IoTEF 2022

Towards Analysis of the Performance of IDSs in Software-Defined Networks

Nadia Niknami, Emily Inkrott, and Jie Wu

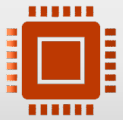
Temple University

Intrusion detection System

Intrusion : Attempting to break into or misuse the system.

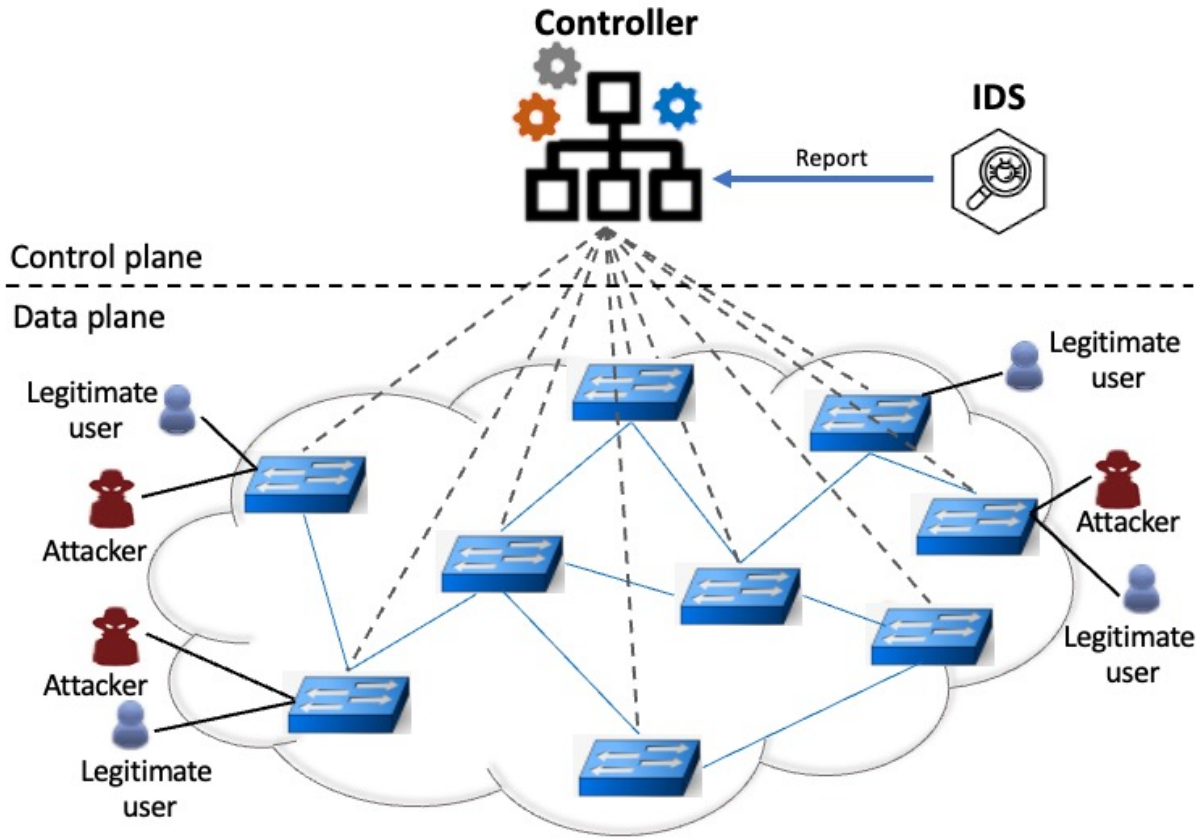
Intruders may be from outside the network or legitimate users of the network.

Intrusion can be a physical, system or remote intrusion.



Intrusion Detection Systems look for attack signatures, which are specific patterns that usually indicate malicious or suspicious intent

