

Untersuchung der Performance des Invisible Internet Protocols (I2P)

Bachelorarbeit

Moritz Küttel

Hochschule Luzern Informatik

in Zusammenarbeit mit

DIVA.EXCHANGE

Zwischenpräsentation, 21.4.2020

Inhaltsverzeichnis

- 1 Einleitung und Aufgabenstellung
- 2 Stand der Technik
- 3 Konzept Teststand
- 4 Projektverlauf
- 5 Abschluss

Einleitung

Der Verein DIVA.EXCHANGE entwickelt einen Softwareprototypen
für eine *dezentrale* Handelsplattform

Benutzer sollen Güter und digitale Werte austauschen können

ohne sich zu kennen

und

ohne gegenseitiges vertrauen

DIVA.EXCHANGE Architektur I



Freie Banking-Technologie. Für alle.
DIVA.EXCHANGE: so funktioniert's.

Deine Hardware + deine DIVA Software



- privat
- verteilt
- deins

BENUTZEROBERFLÄCHE
GESCHÄFTSLOGIK
VERSCHLÜSSELUNG

SPEICHER

I2P VERSCHLÜSSELUNG
I2P TRANSPORT

Daten

Internetzugang + I2P Netzwerk



💰 beitragen + verdienen

DIVA.EXCHANGE Architektur II

Der Software-Prototyp besteht aus drei Schichten:

- **Handelsplattform:** Benutzeroberfläche und Geschäftslogik
- **Speicherschicht:** Blockchain, Speichert die Transaktionen
- **Netzwerkschicht:** Basierend auf dem Invisible Internet Protocol (I2P) für verschlüsselte und anonymisierte Kommunikation zwischen den Knoten

Der Fokus der Arbeit liegt auf der Netzwerkschicht.

Aufgabe I

- **Problemstellung:** Initiale Tests haben ergeben, das jedoch die Netzwerk-Schicht zu “langsam” ist.
 - Roundtrip einer Nachricht im Bereich von 3-8 Sekunden
Latenz im öffentlichen I2P-Netzwerk
- **Ziel:** Herausfinden unter welchen Umständen und Rahmenbedingungen kürzere Latenzzeiten erreicht werden können
- **Fragestellung:** Verringert sich die Latenz der Nachrichten je mehr Knoten sich am Netzwerk beteiligen?
- **Vorgehen:** Mittels eines Teststands sollen Latenzmessungen durchgeführt werden, um die Fragestellung empirisch beantworten zu können.
- **Vision:** Könnte dies belegt werden, könnten mehr Leute überzeugt werden einen I2P-Knoten zu betreiben. Dies würde das Netzwerk stärken.

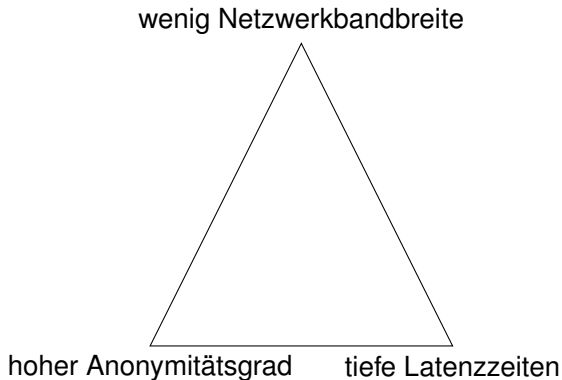
Anforderungen

- Stand der Technik bezügl. I2P und dem zu erstellenden Teststand erfassen
- Das Testnetzwerk soll isoliert sein und abgeschottet vom öffentlichen I2P Netzwerk
- Es sollen verschiedene Messungen mit verschiedenen Konfigurationseinstellungen getätigt werden können.
- Es soll möglich sein schnell (innerhalb von 2h) eine Messung mit anderer Konfiguration zu starten
- Die Anzahl I2Pd-Knoten im Testnetzwerk soll konfigurierbar sein (8-256).
- Die Messungen im Teststand sollen reproduzierbar sein
- Es soll eine quantitative Auswertung durchgeführt werden.

Inhaltsverzeichnis

- ① Einleitung und Aufgabenstellung
- ② Stand der Technik
- ③ Konzept Teststand
- ④ Projektverlauf
- ⑤ Abschluss

Das Anonymitätstrilemma



Es muss ein passender Kompromiss zwischen diesen Aspekten gefunden werden.

