

MC²: Peer to Peer Based Network Masquerading for Mission Critical Clouds.

Francois D'Ugard, fduga002@fiu.edu, Florida International University

Ming Zhao Phd., ming@cis.fiu.edu, Florida International University

Abstract:

Virtualization is an increasingly popular approach to manage rising information technology costs and complexity in every sector of the economy. Cloud computing allows organizations of any size to provision infrastructure resources as needed and flexibly scale technology resources to meet changing demands. Cloud providers pool hardware resources and allocate them based on the requests of their users. In order to efficiently allocate these resources providers must aggregate users of different requirements and workloads onto the same physical infrastructure. However, this approach increases the likelihood that a malicious user can collocate a VM alongside a target VM in order to extract information or disrupt its functioning in some way.

We propose a solution that can deliver mission assurance to mission-critical applications in cloud

computing systems. We will do so by leveraging the unique capabilities of virtualization technology and develop a dynamic and distributed approach to route messages among co-operative virtual machines in typical cloud computing systems.

This project will deliver mission assurance to mission-critical applications in cloud computing systems. Our approach relies on developing a complete network graph on a virtual private network of peer to peer connections. With the purpose of masquerading the messages created by co-operative virtual machines in a typical cloud computing system. Our network graph consists of a peer to peer overlay network that interconnect OpenStack virtual machines and is based on the IP-over-P2P (IPOP) framework. The project will focus on developing an extension to IPOP that will allow for the communications among the VMs to be routed by an overlay network in an OpenStack-based cloud system.

MC²: P2P Based Network Masquerading for Mission Critical Clouds

Francois D'Ugard, Florida International University
Ming Zhao, PhD. Florida International University

IPOP

Problem

Virtualization is an increasingly popular approach to address rising information technology costs and complexity. Cloud service providers pool hardware resources and allocate them based on the requests of their users. In order to efficiently allocate these resources, providers must aggregate users of different requirements and workloads onto the same physical infrastructure.

This approach increases the likelihood that a malicious user can collocate a virtual machine alongside a target virtual machine in order to extract information or disrupt the cloud's functioning in some way. By observing the flow of network traffic among a group of cooperating virtual machines a malicious user is easily able to identify the critical virtual machine within the group.

My role in the project was the design and implementation of a new VPN controller to connect virtual machines using IPV6 addresses. The controller routes packets among the virtual machines randomly in order to masquerade the communication patterns. Making it difficult to identify the mission critical virtual machine.

Current System

Our project leveraged OpenStack, an open-source Cloud Framework solution used by many organizations.

- Despite robust networking options within OpenStack's networking subsystem, it does not provide a mechanism to mask the communication patterns among virtual machines.
- If a malicious user were to observe the communication patterns among virtual machines finding the mission critical virtual machine is as easy as identifying the machine that receives the most inbound communication.

Proposed System

A P2P Based Network Masquerading system that chooses a random path to route packets within specified latency boundaries at specified intervals. Our system depends our cloud network being a complete graph. This allows us to generate a random path of any length dynamically.
Website: <http://mcc-dev.cis.fiu.edu>

Requirements

FUNCTIONAL:

- Join a VM to the network.
- Disconnect a VM from the network at any time.
- Set up an open-source XMPP server for the collaborating VMs to discover each other and join the network.
- Randomly choose a communication path for packets.
- View the system help.

NON-FUNCTIONAL:

- Support the execution of unmodified applications that use the standard TCP and UDP protocols.
- Not impose constraints in the network infrastructure.
- Make all features available through command-line user interface suitable for a computer savvy user.

