Crypto routing with WireGuard: Proof-of-a-concept implementation

***Abstract*—WireGuard is a recent development of novel VPN protocol that requires 1-RTT to establish secure, authenticated channel between the peers. WireGuard revolves around the idea of crypto routing - routing based on the public keys of the peers.**

WireGuard uses EC curve X25519 for identification and authentication, and a set of novel algorithms to secure data plane traffic - ChaCha20 and Blake2s algorithms. In this document we present a simple implementation of WireGuard protocol in userspace using Python language. Our implmentation, although a proof-of-a-concept, allows for achiving 70Mb/s throughput which is sufficient for individual usage.

I. Data processing and basic results

```
sudo ip route add 10.1.1.0/24 via 10.1.1.5

sudo ip route add 10.1.1.0/24 via 10.1.1.6

add route 10.1.1.6 255.255.255.255 mRpANbnoDzXz8jczMe/3+aQW5YWqZhLiY+UZhUlKHG4= 14501 192.168.64.19

add route 10.1.1.0 255.255.255.0 8aW8cY51u1DlEoOrco9du8zv8lt/WhC7dMEuSZoZBkE= 14500 192.168.64.16
```

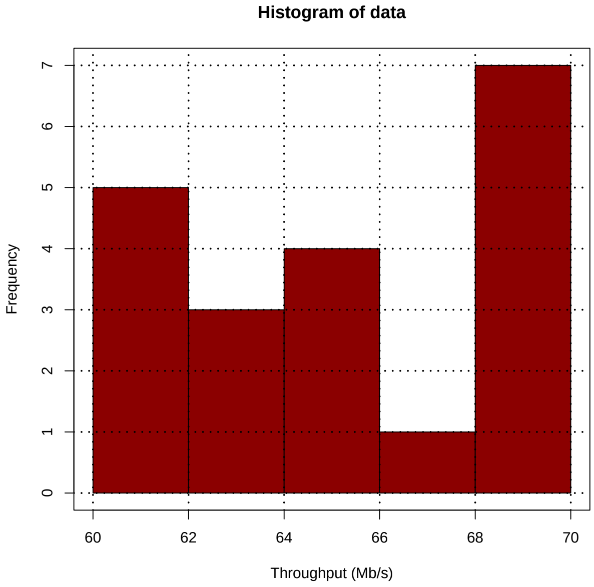

Fig. 1: Distribution of throughput