I2P

Kamil Niewiara

Wydział Matematyki, Fizyki i Informatyki
Politechnika Krakowska im. Tadeusza Kościuszki

19 czerwca 2019

Co to jest I2P?

I2P (ang. Invisible Internet Project), czyli projekt niewidzialnego internetu to sieć peer-to-peer (wszyscy użytkownicy mają te same upranienia, mogą być zarówno klientem jak i serwerem) charakteryzująca się komutacją pakietów (dzieleniu strumienia danych na mniejsze kawałki i przesyłania je osobnymi węzłami), wielowarstwowym szyfrowaniem transmisji oraz rozproszoną organizacją. Sieć powstała w 2003 roku, kiedy to część programistów biorących udział w projekcie innej anonimowej sieci, Freenet, odłączyła się i stworzyła I2P.

Do czego służy?

Sieć I2P ukrywa nasz adres IP, co uniemożliwia rozpoznanie naszej wirtualnej tożsamości oraz zapewania prawie stuprocentowe bezpieczeństwo przesyłanym danym. Z tego powodu może być używana przez wszystkich, którzy nie chcą być inwigilowani przez służby państw i korporacje, w tym również przestępców. Anonimowa sieć służyć może też do omijania cenzury i blokady informacyjnej w państwach, które nie respektują wolności słowa.

Baza danych netDb

Każdy użytkownik I2P stanowi węzeł (router), który bierze udział w trasowaniu połączeń. Każdy węzeł jest częścią rozproszonej bazy danych netDb i przechowywana jest w nim i uaktualniana część informacji. Tworzone są dwa zestawy informacji:

- **routerInfo** - etykieta węzła I2P, która zawiera między innymi adres IP, klucze kryptograficzne do automatycznego szyfrowania odbieranych połączeń, sygnaturę potwierdzającą tożsamość.
- **leaseSet** - zawiera informację o otwartych tunelach odbiorczych i nadawczych, którymi użytkownicy wysyłają pakiety.

Za pomocą bazy netDb ustala się odpowiednie ścieżki dostępu do innych węzłów sieci I2P.

Trasowanie czosnkowe

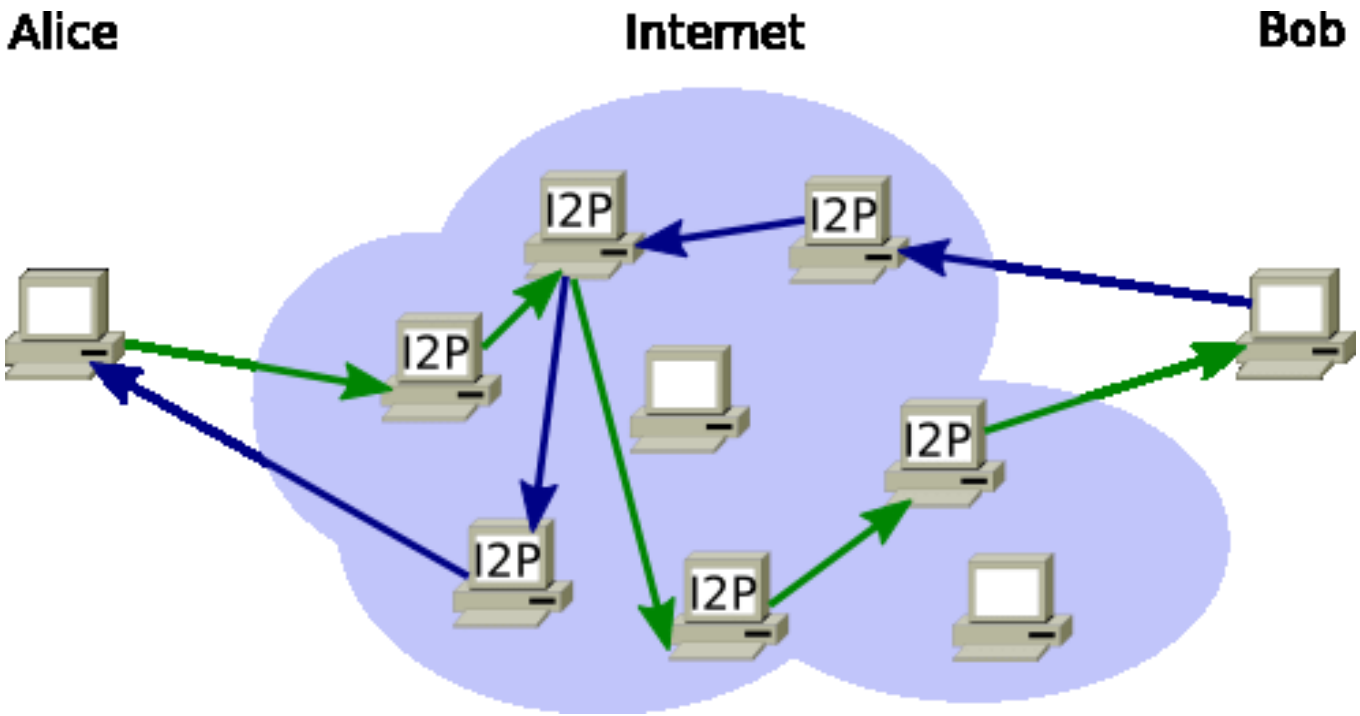
Przykładowy schemat działania sieci I2P:

