P2PRIV

Anonimowa sieć nakładkowa niskich opóźnień oparta na protokole P2PRIV

Autor: Krzysztof Lasota
Opiekun naukowy: dr inż. I. Margasiński

Plan prezentacji

- Wprowadzenie
- Systemy P2P
- Anonimowość
- Sieci MIX-NET
- P2PRIV
- Implementacja
- Podsumowanie

Wprowadzenie

Potrzeby:
- ochrona prywatności
- brak wolności słowa
- cenzura

Motywacja:
- brak wydajnego systemu zapewniającego wysoki poziom anonimowości

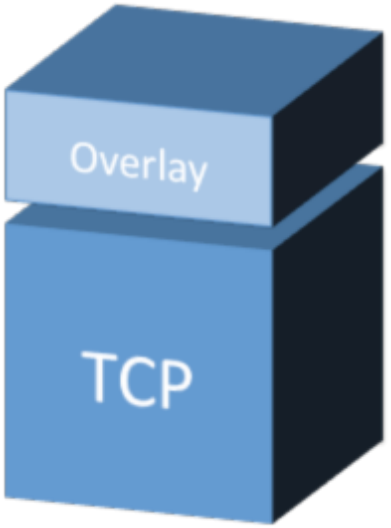
Celem pracy jest implementacja wydajnego systemu umożliwiającego anonimowe pobieranie plików.

Systemy P2P

Rozproszone sieci nakładkowe .

Typy sieci:

- Czysty P2P
- Hybrydowy P2P



Anonimowość

Pfitzmann i Hansen zdefiniowali anonimowość jako stan bycia nieidentyfikowalnym wśród elementów zbioru.

Istniejące rozwiązania

TOR

Crowds

Tarzan

Mixminion

Onion Routing

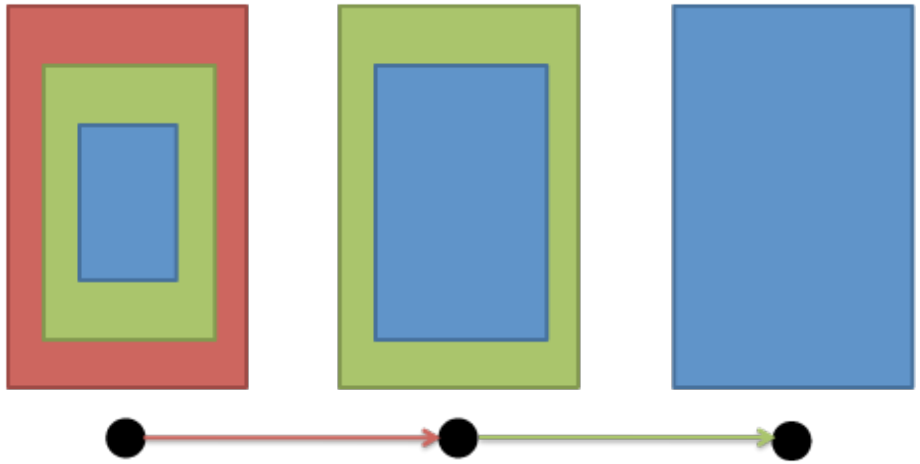
Cebolla

MorphMix

MixMaster

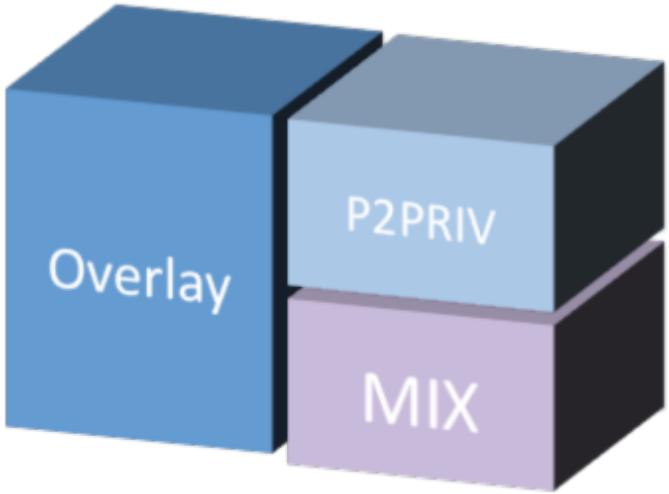
Sieci MIX-NET

- Koncepcja działania – Chaum (1981)
- Zastosowanie
- Rodzaje Mix-Netów:
  - Continuous MIX
  - Pool MIX



