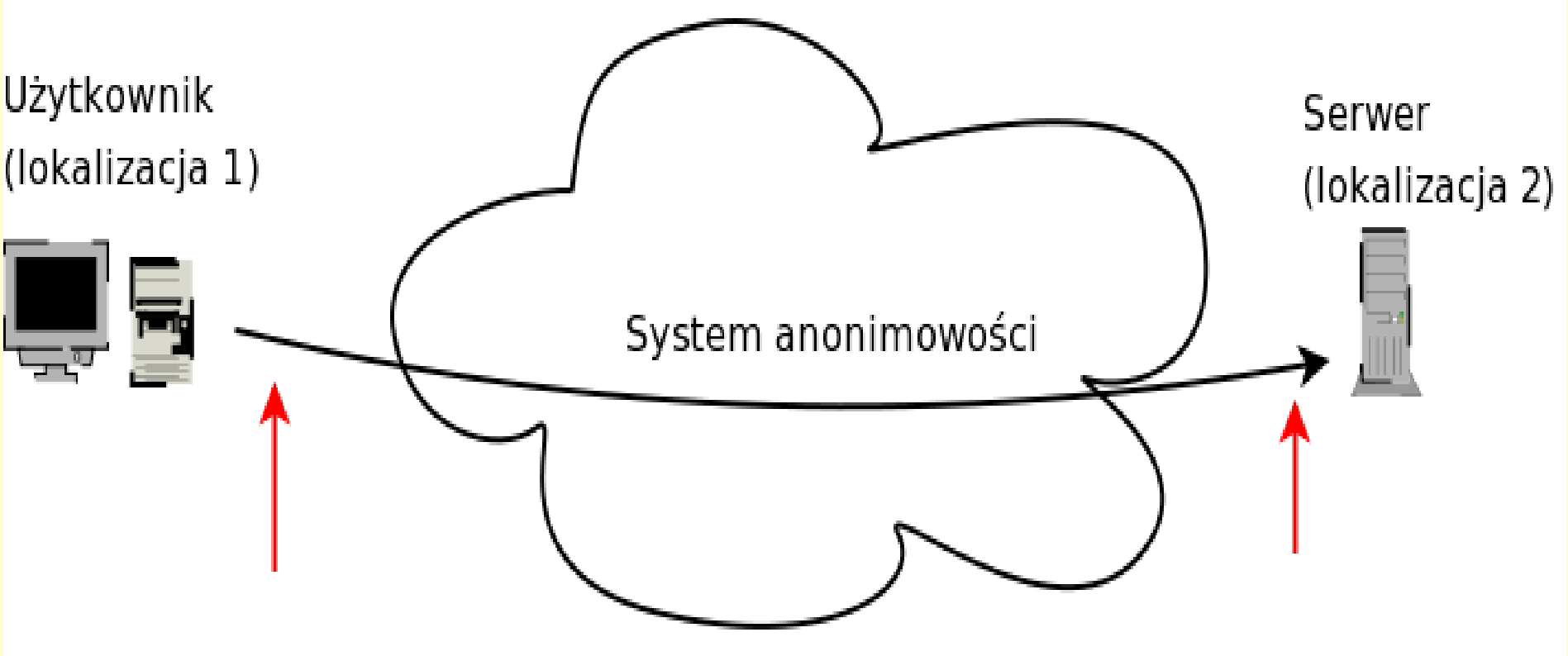
Model ataku: atakujący

- Dostęp do ruchu w dwóch punktach:
  - między pierwszym węzłem systemu anonimowości a jedną stroną
  - między ostatnim węzłem systemu anonimowości a drugą stroną
- Modyfikacje z jednej strony, sprawdzenie z drugiej
- Bez modyfikacji systemu anonimowości (wszystkie operacje są legalne)

