Escuela de Ingeniería y Arquitectura
Universidad de Zaragoza

Defensa proactiva y reactiva ante ataques DDoS en un entorno simulado de redes definidas por software

Trabajo Fin de Grado

Autor
Jorge Paracuellos Cortés

Director
Ricardo J. Rodriguez

Abril 2016

Índice

Índice

Introducción

Motivación

- Incremento de amenazas debido a ataques
- Nueva arquitectura de red en desarrollo
- Adaptación de las empresas tecnológicas

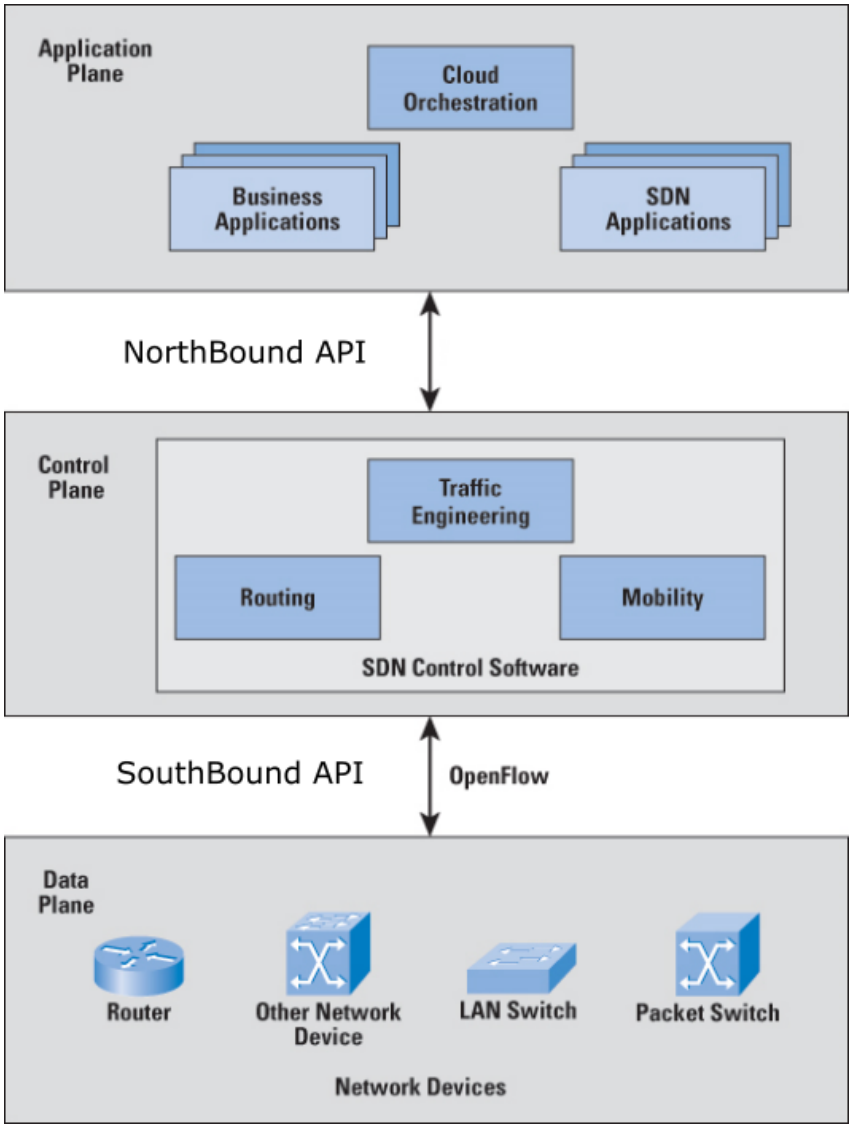
Introducción

Objetivos TFG

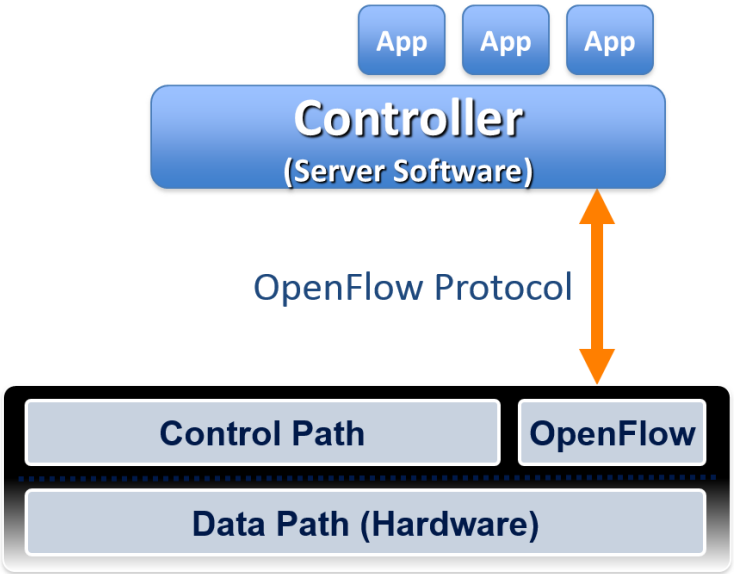
- Familiarización con la tecnología Software Defined Network (SDN)
- Estudio controladores SDN
- Estudio tipos de ataques Distributed Denial of Service (DDoS)
- Diseño e implementación de un mecanismo de defensa proactivo y reactivo
- Evaluación en diferentes escenarios y configuraciones