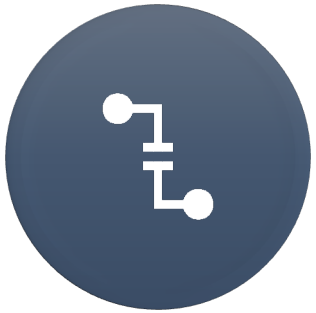
Performance of IDSs in SDN



Detection engine

NUMBER OF RULES

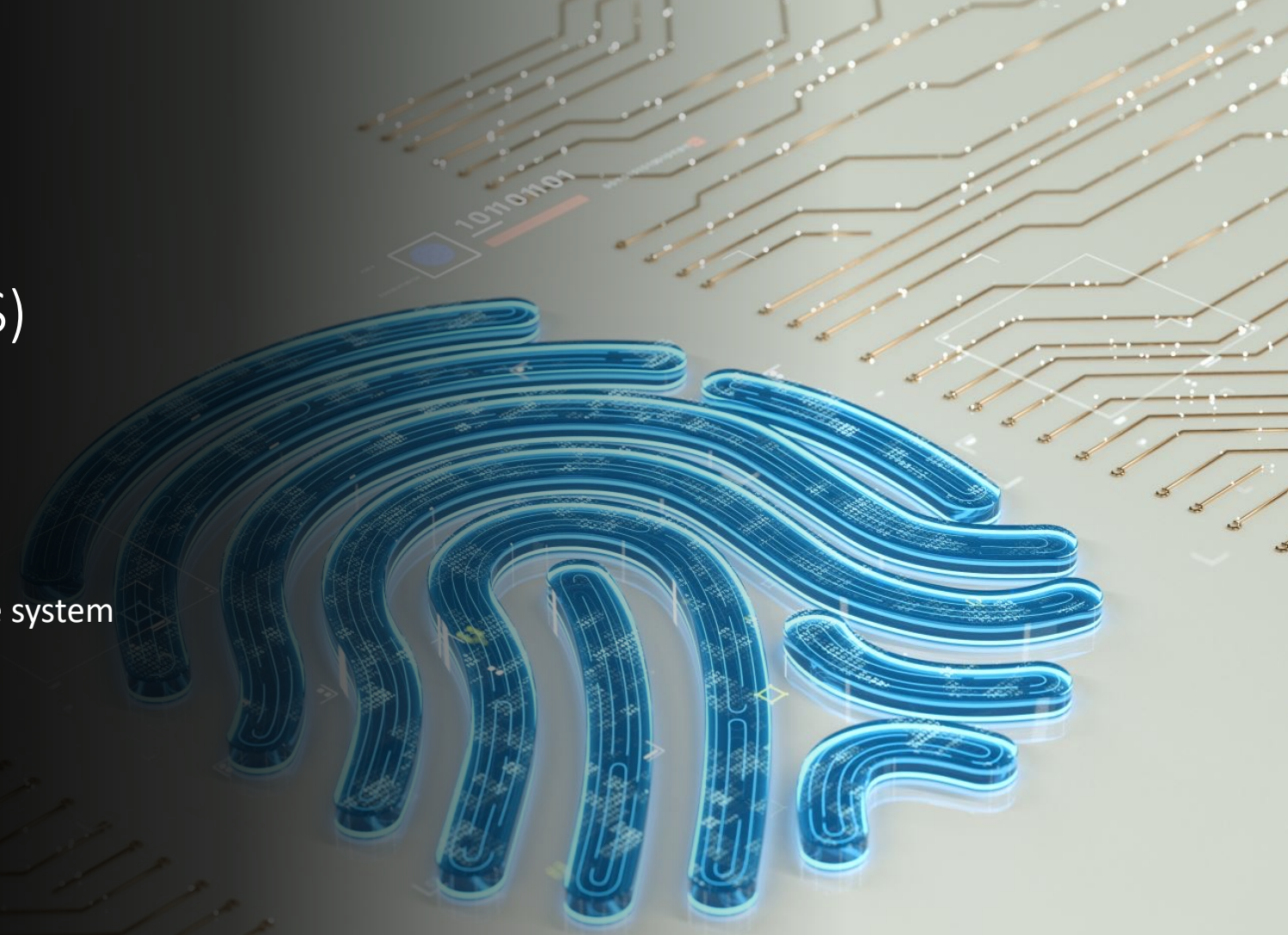
TRAFFIC LOAD ON THE NETWORK



SPEED OF NETWORK AND MACHINE

EFFICIENCY OF DETECTION ALGORITHM

Intrusion Detection Systems (IDS)



- Different ways of classifying an IDS
  - Anomaly detection
    - Trace deviation from a normal state of the system
  - Signature based misuse
    - Detects an attack from its fingerprints
  - Host-based (HIDS)
    - Monitor internal components
  - Network-based (NIDS)
    - Monitor network packets by some sensors

Snort

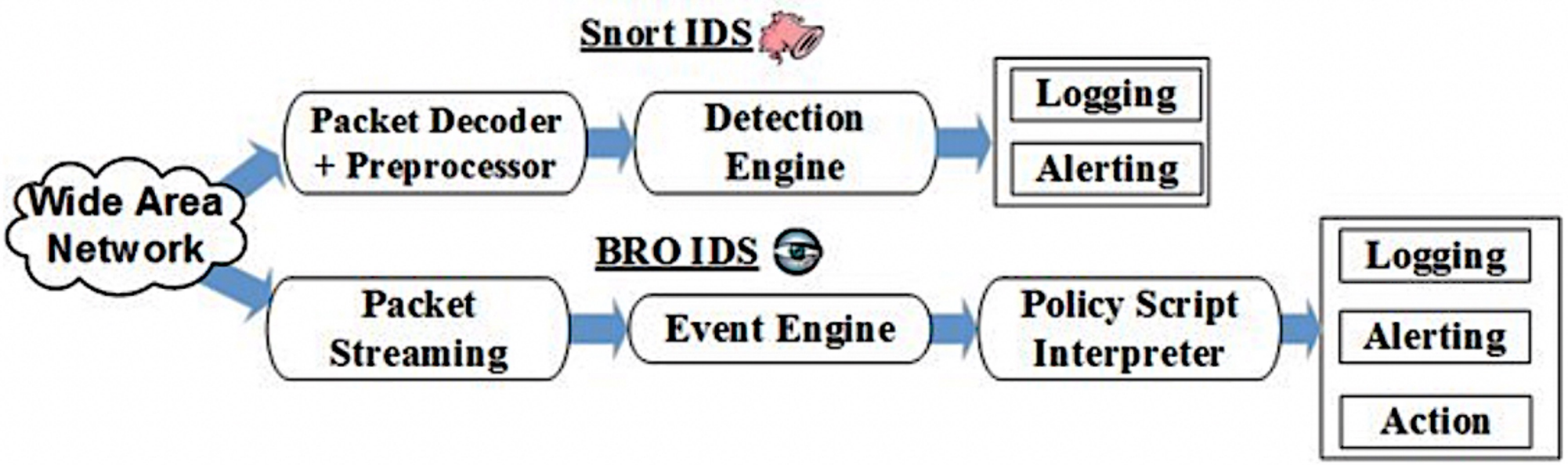
- Signature-based detection engine
- A multi-mode packet analysis tool
  - Sniffer
  - Packet Logger
  - Forensic data analysis tool

