Denial-of-Service Attack: Introduction and Mitigation

Guest Lecture for
Internet Technologies (COMP90007)
Semester 1, 2021

Yi Han

School of Computing and Information Systems

About me

- Research fellow @CIS
- Research interests: machine learning, social media analysis, cyber security
- Currently working on fake news detection
- Teaching: Security Analytics (COMP90073)
- Contact: yi.han@unimelb.edu.au

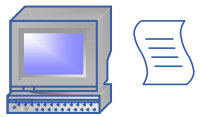
Outline

- Denial-of-Service (DoS) attack and Distributed Denial-of-Service (DDoS) attack
- Part 1: Introduction
  - An early example
  - Common types of DDoS attack
    - Resource-depletion attack
    - Bandwidth-depletion attack
  - Current status and new trends
- Part 2: Mitigation
  - Reinforcement learning for throttling DDoS attacks

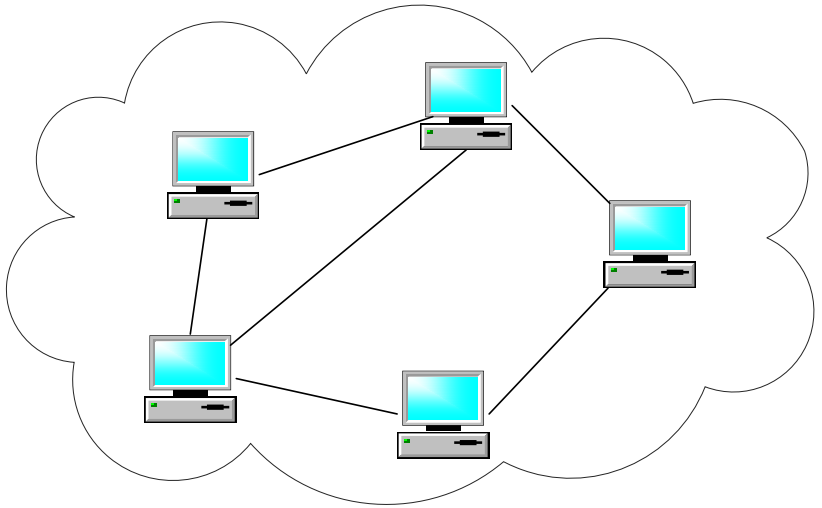
DoS & DDoS: Introduction

Denial of service attack – an early example

- Denial-of-Service attack
  - Malicious attempt to make a critical service unavailable to legitimate users
- Morris worm
  - November, 1988
  - Robert Morris, graduate student @Cornell



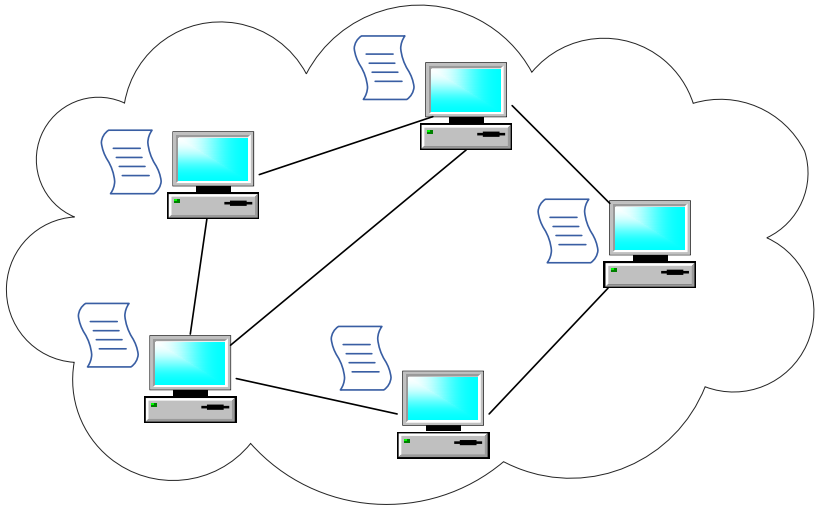
http://www.flickr.com/photos/intelfreepress/10477292993/



Denial of service attack – an early example

- Denial-of-Service attack
  - Malicious attempt to make a critical service unavailable to legitimate users
- Morris worm
  - November, 1988
  - Robert Morris, graduate student @Cornell

http://www.flickr.com/photos/intelfreepress/10477292993/

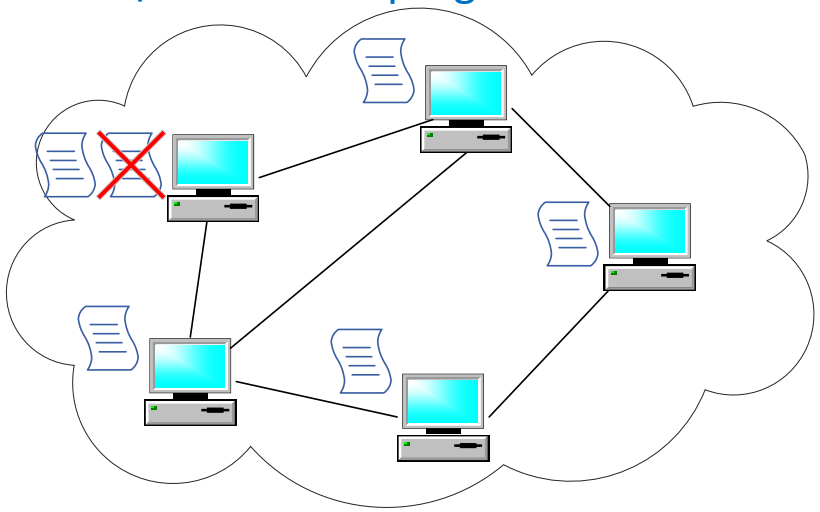


Denial of service attack – an early example

- Denial-of-Service attack
  - Malicious attempt to make a critical service unavailable to legitimate users
- Morris worm
  - November, 1988
  - Robert Morris, graduate student @Cornell

http://www.flickr.com/photos/intelfreepress/10477292993/

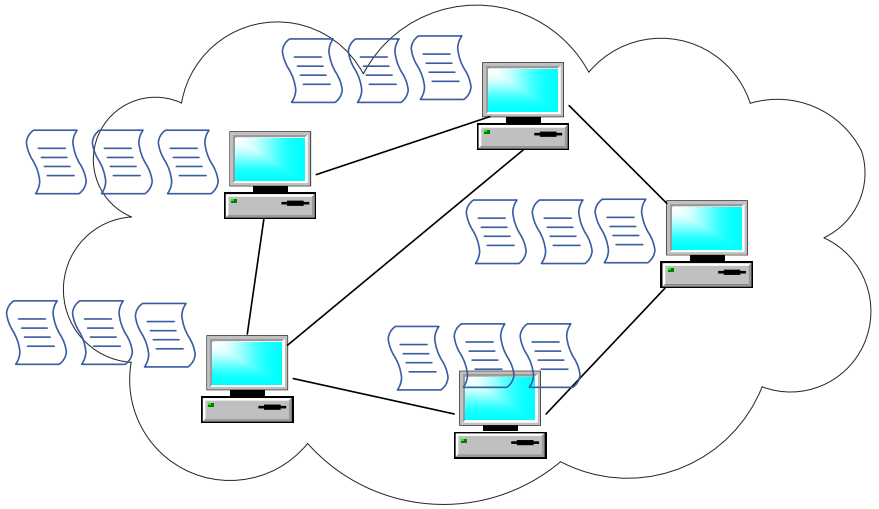
Multiple copies → roll a dice to decide which to kill
But 1/7 times the program would not terminate itself



Denial of service attack – an early example

- Denial-of-Service attack
  - Malicious attempt to make a critical service unavailable to legitimate users
- Morris worm
  - November, 1988
  - Robert Morris, graduate student @Cornell

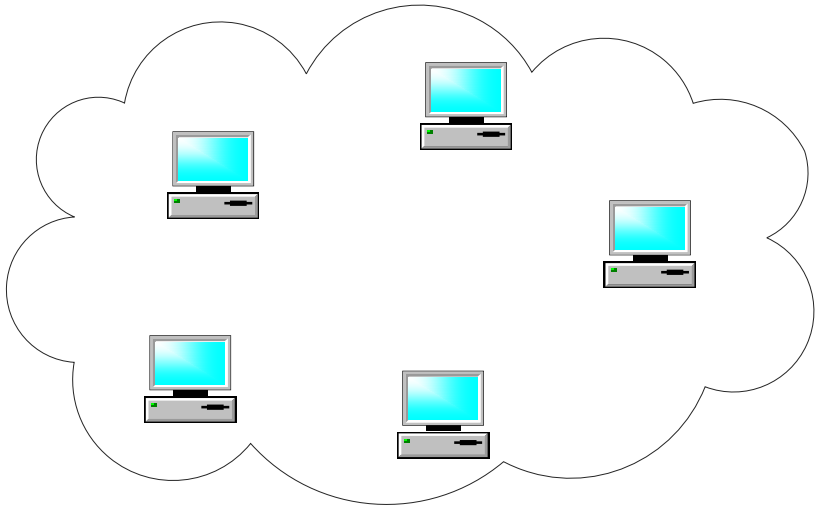
http://www.flickr.com/photos/intelfreepress/10477292993/



Denial of service attack – an early example

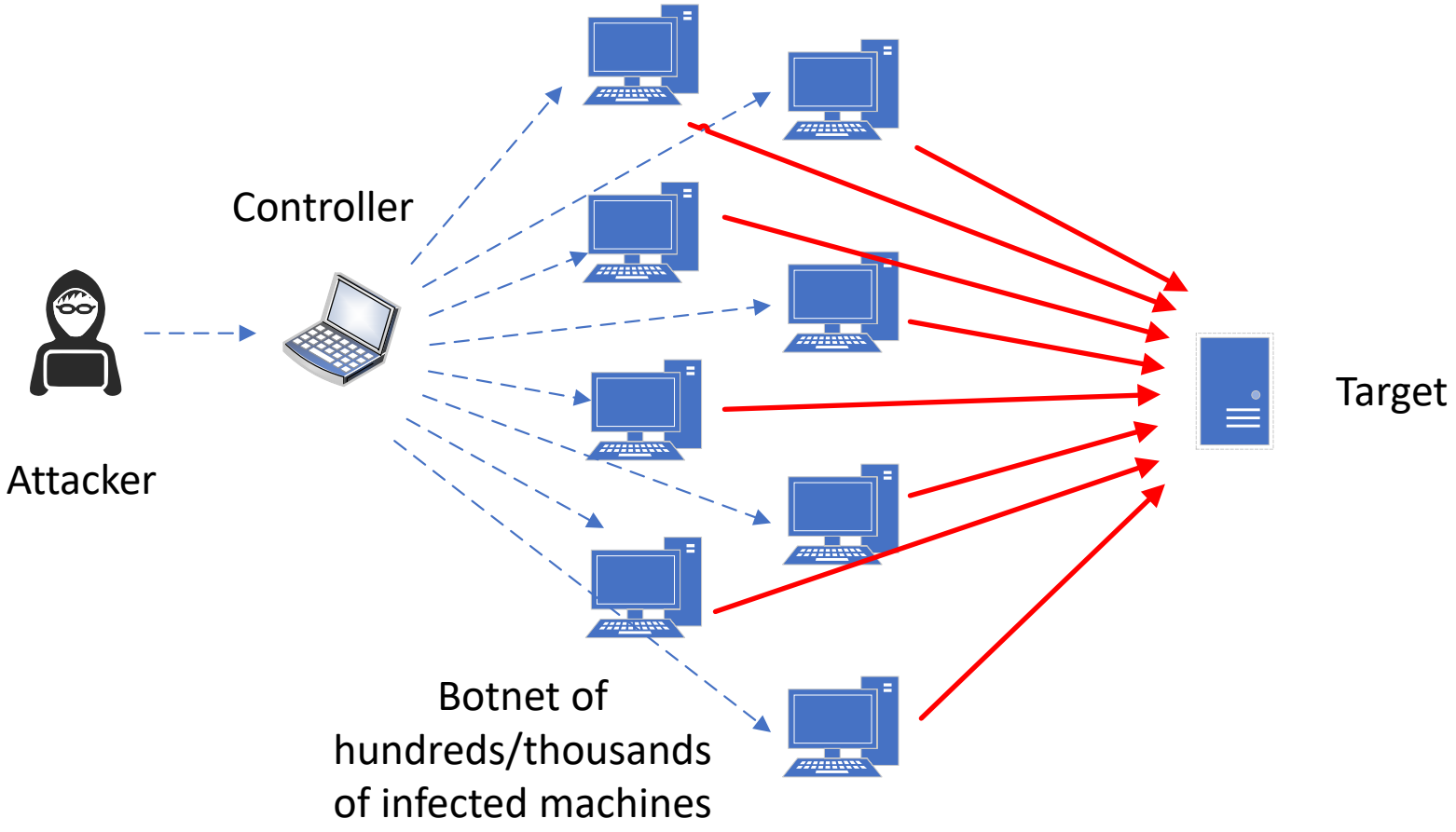
- Denial-of-Service attack
  - Malicious attempt to make a critical service unavailable to legitimate users
- Morris worm
  - November, 1988
  - Robert Morris, graduate student @Cornell

http://www.flickr.com/photos/intelfreepress/10477292993/



Distributed denial of service attack

- A typical DDoS attack

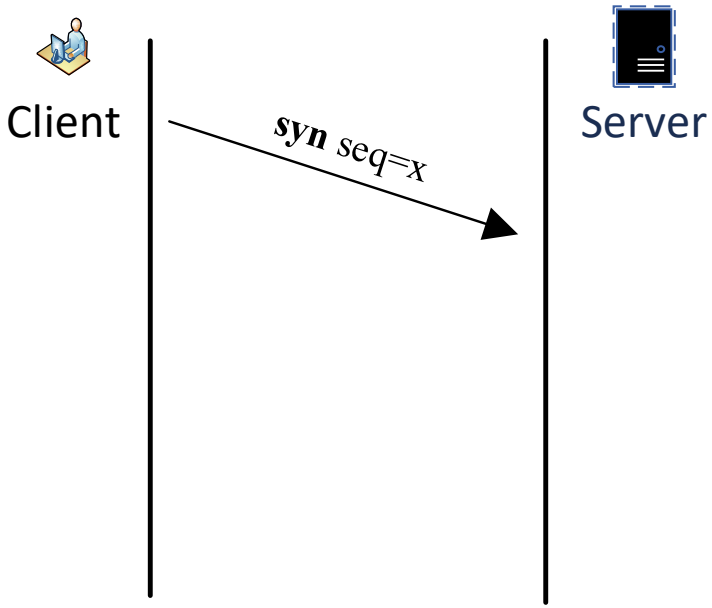


Common type – resource-depletion attack

- Common types of DDoS attack – resource-depletion attack
  - Exhaust the target's resources
  - Example: SYN flood

Common type – resource-depletion attack

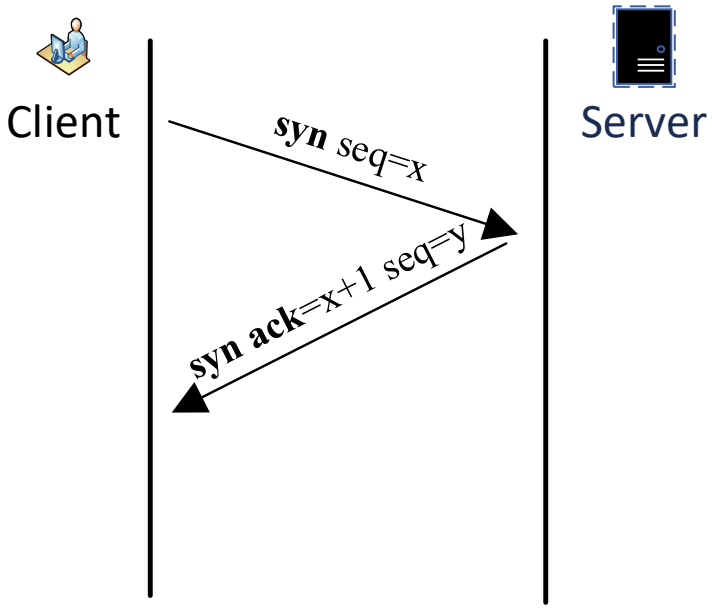
- Common types of DDoS attack – resource-depletion attack
  - Exhaust the target's resources
  - Example: SYN flood