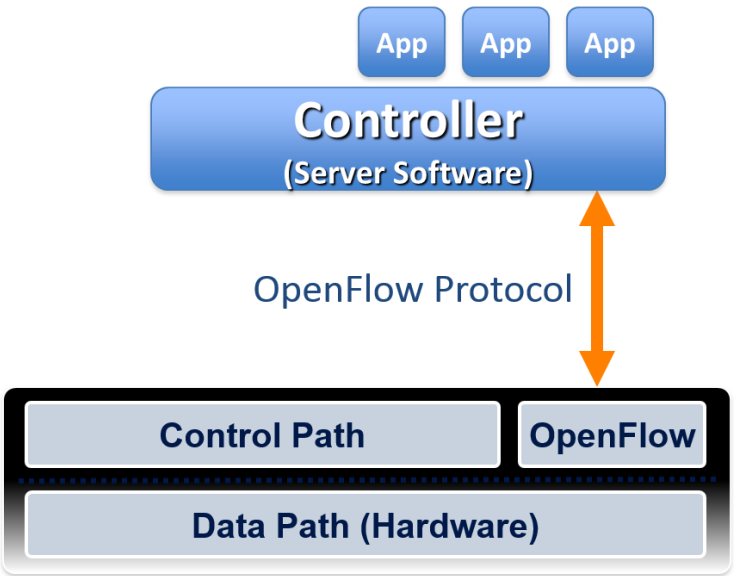
Índice

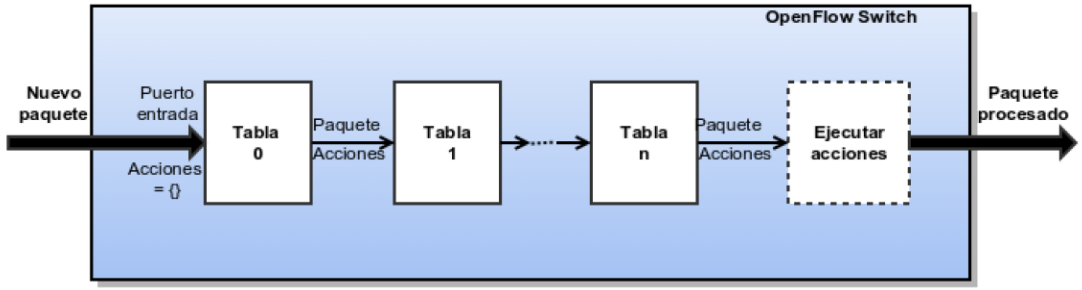
Conceptos SDN
Arquitectura SDN

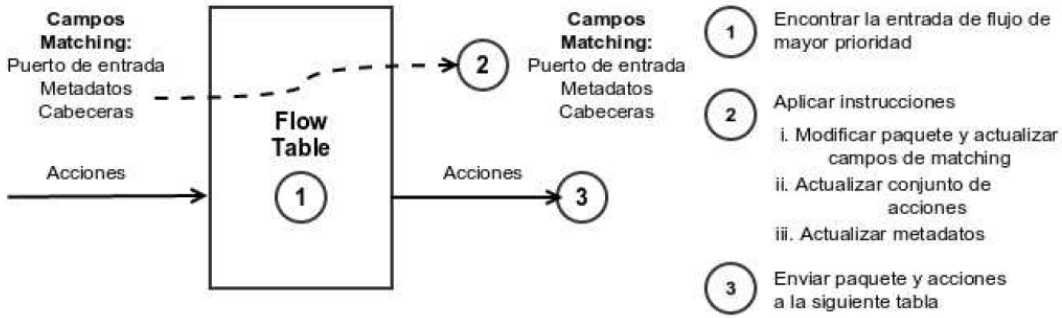


Conceptos SDN
Protocolo OpenFlow




App
App
App
Controller
(Server Software)
OpenFlow Protocol
Control Path
OpenFlow
Data Path (Hardware)


OpenFlow Switch
Nuevo paquete
Puerto entrada
Acciones = {}
Tabla 0
Paquete Acciones
Tabla 1
Tabla n
Paquete Acciones
Ejecutar acciones
Paquete procesado


Campos Matching:
Puerto de entrada
Metadatos
Cabeceras
Acciones
Flow Table
1
2
3
Campos Matching:
Puerto de entrada
Metadatos
Cabeceras
Acciones
1 Encontrar la entrada de flujo de mayor prioridad
2 Aplicar instrucciones
i. Modificar paquete y actualizar campos de matching
ii. Actualizar conjunto de acciones
iii. Actualizar metadatos
3 Enviar paquete y acciones a la siguiente tabla

Conceptos SDN

Comparativa controladores SDN de código abierto

	Pox	FloodLight	OpenDayLight
Interfaces	SB	SB & NB	SB & NB
Virtualización	Mininet & Openv Switch	Mininet & Openv Switch	Mininet & Openv Switch
GUI	Sí	Web UI	Sí
REST API	No	Sí	Sí
Documentación	Escasa	Media	Media
Lenguaje Programación	Python	Java + cualquier lenguaje que utilice REST	Java
Modularidad	Media	Alta	Alta
S.O. Soportado	Linux, Mac Os and Windows	Linux, Mac Os and Windows	Linux
Edad	3 años	4 años	2 años
Soporte OpenFlow	OF v1.0	OF v1.3	OF v1.3
OpenStack Networking	No	Medio	Medio

Características

- Apoyo de la industria (Intel, Cisco, Nec ...)
- Proyecto de código abierto
- Desarrollo en Java
- Extensa documentación y comunidad activa en constante movimiento
- Arquitectura modular