System Design

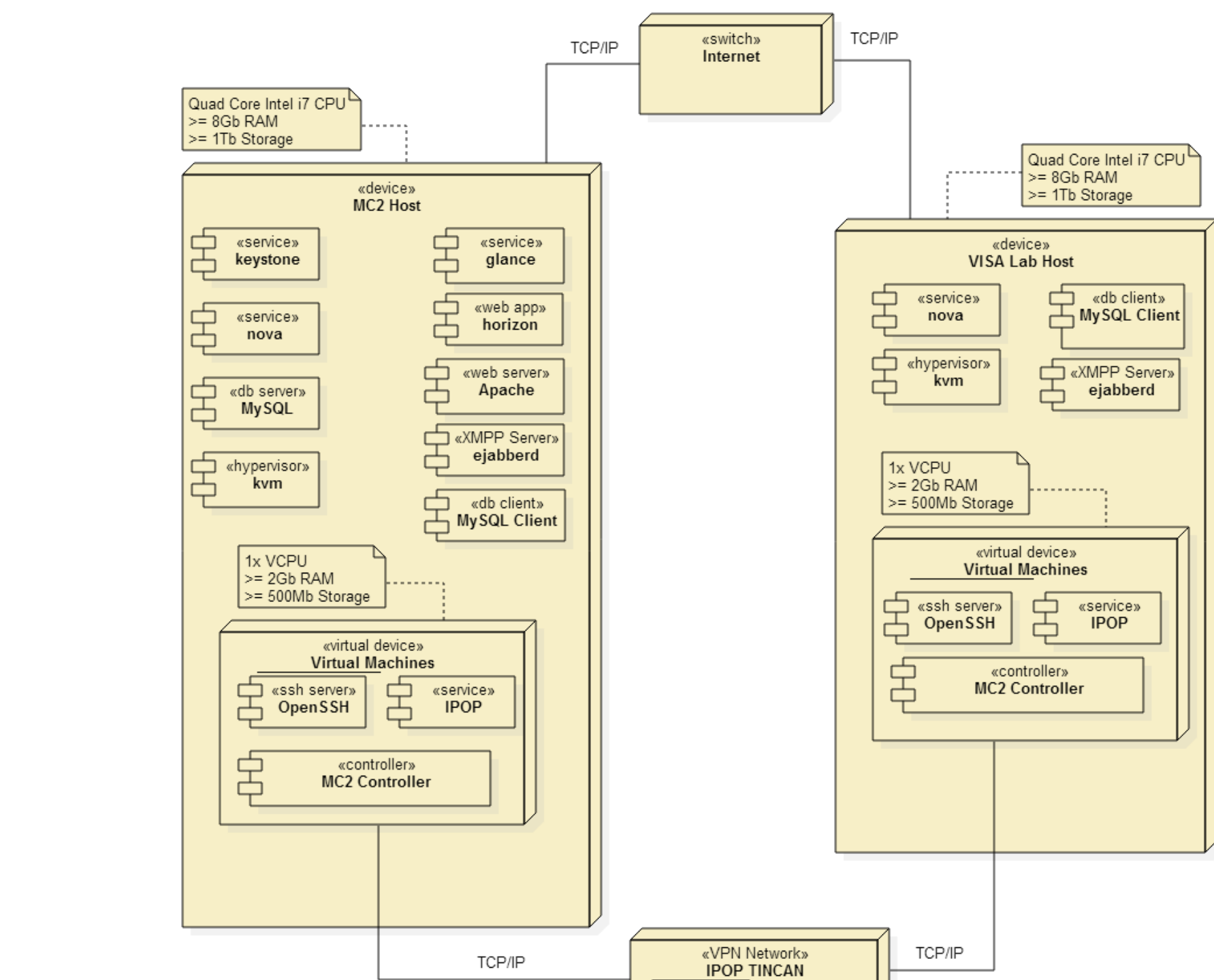


Figure 1. Hardware Software Mapping

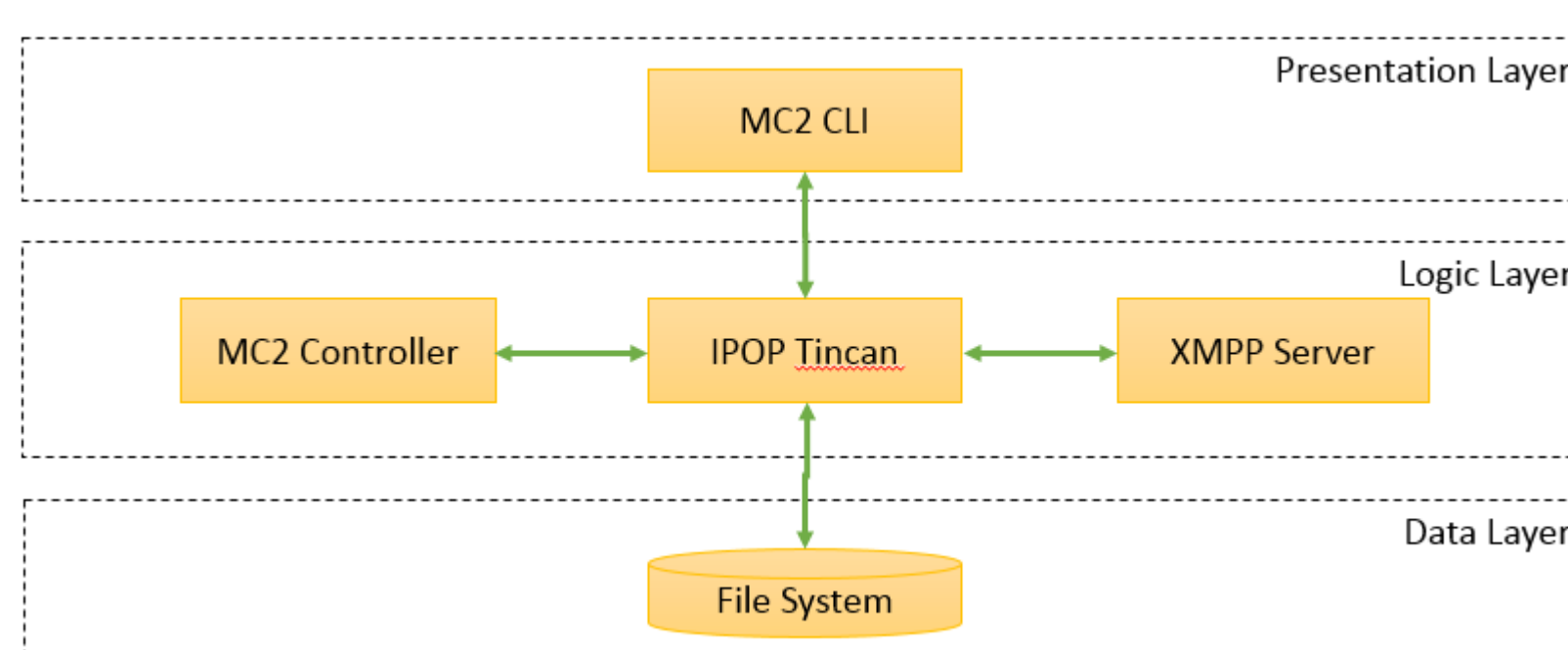


Figure 2. 3-Tier Software Architecture

Object Design