TCP handshake

Common type – resource-depletion attack

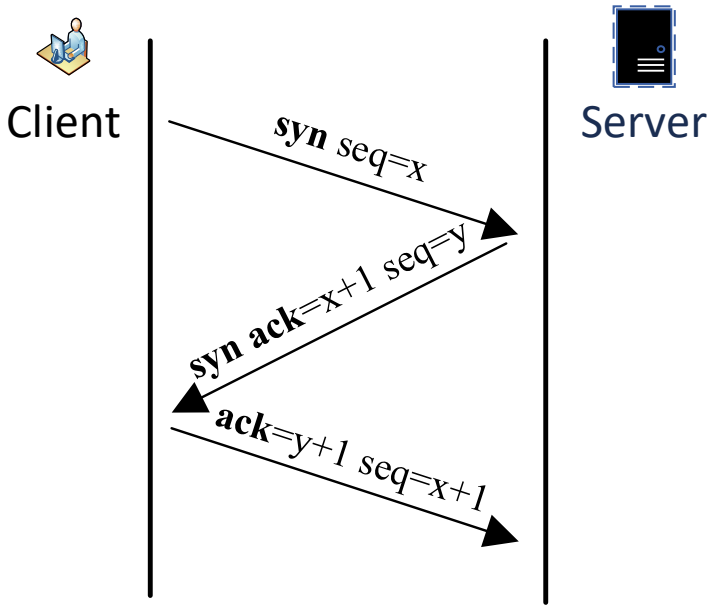
- Common types of DDoS attack – resource-depletion attack
  - Exhaust the target's resources
  - Example: SYN flood



TCP handshake

Common type – resource-depletion attack

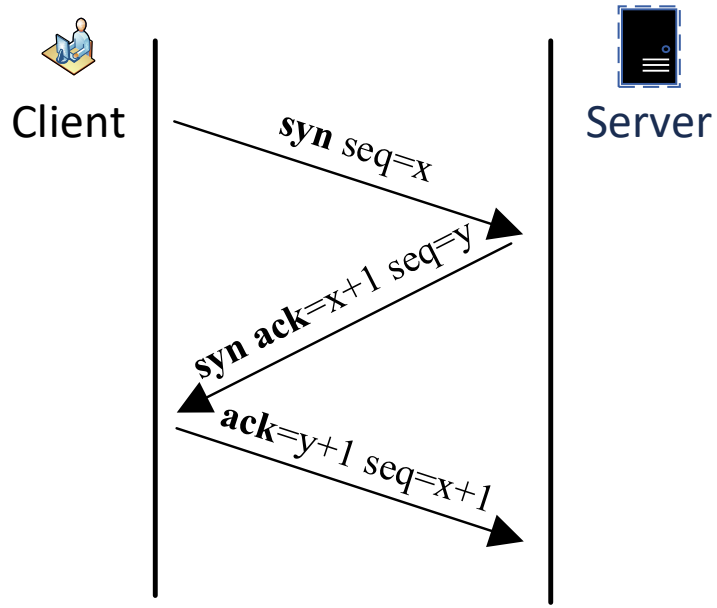
- Common types of DDoS attack – resource-depletion attack
  - Exhaust the target's resources
  - Example: SYN flood



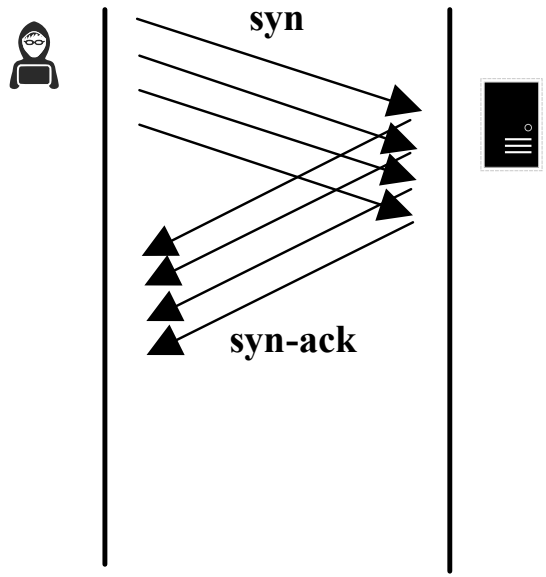
TCP handshake

Common type – resource-depletion attack

- Common types of DDoS attack – resource-depletion attack
  - Exhaust the target's resources
  - Example: SYN flood



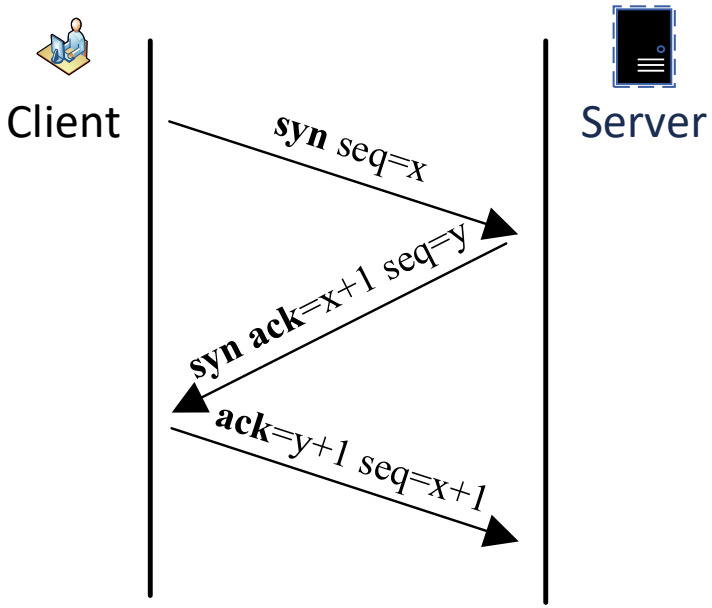
TCP handshake



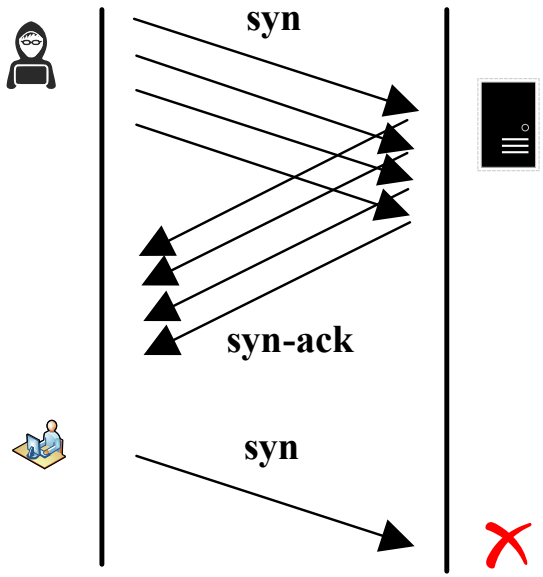
SYN flood

Common type – resource-depletion attack

- Common types of DDoS attack – resource-depletion attack
  - Exhaust the target's resources
  - Example: SYN flood



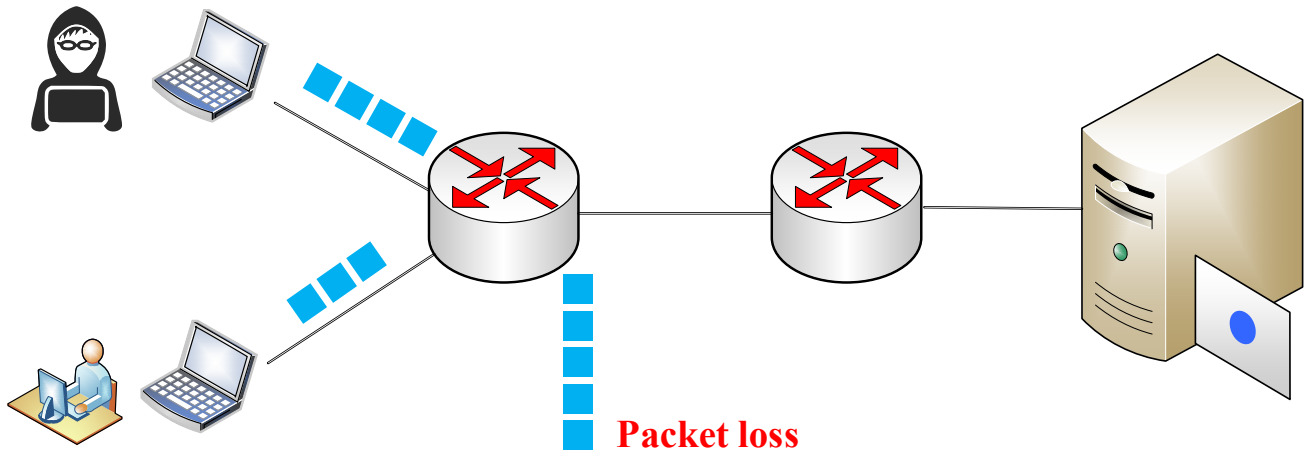
TCP handshake



SYN flood

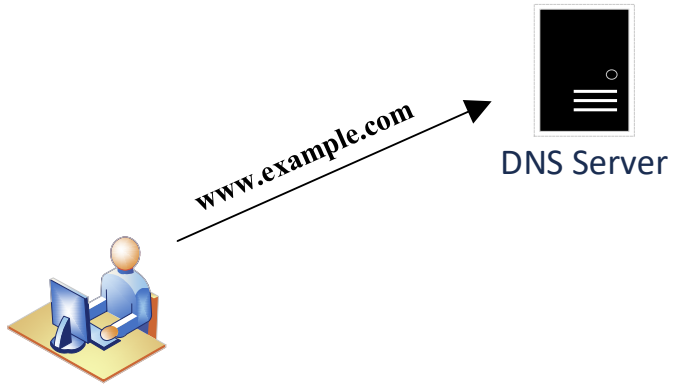
Common type – bandwidth-depletion attack

- Common types of DoS attack – bandwidth-depletion attack
  - Overload the communication channel



Common type – bandwidth-depletion attack

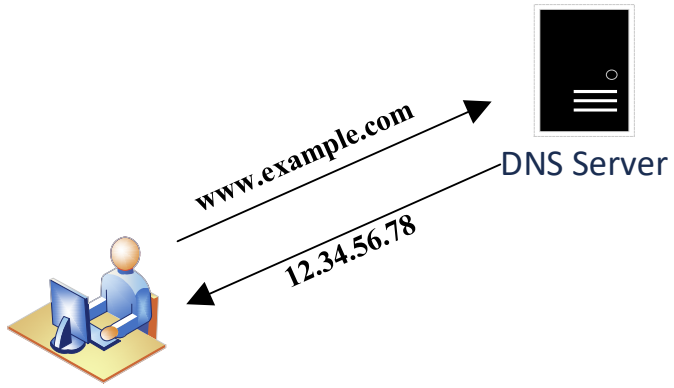
- Common types of DoS attack – bandwidth-depletion attack
  - Overload the communication channel
  - Example: DNS amplification



DNS server

Common type – bandwidth-depletion attack

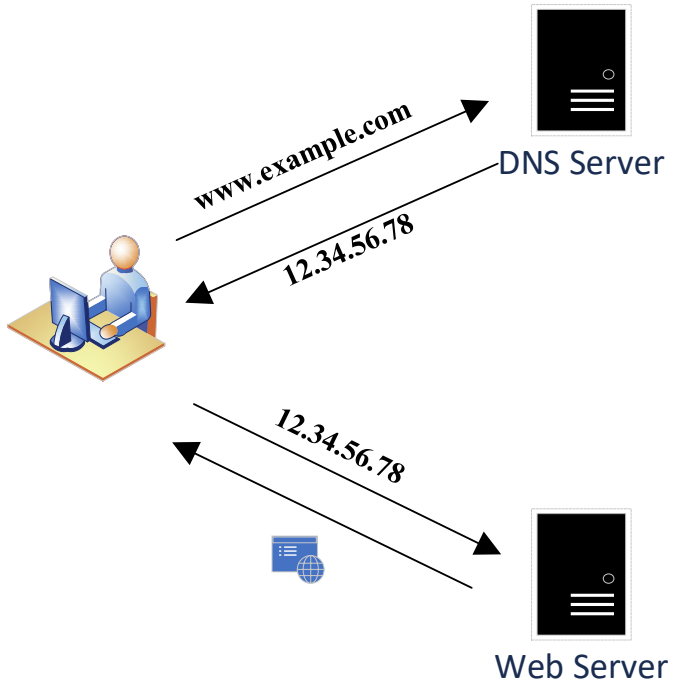
- Common types of DoS attack – bandwidth-depletion attack
  - Overload the communication channel
  - Example: DNS amplification



DNS server

Common type – bandwidth-depletion attack

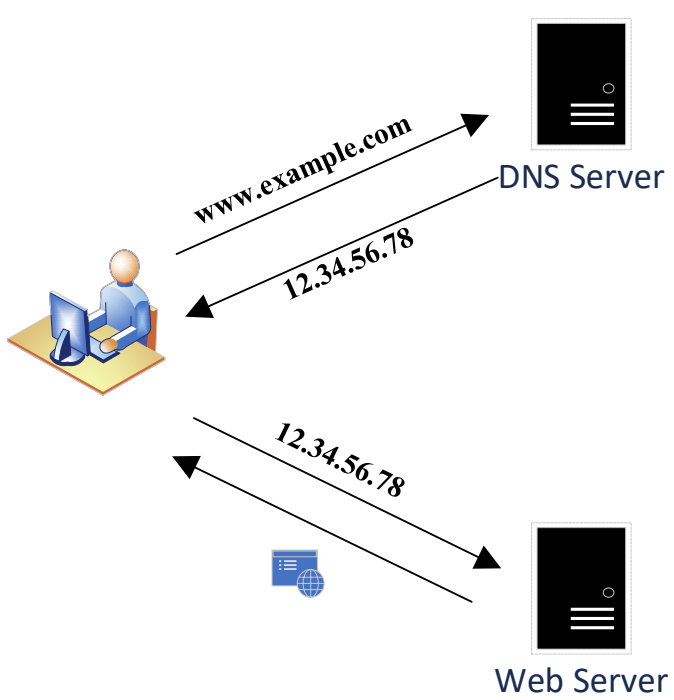
- Common types of DoS attack – bandwidth-depletion attack
  - Overload the communication channel
  - Example: DNS amplification