Índice

Ataques DDoS

Clasificación

- Inundación
- Reflexión
- Amplificación

Ataques DDoS

Clasificación

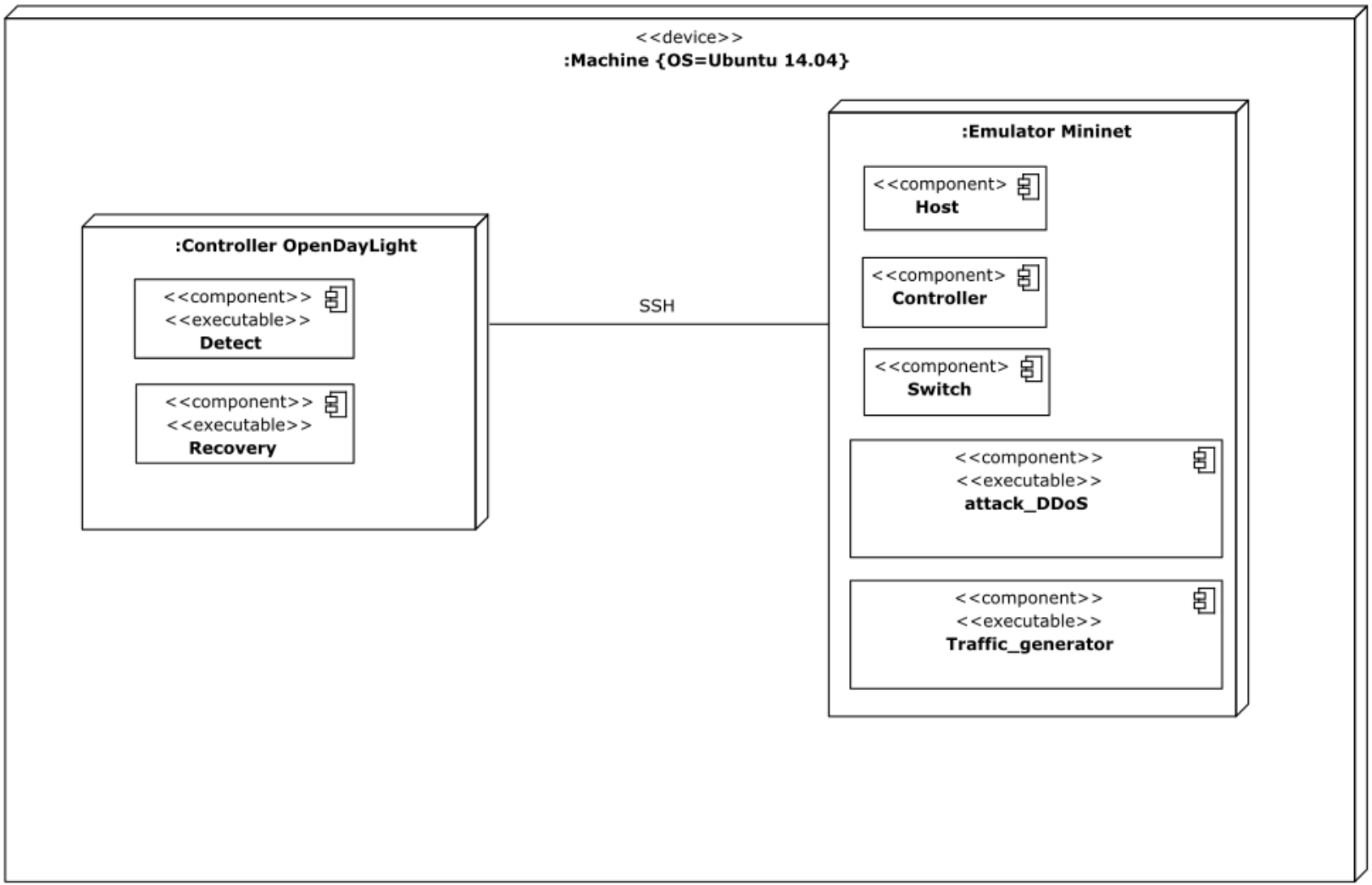
- Inundación
- Reflexión
- Amplificación

Mecanismos de defensa ante DDoS

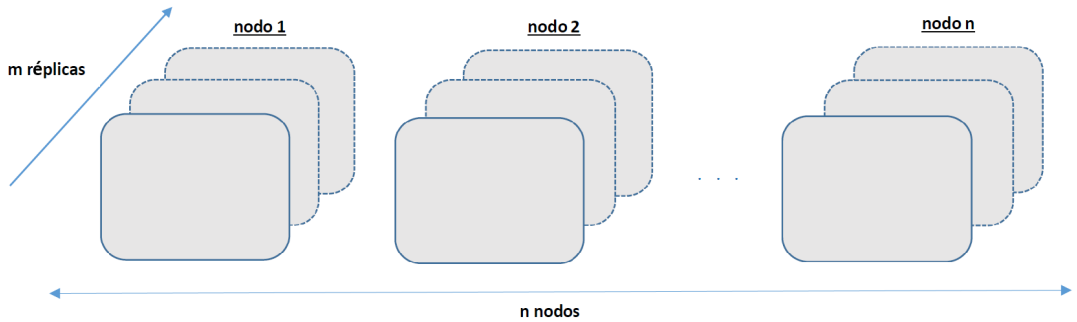
- Prevención
- Detección
  - Patrones
  - Anomalías
- Identificación del origen
- Mitigación