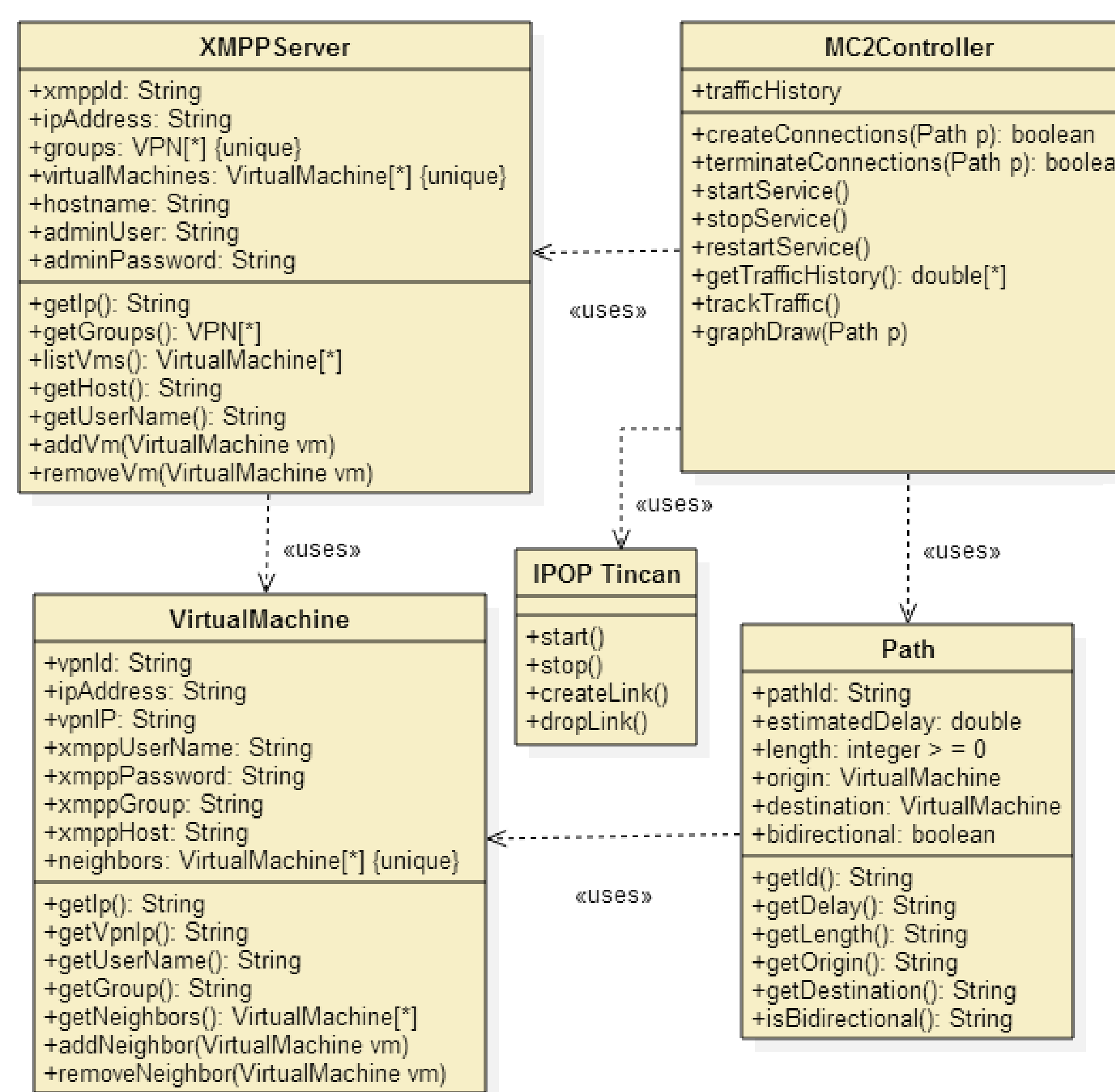


Figure 3. Class Diagram

Implementation

- $G = (V, E)$
Multi-hop Path(source s , destination d , hops h)
if $s == d$ || $h == 1$
return send_to(d , $h-1$)
Return send_to($random.choice(G.V)$, $h-1$)
- The function MST() returns a minimum spanning tree.
- The function RDFW() finds a random depth first walk.
Random Source Routing (Graph G , Max Latency ml)
if $ml < MST(G)$
Return None
Return RDFW(G)