Invisible Internet Protocol (I2P)



- Dezentrales, Peer-to-Peer-Netzwerk bestehend aus I2P-Routern/Knoten
- Overlay-Netzwerk, "verstecktes" Netzwerk innerhalb vom bestehenden IP-Netzwerk
- Nachrichtenbasiert (vergleichbar mit IP/UDP)
- Mischnetzwerk, Nachrichten können über mehrere Knoten geroutet werden, um Herkunft zu verschleiern
- End-to-End Verschlüsselung von Nachrichten

Wir legen den Fokus auf die C++-Implementation (i2pd) und nicht auf die Java-Implementation (i2p).

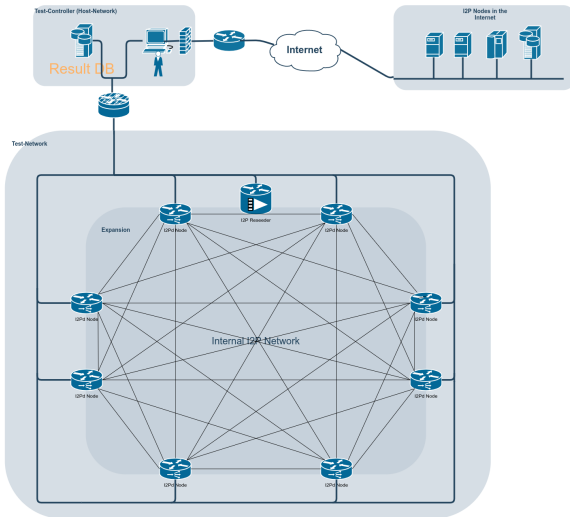
Inhaltsverzeichnis

- ① Einleitung und Aufgabenstellung
- ② Stand der Technik
- ③ Konzept Teststand
- ④ Projektverlauf
- ⑤ Abschluss

Konzept I

- **Reproduzierbarkeit:** Infrastruktur des Teststands als Code, Privates Testnetzwerk
- **Deployment:** Ein Container pro I2P-Router/Knoten
- **Konfigurierbarkeit:** Anzahl Container/Knoten, verschiedene Router-Konfigurationen
- **Isolierung:** Abschotten vom öffentlichen Netzwerk, VM mit Firewallregeln
- **Latenzmessung:** Verschicken von Nachrichten von Knoten an andere. *Latenz = Ankunftszeitpunkt – Sendezeitpunkt*
- **Bootstrapping:** Extra Container welche initialen Netzwerkkoordinaten der Knoten verteilt (reseeder)

Konzept II



Inhaltsverzeichnis

- ① Einleitung und Aufgabenstellung
- ② Stand der Technik
- ③ Konzept Teststand
- ④ Projektverlauf**
- ⑤ Abschluss

Projektverlauf

- 1. Ansatz NixOS/NSpawn Container
 - Erst Probleme mit der Netzwerkkonfiguration
 - Probleme mit Docker-Kompatibilität
 - Skaliert nicht auf mehr als ein paar dutzend Container. Zu viel RAM benötigt lediglich zum Berechnen der verschiedenen Container-Konfigurationen.
- Deshalb umgestiegen auf docker-compose-Ansatz
 - 256 i2pd-Container konnten erstellt werden
 - Wiederverwendung bestehender Docker-Container
 - Anfangs triviale Netzwerkkonfiguration, aber ich stosse damit an Grenzen.

Jetziger Stand

Folgendes im Teststand ist implementiert:

- Konfigurierbare Anzahl-Knoten
- Isolierung vom öffentlichen Netzwerk
- Bootstrapping / Reseeding erfolgreich
- Anfangen mit TCP-Server zum Messen der Latenz
- Probleme mit der Netzwerkkonfiguration

Das Projekt ist im Verzug, der Teststand sollte bereits Ende letzte Woche fertig sein.

Inhaltsverzeichnis

- ① Einleitung und Aufgabenstellung
- ② Stand der Technik
- ③ Konzept Teststand
- ④ Projektverlauf
- ⑤ Abschluss

Weiteres Vorgehen

- Lösen der Netzwerkkonfigurationsprobleme
- Fertigstellung des TCP-Servers zur Latenzmessung
- Verschicken von Nachrichten und Latenzmessung
- Durchführen von Messungen mit verschiedenen Konfigurationen
- Auswertung und Vergleich der Messungen

Abschluss

Danke für Ihre Aufmerksamkeit.

Zeit für Fragen.