Índice

Arquitectura del sistema
Diagrama de despliegue

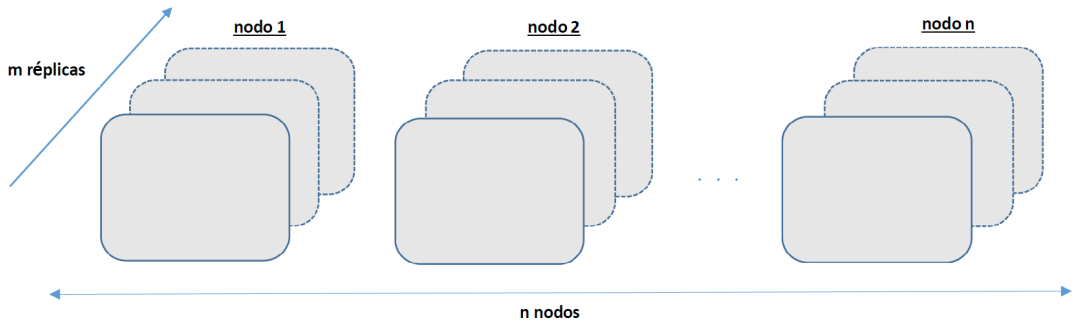


Arquitectura del sistema
Explicación formal

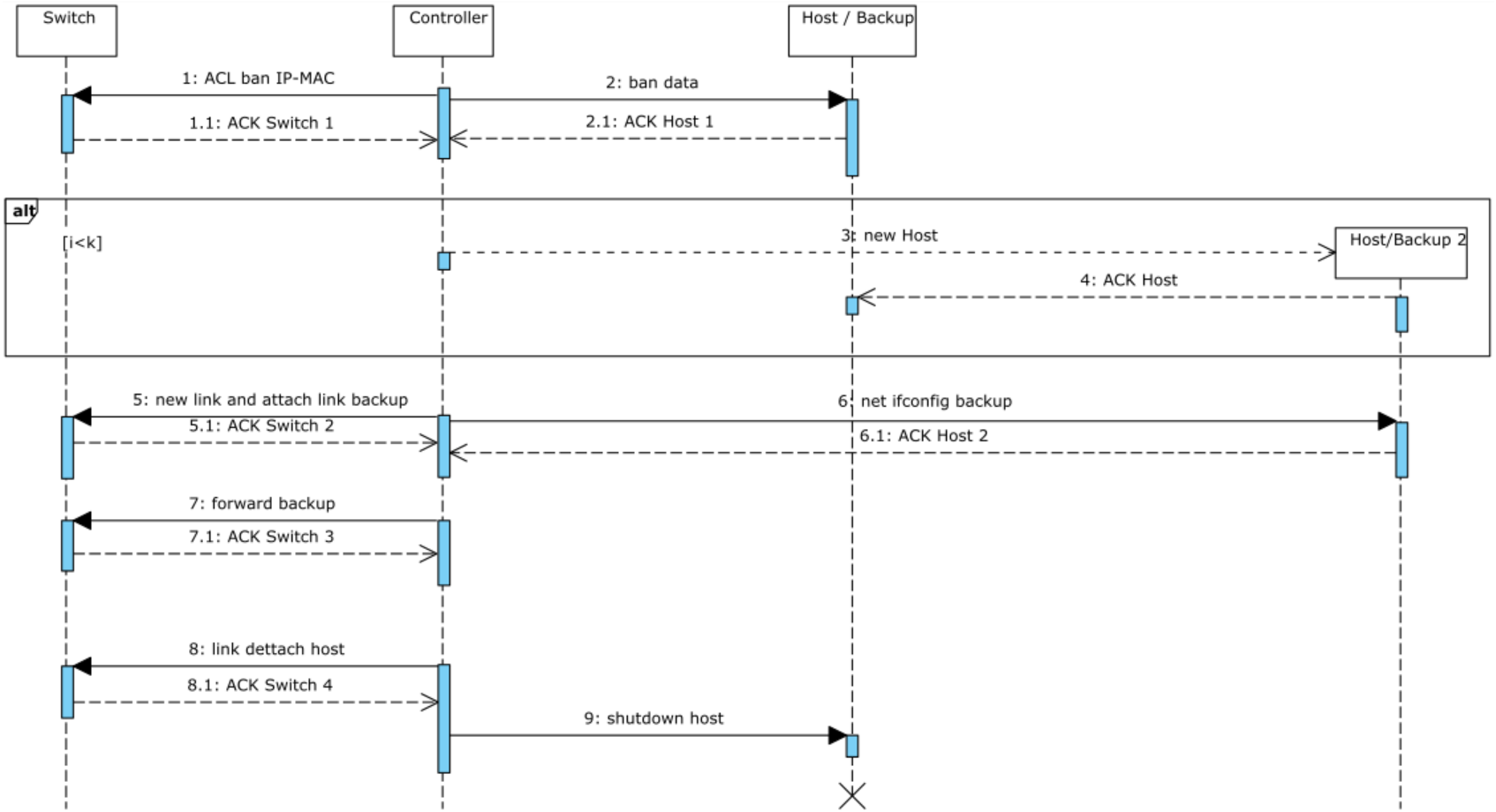


Parámetros

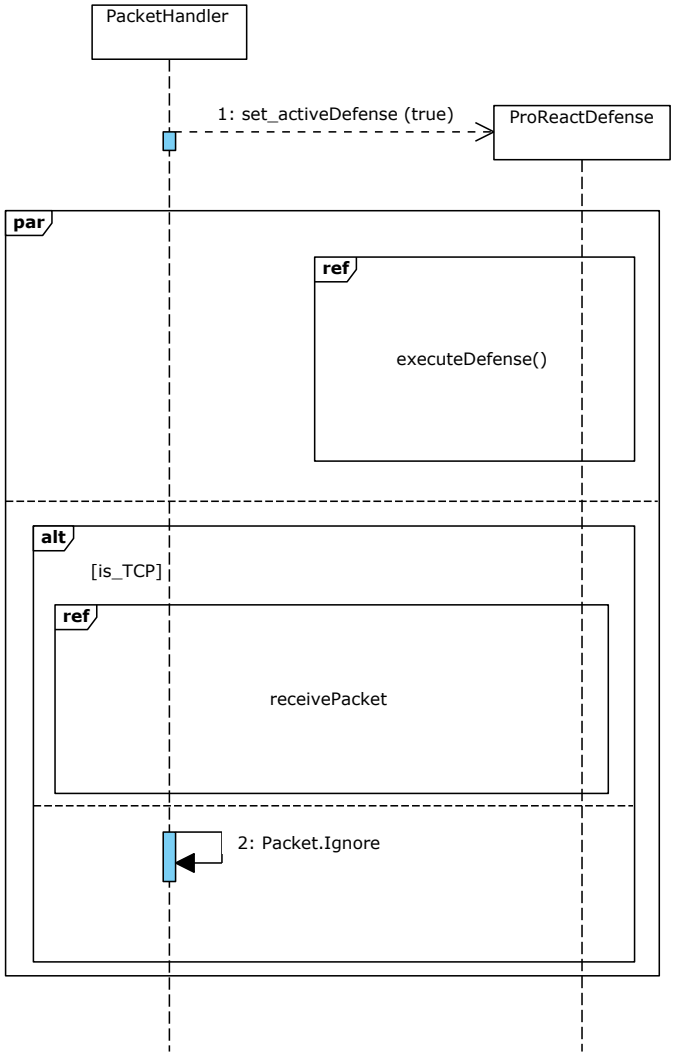
- T_{coste} : tiempo que tarda en recuperarse un nodo
- T_{slot} : tiempo que tarda en recuperar $k < n$ réplicas en paralelo