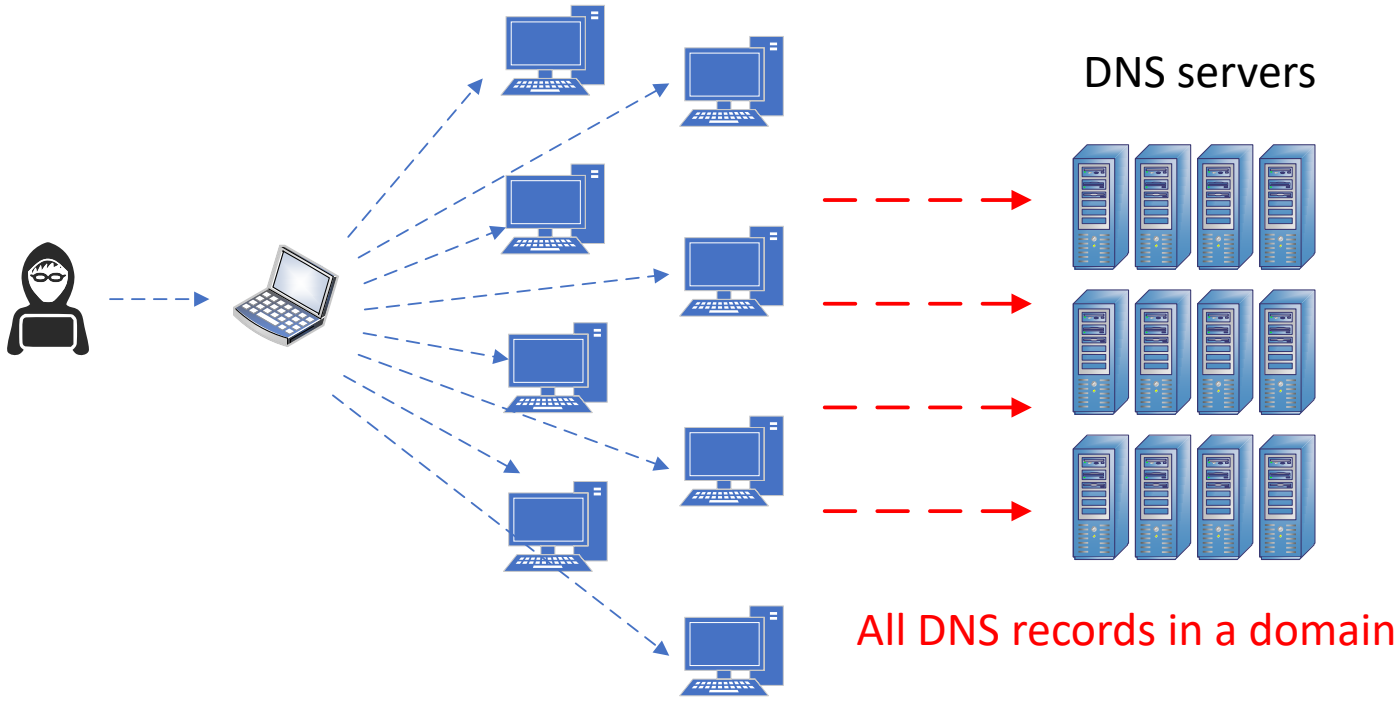
DNS server

Common type – bandwidth-depletion attack

- Common types of DoS attack – bandwidth-depletion attack
  - Overload the communication channel
  - Example: DNS amplification

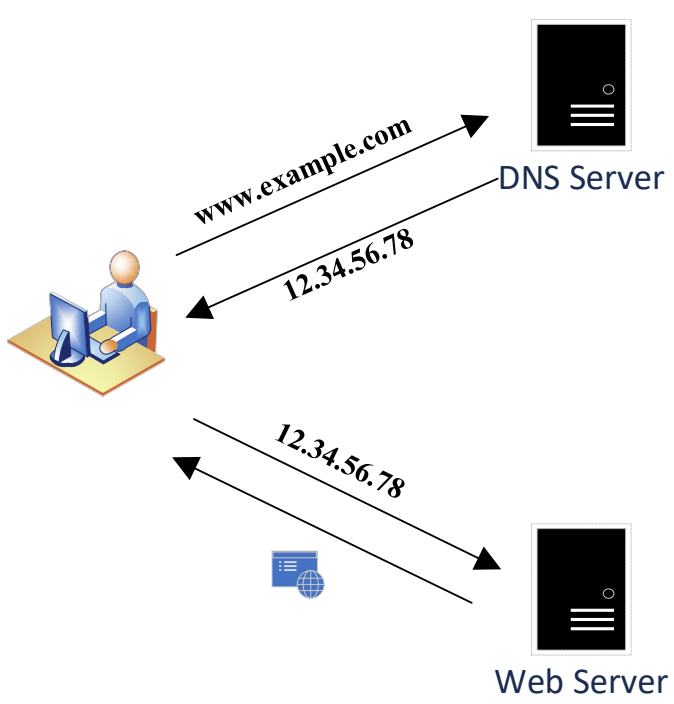


DNS server

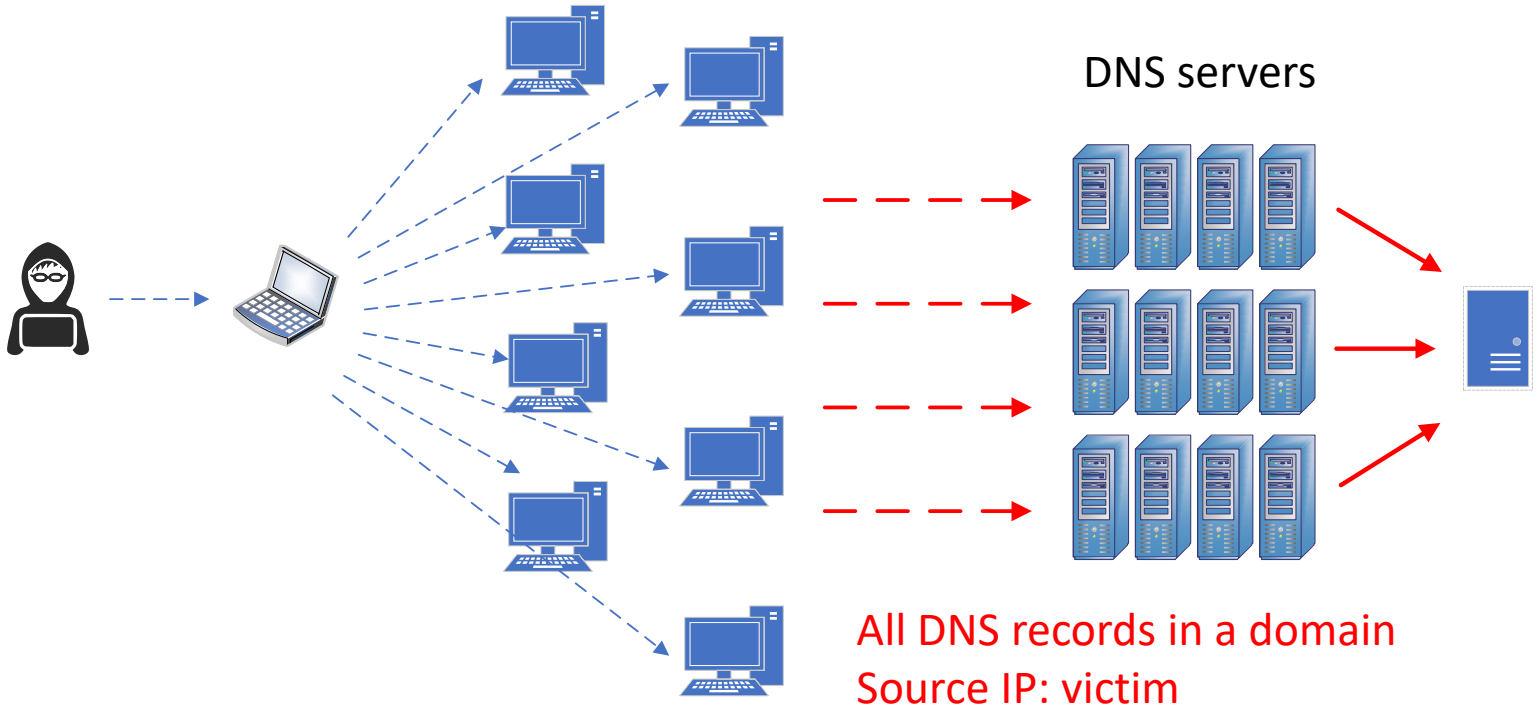


Common type – bandwidth-depletion attack

- Common types of DoS attack – bandwidth-depletion attack
  - Overload the communication channel
  - Example: DNS amplification



DNS server

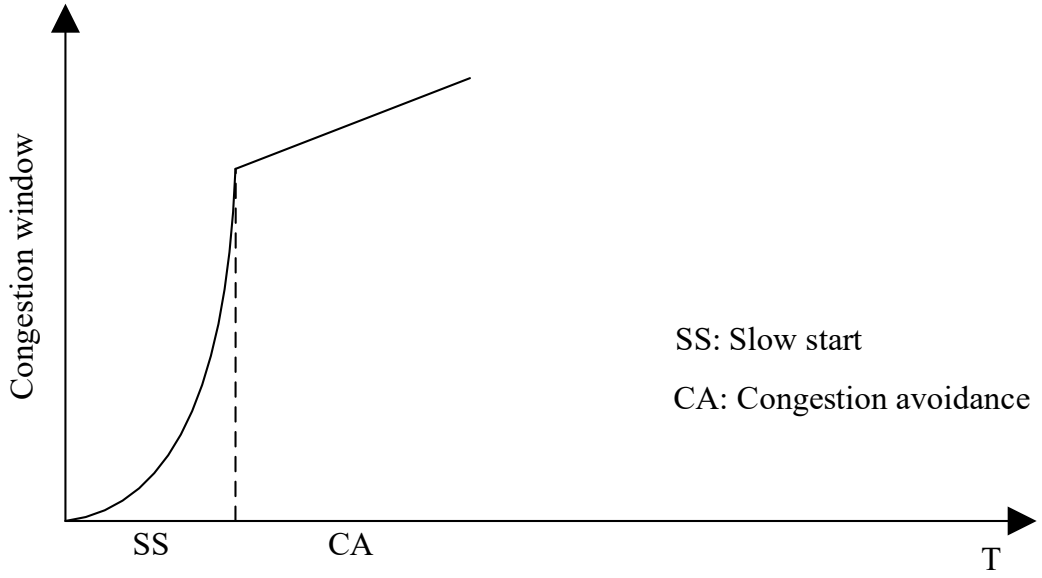


Low-rate DoS attack

- Low-rate DoS attack
  - TCP congestion control mechanism
    - Slow start
    - Congestion avoidance (AIMD)
    - Fast retransmit
    - …

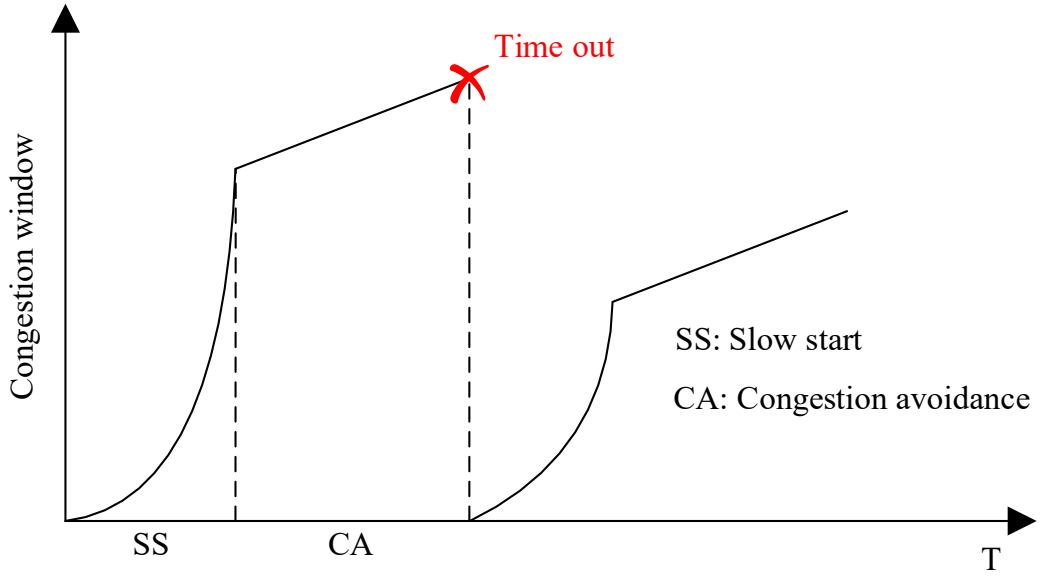
Low-rate DoS attack

- Low-rate DoS attack
  - TCP congestion control mechanism
    - Slow start
    - Congestion avoidance (AIMD)
    - Fast retransmit
    - …



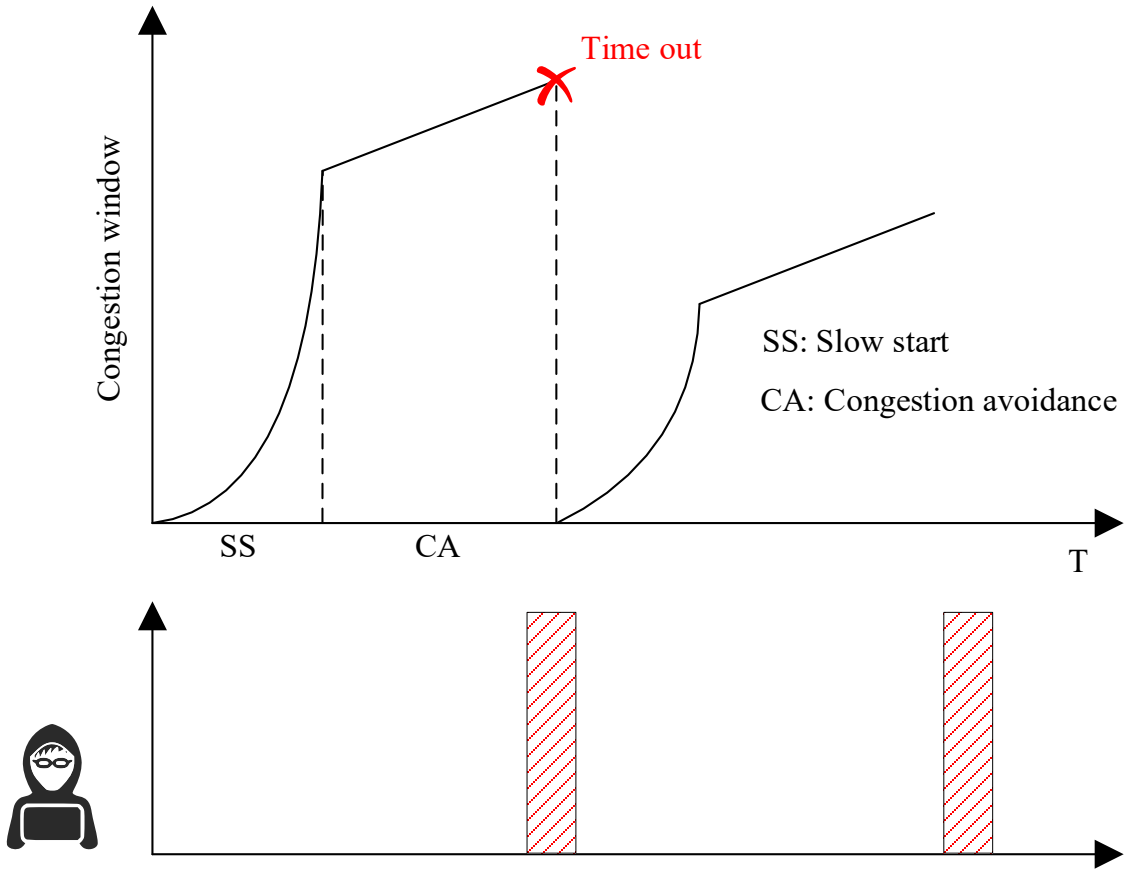
Low-rate DoS attack

- Low-rate DoS attack
  - TCP congestion control mechanism
    - Slow start
    - Congestion avoidance (AIMD)
    - Fast retransmit
    - …



