Accelerating cryptographic operations in networks

M.J.A. Brohet

Abstract

Cloud services are growing in demand and require high throughput, maximum flexibility and low costs, while the data that is being processed must remain protected. Safeguarding the traffic can be achieved using cryptographic operations, but a performance hit cannot always be mitigated. Up to recently, the mostly followed way to accelerate such operations is by employing specialised hardware that is rather expensive and prone to a vendor lock-in, but a new wave of programmable hardware is now emerging. Netronome's Agilio LX NICs have crypto-accelerators embedded and are easily and fully programmable using P4 and other programming languages, which fits the tradition of software-defined networks. In this thesis, we build a proof-of-concept with the Agilio LX that secures IP connections using IPsec and evaluate the performance in terms of throughput and latency. The results are promising. With our test equipment limited to 10 Gbps, we were able to achieve full transmission speed with frames carrying an encryption payload of 512 B with a relatively small increase in latency.