- Snort is based on library packet capture (libpcap)
- Two modes: IDS and IPS
- Snort does not evaluate the rules in the order that they appear in the snort rules file. In default, the order is :
  - Alert rules
  - Pass rules
  - Log rules

Bro/Zeek IDS

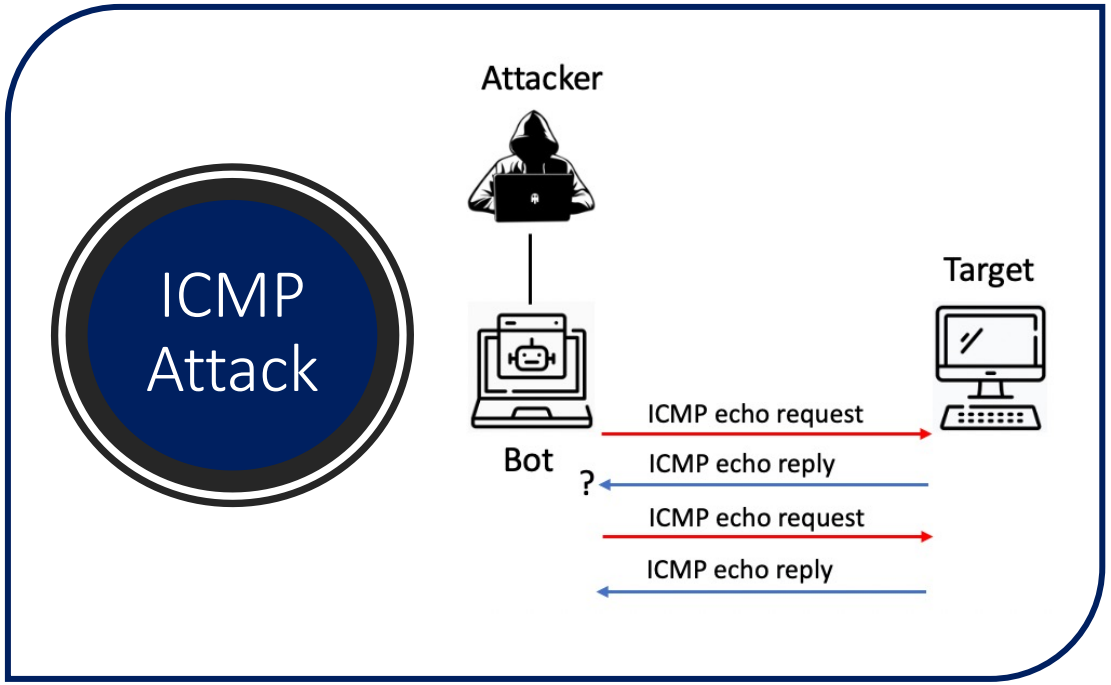
- Anomaly detection IDS
- It reads all traffic passing through the network and generates quite a number of logs in tab-delimited columns.
- It has an extensive set of logs describing network activity. These logs include not only a comprehensive record of every connection seen on the wire, but also application-layer transcripts.
- It is not like a firewall or intrusion prevention system. Rather, Zeek sits on a “sensor,” a hardware, software, virtual, or cloud platform that quietly and unobtrusively observes network traffic.

