



Vasco Regal Sousa

Multiple Client Wireguard Based Private and
Secure Overlay Network

DOCUMENTO PROVISÓRIO

“An idiot admires complexity,
a genius admires simplicity.”

— Terry A. Davis

o júri / the jury

presidente / president

ABC

Professor Catedrático da Universidade de Aveiro (por delegação da Reitora da Universidade de Aveiro)

vogais / examiners committee

DEF

Professor Catedrático da Universidade de Aveiro (orientador)

GHI

Professor associado da Universidade J (co-orientador)

KLM

Professor Catedrático da Universidade N

**agradecimentos /
acknowledgements**

Ágradecimento especial aos meus gatos. . .

Desejo também pedir desculpa a todos que tiveram de suportar o meu desinteresse pelas tarefas mundanas do dia-a-dia, . . .

Abstract

An overlay network is a group of computational nodes that communicate with each other through a virtual or logic channel, built on top of another network. Although there are already numerous services and protocols implementing this mechanic, scalability and administration agility are among the most desired characteristics of such a network topology. Hence, this document presents a centralized solution for the creation and control of secure overlay networks for multiple nodes - from client management to operation auditing. In the University of Aveiro, namely the autonomous robot ecosystem residing in the IRIS lab, supporting such a networking architecture would prove to be particularly interesting, both for development and project organization. Therefore, this context is used as a validation environment. ...

Contents

Contents	i
List of Figures	iii
List of Tables	v
1 Introduction	1
1.1 Motivation	1
1.2 Objectives	1
1.3 Document Structure	2
2 State of the Art	3
2.1 Encrypted Peer to Peer Communications / VPNs	3
2.1.1 Wireguard	3
Routing	3
Cipher Suite	3
Security	4
Performance	4
2.2 Control Platforms	4
Bibliography	5

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Motivation

Network security has become a topic of evergrowing interest among any information system. Companies strive to ensure their communications follow principles of integrity and confidentiality while minimizing attack vectors that could compromise services and data. With such goals in mind, network topologies are subjected to policies which apply rules and conditions to inbound and outbound traffic. One such mechanism is the use of Virtual Private Network (VPN) .

Traditional VPN services consist in the establishment of a secure, encrypted channel between a client and a network, through an insecure communication medium.

The University of Aveiro (UA)’s Intelligent Robotics and Systems Laboratory (IRIS-Lab) conducts research projects using autonomous mobile robots, which communicate through a Wi-Fi network. Currently, this network is confined to the premises of the IRIS-Lab, preventing the robots from operating in the remaining UA’s buildings. Although the ua’s Wi-Fi infrastructure covers most of its edifices, which can be used by the robots, due to security mechanisms, this network proves to be highly restraining, not allowing Peer to Peer (P2P) communications through the Robot Operating System (ROS) - the operating system the robots run on - middleware without additional network equipments. Moreover, these constraints keep developers from being able to interact with the robots through their personal machines, which, if otherwise possible, would be of great interest.

1.2 Objectives

The main goal of this dissertation is to implement a private overlay network manager to be used exclusively by UA’s clients. The concept of a manager entails both the definition of a network’s client universe (which nodes should be allowed to connect to a certain network) and its respective identification and authentication mechanisms.

In the IRIS-Lab scenario, the management platform should provide operations to achieve communication between a team of robots, regardless of their physical location within the campus. Moreover, the authentication and connection to a desired overlay network by the robots must be a seemingless operation, requiring little to no manual configuration.

Finally, all traffic must be encrypted and properly authenticated, to ensure the privacy of the communication.

1.3 Document Structure

This document presents an implementation proposal of such an overlay network manager. With this goal in mind, it is structured in two main chapters - State of The Art and Methodology. The former consists in an exploration of the current state of the art, providing an analysis not only of potential tools, protocols and frameworks suitable for the scope of the dissertation but also of published research conducted covering similar topics and scenarios while the latter establishes the work methodology to be taken for the development and results gathering process.

Chapter 2

State of the Art

2.1 Encrypted Peer to Peer Communications / VPNs

2.1.1 Wireguard

Wireguard [2] is an open-source layer 3 network tunnel implemented as a kernel virtual network interface. Wireguard offers both a robust cryptographic suite and transparent session management, based on the fundamental principle of secure tunnels: peers in a Wireguard communication are registered as an association between a public key - analogous to the OpenSSH keys mechanism - and a tunnel source IP address.

One of Wireguard's selling points is its simplicity. In fact, compared to similar protocols, which generally support a wide range of cryptographic suites, Wireguard settles for a singular one. Although one may consider the lack of cipher agility as a disadvantage, this approach minimizes protocol complexity, increasing security robustness by avoiding SSL/TLS vulnerabilities commonly originated from such agility.

Routing

Peers in a Wireguard communication maintain a data structure containing its own identification - both the public and private keys - and interface listening port. Then, for each known peer, an entry is present containing an association between a public key and a set of allowed source ips.

This structure is queried both for outgoing and incoming packets. To encrypt packets to be sent, the structure is consulted and, based on the destination address, the desired peer's public key is retrieved. As for receiving data, after decryption (with the peer's own keys), the structure is used to verify the validity of the packet's source address, which, in other words, means checking if there's a match between the source address and the allowed addresses present on the routing structure.

Optionally, Wireguard peers can configure one additional field, an internet endpoint, defining the listening address where packets should be sent. If not defined, the incoming packets' source address is used instead.

Cipher Suite

As aforementioned, Wireguard offers a single cipher suite for encryption mechanism in its ecosystem. The peer's pre-shared keys consist in Curve25519 points [1]

Security

Performance

2.2 Control Platforms

Bibliography

- [1] Daniel J Bernstein. Curve25519: new diffie-hellman speed records. In *Public Key Cryptography-PKC 2006: 9th International Conference on Theory and Practice in Public-Key Cryptography, New York, NY, USA, April 24-26, 2006. Proceedings 9*. Springer, 2006.
- [2] Jason A Donenfeld. Wireguard: next generation kernel network tunnel. In *NDSS*, 2017.