- Aby połączyć się z komputerem docelowym B, w sieci I2P nasz komputer najpierw wyszukuje w netDb klucze kryptograficzne i dane o bramie wejściowej tunelu odbierającego serwera B. Następnie żądania do serwera B są szyfrowane za pomocą jego klucza publicznego algorytmem ElGamal i wiązane w pakiet zwany główką czosnku.
- W następnej kolejności nasz komputer tworzy tunel wysyłający: wybiera z sieci I2P trzy losowe węzły (ostatni z nich to bramka wyjściowa), a ich klucze publiczne szyfrują naszą główkę czosnku. Główka czosnku przechodząc przez kolejne węzły jest deszyfrowana przez ich klucze prywatne. Gdy opuszczaja ona bramę wyjściową, ta kładzie na przesyłany pakiet międzytunelową warstwę szyfrowania.

Trasowanie czosnkowe

- Komputer B tworzy tunel odbierający między trzema innymi losowymi węzłami sieci I2P, ostatni z nich to bramka wejściowa, do której wchodzi główka czosnku. W bramie wejściowej międzytunelowa warstwa szyfrowania jest zdejmowana. Pakiet przechodząc przez kolejne węzły jest ponownie szyfrowany kluczami publicznymi, natomiast klucze prywatne są przekazywane do komutera B. Gdy główka dotrze do komputera B, ten kolejno zdejmuje z niej kolejne warstwy szyfru za pomocą, otrzymanych wcześniej z węzłów, kluczy prywatnych.
- Aby odczytać wiadomość trzeba ją na końcu deszyfrować za pomocą klucza prywatnego ElGamal.

Przedstawiony wyżej mechanizm nosi nazwę trasowania czosnkowego (garlic routing).



Rysunek: Schemat I2P. Rysunek można znaleźć w [4].

Możliwości

W sieci I2P istnieją usługi o funkcjonalności podobnej do sieci internet:

- strony internetowe umieszczone w I2P, to tzw. Eepsite, na których potrzebę stworzono pseudodomenę z rozszerzeniem .i2p
- serwery IRC
- anonimowe serwery proxy działające dla stron www znajdujące się poza siecią I2P
- mechanizmy wymiany plików pomiędzy użtkownikami
- zdecentralizowany i anonimowy system maili I2P-Bote

I2P, a Tor

Można porównać te dwie anonimowe sieci:

- I2P jest dużo mniej popularna od TORa i raczej nie stanowi dla niego konkurencji, ma też o wiele mniejszą liczbę użytkowników. Tor ma również większe wsparcie ze strony specjalistów oraz więcej środków finansowych.
- Do zalet I2P należy traktowanie wszystkich użytkowników jako węzły, a nie tylko wybranych jak w Torze (pełna decentralizacja), szersze wsparcie dla protokołów sieciowych, jest też szybsza.

Źródła

[1] Tomasz Ciborski,
Ukryta tożsamość. Jak się obronić przed utratą prywatności,
Helion, 2015

[2] http://www.benchmark.pl/testy_i_recenzje/siec-i2p.html

[3] https://geti2p.net/pl/docs/how/tech-intro

[4] https://www.researchgate.net/figure/I2P-architecture-Guide-2017_fig2_317115265