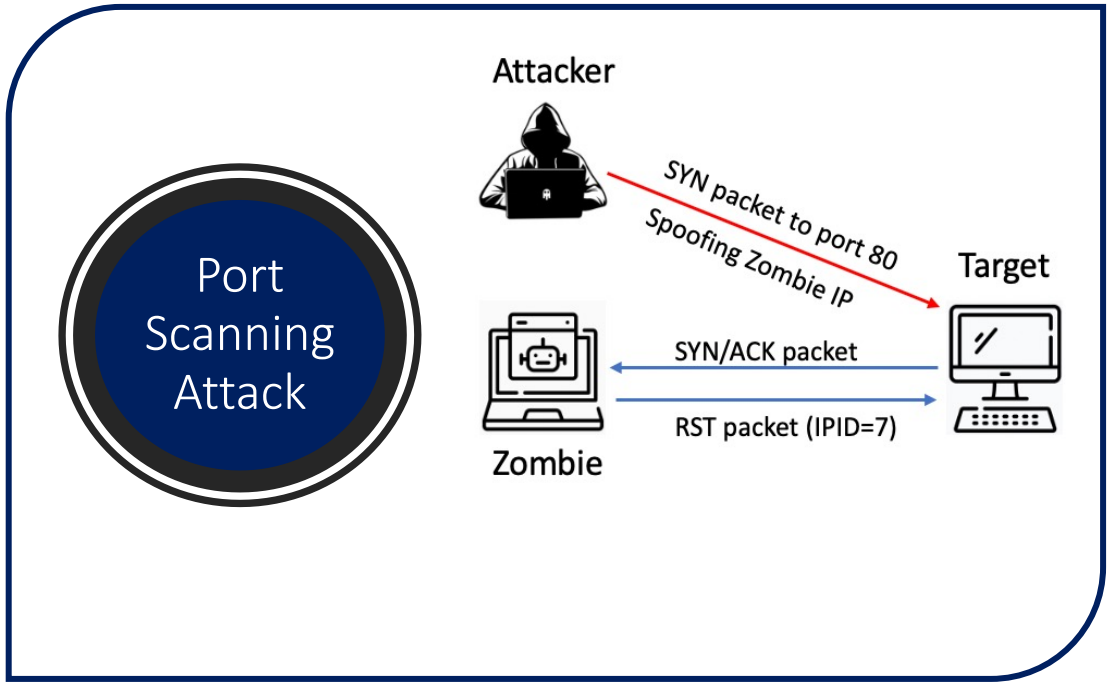
Signature-based vs Anomaly-based

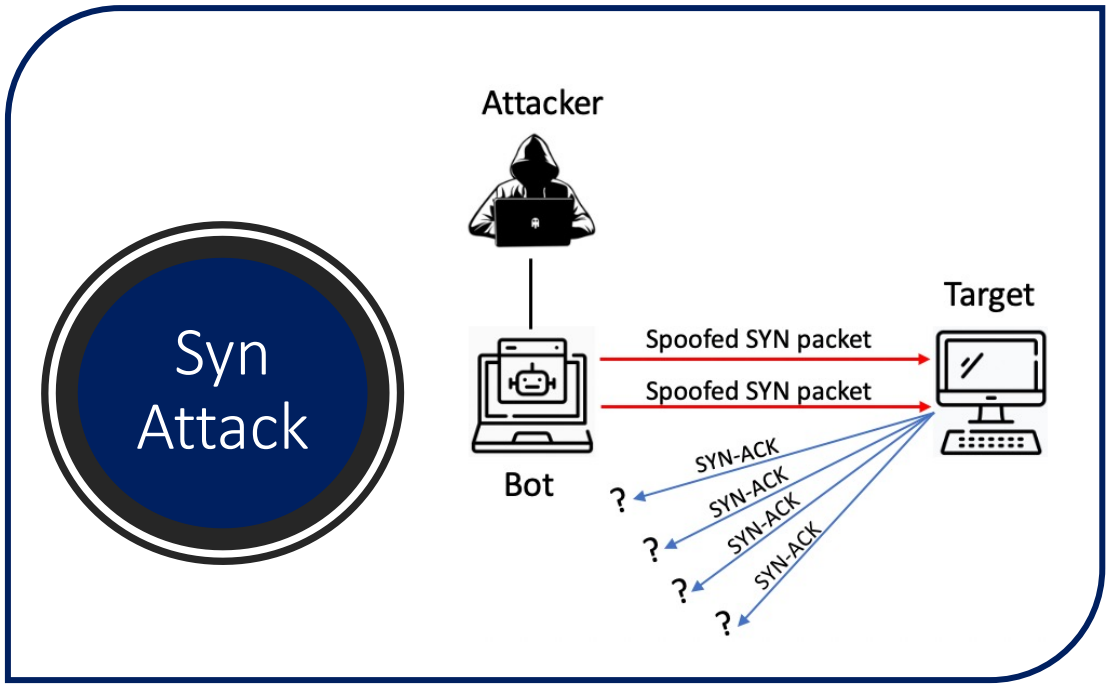


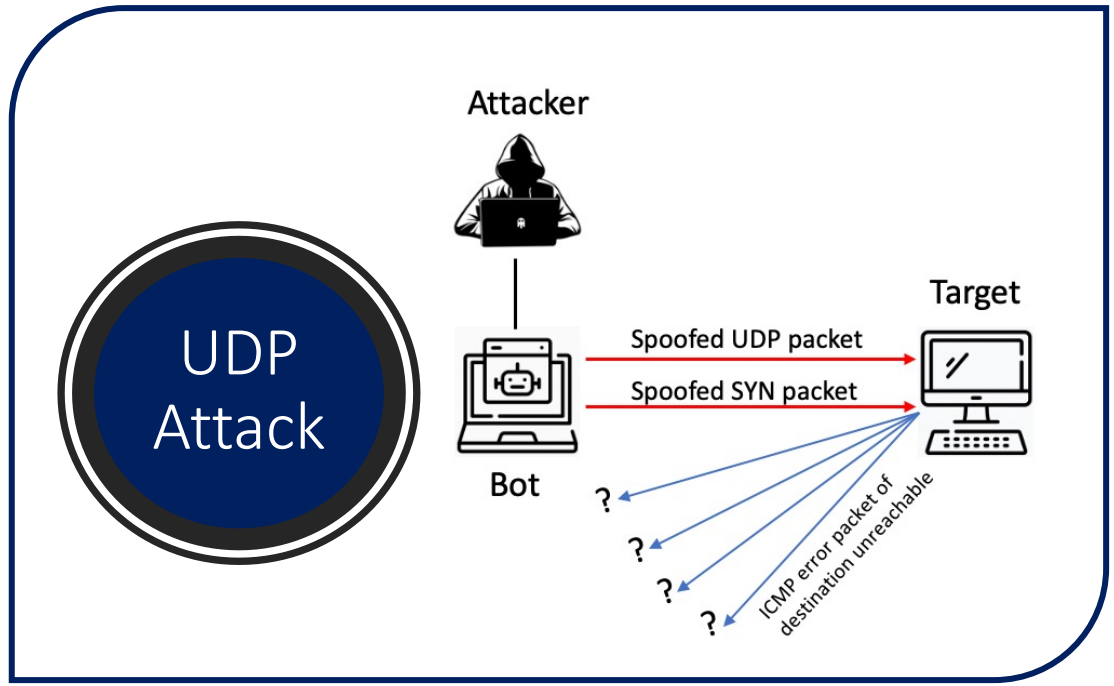
Attacks

- ICMP