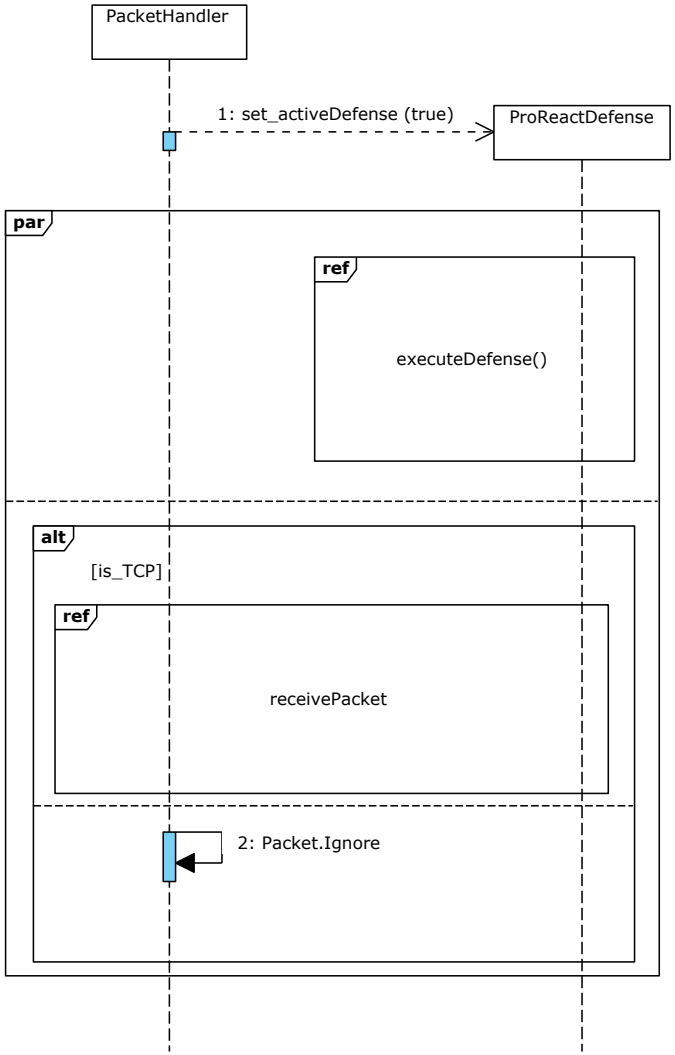


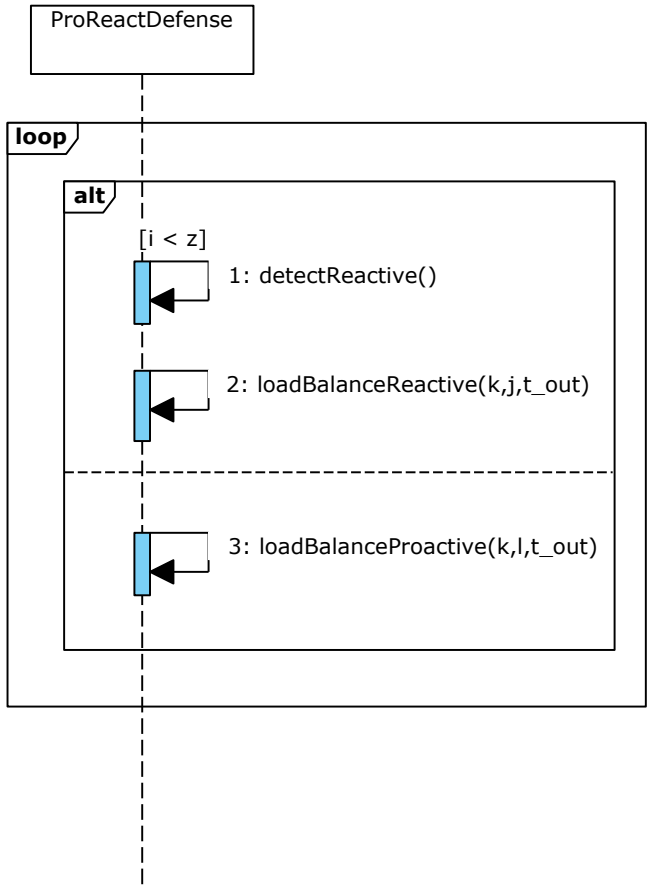
Arquitectura del sistema
Funcionamiento: Rejuvenecimiento



