

A Study of Protocols to Enable and Secure Communications at the Network Edge in Restrictive Network Locations



Cameron P Fitze, School of Applied Computing, University of Wales Trinity St David



1. Introduction

Aim:

Study of obfuscated Internet Protocols for the purpose of secure and permissible communications.

Objectives:

Identify existing implementations of obfuscated protocols, test within the NS3 environment, and produce a custom obfuscated protocol, to be tested within NS3

Problem statement:

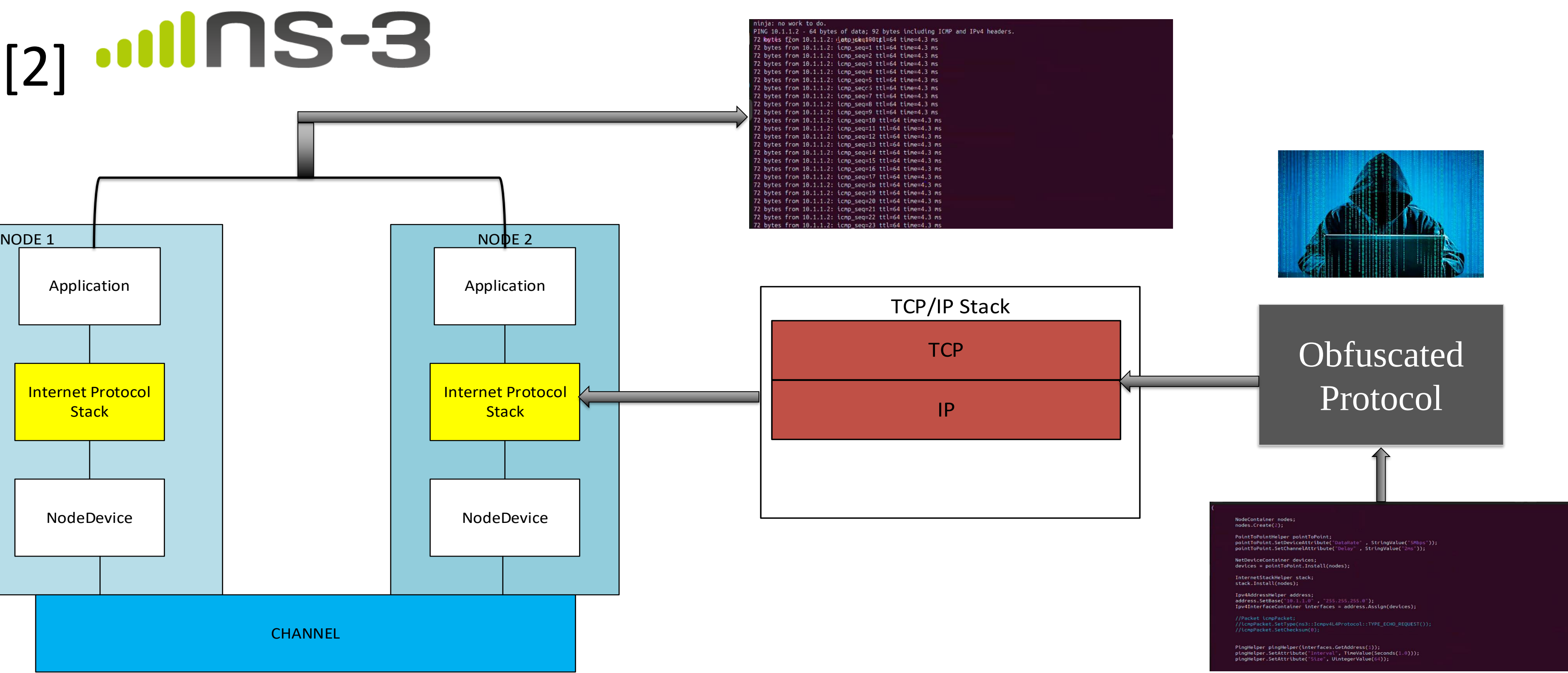
Network traffic classification is becoming more common for reasons of internet censorship and ISP traffic restrictions [1]

2. Hypothesis

Using or modifying existing lightweight, and generally permitted protocols from the network or transport layers of the OSI stack, obfuscation of protocol used, or covert communications using an unbenign protocol, should be possible and proven using a software simulation environment

3.1 Model

- This model shows how NS3 facilitates the testing of custom obfuscated protocol C++ code for this project
- Obfuscated protocols investigated under this project provide the Internet Protocol Stack for the NS3 nodes under test
- The application output is the test script, which for this research was an ICMP “ping” test



3.2 Results

- TCP/IP protocols such as ICMP can be tested within NS3
- Obfuscation of protocols is possible to implement within the code, but requires further enhancements and results can be observed on terminal logs or in PCAP files.
- This model provides a basis to test future development of obfuscated internet protocols

4. Conclusions

NS3 provides an air-gapped environment for safe testing of development Internet protocols

Obfuscated protocols are alternative and not widely adopted methods to achieve VPN-like behaviours

Existing permitted protocol may not always be permitted

5. Future Work

Focus on creating an obfuscated protocol stack

Prove in simulation

Implement on an air-gapped network test environment using real-world hardware and devices, and applying custom network and firewall security policies to test security of protocol.

References

- [1] Likun Liu, Haining Yu, Shilin Yu, Xiangzhan Yu. 2022. Security and Communication Networks. *Special Issue of Artificial Intelligence for Cyberspace Security*
- [2] nsnam 2011-2025

Acknowledgments

I would like to express my appreciation to my final project advisor, Dr. Stephen Mosey, for providing helpful and insightful feedback and input during the tenure of this project

Further information

2111737@student.uwtsd.ac.uk