- Port Scanning
- SYN
- UDP

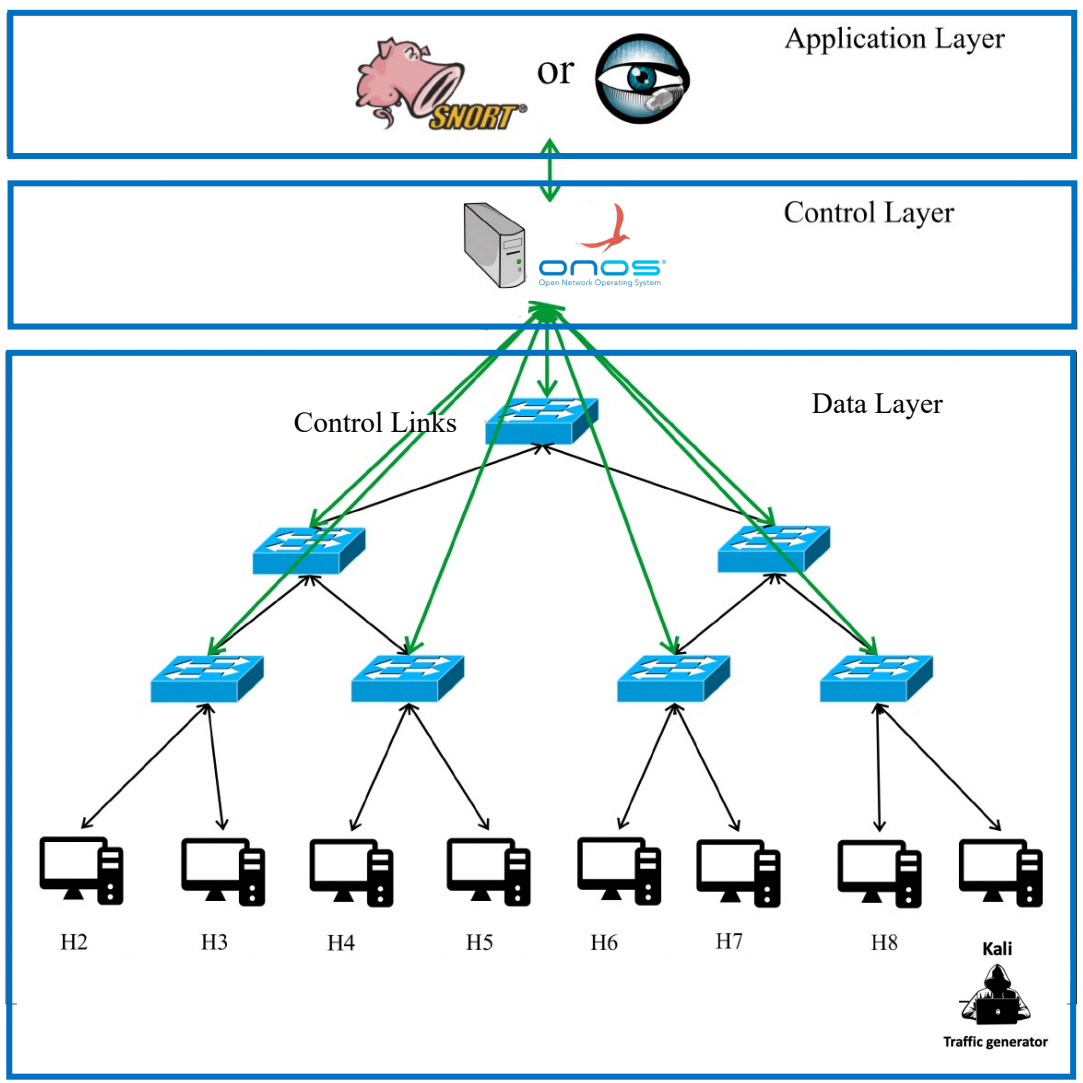

ICMP Attack
Attacker
Target
Bot
ICMP echo request
ICMP echo reply
ICMP echo request
ICMP echo reply