Figure 4. Routing Algorithms

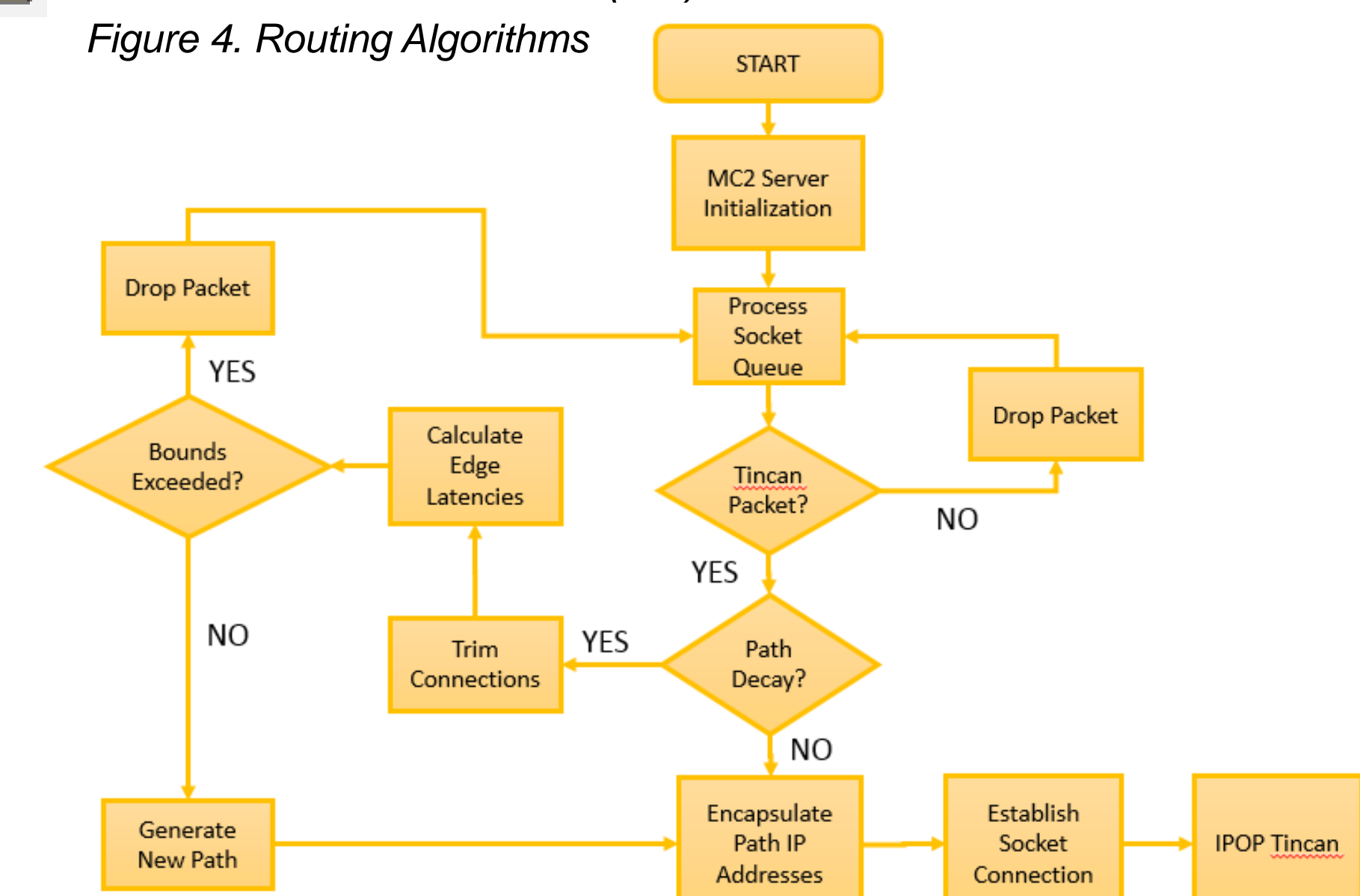


Figure 5. MC2 Controller Event Diagram

Verification

The functions of the system were unit tested using unittest, the Python unit testing framework. Integration testing within the major subsystems was performed using the bottom-up testing strategy.

During system testing, we verified the functionality of our systems components including the random path generator.

In particular, our system testing included the following:

- Usability testing of the command line tools that provide Compatibility testing of IPOP Tincan and the MC2 Controller.
- Functionality testing of the random path generating algorithms.