P2PRIV

Nakładkowa sieć P2P
służąca do szybkiego i anonimowego
pobierania danych



P2PRIV - „Peer-to-peer direct and anonymous distribution overlay”

P2PRIV - Opis systemu

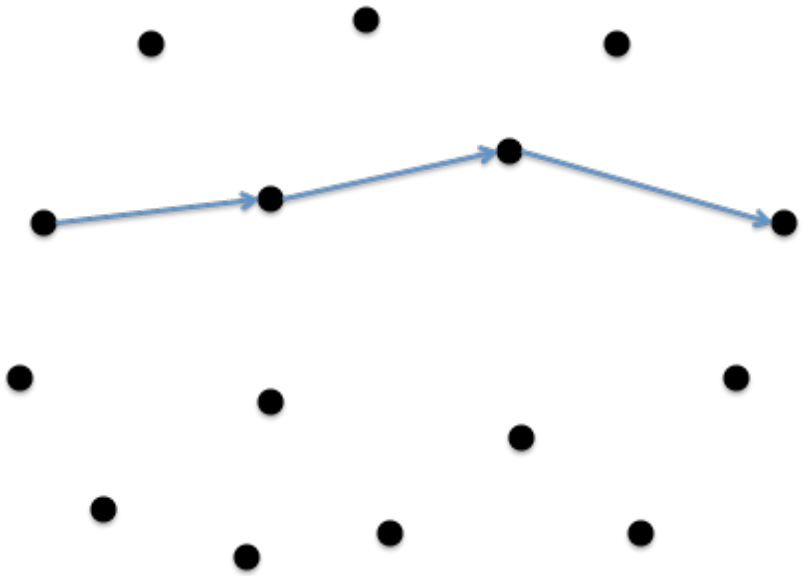
Anonimowość odbiorcy pliku jest zapewniona na postawie niemożliwości wskazania inicjatora żądania pobierania, ponieważ dany zasób jest ściągany również przez losową ilość, losowo wybranych węzłów zwanych „klonami”.

Każdy z węzłów należących do kaskady klonów (inicjator oraz klony) pobierają dany zasób po losowo wybranym czasie.

P2PRIV - Opis architektury 1/3

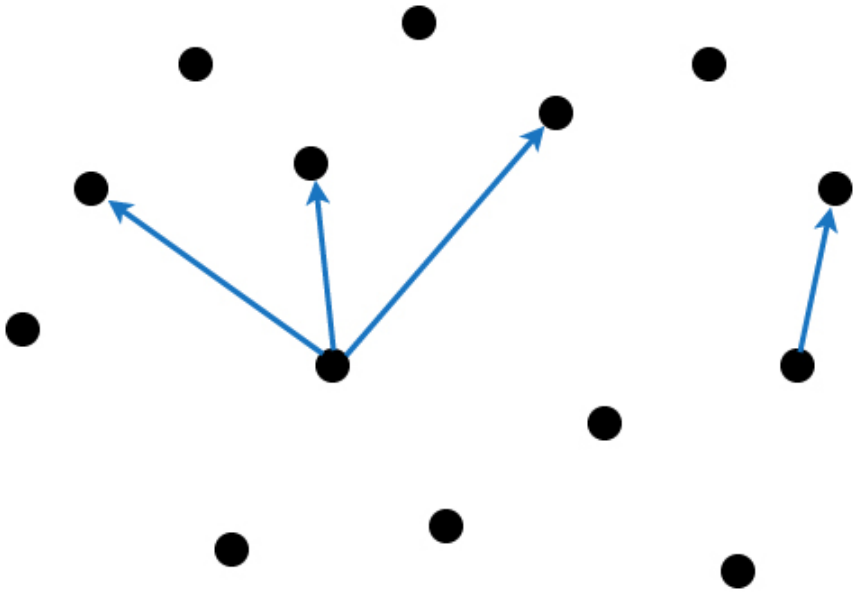
- Oddzielenie przesyłania wiadomości sygnalizacyjnych zapewniających anonimowość od pozostałych
- wiadomości sygnalizacyjne przekazywane przez sieć mix-net
- równoległy pobór danych