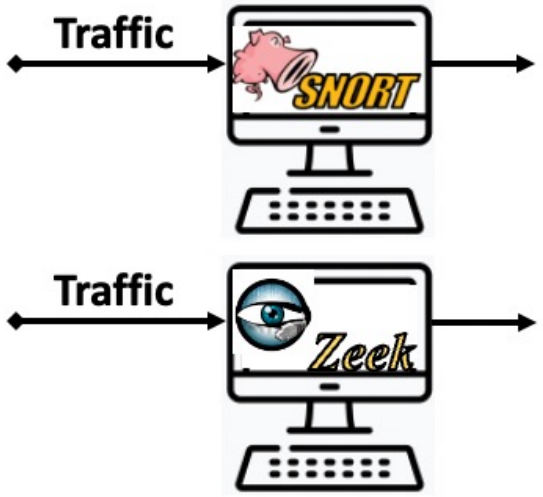

Port Scanning Attack
Attacker
SYN packet to port 80
Spoofing Zombie IP
Target
SYN/ACK packet
RST packet (IPID=7)
Zombie

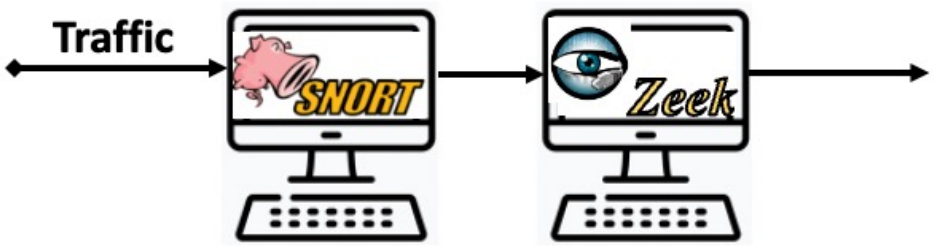

Syn Attack
Attacker
Target
Spoofed SYN packet
Spoofed SYN packet
Bot
SYN-ACK
SYN-ACK
SYN-ACK
SYN-ACK


UDP Attack
Attacker
Target
Spoofed UDP packet
Spoofed SYN packet
Bot
ICMP error packet of destination unreachable