Screenshots

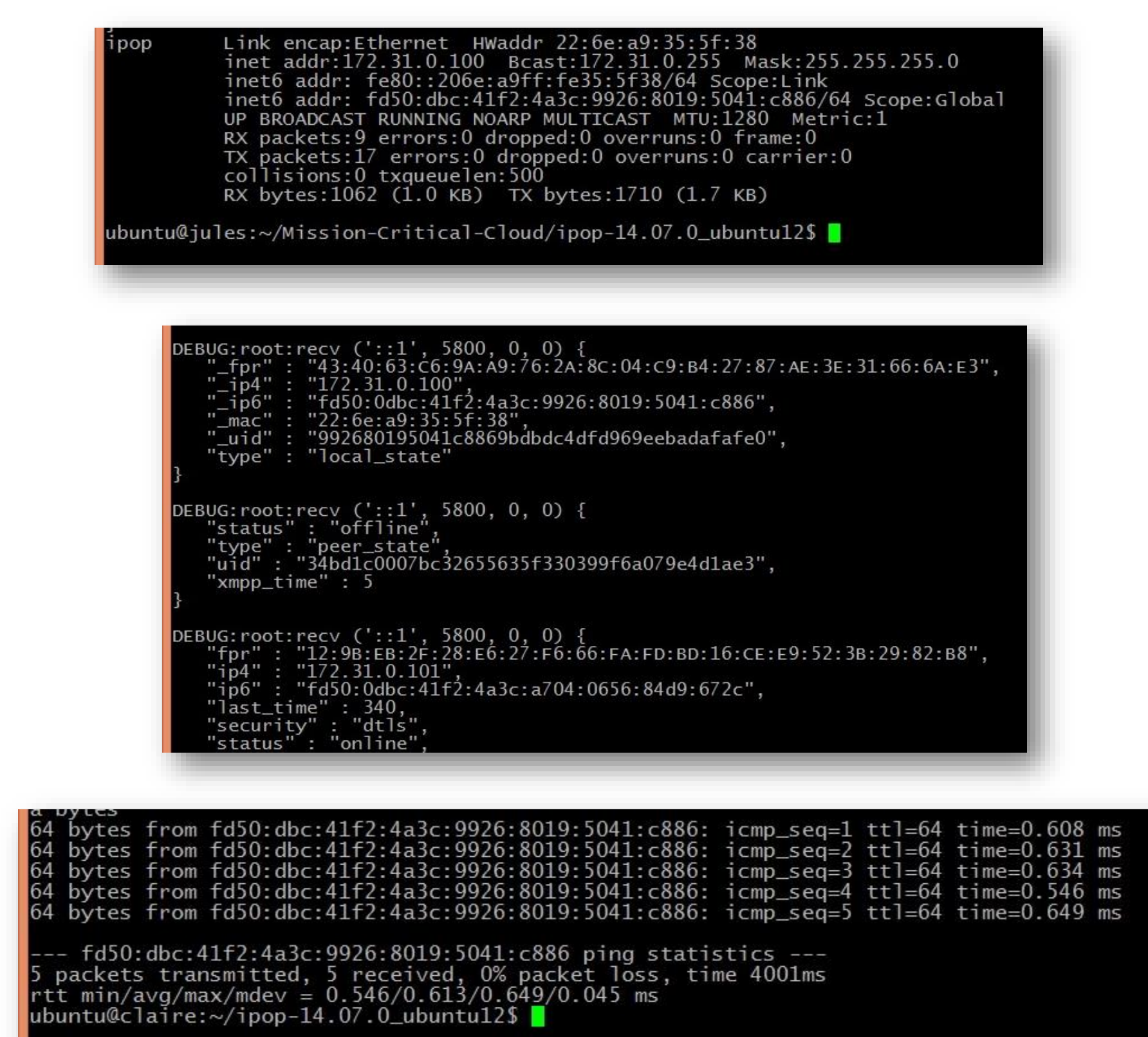


Figure 6. MC2 Controller Screen Shots

Summary

Mission-critical VMs running in clouds may be at risk of attack. These risks are only expected to increase as businesses and governments embrace the Cloud business model as a way of creating cost-effective and easily scalable IT solutions. We propose a solution that transparently enhances VM security using existing building blocks in an innovative way, with the potential of incurring little performance overhead as the state of the art of those basic functionalities advances.

My main contribution to the project was:

- The design and implementation of a new IPOP controller.
- This controller interacts with IPOP Tincan to randomly generate a communication path to route packages within the VPN.

Our proposed system can be extended and improved by:

- Exposing its features through the OpenStack Dashboard.
- Better error handling when no random path is found with acceptable latency boundary.

Acknowledgement

The material presented in this poster is based upon the work supported by the VISA. Lab at FIU. I am thankful to the help that I received from my mentor Dr. Ming Zhao and IPOP's author Dr. Renato Figueiredo.