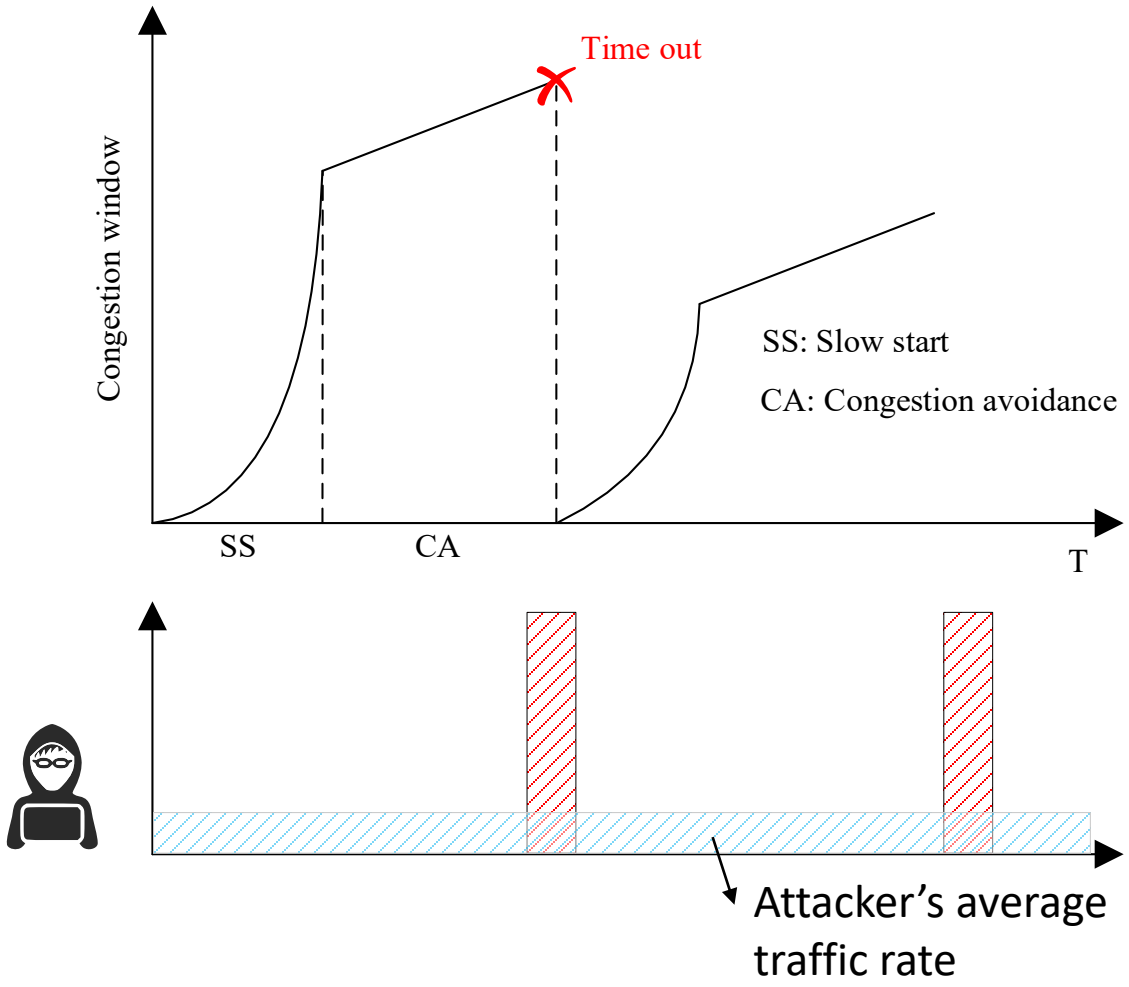
Low-rate DoS attack

- Low-rate DoS attack
  - TCP congestion control mechanism
    - Slow start
    - Congestion avoidance (AIMD)
    - Fast retransmit
    - …



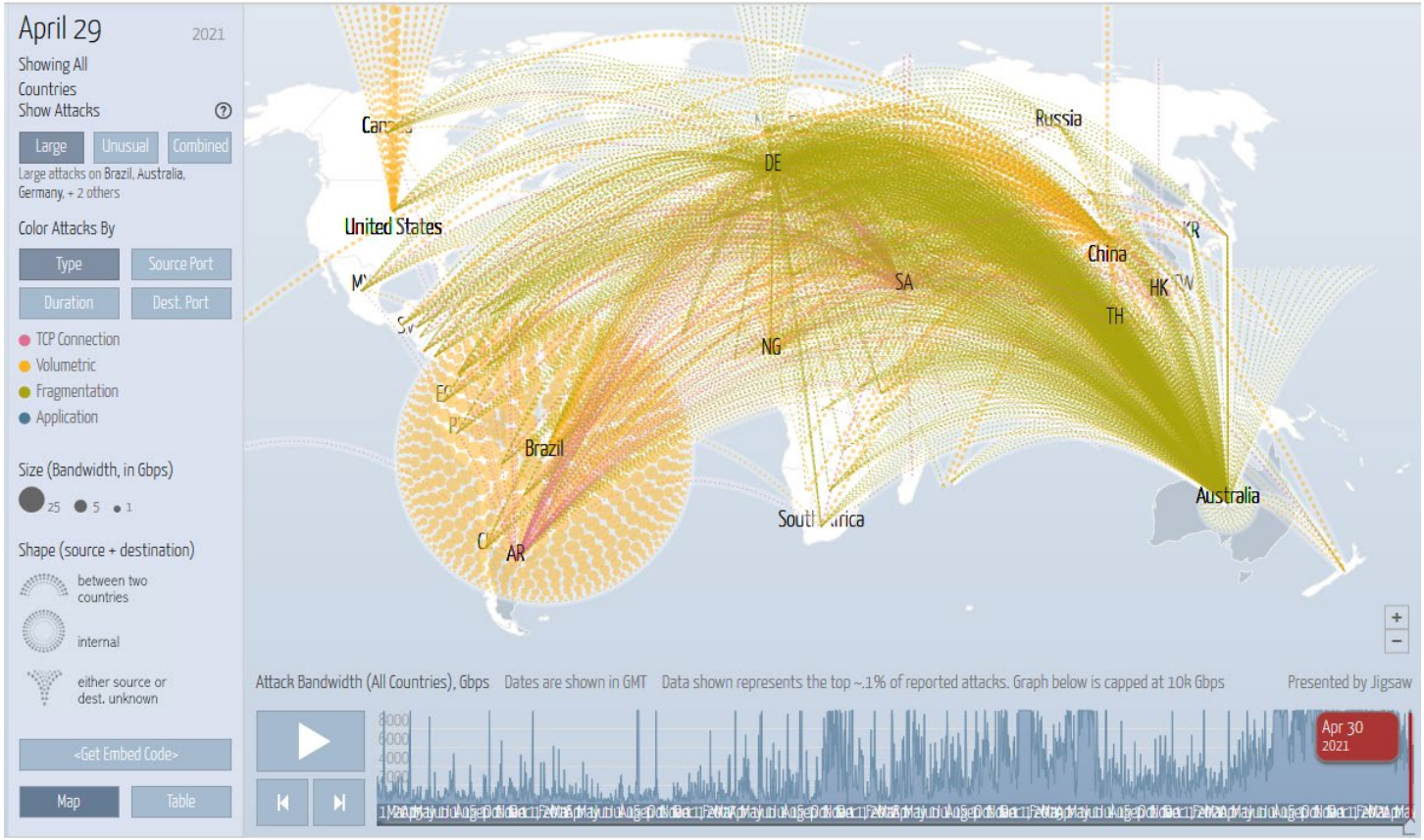
Low-rate DoS attack

- Low-rate DoS attack
  - TCP congestion control mechanism
    - Slow start
    - Congestion avoidance (AIMD)
    - Fast retransmit
    - …



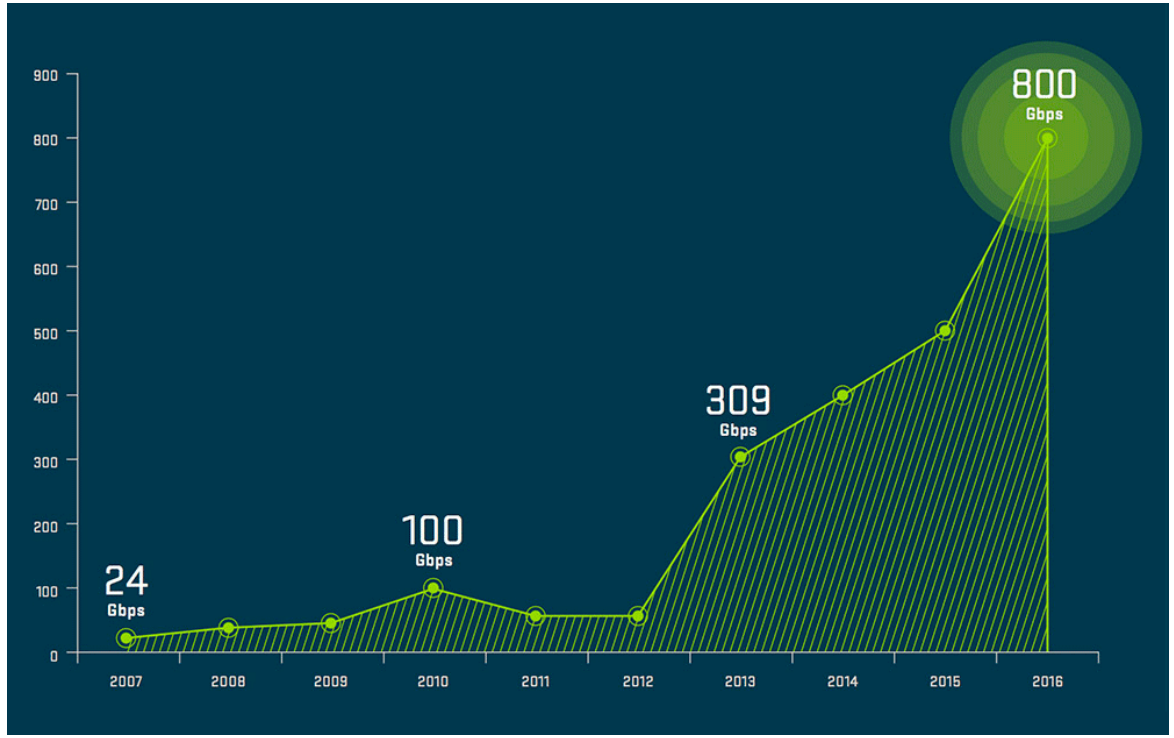
Current status

- DDoS attacks still occur almost every hour globally
  - http://www.digitalattackmap.com/
  - Statistics are gather by Arbor's Active Threat Level Analysis System from 330+ ISP customers with 130Tbps of global traffic



New trends of DDoS attack

- New trends of DDoS attack
  - Increase in quantity and severity
  - Application-layer attack
  - Internet-of-Things
  - 5G

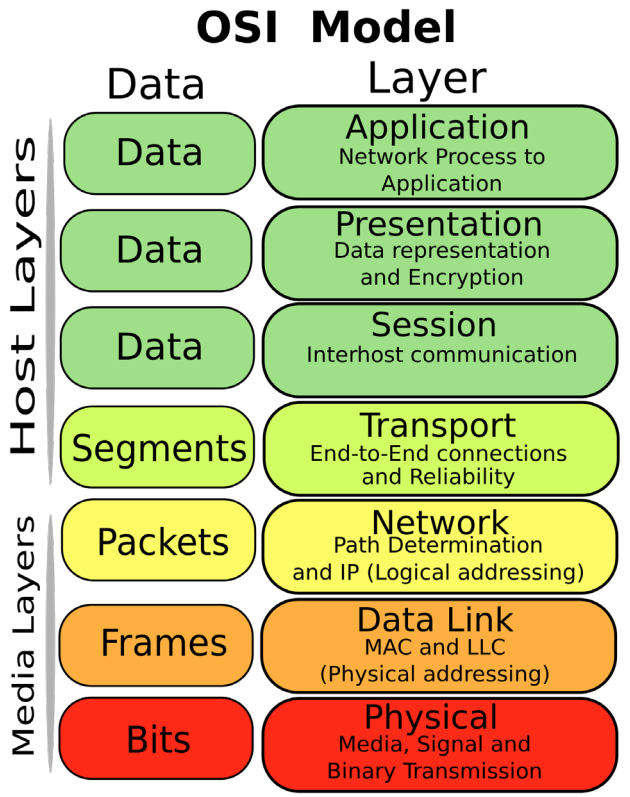


Trend in maximum DDoS attack rate

[Source: Arbor 12th Annual World Infrastructure Security Report, 2017]

New trends of DDoS attack

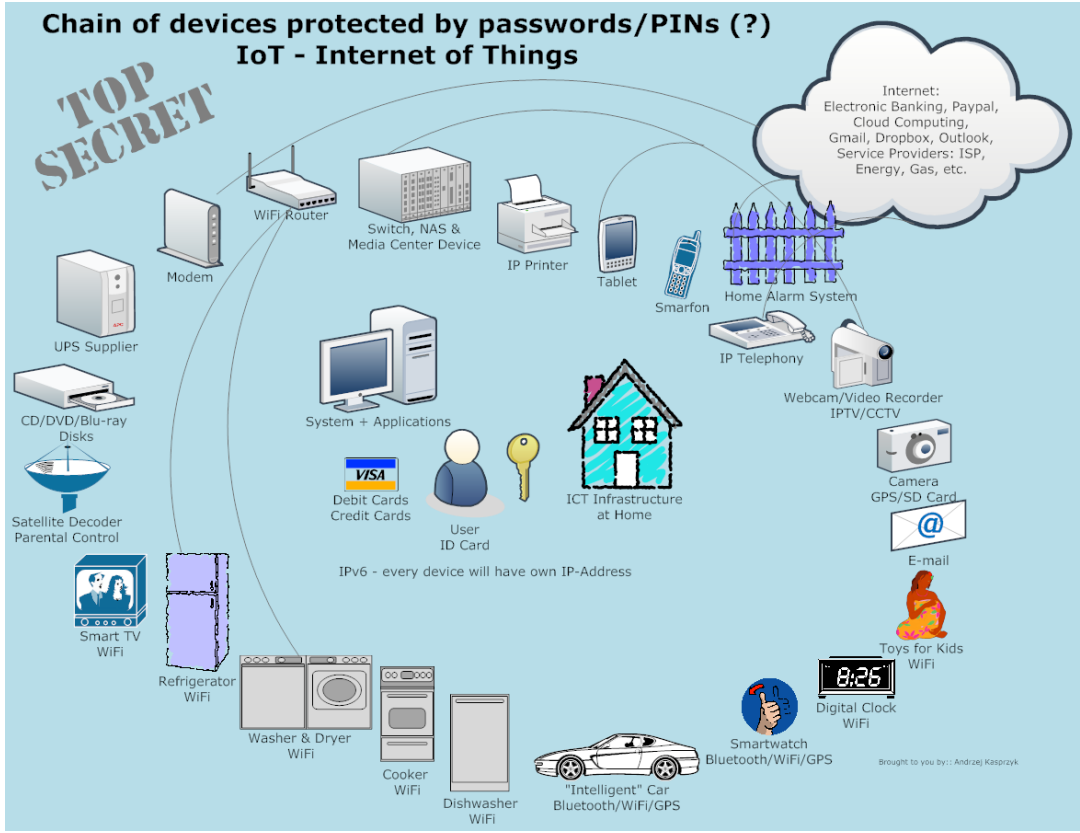
- New trends of DDoS attack
  - Increase in quantity and severity
  - Application-layer attack
  - Internet-of-Things
  - 5G



https://commons.wikimedia.org/wiki/File:Osi-model-jb.svg

New trends of DDoS attack

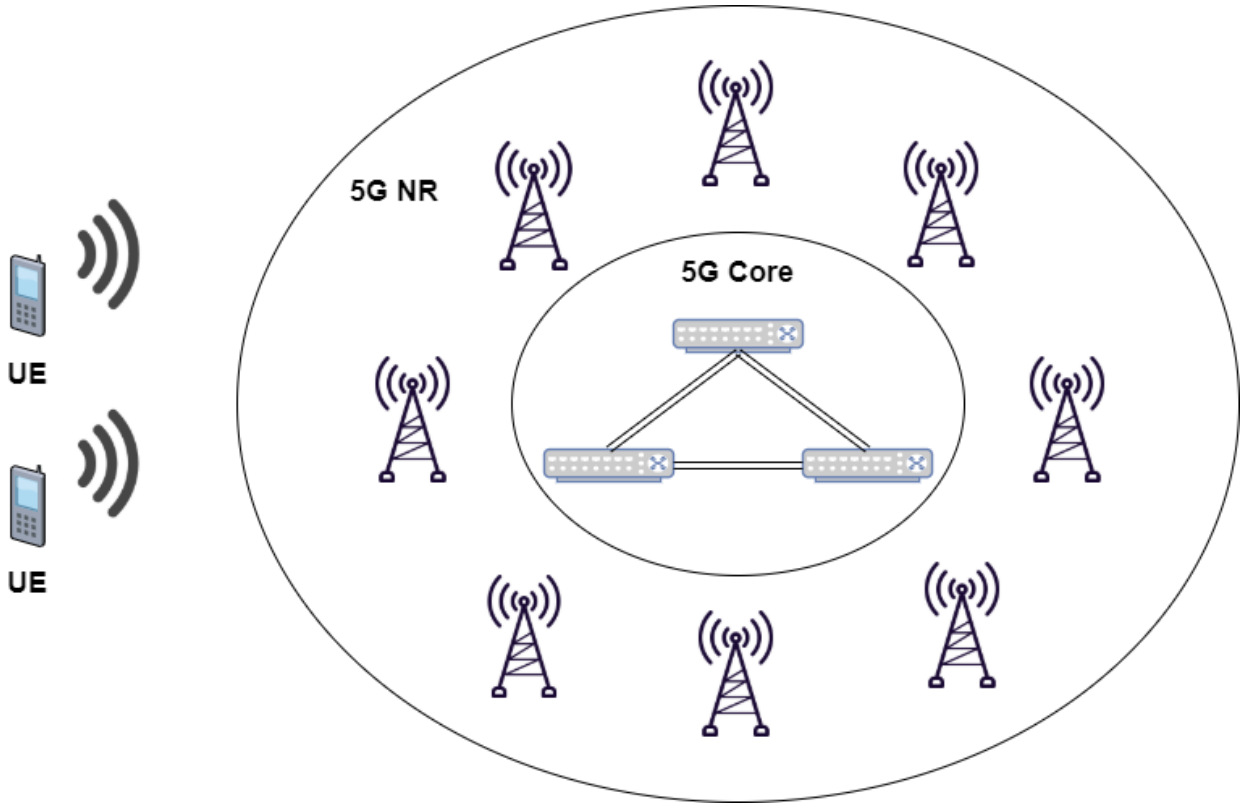
- New trends of DDoS attack
  - Increase in quantity and severity
  - Application-layer attack
  - Internet-of-Things
  - 5G



https://commons.wikimedia.org/wiki/File:Chain_of_home_devices_(including_IoT)_with_passwords_or_pin.png

