INTRODUCTION TO BLOCKCHAIN AND CRYPTOCURRENCY

Project

April 17, 2020

Praveen Kumar - 1601041
Abhinav Jha - 1601002
Apoorva Sharma- 1601008
Ashok Kumar - 1601009

Contents

0.1 Problem Statement

A network which consists of **RSU (Road Side Units)** and Crowdsourced **OBU (On Board Unit)**. The head OBU is agreed on the shortest path after consulting the the other OBUs based on **PBFT consensus algorithm**.
Do the simulation of the above problem (No need to use any crypto premitive). Use PBFT algorithm to select a newhead OBU in a new session.

0.2 Overview

Glimpse Idea-

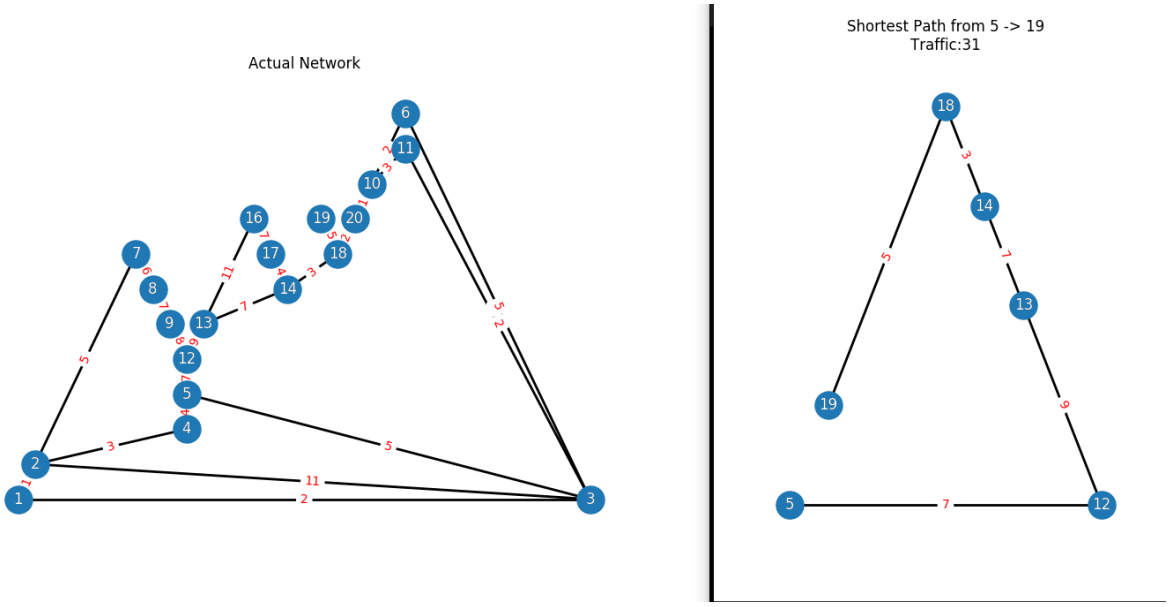

Figure 1: Road Network

- A road network where nodes represent the OBU's.
- A vehicle queries the nearest RSU for the shortest path to its destination.
- The shortest path is calculated over the traffic offered by the path.
- The head OBU is elected which in turn perform the consensus and delivers the result to the end-user.

0.3 Algorithm + Working

0.3.1 Objects

- GRAPH - Contains all the nodes and edges associated with the Road Network.

- VIEW - Contains all the variables associated with a round/view.
- MESSAGE - Contains all the variables required to generate a message in the algorithm like - (body, digest, PrK, viewNo. etc)
- DISPLAY-PATH - This object visualizes the graph fed to it.
- PBFT - The main class which controls the working of the whole algorithm.
- SHORTEST-PATH - It finds the shortest path from the source and destination, we used Djikstra Algorithm over Floyd Warshall to find the shortest path because of its computational efficiency in the dynamic routing.

0.3.2 Algorithm

The algorithm comprises of 3-Phases-

- PHASE-1 - PRE-PREPARE
- PHASE-2 - PREPARE
- PHASE-3 - COMMIT
- ROUND-CHANGE - Whenever the leader fails, a new leader is elected and the alive backups are moved to a new round. This maintains liveness in the algorithm

0.3.3 Working

- PHASE-1: The elected leader sends PRE-PREPARE messages to all the backups. The message includes - (message, digest, PrK, ViewNo). If the Leader is Faulty, then we re-elect a new leader, change the current view and move the valid backups to the new view.
- PHASE-2: Each backup validates its message via a valid method which checks the following:
  - If the digest is for the message stored at the backup.(by decrypting the message using the PrK of leader).
  - The backup belongs to the current Round.

  If both are TRUE, then the backup sends a PREPARE message to all the backups.
- PHASE-3: Each backup compares its PREPARE and PRE-PREPARE, if they are equal then the backup sends a COMMIT message to all the backups.
- Finally, if the backup have more than 2F Commit messages then the backup commits the messages to a commit-pool. And the message with maximum count is treated as the result that has to be delivered to the end-user.

0.4 Highlights

0.4.1 Shortest Path Algorithm

- Djikstra Algorithm for computing the Shortest Path from source to target.
  - Since the traffic never remains constant at any moment of time, Djikstra would be preferred.
  - We have to compute everytime.
- Floyd Warshall for computing the shortest Path.
  - If the network traffic changes not very often then floyd warshall would have been preferred.
  - However, in this scenario, the network is dynamic so using Floyd warshall would not be efficient.

0.5 How to use it

0.5.1 Dependencies

- Environment - Python3 (can be installed using ‘sudo apt-get install python3‘)
- Libraries - pandas, matplotlib, networkx, collections, heapq and cryptography module. (can be installed using ‘pip install $library_name‘)

0.5.2 To run

- python3 main.py
- To change the graph structure, make changes in the ‘graph.txt‘ file (format specified in the file).