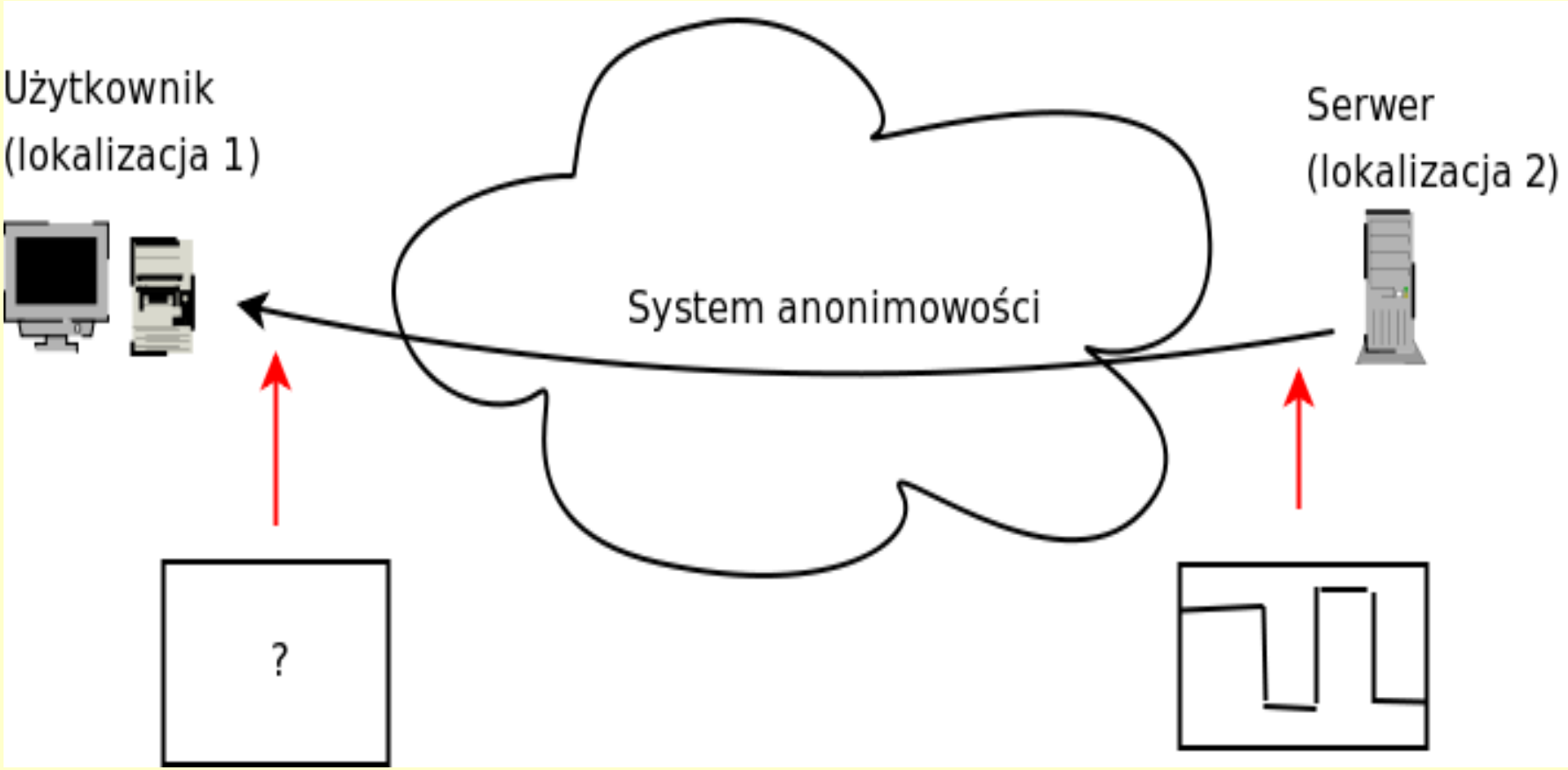
Atakujący: model realistyczny



Konfiguracja testowa



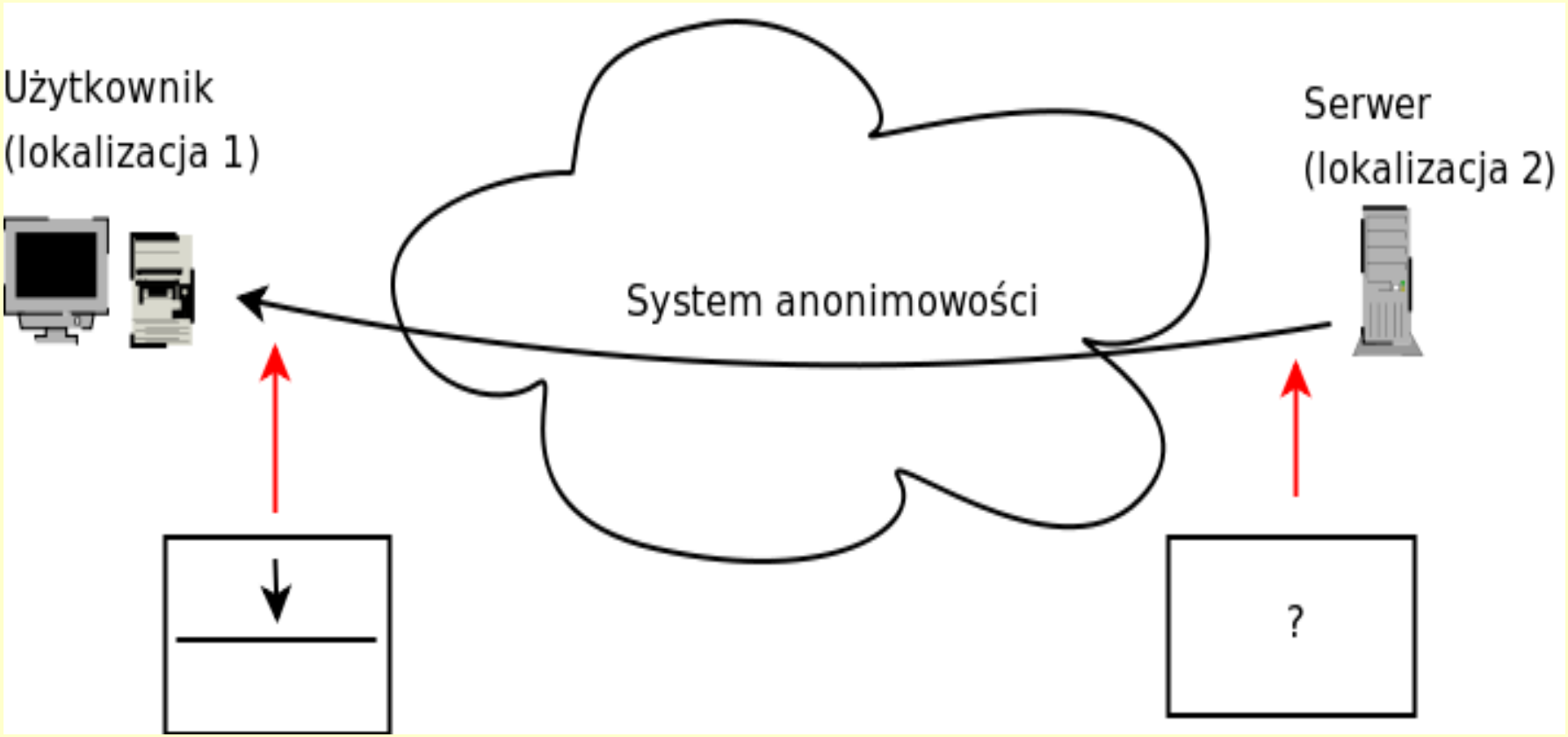
Atak “do przodu”



Atak “do przodu”: wyjaśnienie

- Własności protokołu TCP:
  - druga strona (odbierający) otrzymuje dane w tej samej kolejności, w jakiej zostały wysłane
  - w konfiguracji z wieloma węzłami opóźnienia będą tylko wzrastać
  - sterowanie przepływem

Atak “do tyłu”


Użytkownik
(lokalizacja 1)
Serwer
(lokalizacja 2)
System anonimowości
?

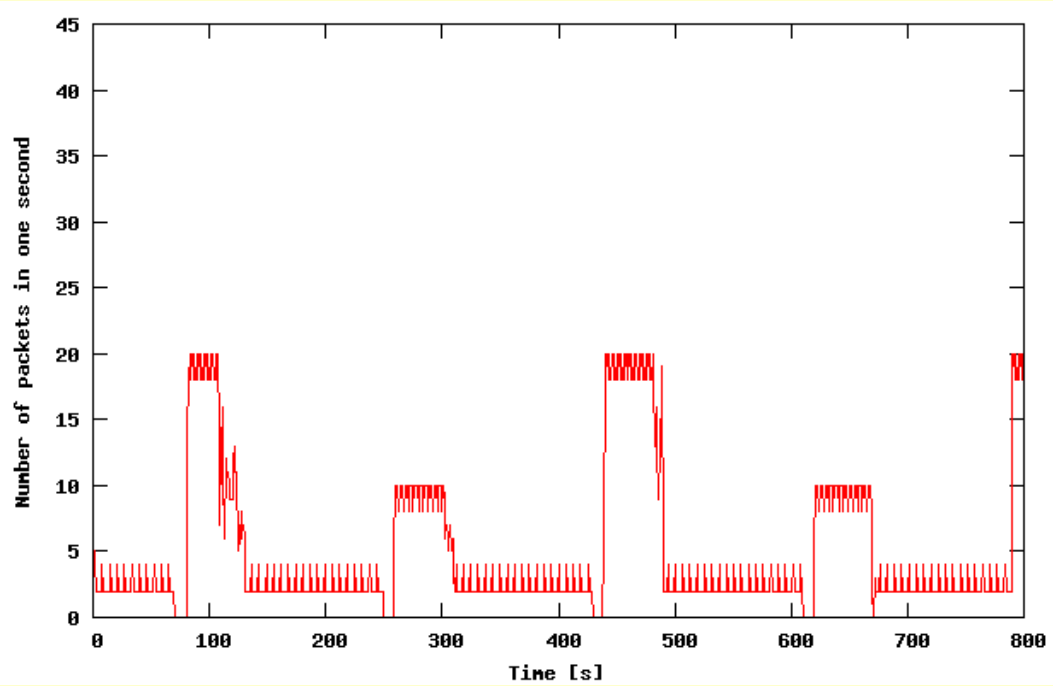
Atak “do tyłu”: wyjaśnienie

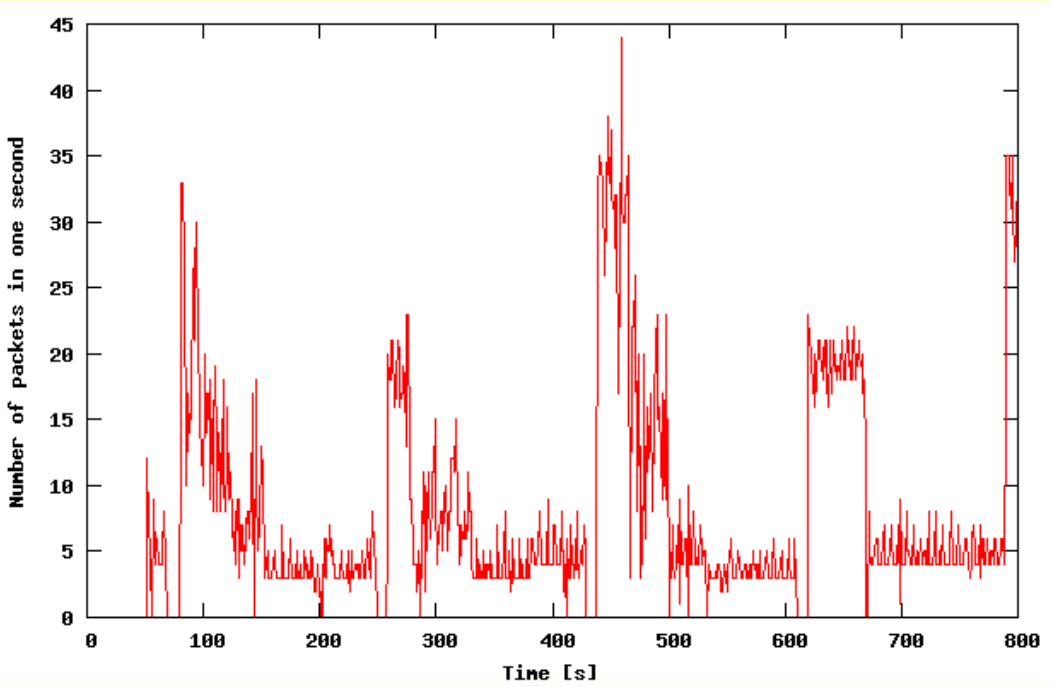
- Własności protokołu TCP:
  - druga strona (odbierający) otrzymuje dane w tej samej kolejności, w jakiej zostały wysłane
  - mechanizm okna: maksymalna ilość danych znajdujących się w sieci
  - w konfiguracji z wieloma węzłami: zatrzymanie transmisji do opróżnienia buforów na kolejnych etapach

