Discrete modeling of transaction propagation in ₿itcoin

Author: Tomáš Marek
Supervisor: Ing. Jan Zavřel
2024

Objectives

- **create a design for a highly simplified Bitcoin client** that can create, receive, and send messages representing Bitcoin transactions and that operates according to the **algorithm from the Bitcoin Core Project** implementation
- create a **simulation model** in OMNeT++ simulator
- simulate the Bitcoin network with a **monitoring node** that keeps track of the messages from Bitcoin clients and exports a **CSV file** with collected information
- **analyze** the message propagation and the behavior of the simulation
- **identify any significant nodes** in the Bitcoin network
- **identify possible source nodes** of transactions

Topology of the simulation network

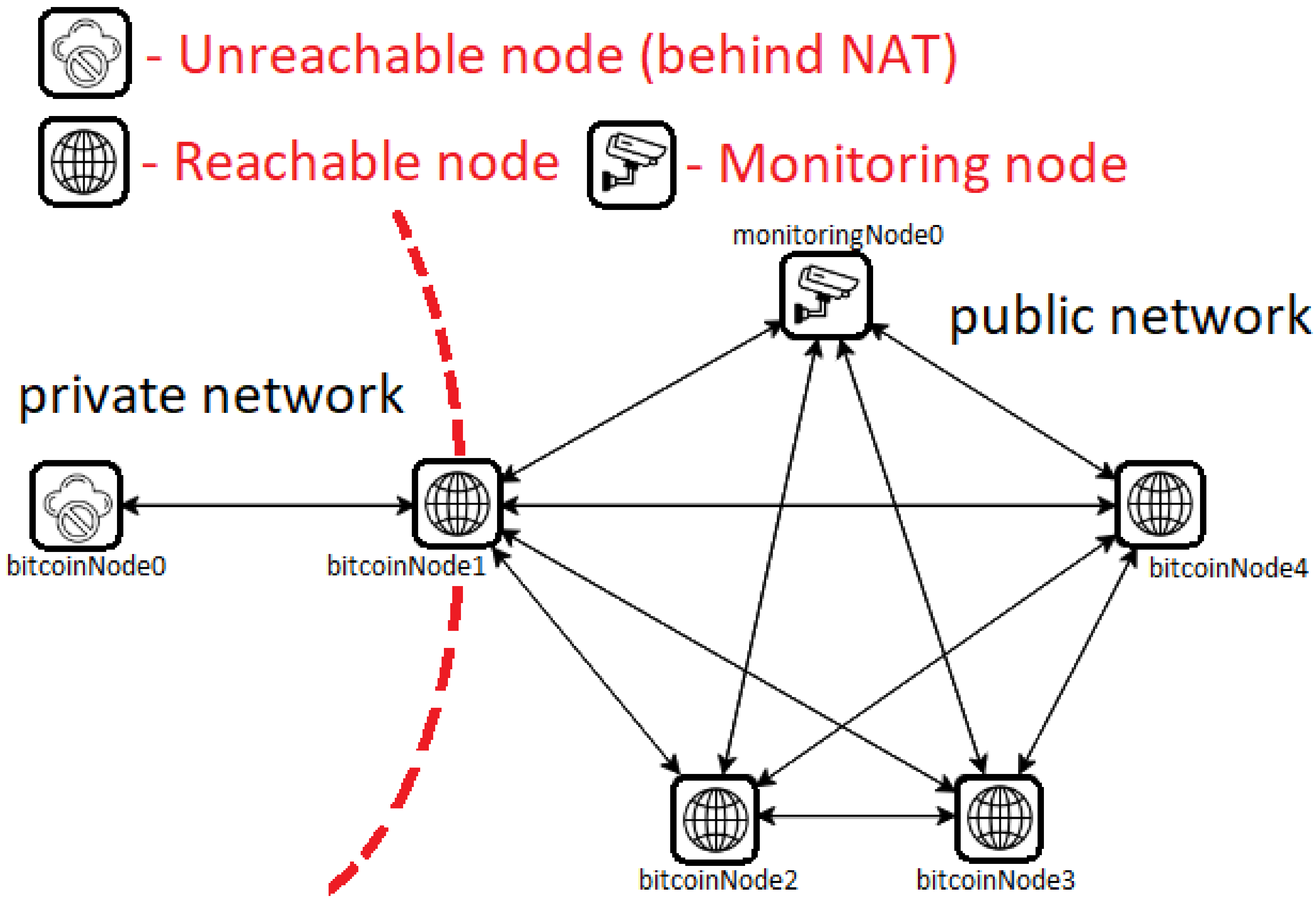