P2PRIV – Opis architektury 2/3

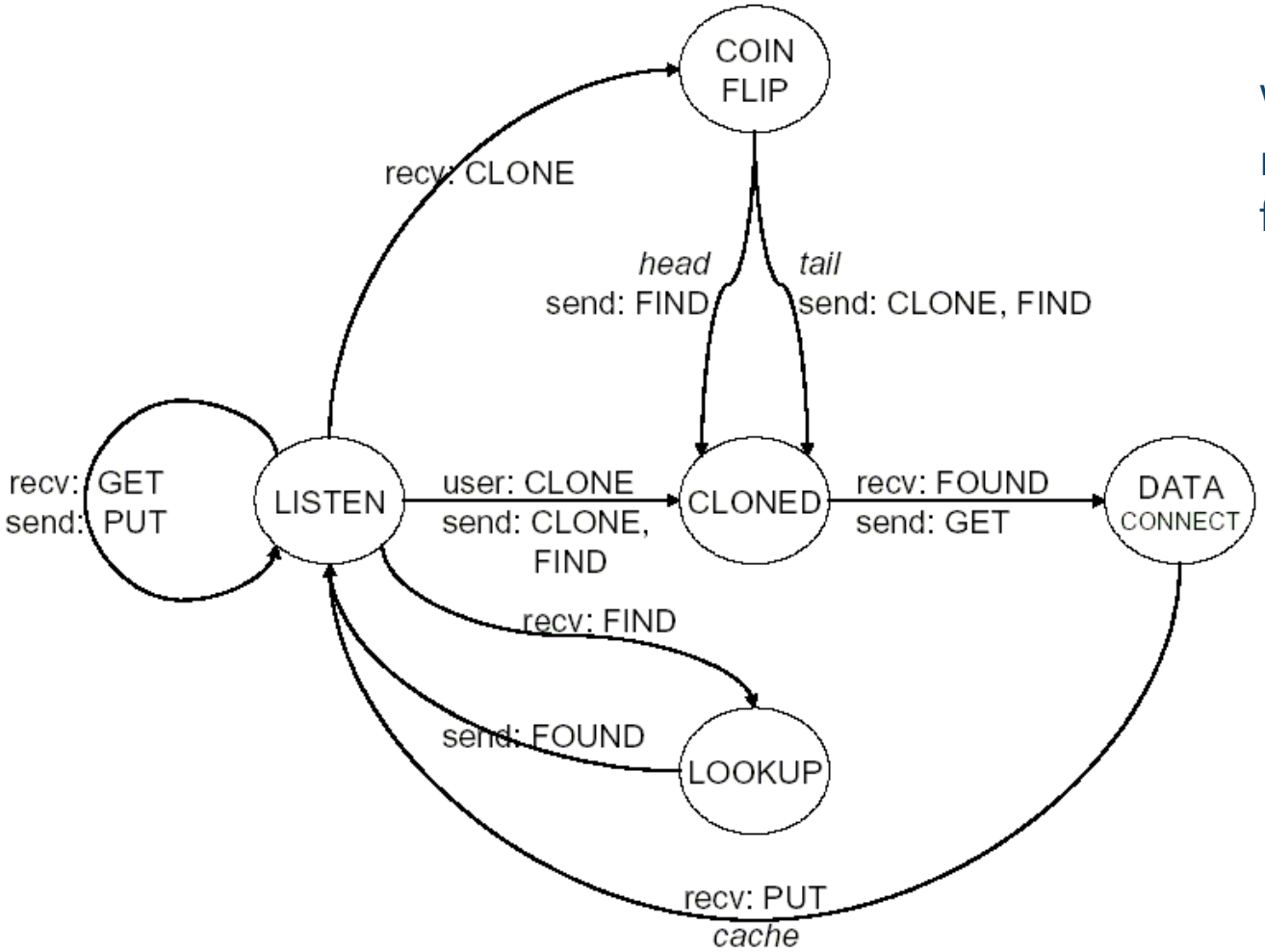


Kaskadowy pobór danych

Równoległy pobór danych

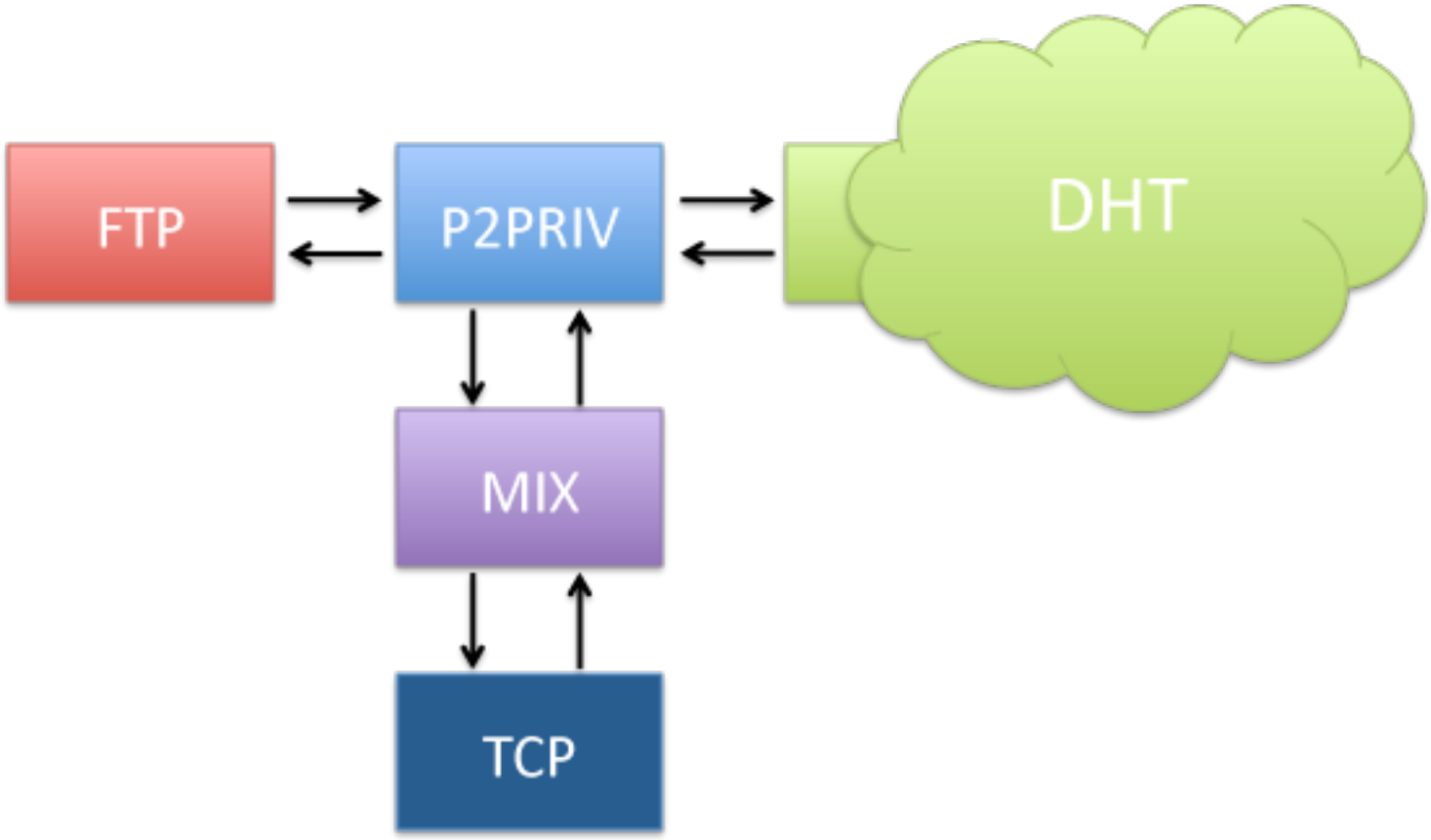


P2PRIV - Opis architektury 3/3



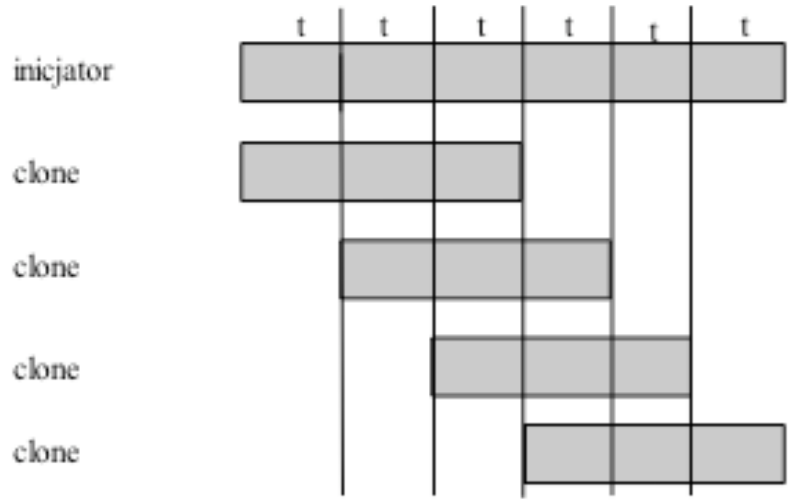
Wszystkie węzły mają jednakową funkcjonalność.

Implementacja



Zaimplementowane mechanizmy zapewniające anonimowość – podwarstwa P2PRIV

Funkcja losowego przedziału czasu



Rys 2. Przedziały czasów dla poszczególnych węzłów przed dodaniem tajnej liczby ms

Zaimplementowane mechanizmy zapewniające anonimowość – podwarstwa MIXNET 1/2

- Każdy węzeł posiada parę kluczy (algorytm RSA)
- Klucze sesyjne tworzone za pomocą algorytmu AES
- stała długość wiadomości
- bufory: ilościowy, czasowy
- mieszanie bufora
- znacznik czasowy wiadomości