Arquitectura del sistema
Implementación

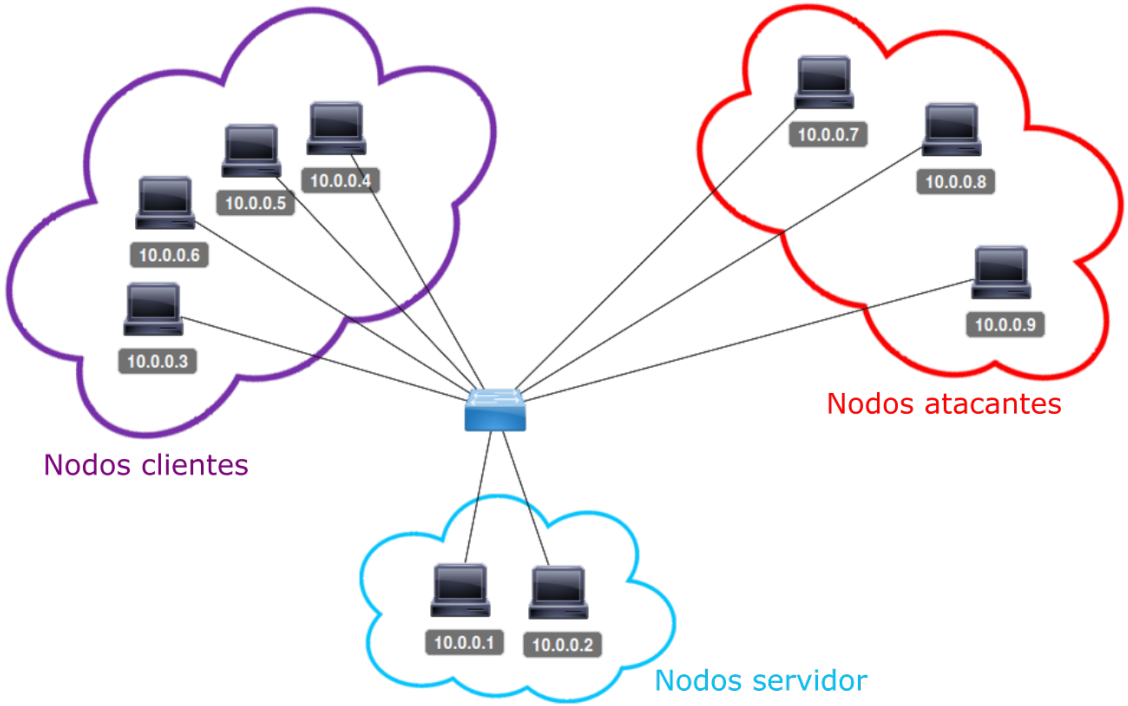



PacketHandler
1: set_activeDefense (true)
ProReactDefense
par
ref
executeDefense()
alt
[is_TCP]
ref
receivePacket
2: Packet.Ignore


ProReactDefense
loop
alt
[i < z]
1: detectReactive()
2: loadBalanceReactive(k,j,t_out)
3: loadBalanceProactive(k,l,t_out)

Índice

Evaluación y resultados
Topología de los escenarios



Archivo de 105MBytes servido a 1,46MBytes/s

Tiempo de servicio entre 66 y 68 segundos

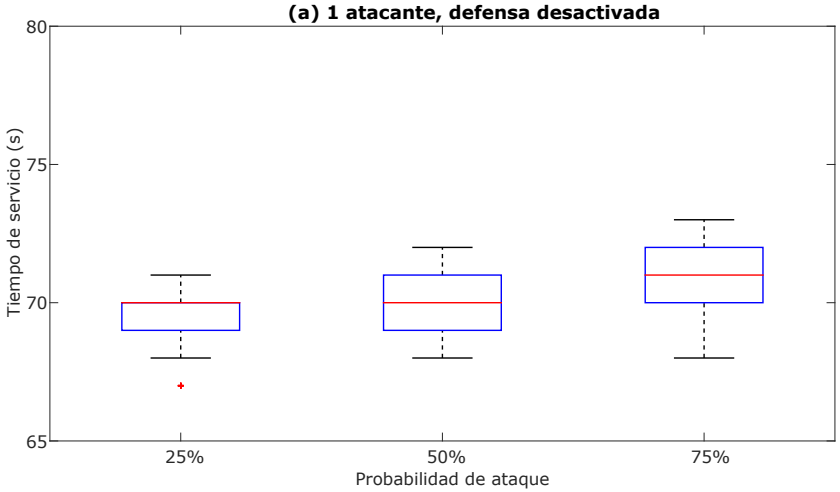
Escenarios

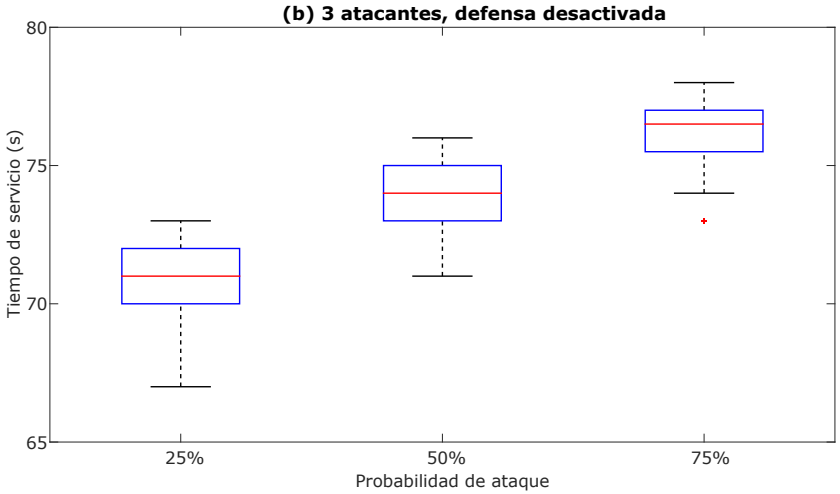
- 1 atacante
- 2 atacantes
- 3 atacantes