Wyniki

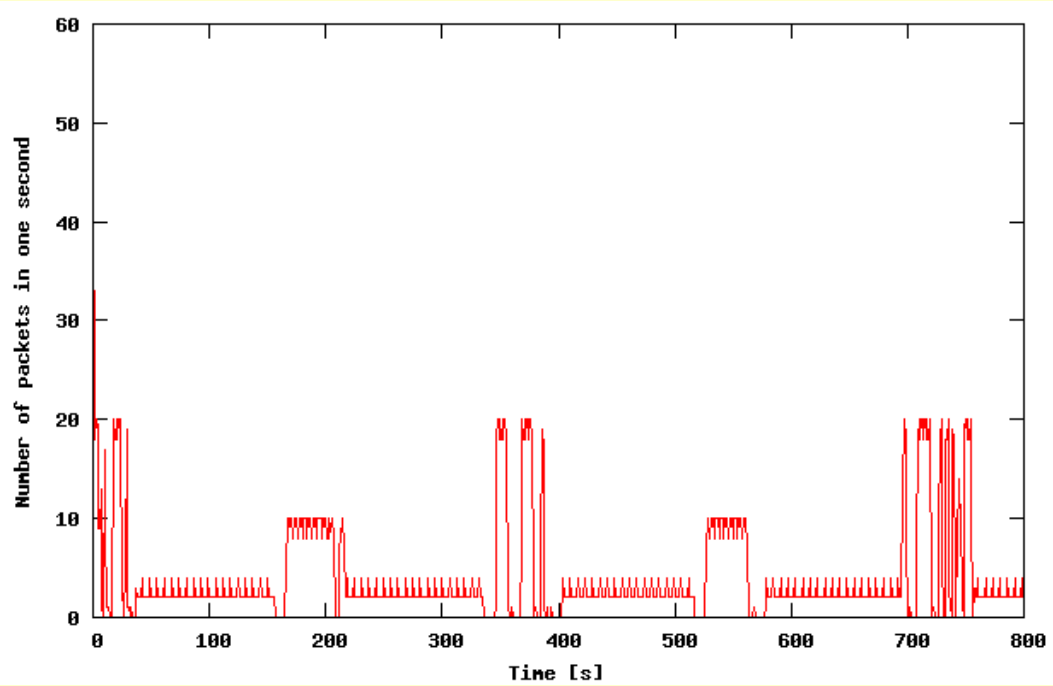
- Atak “do przodu”
  - Tor: tak (b. małe zmiany)
  - JAP: tak (małe zmiany)
- Atak “do tyłu”
  - Tor: tak (dużo szybciej niż oczekiwano)
  - JAP: nie (?)