New trends of DDoS attack

- New trends of DDoS attack
  - Increase in quantity and severity
  - Application-layer attack
  - Internet-of-Things
  - 5G



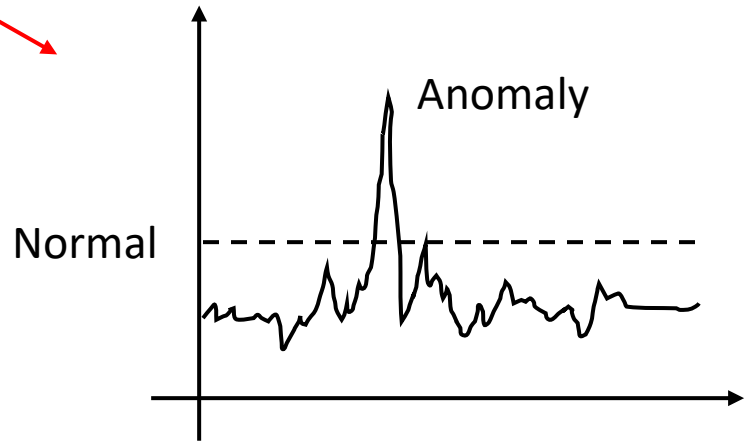
https://commons.wikimedia.org/wiki/File:5G_Architecture.png

DoS & DDoS: Mitigation

DDoS mitigation

- DDoS mitigation
  - Detection: distinguish attack from normal traffic
    - Signature-based: identify attack signatures
    - Anomaly-based: define normal traffic
  - Filtering: drop malicious traffic
- Automated by machine learning
  - Supervised learning
  - Unsupervised learning
  - Reinforcement learning

Example:
if (src_ip == dst_ip && src_prt == dst_prt)
then “attack”

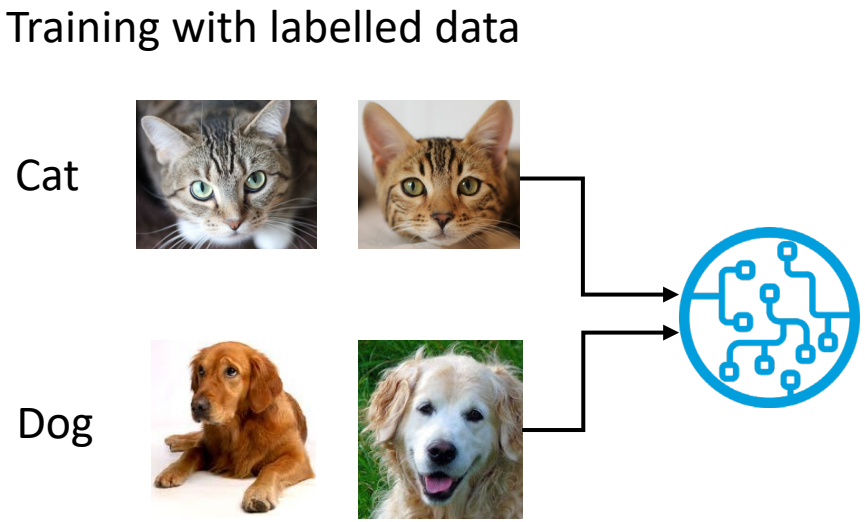


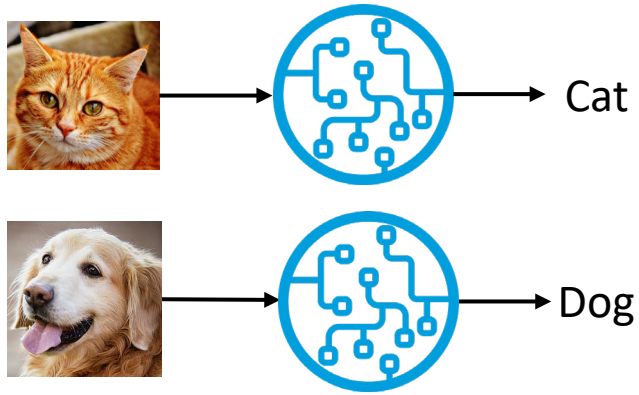
DDoS mitigation

- DDoS mitigation
  - Detection: distinguish attack from normal traffic
    - Signature-based: identify attack signatures
    - Anomaly-based: define normal traffic
  - Filtering: drop malicious traffic
- Automated by machine learning
  - Supervised learning
  - Unsupervised learning
  - Reinforcement learning

DDoS mitigation

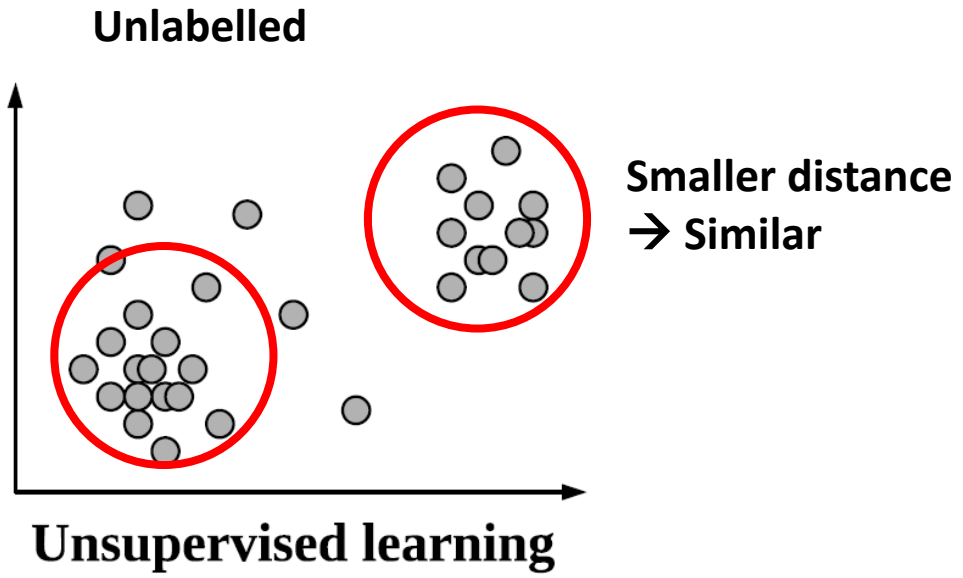
- DDoS mitigation
  - Detection: distinguish attack from normal traffic
    - Signature-based: identify attack signatures
    - Anomaly-based: define normal traffic
  - Filtering: drop malicious traffic
- Automated by machine learning
  - Supervised learning
  - Unsupervised learning
  - Reinforcement learning





DDoS mitigation

- DDoS mitigation
  - Detection: distinguish attack from normal traffic
    - Signature-based: identify attack signatures
    - Anomaly-based: define normal traffic
  - Filtering: drop malicious traffic
- Automated by machine learning
  - Supervised learning
  - Unsupervised learning
  - Reinforcement learning



DDoS mitigation

- DDoS mitigation
  - Detection: distinguish attack from normal traffic
    - Signature-based: identify attack signatures
    - Anomaly-based: define normal traffic
  - Filtering: drop malicious traffic
- Automated by machine learning
  - Supervised learning
  - Unsupervised learning
  - Reinforcement learning

Reinforcement learning

- Applications of reinforcement learning

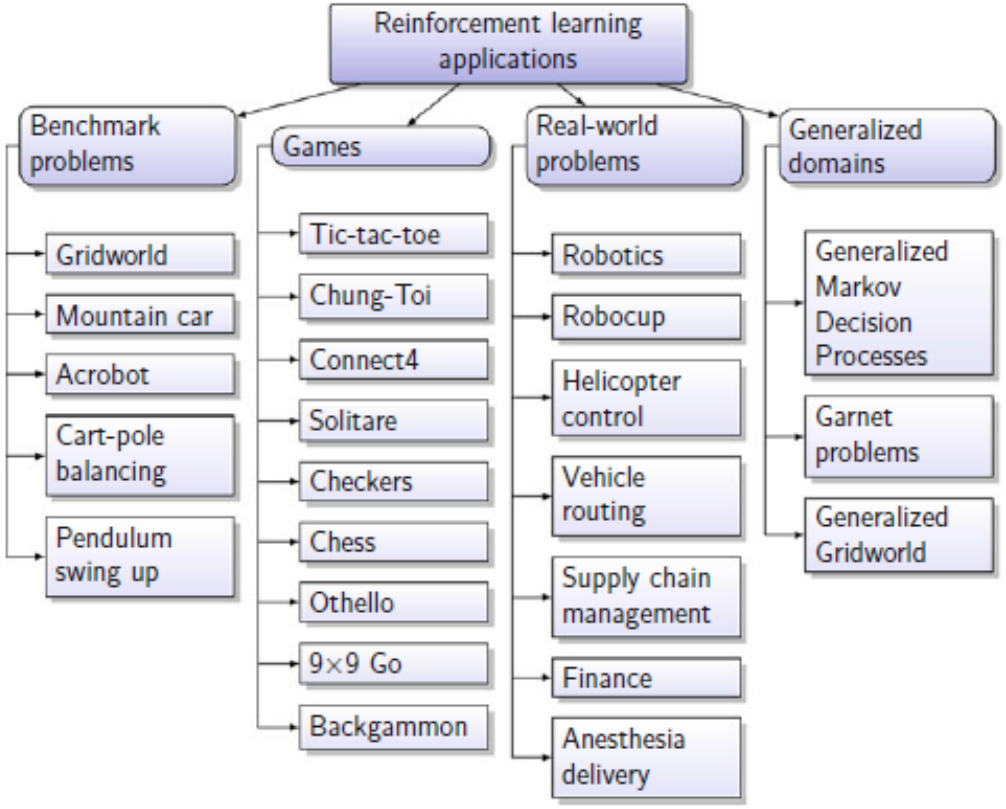
https://www.youtube.com/watch?v=VCdxqn0fcnE

https://www.tesla.com/videos/autopilot-self-driving-hardware-neighborhood-long

Reinforcement learning

- Applications of reinforcement learning

https://www.youtube.com/v



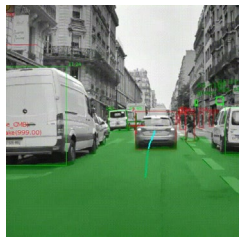
deos/autopilot-self-driving-ong

Reinforcement learning

- Key elements in a reinforcement learning problem

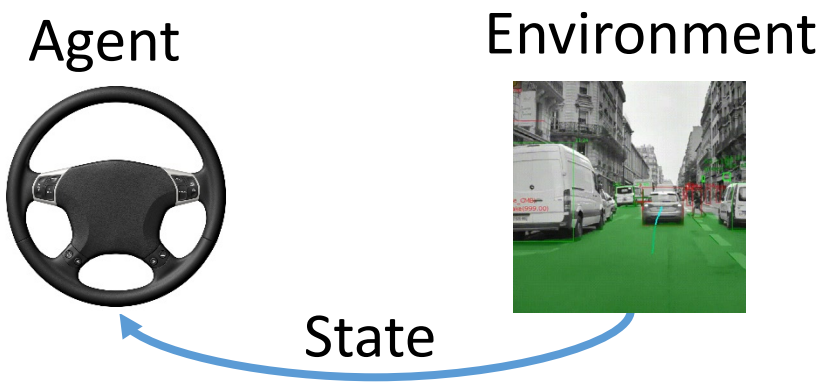
Agent

Environment



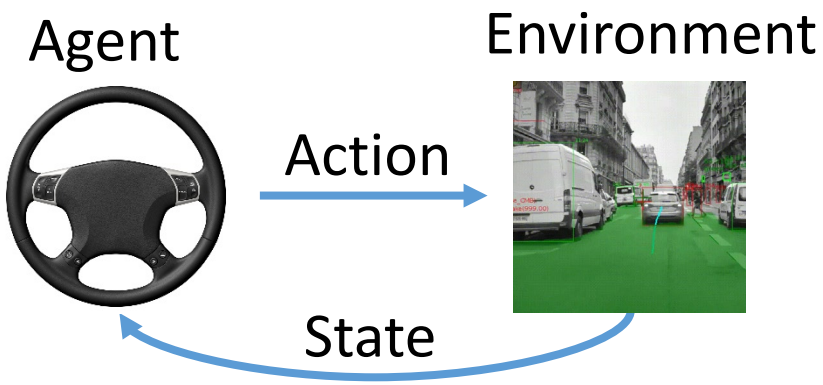
Reinforcement learning

- Key elements in a reinforcement learning problem



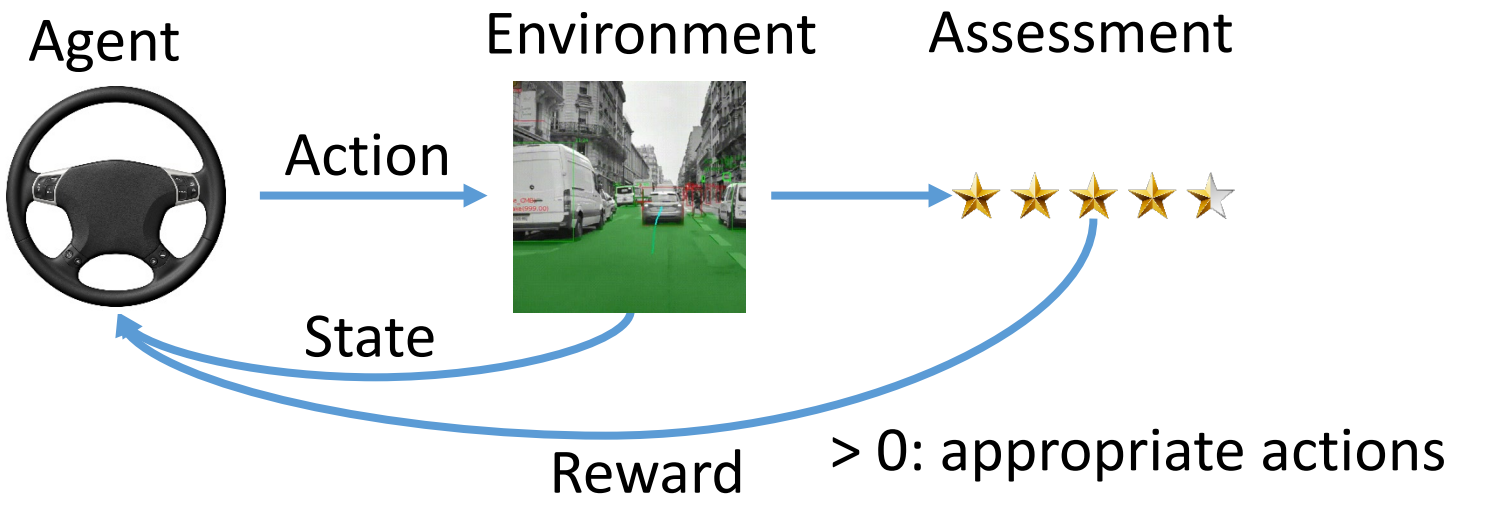
Reinforcement learning

- Key elements in a reinforcement learning problem



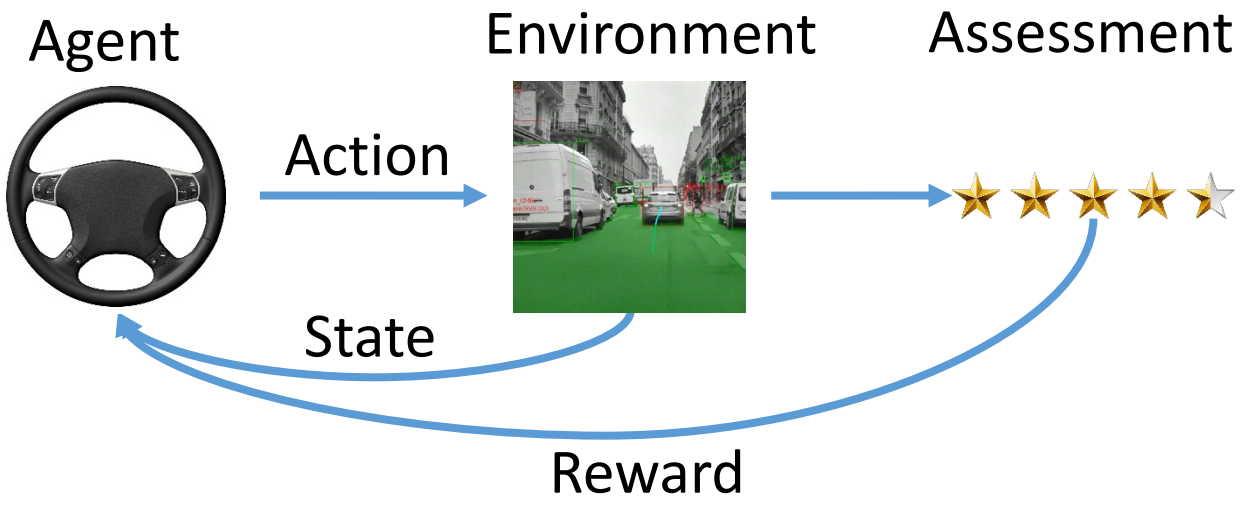
Reinforcement learning

- Key elements in a reinforcement learning problem



Reinforcement learning

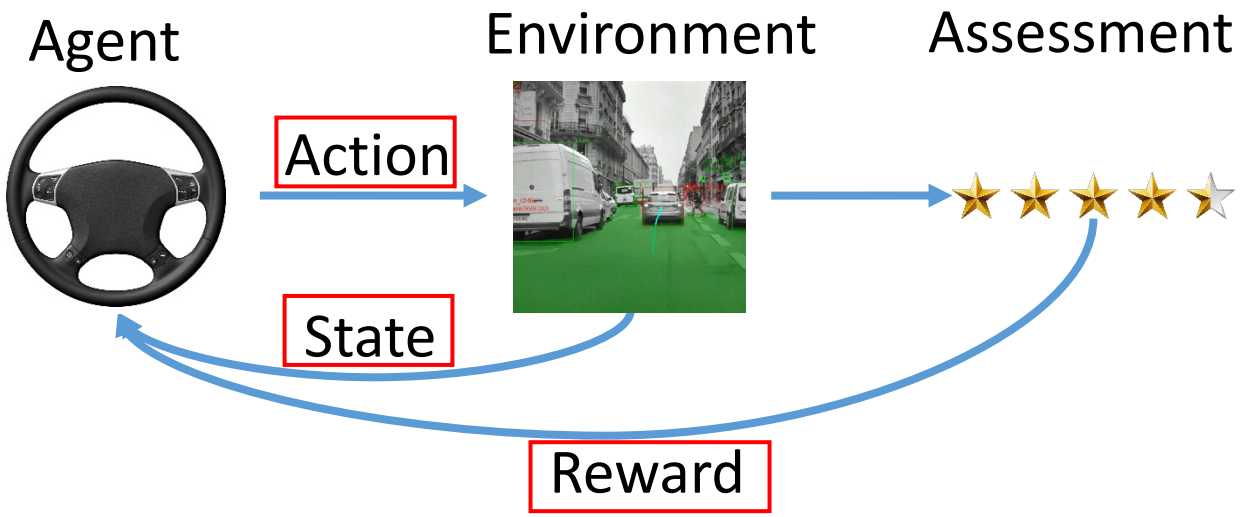
- Key elements in a reinforcement learning problem



Goal: Maximise cumulative rewards

Reinforcement learning

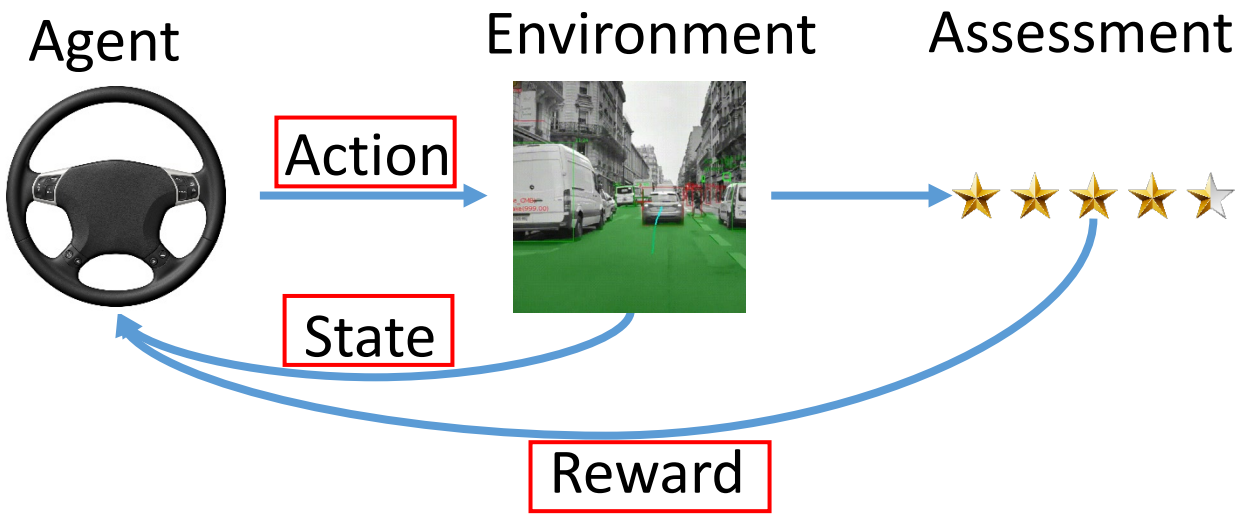
- Key elements in a reinforcement learning problem



Goal: Maximise cumulative rewards

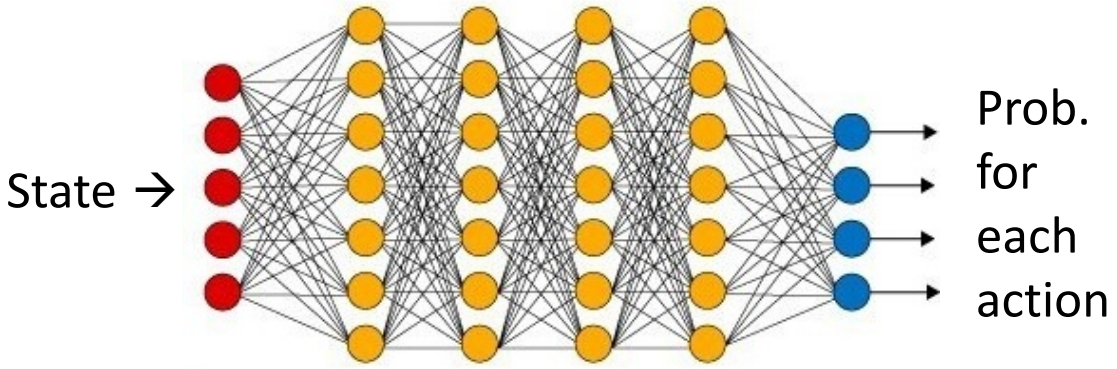
Reinforcement learning

- Key elements in a reinforcement learning problem



Goal: Maximise cumulative rewards

Training goal: $max \sum reward$

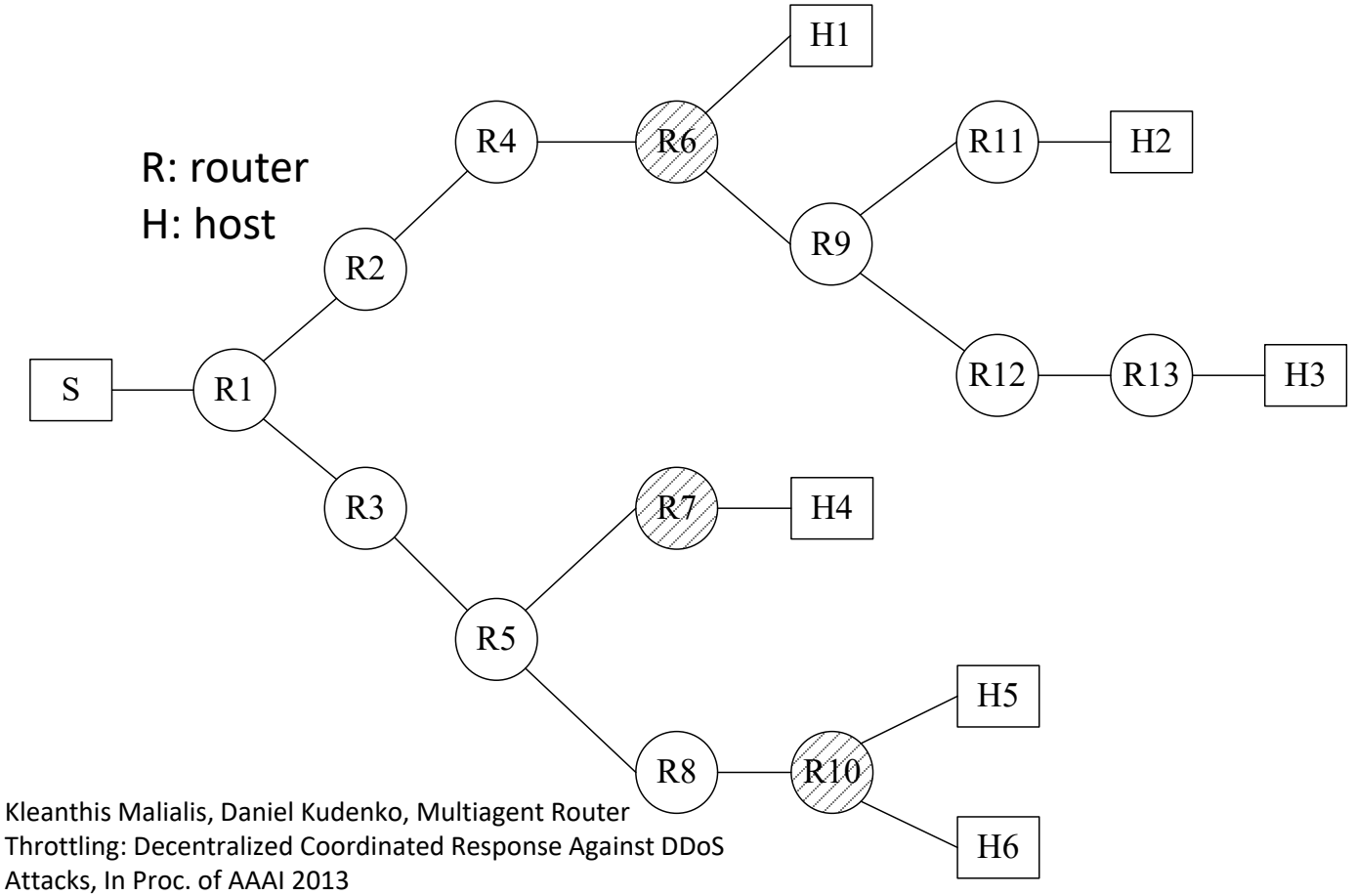


Deep neural network (DNN)

Applying RL to throttle flooding DDoS attacks

Problem setup

- A mixed set of legitimate users & attackers
- Aggregated traffic at $s \in [L_s, U_s]$
- RL agents decides the drop rates

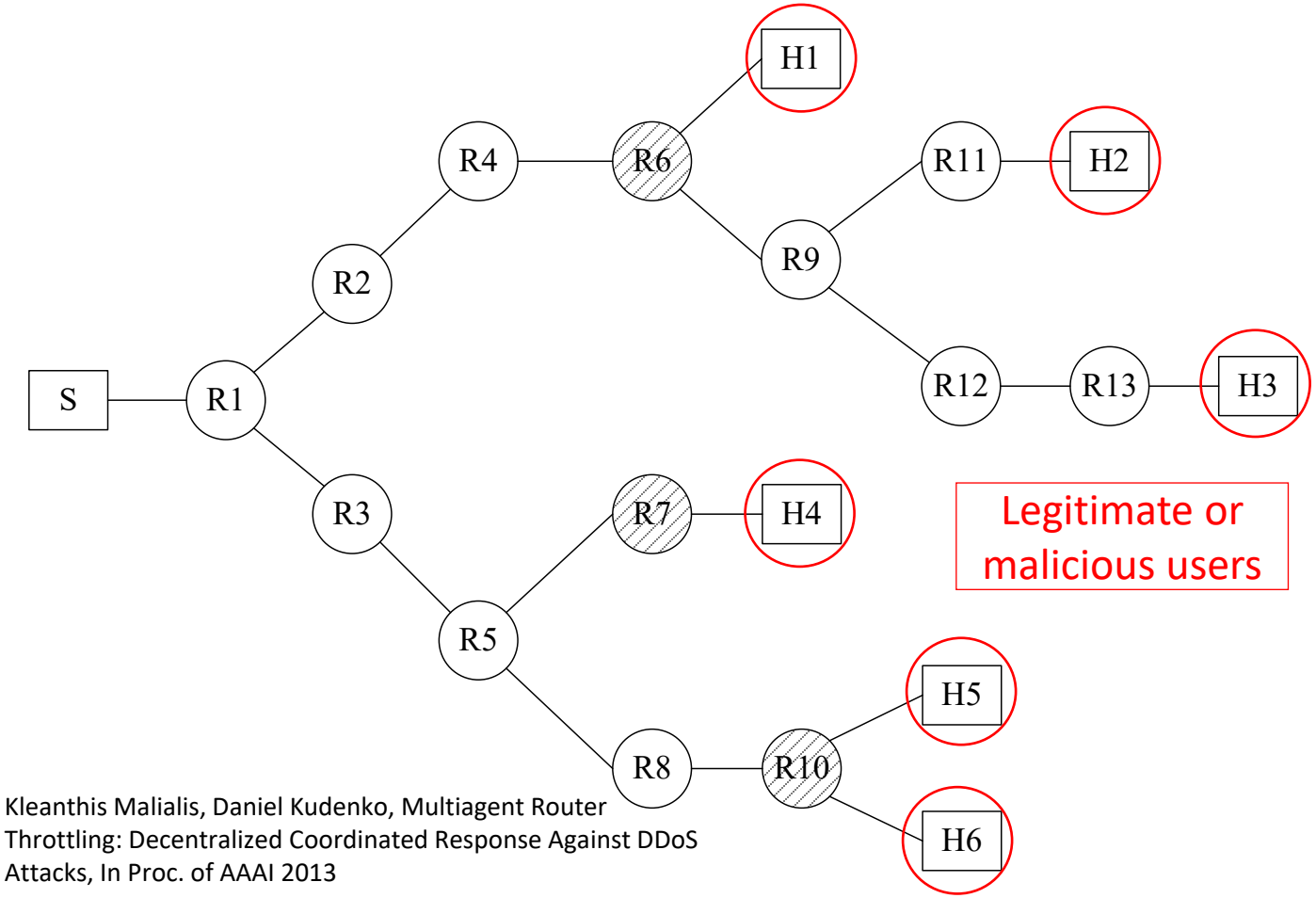


Kleanthis Malialis, Daniel Kudenko, Multiagent Router Throttling: Decentralized Coordinated Response Against DDoS Attacks, In Proc. of AAAI 2013

Applying RL to throttle flooding DDoS attacks

Problem setup

- A mixed set of legitimate users & attackers
- Aggregated traffic at $s \in [L_s, U_s]$
- RL agents decides the drop rates

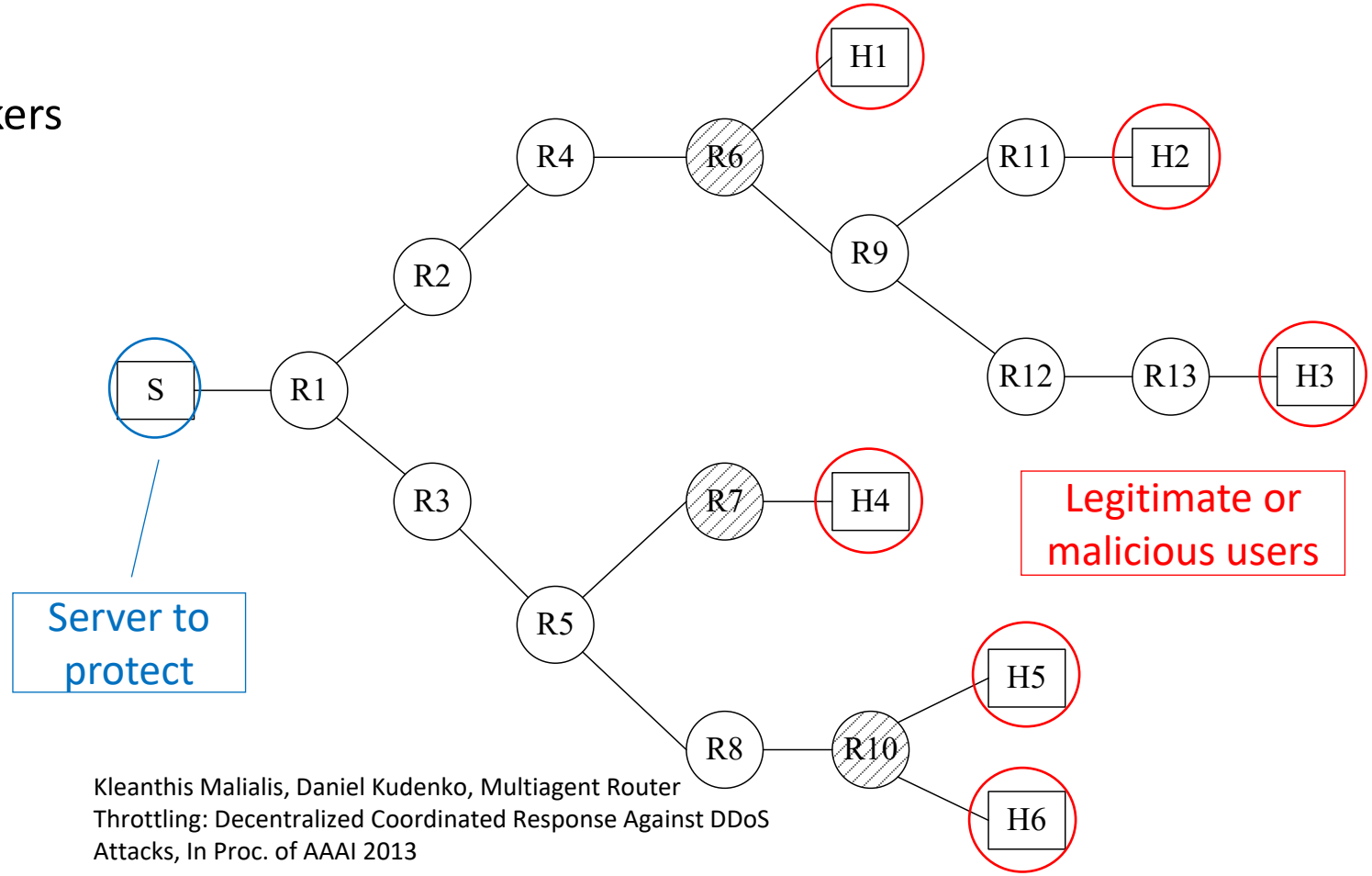


Kleanthis Malialis, Daniel Kudenko, Multiagent Router Throttling: Decentralized Coordinated Response Against DDoS Attacks, In Proc. of AAAI 2013

Applying RL to throttle flooding DDoS attacks

Problem setup

- A mixed set of legitimate users & attackers
- Aggregated traffic at $s \in [L_s, U_s]$
- RL agents decides the drop rates

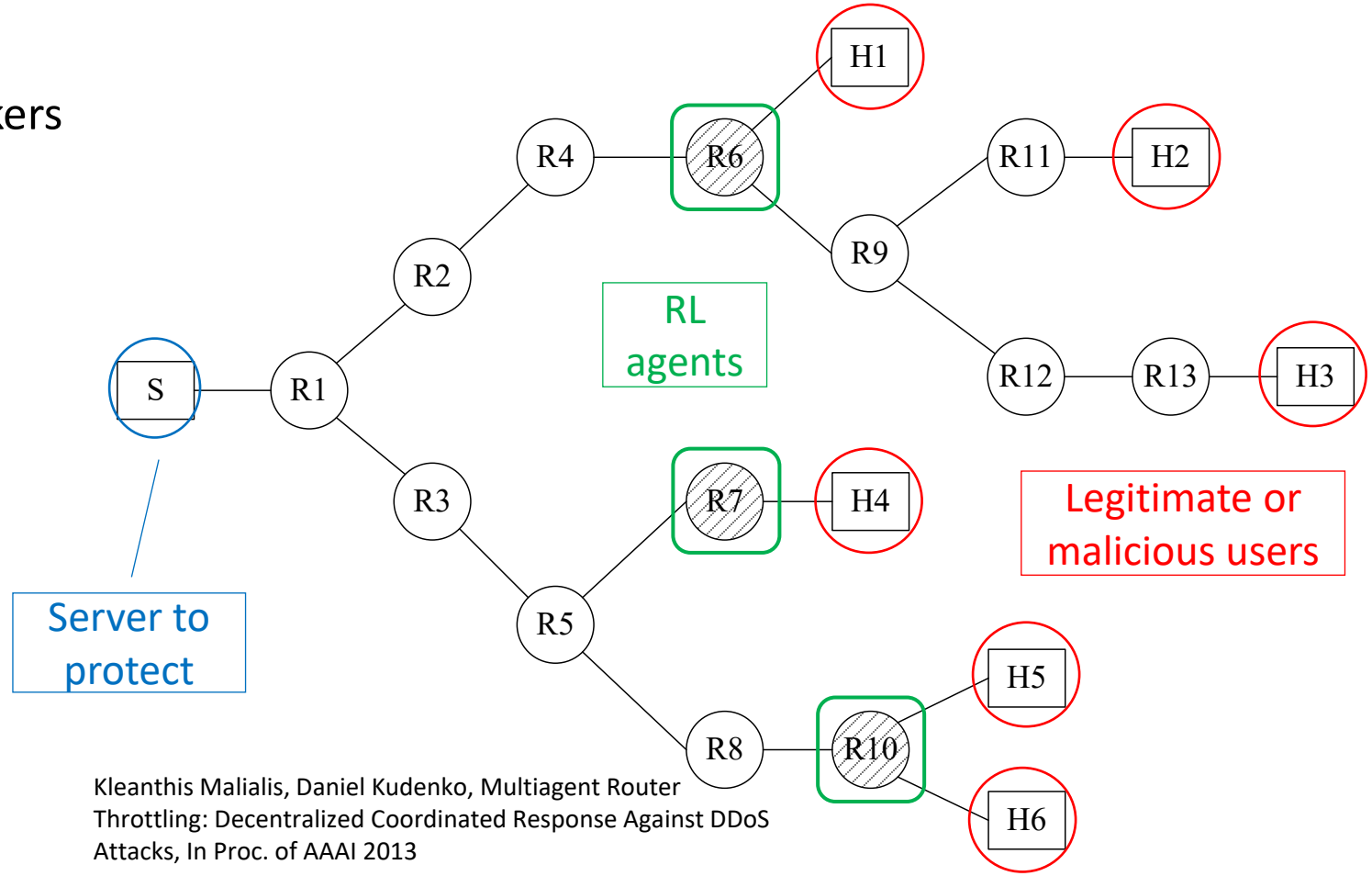


Kleanthis Malialis, Daniel Kudenko, Multiagent Router Throttling: Decentralized Coordinated Response Against DDoS Attacks, In Proc. of AAAI 2013

Applying RL to throttle flooding DDoS attacks

Problem setup

- A mixed set of legitimate users & attackers
- Aggregated traffic at $s \in [L_s, U_s]$
- RL agents decides the drop rates

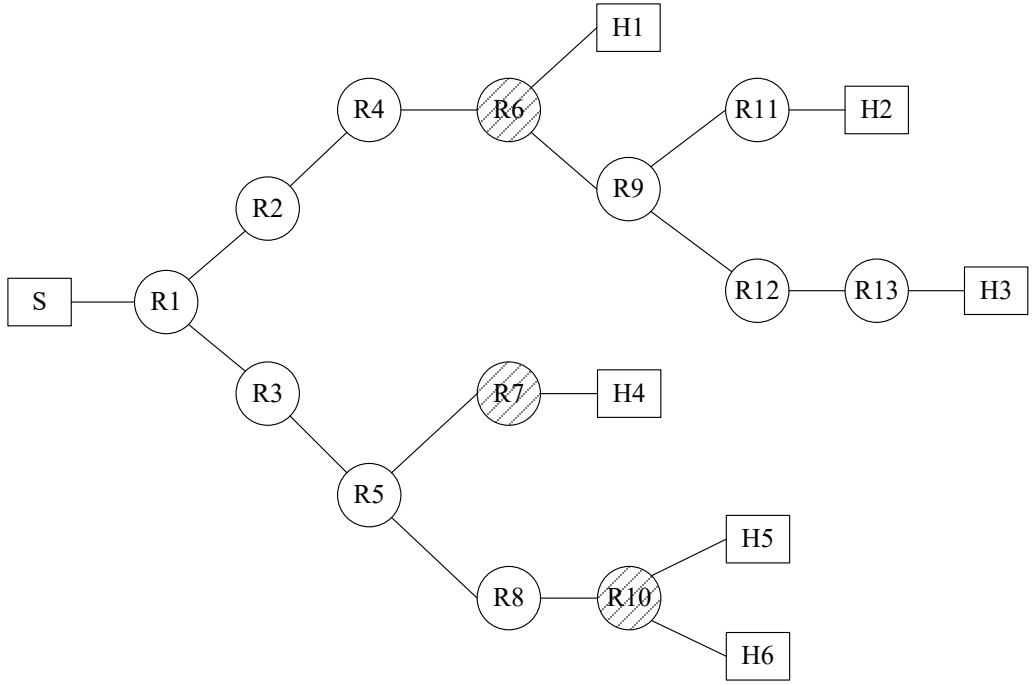


Kleanthis Malialis, Daniel Kudenko, Multiagent Router Throttling: Decentralized Coordinated Response Against DDoS Attacks, In Proc. of AAAI 2013

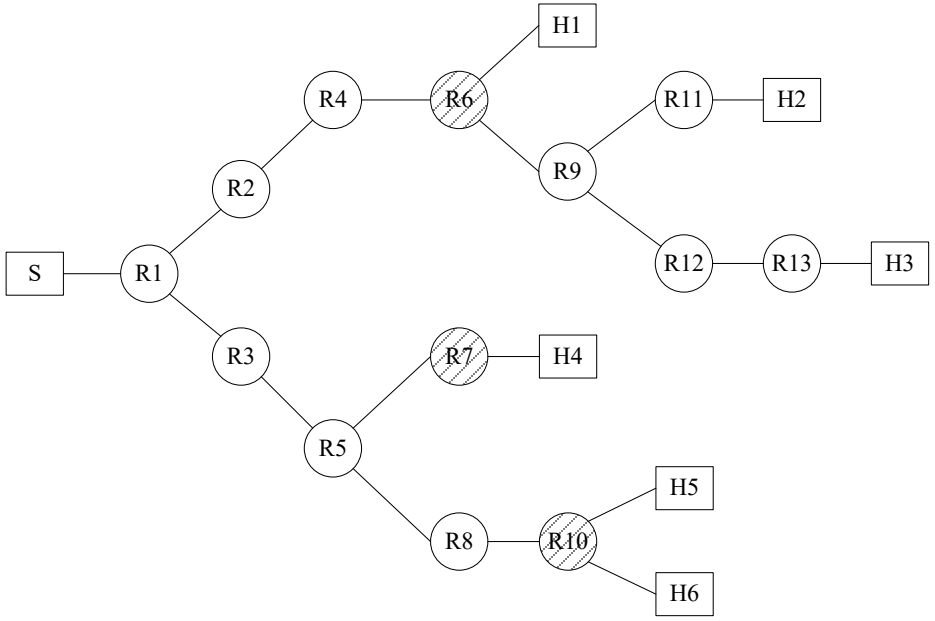
Applying RL to throttle flooding DDoS attacks

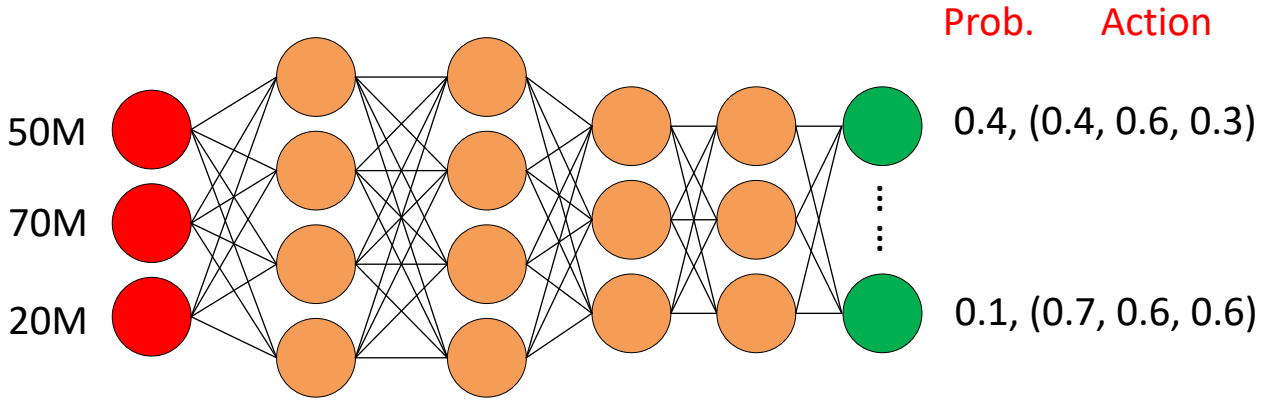
RL problem formalisation

- State space
  - Aggregated traffic arrived at the router over the last *T* seconds
- Action set
  - Percentage of traffic to drop: 0, 10%, 20%, 30%, … 90%
- Reward
  - Aggregated traffic at $s > U_s$?
  - Legitimate traffic reached *s*

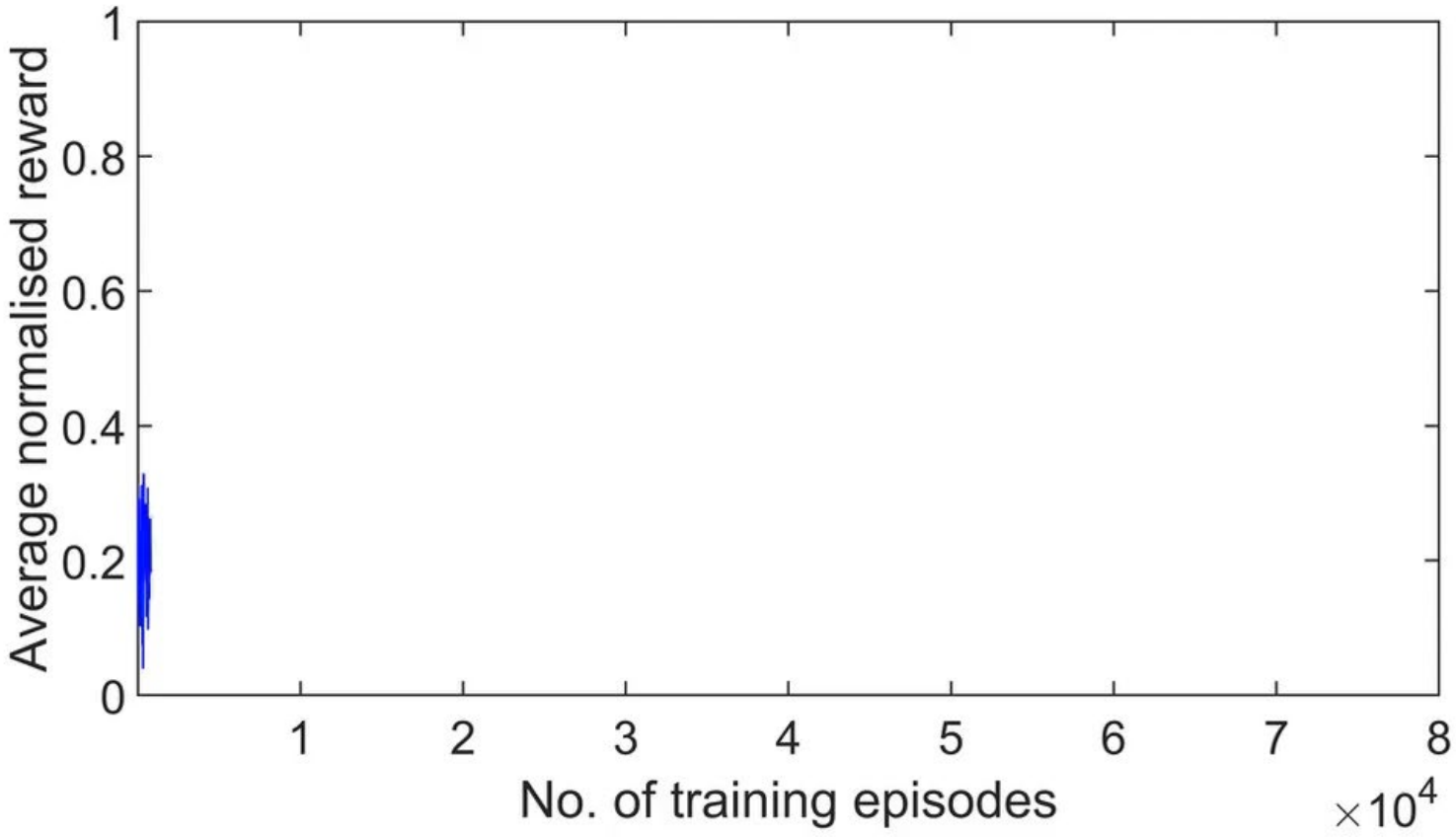


Train RL agent

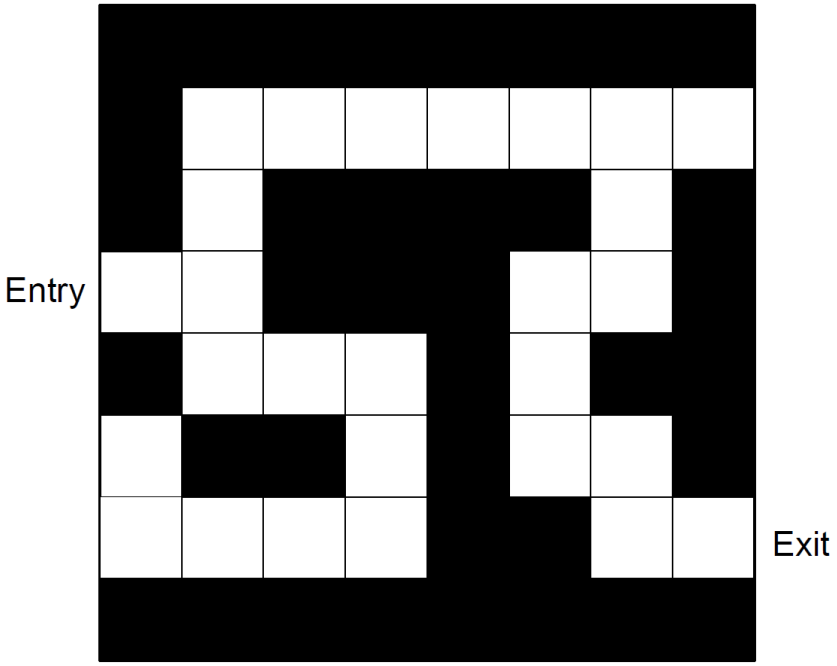




Train RL agent

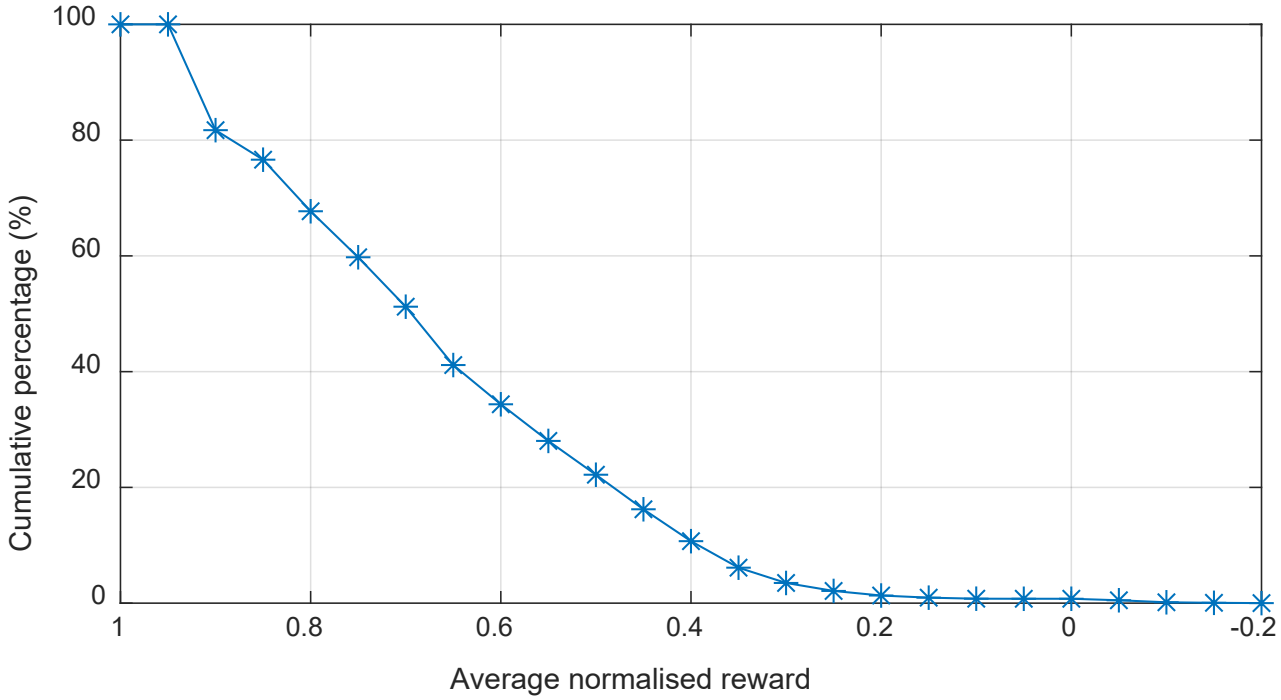


Train RL agent



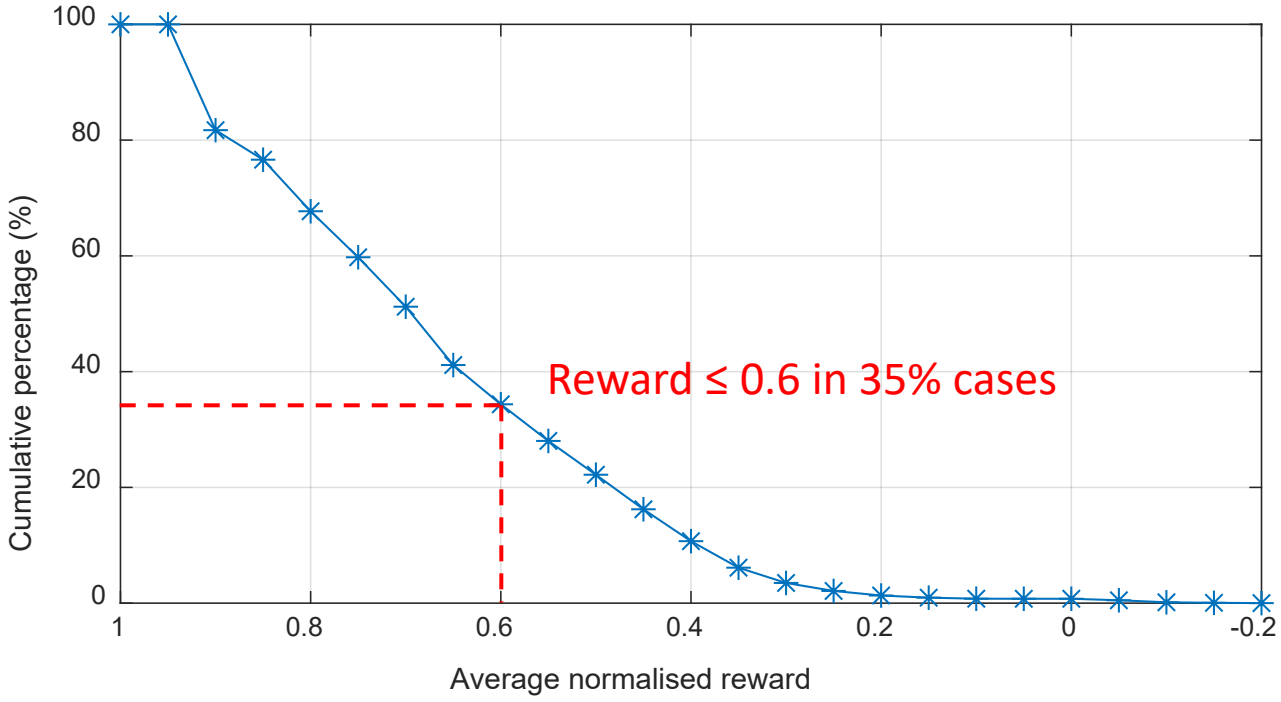
Test RL agent

10000 cases (may not be seen in training)



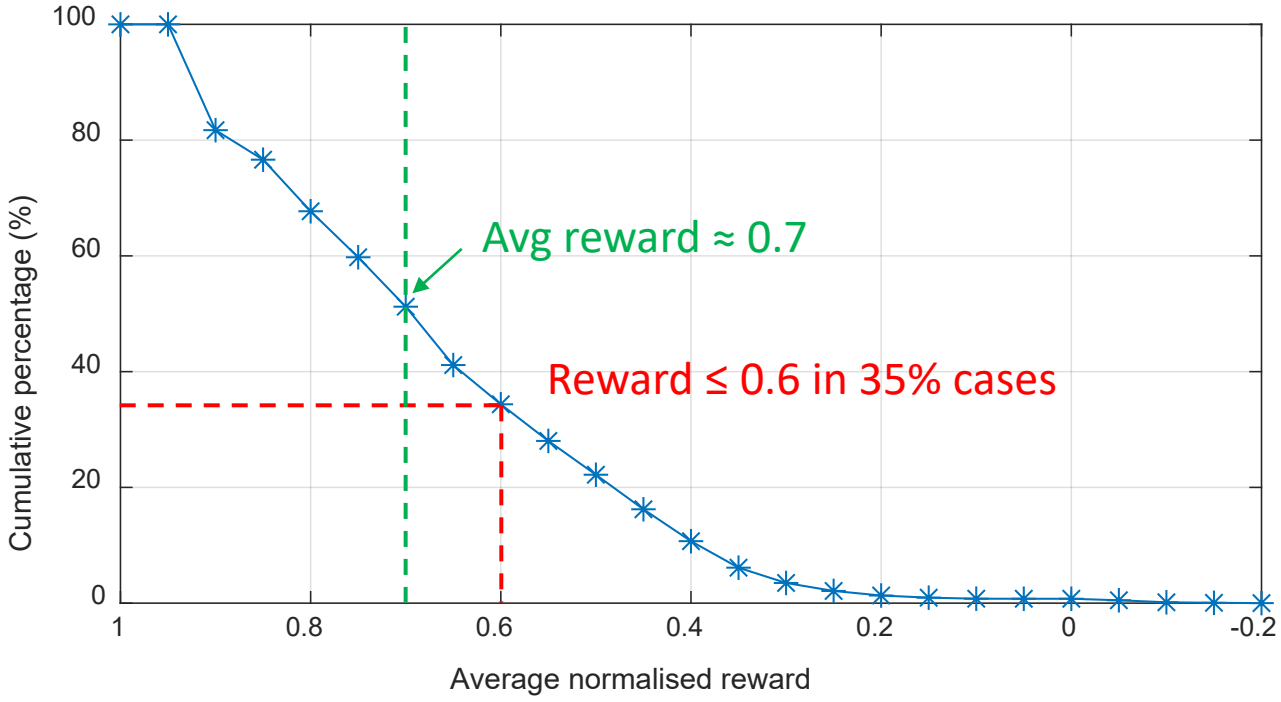
Test RL agent

10000 cases (may not be seen in training)



Test RL agent

10000 cases (may not be seen in training)



Want more? MIT(Cyber Security)

Structure of MIT (Cyber Security) (200 points)

Advanced Specialization Elective (25 pints)	
COMP90049	Knowledge Technologies
ISYS90070	Information Security Consulting
SWEN90006	Security & Software Testing

Advanced Core (37.5 points)	
COMP90055	Research Project
SWEN90016	Software Processes and Management

Foundation Subjects (50 points)	
COMP90007	Knowledge Technologies
COMP90038	Algorithms and Complexity
COMP90041	Programming and Software Development
INFO90002	Database Systems and Information Modelling

Advanced Elective (37.5 points)	
SWEN90010	High Integrity Systems Engineering
COMP90074	Web Security [NEW]
COMP90073	Security Analytics [NEW]
COMP90018	Mobile Computing Systems Programming
COMP90051	Statistical Machine Learning
COMP90054	AI Planning for Autonomy
COMP90057	Advanced Theoretical Computer Science
ENGR90033	Internship Or Industry Based IT Experience Project

Core Specialisation (25 points)	
COMP90015	Distributed Systems
COMP90043	Cryptography and Security

COMP90073 Security Analytics

- Security Analytics
  - Handbook: https://handbook.unimelb.edu.au/2021/subjects/comp90073
  - Examine how to automate the analysis of network data to detect and predict security vulnerabilities
  - Three parts:
    - Introduce the types of data sources that are relevant to detecting different types of security threats.
    - Introduce methods from machine learning that are widely used for cyber security analysis.
    - Introduce some of the theoretical challenges and emerging issues for security analytics research.