Probabilidad de ataque

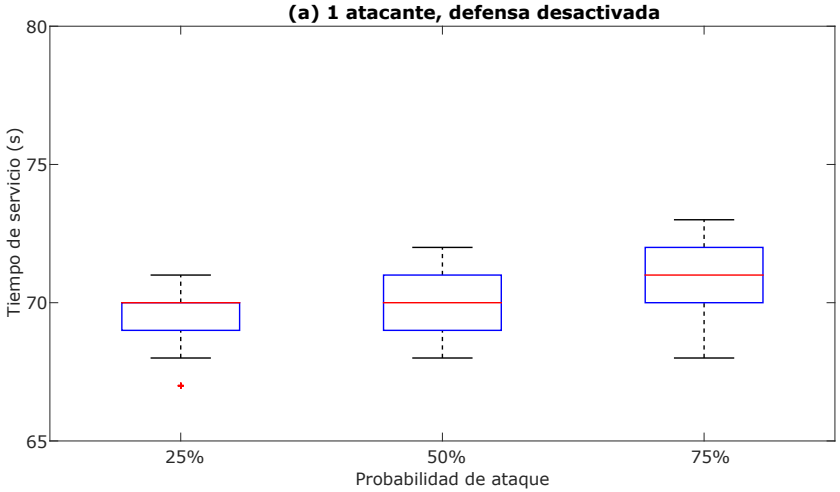
- 25%
- 50%
- 75%

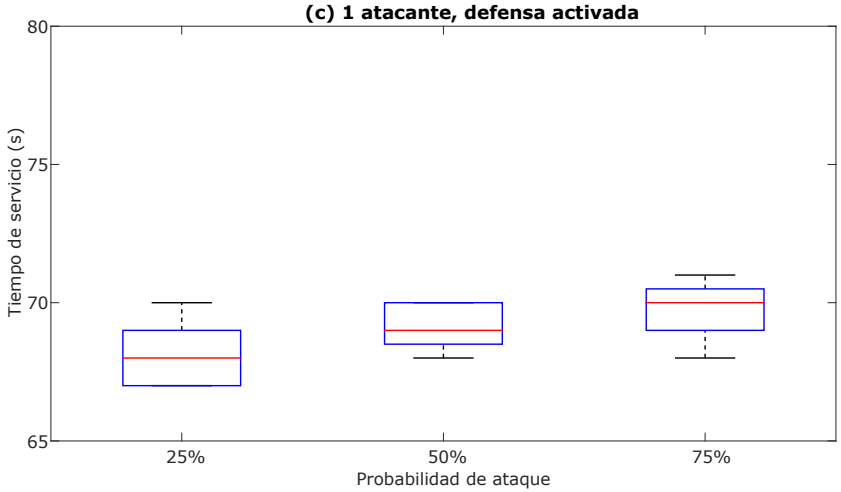
Evaluación y resultados
Comparativa tiempos de servicio

