



Universidade de Aveiro
2023

**Vasco Jorge
Regal Sousa**

**Rede Overlay Privada e Segura Para Múltiplos
Clientes Baseada em Wireguard**

**Multiple Client Wireguard Based Private and Secure
Overlay Network**

PROPOSTA

DE TESE



Universidade de Aveiro
2023

Vasco Jorge
Regal Sousa

Rede Overlay Privada e Segura Para Múltiplos
Clientes Baseada em Wireguard

Multiple Client Wireguard Based Private and Secure
Overlay Network

PROPOSTA

DE TESE

“An idiot admires complexity, a genius admires simplicity”

— Terry A. Davis



Universidade de Aveiro
2023

**Vasco Jorge
Regal Sousa**

**Rede Overlay Privada e Segura Para Múltiplos
Clientes Baseada em Wireguard**

**Multiple Client Wireguard Based Private and Secure
Overlay Network**

Proposta de Tese apresentada à Universidade de Aveiro para cumprimento dos requisitos necessários à conclusão da unidade curricular Proposta de Tese, necessária para obtenção do grau de Mestre em Engenharia Informática, sob a orientação científica do Doutor Eurico Farinha Pedrosa, Professor do Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro, e do Doutor André Marnoto Zúquete, Professor catedrático do Departamento de Eletrónica, Telecomunicações e Informática da Universidade de Aveiro.

Dedico este trabalho.

o júri / the jury

presidente / president

Prof. Doutor João Antunes da Silva
professor associado da Faculdade de Engenharia da Universidade do Porto

vogais / examiners committee

Prof. Doutor João Antunes da Silva
professor associado da Faculdade de Engenharia da Universidade do Porto

Prof. Doutor João Antunes da Silva
professor associado da Faculdade de Engenharia da Universidade do Porto

Prof. Doutor João Antunes da Silva
professor associado da Faculdade de Engenharia da Universidade do Porto

Prof. Doutor João Antunes da Silva
professor associado da Faculdade de Engenharia da Universidade do Porto

Prof. Doutor João Antunes da Silva
professor associado da Faculdade de Engenharia da Universidade do Porto

**agradecimentos /
acknowledgements**

Agradeço toda a ajuda.

Palavras Chave

rede overlay, wireguard, vpn.

Resumo

Uma rede overlay consiste num conjunto de nós computacionais que comunicam-se entre si através de um canal virtual ou lógico, montado numa camada em cima de uma outra rede já existente. Embora existam já vários serviços e protocolos que suportam estas funcionalidades, uma das características mais aliciantes de uma rede overlay é a sua capacidade de escalabilidade e agilidade de administração. Neste sentido, este documento apresenta uma solução centralizada para a gestão e controlo de redes overlay seguras - desde gestão de clientes a auditoria de operações. Sendo a Universidade de Aveiro, nomeadamente o ecossistema de redes autónomas que reside no IRIS lab, um contexto em que o suporte a redes overlay seria extremamente benéfico tanto no desenvolvimento como operacionalmente, este projeto, é também analisado como um potencial caso de uso para um sistema deste tipo.

Keywords

overlay network, wireguard, vpn.

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 model, scalability and administration agility are among the most desired characteristics for such a network topology. Hence, this document presents a centralized architecture for the creation and control of secure overlay networks for multiple nodes, from client management to operation auditing. In the University of Aveiro, namely in the autonomous robot ecosystem residing in the IRIS lab, supporting such a network 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
List of Code Snippets	vii
Glossary	ix
1 Introduction	1
1.1 Motivation	1
1.2 IRIS-Lab Context	1
1.3 Objectives	1
2 Requirements and State of the Art	3
2.1 Encrypted Peer to Peer Communications / VPNs	3
2.1.1 Wireguard	3
2.2 NAT Traversal	3
2.3 Mesh Networks	3
3 Methodology	5
A Additional content	7

List of Figures

List of Tables

List of Code Snippets

Glossary

IRIS-Lab Intelligent Robotics and Systems
Laboratory
UA University of Aveiro

ROS Robot Operating System
p2p Peer to Peer

Introduction

1.1 MOTIVATION

1.2 IRIS-LAB CONTEXT

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.

1.3 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 seamless operation, requiring little to no manual configuration.

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

Requirements and State of the Art

This chapter covers the analysis and discussion not only of the motives and advantages behind the chosen tools and protocols to be used in this project but also but also of the common approaches and methodologies conducted in research in similar scenarios.

At its core, the system requires three main dimensions:

- A protocol for encrypted, reliable and efficient p2p communication
- A control platform for management of clients and authentication tokens
- A mechanism for scalability, able to transform the many p2p channels into one mesh network

2.1 ENCRYPTED PEER TO PEER COMMUNICATIONS / VPNs

2.1.1 Wireguard

2.2 CONTROL PLATFORMS

2.2.1 Tailscale

2.2.2 Headscale

2.3 MESH NETWORKS

2.4 NAT TRAVERSAL

CHAPTER 3

Methodology

APPENDIX **A**

Additional content