Testbed setup for IDS mode





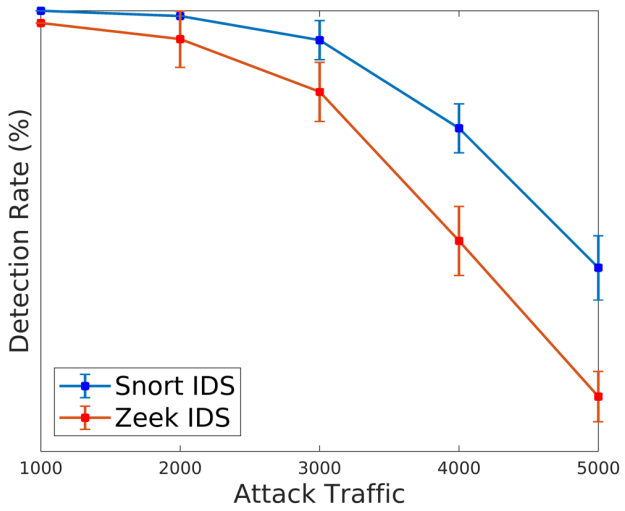


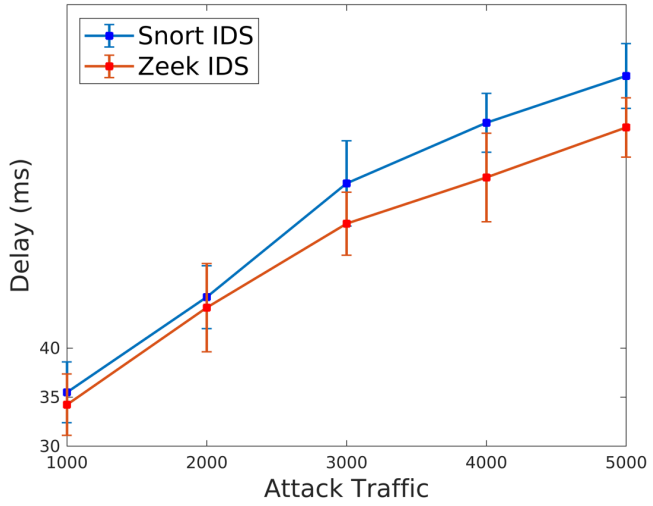
Evaluation

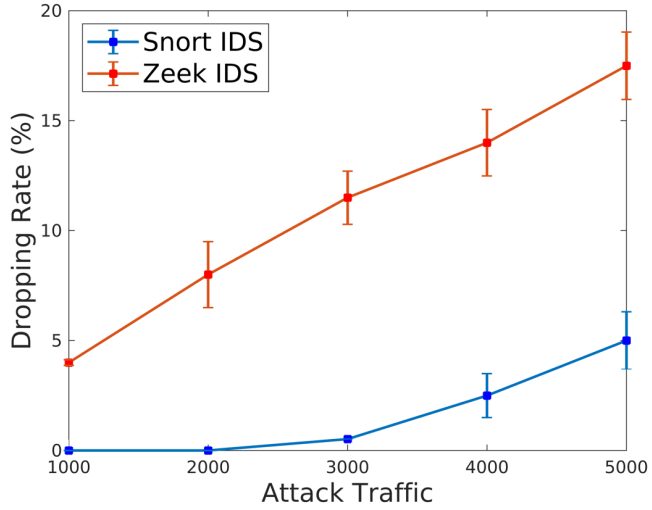
Detection rate

Dropping rate

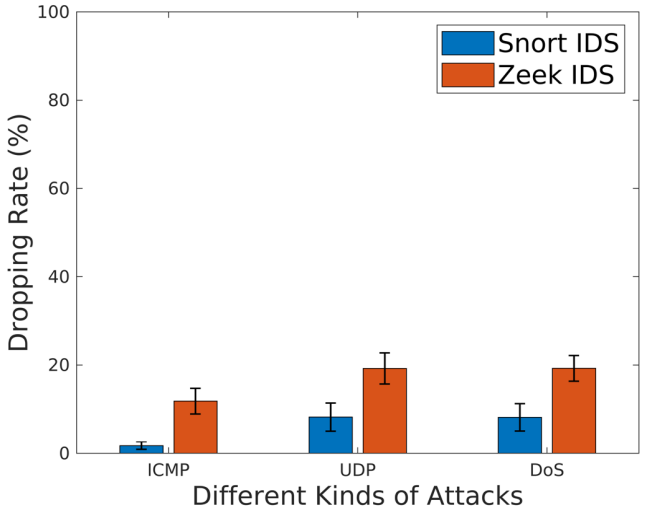
Delay

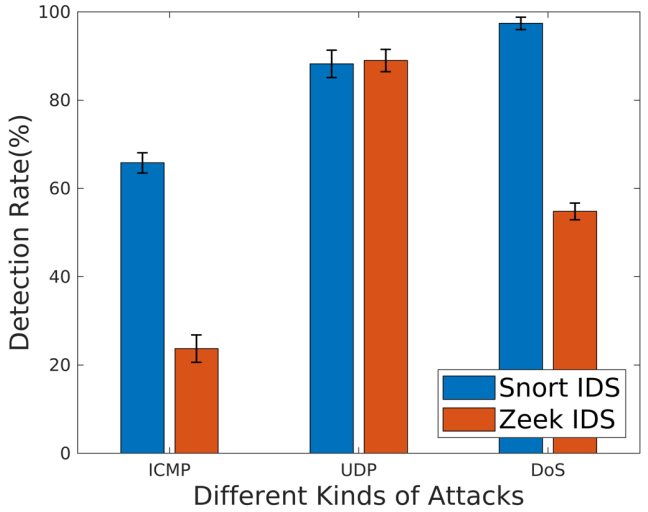


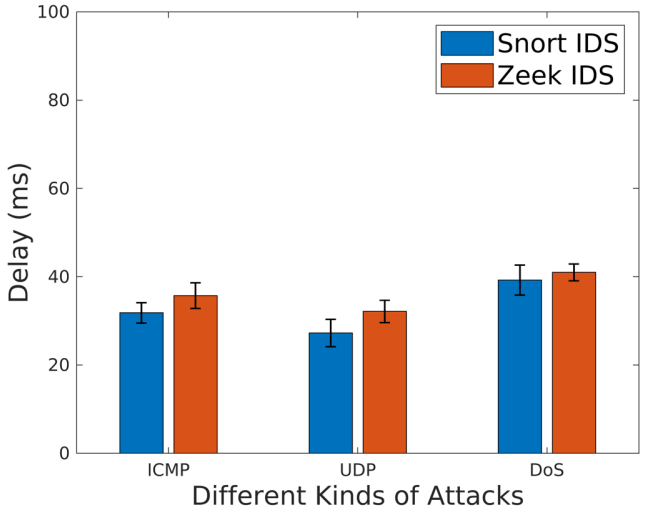




Evaluation Results

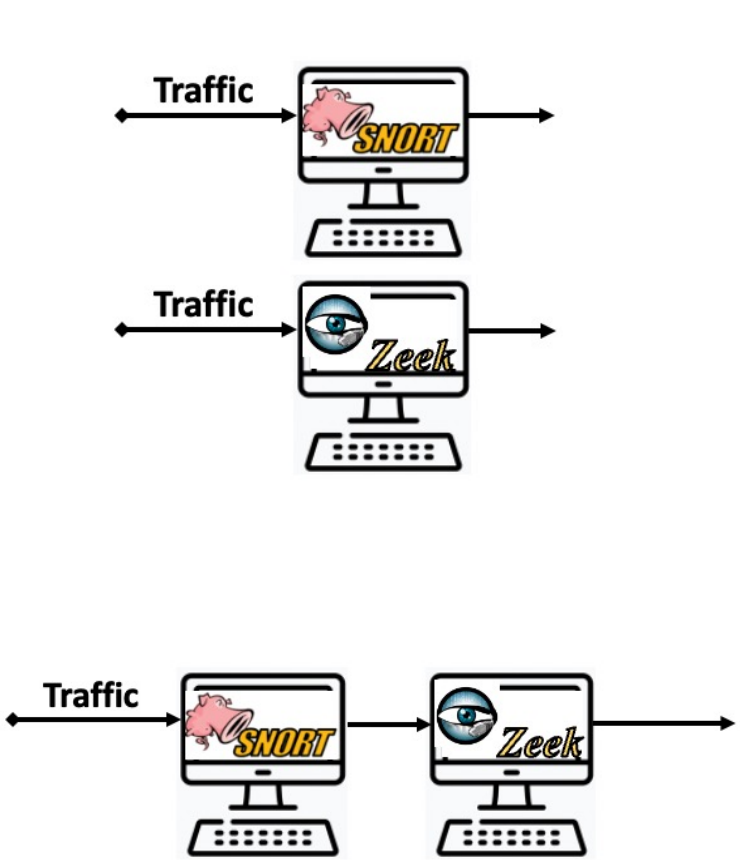


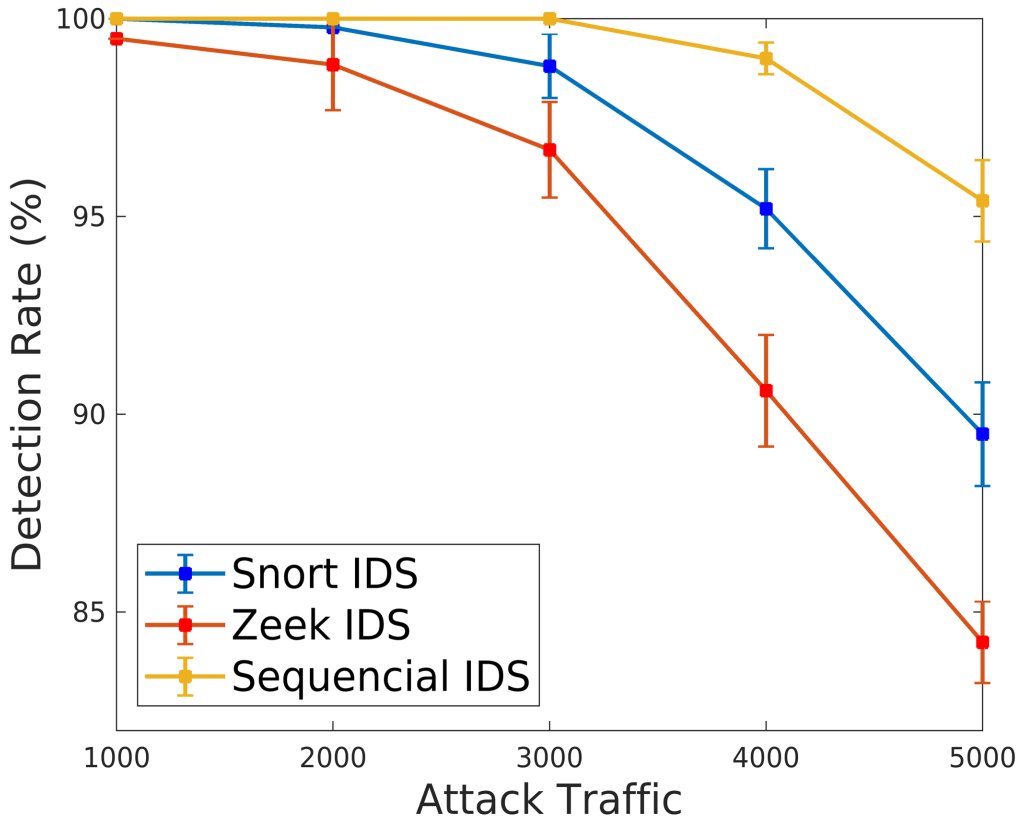




IDS	Attacks									
	ICMP		SYN		UDP		DoS		Port Scan	
	Detection	Flag	Detection	Flag	Detection	Flag	Detection	Flag	Detection	Flag
Snort	Yes	Not Bad	Yes	Bad	Yes	Bad	Yes	Bad	Yes	Not Bad
Zeek	No	Not flagged	Yes	Weird	Yes	Weird	Yes	Not flagged	Yes	Not flagged

Evaluation Results





Evaluation Results

Conclusion

- The analysis regarding attacks is primarily done outside of Zeek and the focus for Zeek is on collecting detailed information about the traffic
- Classical signature based IDS like Snort is instead more used as actual IDS, i.e the focus is on matching specific attack signatures .
- In the case of having single IDS, Snort IDS can be said to be above Zeek IDS in the case of detection rate, dropping rate, but not for delay.
- Under default configuration, neither Snort IDS nor Zeek IDS detect the port scanning attack.