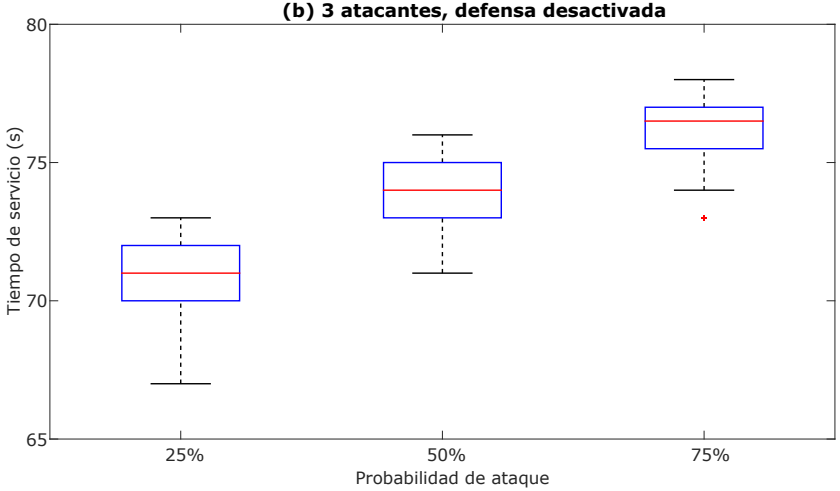


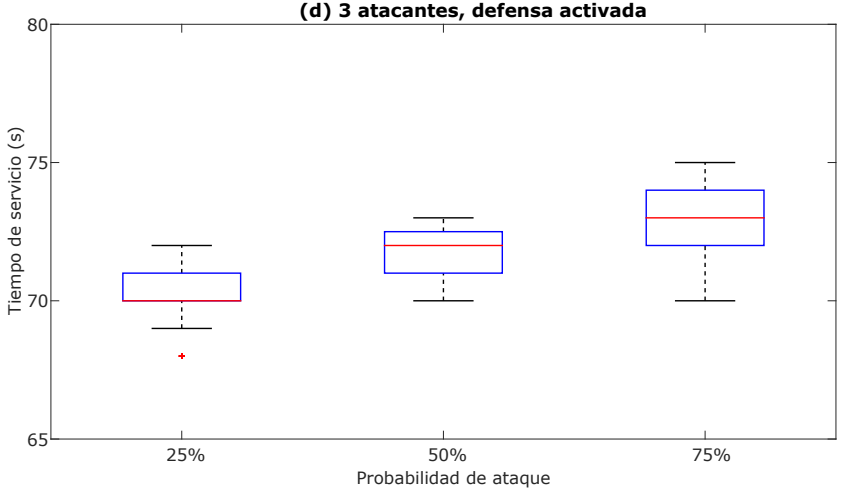


Evaluación y resultados
Comparativa tiempos de servicio

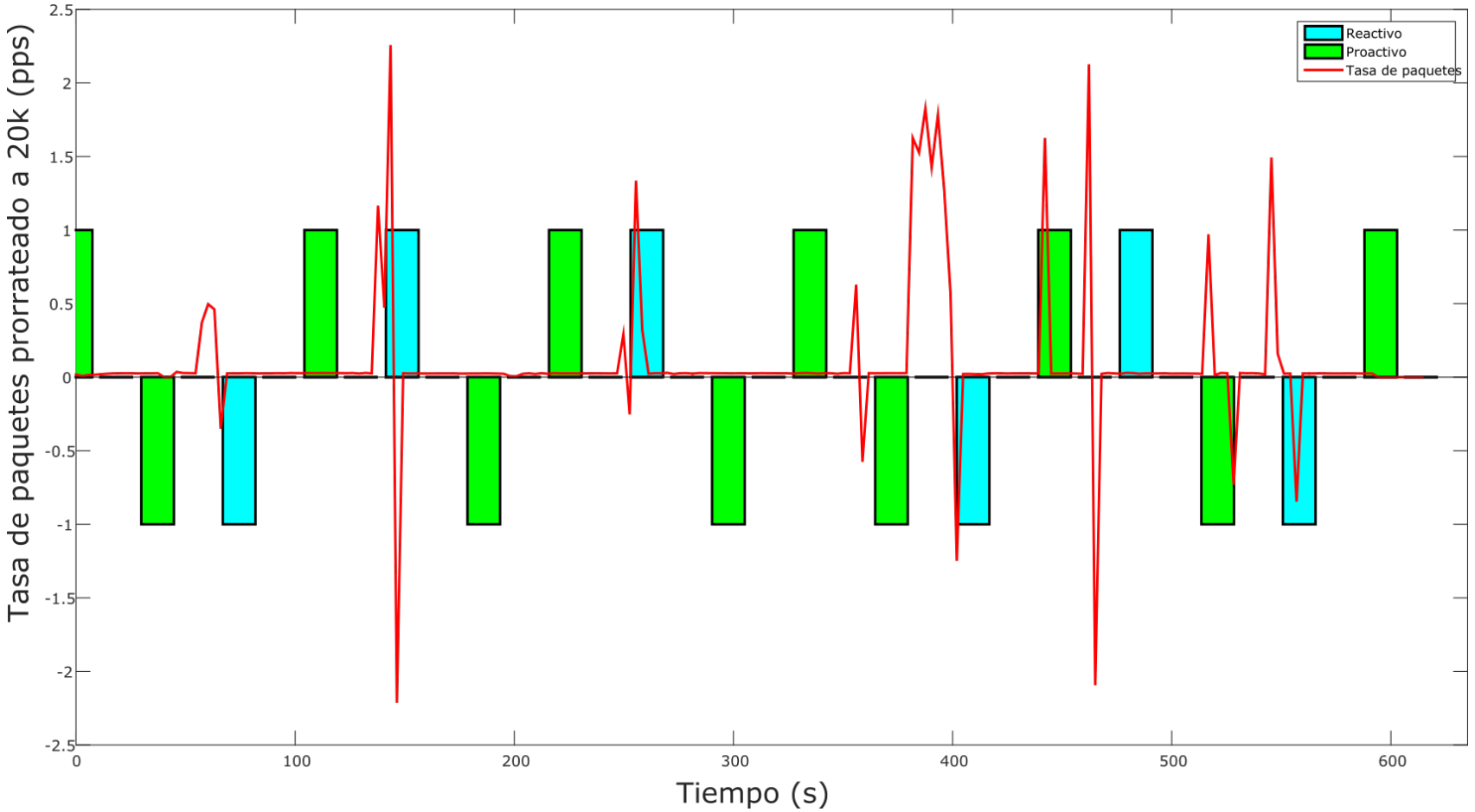








Evaluación y resultados
Funcionamiento del sistema ante ataques DDoS



Índice

Trabajo relacionado

Áreas de estudio

- Vulnerabilidades de SDN
  - Estudio de amenazas y posibles soluciones
- Mecanismos proactivos
  - Aplicados sobre SDN en un ámbito distinto
- Mecanismos reactivos
  - Implementan sistemas de defensa sobre SDN
- Mecanismos proactivos y reactivos
  - Desarrollados en otras áreas

Trabajo relacionado

Áreas de estudio

- Vulnerabilidades de SDN
  - Estudio de amenazas y posibles soluciones
- Mecanismos proactivos
  - Aplicados sobre SDN en un ámbito distinto
- Mecanismos reactivos
  - Implementan sistemas de defensa sobre SDN
- Mecanismos proactivos y reactivos
  - Desarrollados en otras áreas

Contribución

Mecanismo proactivo y reactivo para mitigar ataques DDoS siendo capaz de gestionar y modificar la arquitectura de red SDN

Índice

Conclusiones y líneas futuras

Conclusiones

- Estudio y comprensión de la arquitectura de red SDN
- Estudio y comprensión de los distintos ataques DDoS
- Implementación del mecanismo de defensa proactivo y reactivo en OpenDayLight
- Corroboración de la viabilidad y funcionamiento de la defensa

Conclusiones y líneas futuras

Conclusiones

- Estudio y comprensión de la arquitectura de red SDN
- Estudio y comprensión de los distintos ataques DDoS
- Implementación del mecanismo de defensa proactivo y reactivo en OpenDayLight
- Corroboración de la viabilidad y funcionamiento de la defensa

Líneas futuras

- Formalizar el proyecto mediante modelos de Markov
- Actualizar la versión Beryllium de OpenDayLight
- Añadir mecanismos de detección
- Complementar con un *honeypot*

Muchas gracias por su atención

Universidad
Zaragoza