INFORMATICS INSTITUTE OF TECHNOLOGY

In Collaboration with

UNIVERSITY OF WESTMINSTER

Anon-Sec-Net:

Anonymous and Secure Communication

at the Network Layer

A dissertation by

Mr. Pramuditha Relapanawa

Supervised by

Dr Manjula Sandirigama

Submitted in partial fulfillment of the requirements for the MSc in Cyber Security & Forensics degree at the University of Westminster.

August 2022

Abstract

We are living in the mass surveillance age. Each day, people are having less right to privacy than what they had the previous day. Even though privacy a universally declared human right, it does not stop the governments and corporations violating it in a large scale. Furthermore, privacy considered being an essential component to practice the freedom of expression to its complete extend as well. In the cyber space, anonymous commutation platforms ensures that users are being able the practice the freedom of expression freely. However, current state of anonymous commutation systems does not provide neither anonymity, security nor performances to an acceptable level. Additional, widely used similar systems are proven vulnerable against numerous attack vectors.

This research paper proposes, Anon-Sec-Net, a network layer anonymous communication system. Which provides strong anonymity with low performance requirements. Additionally, Anon-Sec-Net has able to overcome some of the limitations associated with the current systems such as perfect forward secrecy, end-to-end encryption and a strong resistance against traffic analysis attacks. Anon-Sec-Net has thoroughly analyzed against multiple threat actors including global scale passive adversaries.

The research provides a blueprint to design an efficient system. According to the technical and domain expert opinions, the design has proven an efficient solution to the existing problems. The researcher believes the proposed system will benefit the public and the privacy domain in general once this has been implemented as a functioning system.