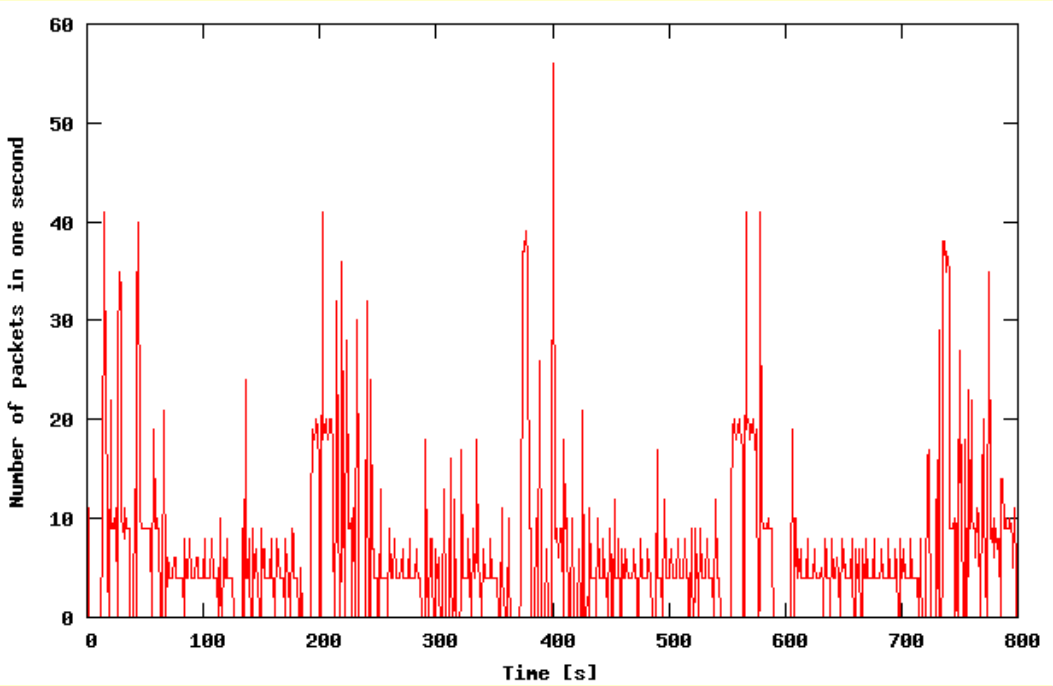
Atak “do przodu”: Tor



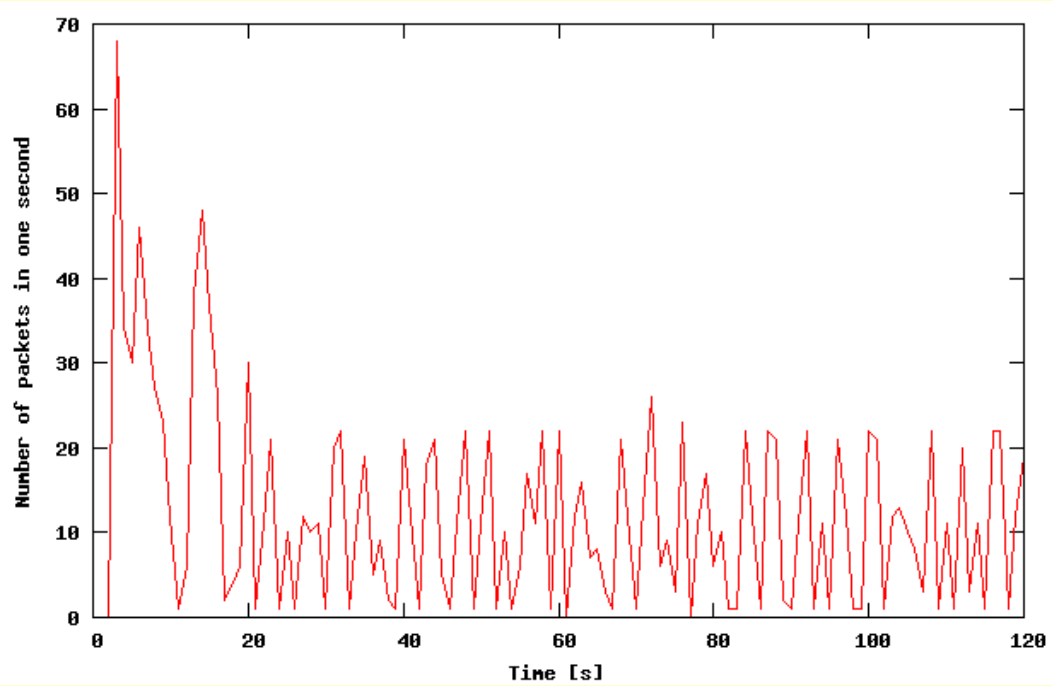


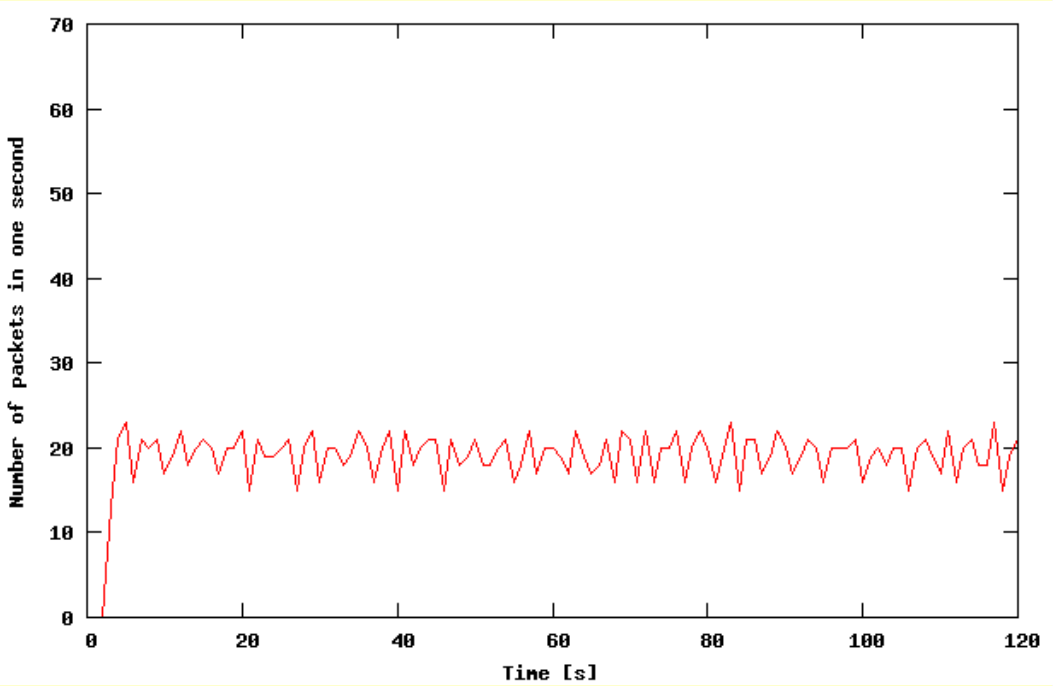
Atak “do przodu”: JAP





Atak “do tyłu”: Tor

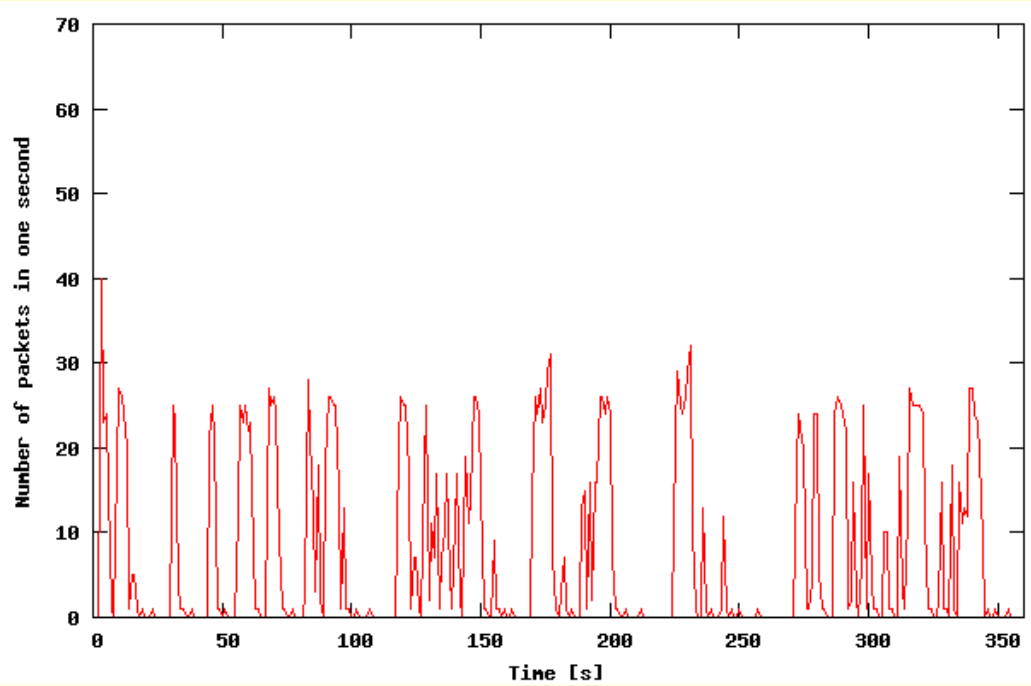


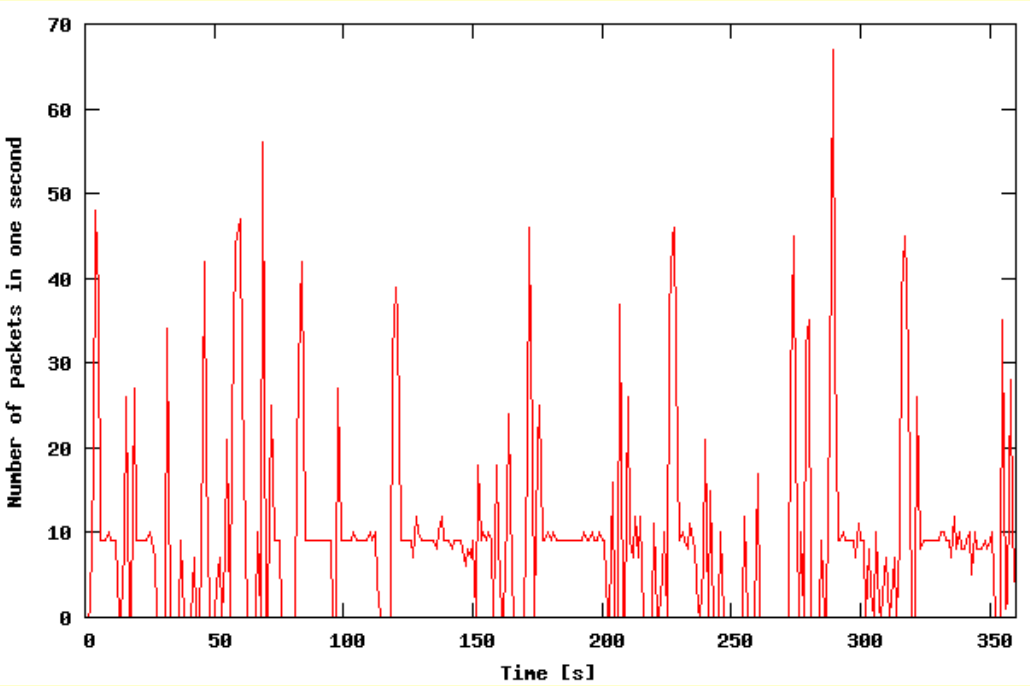


Czas trwania ataku

- Pierwsze “zero window” (26 obwodów), plik ok. 600KB
  - poniżej 200KB – 6
  - 200–400KB – 3
  - 400–600KB – 8
  - powyżej 600KB – 9

Atak “do tyłu”: JAP





Ataki praktyczne

- Atak “do przodu”
  - kilka minut przy ograniczeniu przepływności
  - większa liczba plików
- Atak “do tyłu”
  - Tor – ok. 1MB
  - JAP – nie?

Ataki:podsumowanie

- Oba systemy nie dają większej ochrony niż zestaw proxy
- Potrzebne dodatkowe mechanizmy ochronne
  - architektura
  - protokoły (!)

Marta Rybczyńska
<marta@rybczynska.net>

Analiza ruchu w systemach anonimowości: Tor i JAP