Figure 1: Topology of the simulation network. The bitcoinNode0 generates the transaction (tx). The monitoring node on the top of the topology is connected through outbound connections to all reachable nodes collecting the information about the generated tx from all nodes.

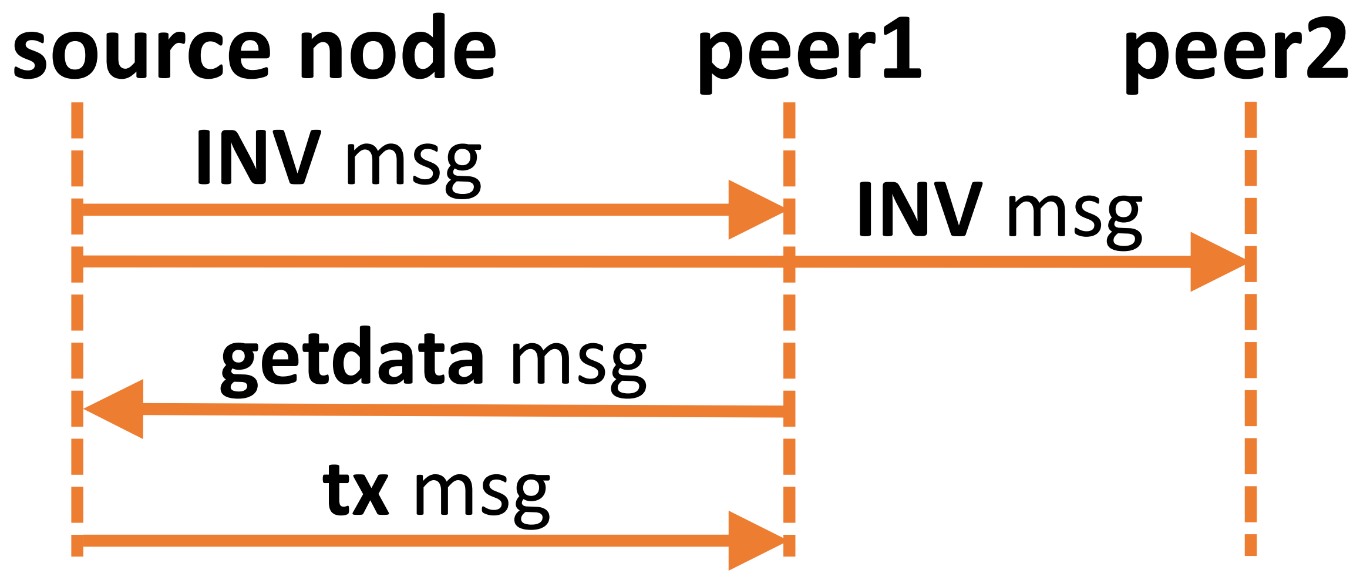
Pseudocode of the Bitcoin client propagation algorithm

```
OUTBOUND_INTERVAL ← 2 seconds
INBOUND_INTERVAL ← 5 seconds
if mempool.contains(receivedTx):
    nothing /* ignore the tx */
else: /* tx is not in the mempool */
    mempool.add(receivedTx)
    for all outbound connections:
      delay ← GetExponentialRand(OUTBOUND_INTERVAL)
      sendToPeer(delay)
    delay ← GetExponentialRand(INBOUND_INTERVAL)
    for all inbound connections:
      sendToPeer(delay)
```

CSV file structure

run, TXID, peer, timestamp

Tx propagation process



Sequence diagram of transaction propagation process, where source node generates the tx.

Excel@FIT 2024

BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY