NTNU

Norwegian University of Science and Technology

Enabling Defensive Deception by Leveraging Software Defined Networks

Ilias Belalis[1], Georgios Kavallieratos[2], Vasileios Gkioulos[2], Georgios Spathoulas[1,2]

[1]Department of Computer Science and Biomedical Informatics, University of Thessaly, Lamia, Greece, ibelalis@uth.gr

[2]Norwegian University of Science and Technology, Department of Information Security and Communication Technology, Gjøvik, Norway, {georgios.kavallieratos, vasileios.gkioulos, georgios.spathoulas}@ntnu.no

UNIVERSITY OF THESSALY

NTNU
Faculty of Information Technology
and Electrical Engineering
Department of Information Security
and Communication Technology

IARIA

Short resume of the presenter

G. Kavallieratos is currently working toward the Ph.D. degree in security of the cyber enabled ship with the Department of Information Security and Communication Technology, Norwegian University of Science and Technology, Gjøvik, Norway.

His research interests include cyber-physical systems security and maritime cyber-security.

Agenda

- Motivation
- Scope
- Background
  - SDN technology
  - Defensive deception techniques
- Literature review
- Literature review results
- Defensive Deception Mechanism Overview
  - Topology
  - SDN Controller
  - Packet Handler
  - Virtual Topology Generator and Honeypot Server
- Defensive Deception Mechanism Scenarios
  - ping command scenario
  - nmap scenario
- Defensive Deception Mechanism – Results
- Conclusions and future work

Motivation

- Increasing complexity of computer networks;
- High dependence on such networks in vital domains (e.g. critical infrastructures);
- The increasing proliferation of such networks increases the attack surface;
- Various cyber-attacks target such network infrastructures;
- Software Defined Networks facilitate the management and programming of large scale networks.

Scope

The scope of this work is:

- To provide a comprehensive survey in existing defensive deception techniques on SDN technology;
- To propose a defensive deception mechanism based on SDN to mislead potential attackers and track malicious activities within the network.

Background

- SDN technology
  - Facilitates the management and configuration of the network.
  - Differentiate the control from the data plane by leveraging various abstraction layers (e.g. Network infrastructure, Network Hypervisor, etc.).
- Defensive Deception techniques
  - Defensive deception techniques increase the security and dependability of SDN.
  - Network-based deception technologies are studied in this work and their application to the SDN is examined.
  - Such techniques are: 1) Network Tarpit, 2) Traffic forging, 3) Deceptive topology, 4) OS obfuscation, 5) Honeytokens, 6) Deceptive attack graphs, 7) Deceptive simulation, 8) Decoy services, 9) Moving Target Defense, 10) Honeypots.

Literature review

- Review of existing approaches for defensive deception techniques on SDN implementations;
- Twelve approaches have been identified in the literature;
- Each approach is analyzed considering 1) the used systems, 2) the defensive deception techniques, and 3) the outcome/results.

Literature review results

- Moving Target Defense increase the adversary workload and uncertainty;
- Honeypots or honeyproxies facilitate the identification of the malicious action before adversaries succeed;
- Five out of twelve approaches focuses on the exhaust of the attacker resources.

Defensive Deception Mechanism

- Due to the static nature of computer networks, intruders are able to detect the structure and identify vulnerabilities which they can then exploit through advanced attacks.

- The approach proposed, aims at misleading such malicious activities by presenting a virtual network topology while it also hides the real network along with possible vulnerabilities.

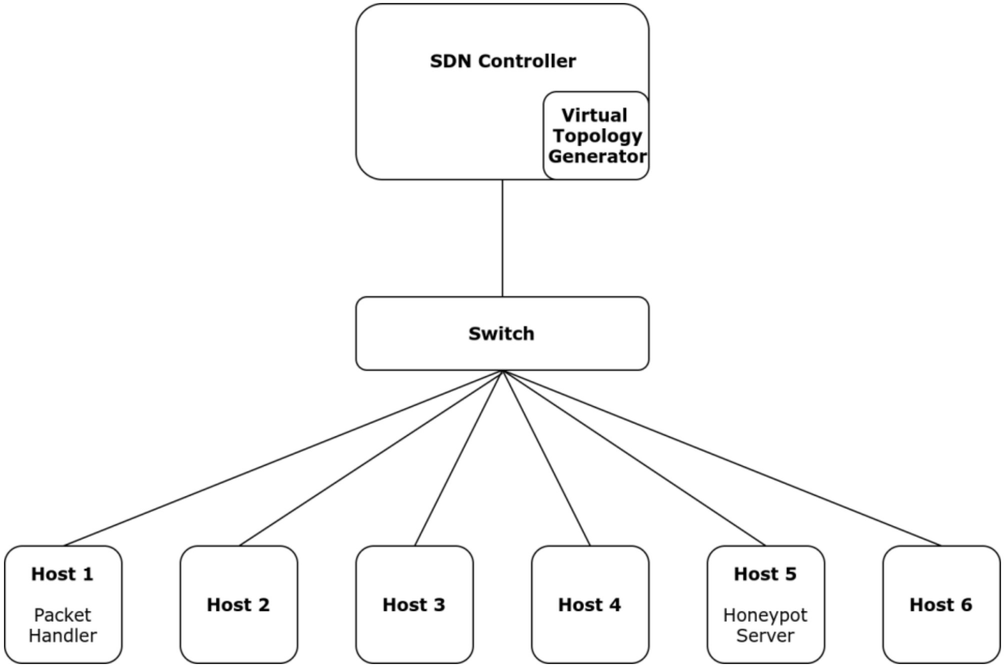
- In the **threat model** of this work, it is assumed that the intruder is trying to locate the computers on the network and collect as much information as possible about each computer in order to continue the attack.

- The main purpose of the deception mechanism is to face those malicious network activities regardless of whether they come from a compromised or a non-compromised host.

Defensive Deception Mechanism - Topology

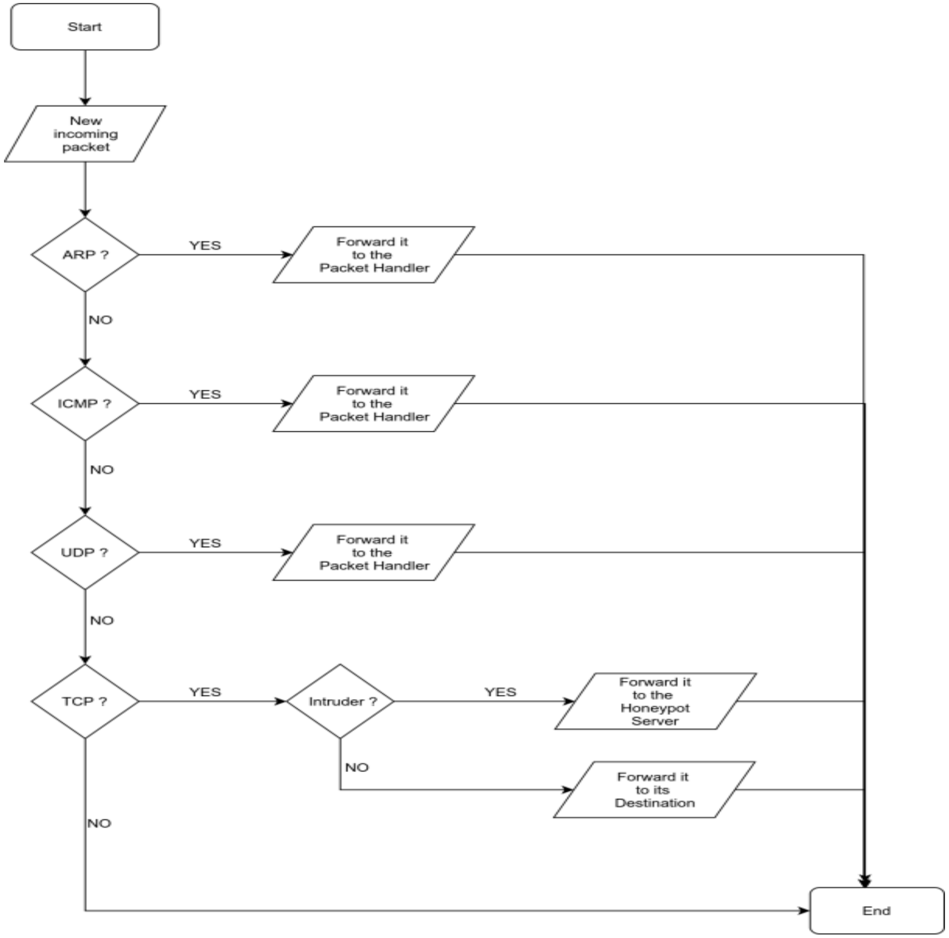
The deception mechanism consists of four essential elements:

- An **SDN Controller** responsible for dynamically creating and managing the flow rules in order to direct and control network traffic,
- A **Packet Handler** responsible for handling network packets and for simulating specific virtual network resources,
- A **Virtual Network Generator** that contains a description of the virtual network components and their connectivity,
- A **Honeypot Server** responsible for the services that honeypots will provide to the attacker after a port scanning.



Defensive Deception Mechanism – SDN Controller

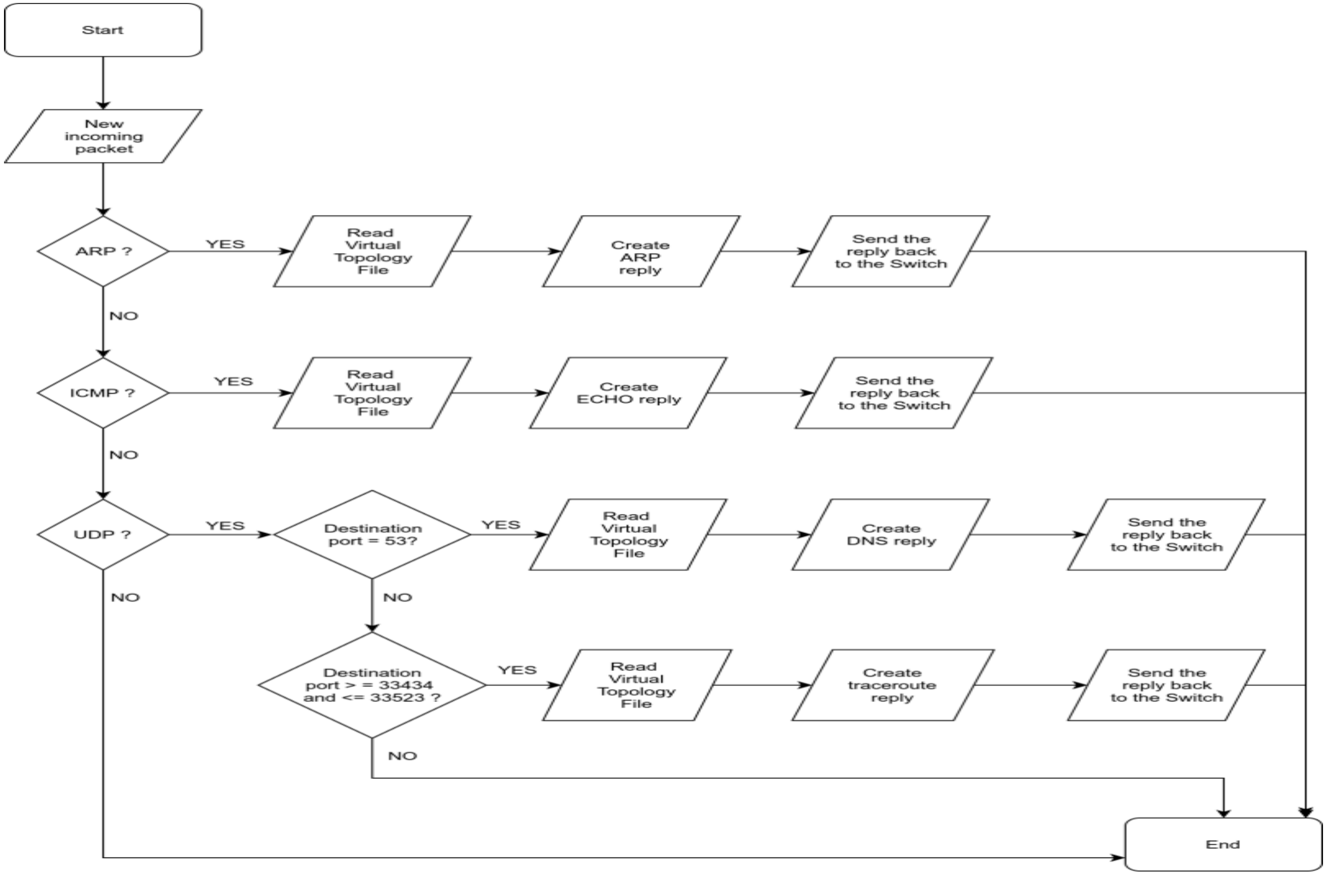
SDN Controller Flowchart


Start
New incoming packet
ARP ?
YES
Forward it to the Packet Handler
NO
ICMP ?
YES
Forward it to the Packet Handler
NO
UDP ?
YES
Forward it to the Packet Handler
NO
TCP ?
YES
Intruder ?
YES
Forward it to the Honeypot Server
NO
Forward it to its Destination
NO
End

- A host can be identified as an intruder by the SDN Controller in two cases.
  - When a host interacts with a honeypot through ping or traceroute commands.
  - When a host makes a port scanning attempt against another host on the network.

Defensive Deception Mechanism – Packet Handler

Packet Handler Flowchart


Start
New incoming packet
ARP ?
YES
Read Virtual Topology File
Create ARP reply
Send the reply back to the Switch
NO
ICMP ?
YES
Read Virtual Topology File
Create ECHO reply
Send the reply back to the Switch
NO
UDP ?
YES
Destination port = 53?
YES
Read Virtual Topology File
Create DNS reply
Send the reply back to the Switch
NO
NO
Destination port > = 33434 and <= 33523 ?
YES
Read Virtual Topology File
Create traceroute reply
Send the reply back to the Switch
NO
End

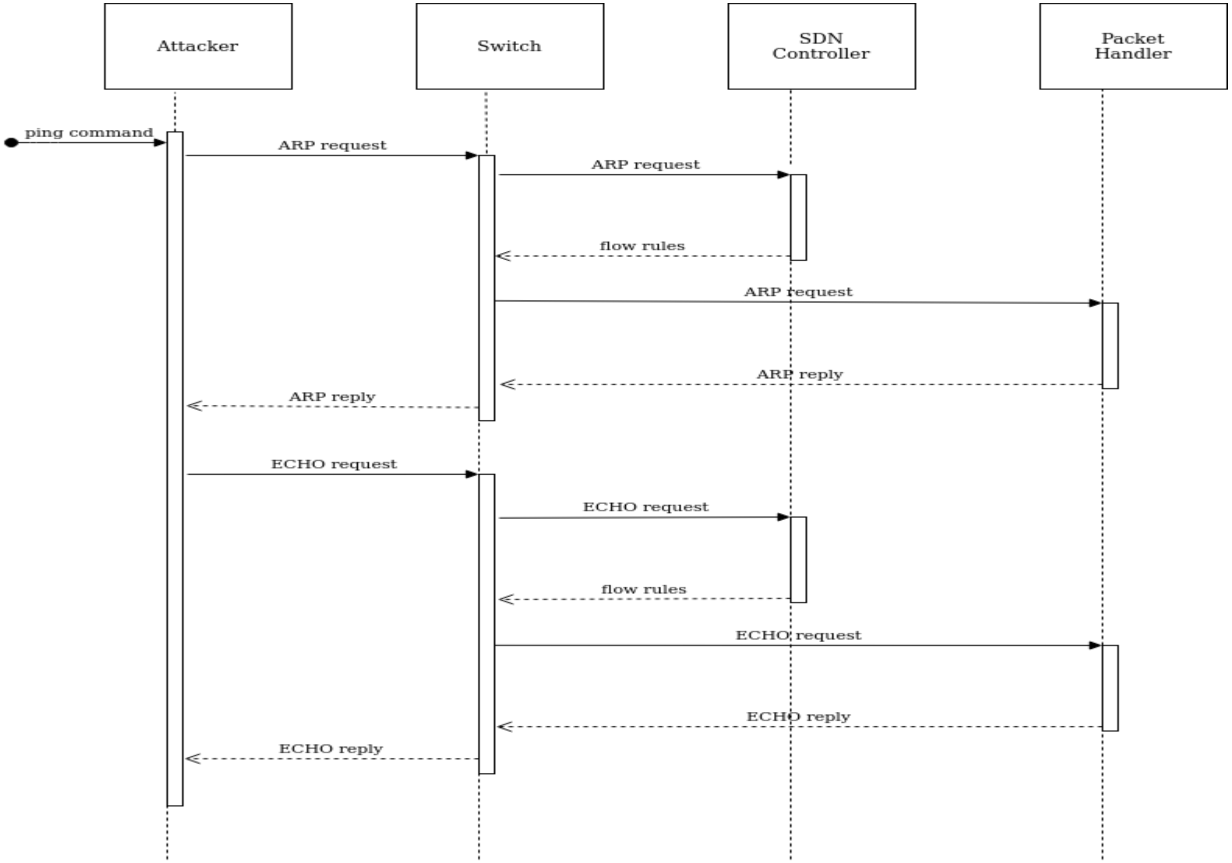
- The role of the packet handler is taken up by one of the hosts created in Mininet.
- Thus, the packets will be forwarded by the switch to the Packet Handler, which in turn will generate a response and send it back to the switch

Defensive Deception Mechanism – Virtual Topology Generator and Honeypot Server

- **Virtual topology generator:** Responsible for creating the virtual topology as well as periodically updating the virtual IP and MAC addresses of the Mininet hosts and honeypots.
- This generator creates a text file that is accessible from the SDN controller and Packet Handler.
- Each line of this file corresponds to a component of the deception mechanism.
- Three types of entities:
  - Mininet Hosts and honeypots:
    - Hostname, real IP and MAC addresses, virtual IP and MAC addresses, the switch port in which is connected the Packet Handler;
    - in case of a Mininet Host there is information about the port that is connected to the switch;
    - in case of a honeypot there is information about the port that the Honeypot Server is connected to the switch.
  - Fake routers
    - Information about the router interface, the virtual IP and MAC addresses as well as the switch port that the Packet Handler is connected to.
  - Routes
    - Information about source host, destination host, and the intermediate hops which are fake router's interfaces.
- From the above information, the Packet Handler can respond to ARP, ICMP and UDP requests.
- **Honeypot Server:** is responsible for generating the virtual set of services for each host, that will be provided to the attacker after a port scanning attempt.
- One of the hosts created in the Mininet has the role of Honeypot Server.
- Honeypot Server has also been implemented in Python and starts services on the computer on which is running.
- Also, these services are periodically updated.

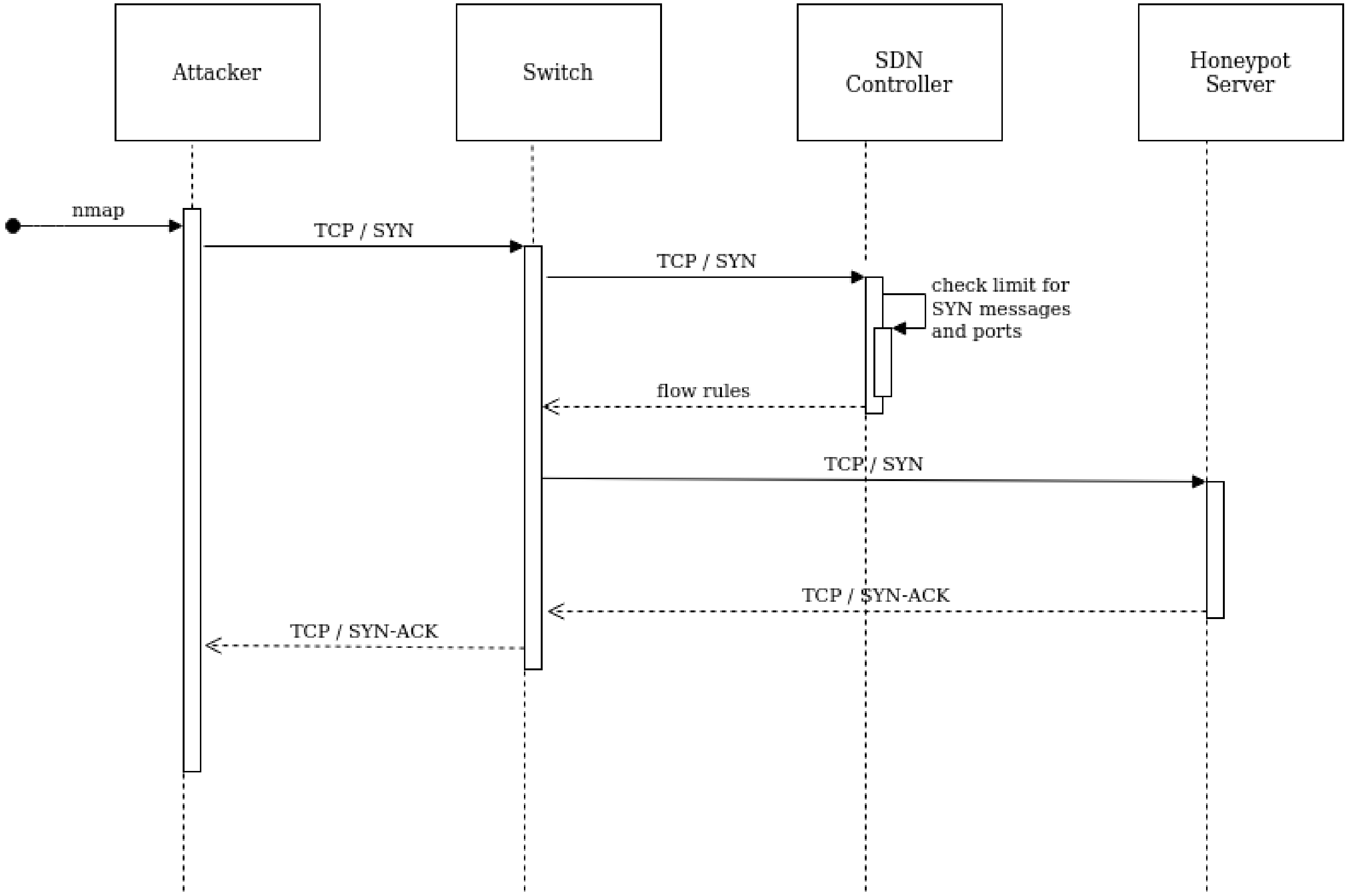
Defensive Deception Mechanism – ping command scenario

- We assume that an attacker will interact with a host on the network via the ping command.

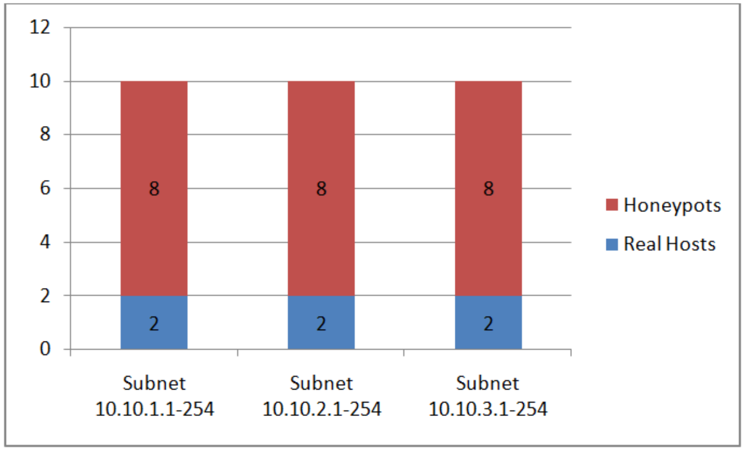


Defensive Deception Mechanism – nmap scenario

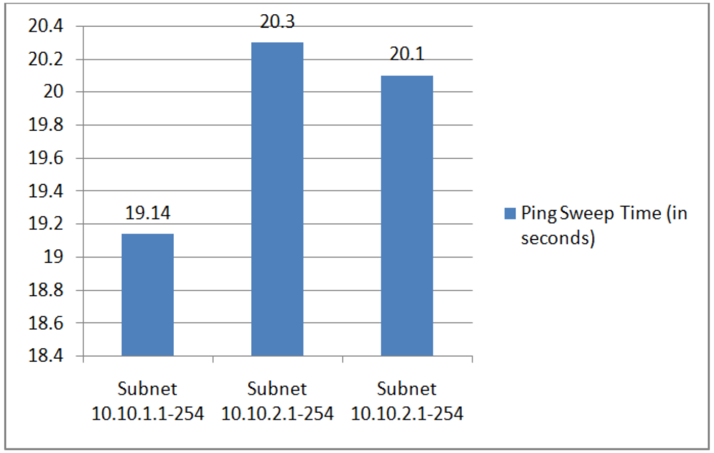
- We assume that an attacker will interact with a host on the network through the nmap program.



Defensive Deception Mechanism – Results (1/2)



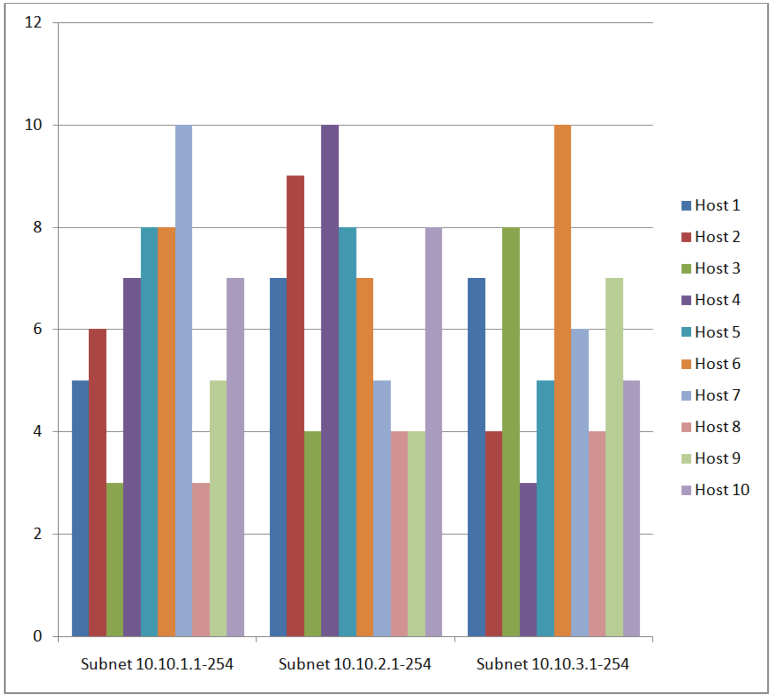
Nmap ping sweep results (computers per subnet)



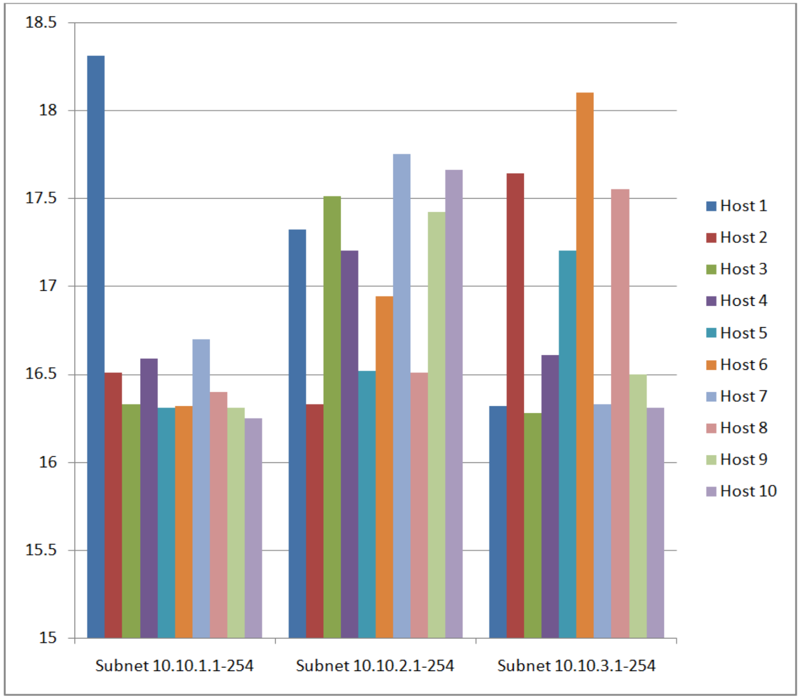
Nmap ping sweep time (in seconds)

- In these scans it was observed that we can increase the number of computers in a network by increasing the number of honeypots.
- Thus, we increase the workload (P1) and uncertainty (P5) of the attacker
- Also, we are able to track attacks and respond before attackers succeed (P2).

Defensive Deception Mechanism – Results (2/2)



Nmap scan results (open ports per computer)



Nmap scan time (in seconds)

- In these scans it has been observed that we can vary the number of services running on a computer.
- Thus, we increase the workload (P1) and uncertainty (P5) of the attacker.
- Also, we are able to detect attacks and respond before attackers succeed (P2).

Conclusions and Future work

- SDN based defense mechanisms aim to mitigate sophisticated cyber attacks that target contemporary computer networks.
- The DDM increases the workload, facilitates the respond before attackers succeed, and increases the uncertainty of the attacker.
- As future work the detection and prevention capabilities of the defense deception mechanism will be enhanced by leveraging machine learning techniques.

Thank you!