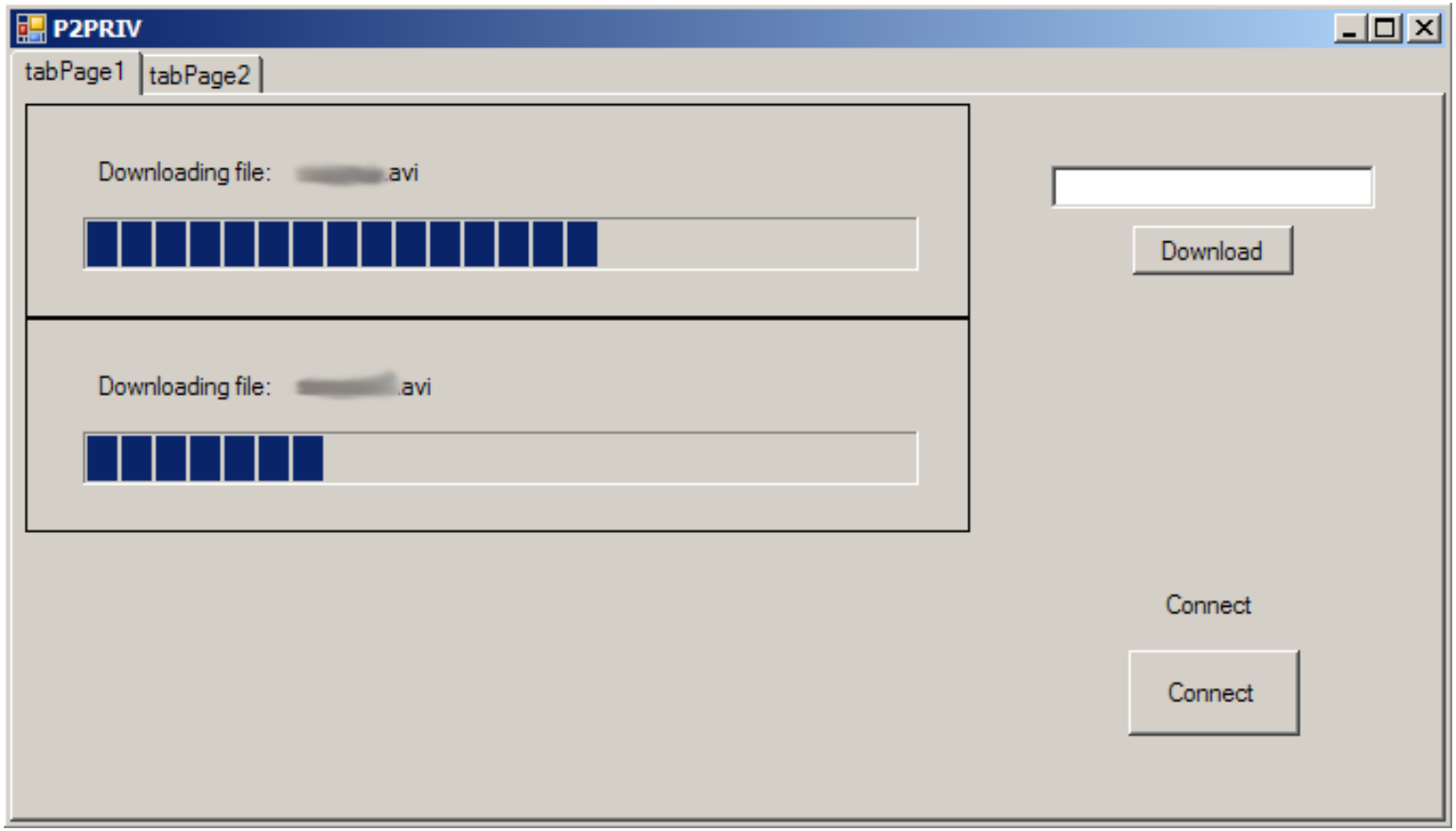
Zaimplementowane mechanizmy zapewniające anonimowość – podwarstwa MIXNET 2/2

Utrzymywanie jak największej liczby dostępnych mixów:

- przy starcie lista dostępnych mixów ograniczona jest do „fingerów” z DHT po czym następuje pobranie listy użytkowników (tylko adresy IP) ze wskazanych węzłów.

- próba uzyskania połączenia na port danych w celu określenia czy dany węzeł wciąż jest aktywny (wykorzystanie bufora czasowego)

GUI aplikacji



Podsumowanie

Mocne strony prototypu:

- zapewnia anonimowość pracy w sieci
- trudność w przeprowadzenia skutecznego ataku DoS na sieć
- duże możliwości konfiguracyjne – kształtowanie ruchu w sieci
- odporność na ataki powtórzeniowe
- szybki pobór danych

Słabe strony prototypu:

- łatwy atak DoS na węzeł
- długi czas podłączania się węzła do sieci
- wymagany publiczny adres IP do pracy

Perspektywy rozwoju

- Dalsza praca nad rozwojem aplikacji
- Zaimplementowanie efektywniejszego sposobu transferu plików
- Przystosowanie do działania w różnych środowiskach i systemach operacyjnych (port Mono)
- Umożliwienie pracy za NAT-em (implementacja UPnP)
- Zmiana sposobu identyfikacji użytkowników
- Porównanie z istniejącymi systemami
- Analiza kwestii bezpieczeństwa i podatności na ataki

P2PRIV

Anonimowe rozproszone sieci P2P niskich opóźnień oparte na architekturze P2PRIV

Autor: Krzysztof Lasota
Opiekun naukowy: Dr inż. I. Margasiński