ARIZONA STATE UNIVERSITY

Dynamic Game based Security Framework in SDN-enabled Cloud Network

Ankur Chowdhary, Sandeep Pisharody, Adel Alshamrani, Dijiang Huang (ASU)

SDNNFVSEC - 03/24/2017

ASU

Index

- Motivation & Problem Description.
- Proposed Solution.
- Game Theoretic Attack Analysis Framework.
- Nash Folk Theorem based Countermeasure Selection.

Motivation

iCloud

Dropbox

Target Hack

Sony Hacked

- By 2020 Cloud we will have 35Zb data online – a 4300% increase from now.
- Cloud will play big role in handling this data.

Problem Description

- Distributed networking and computing elements on cloud pose a big security risk.
- Sophisticated attackers often deploy multi-hop attack to target critical infrastructure.
- Assessing security state of large scale cloud environment is a challenging task.

Proposed Solution

- Analysis of attack as a dynamic game between attacker and defender/admin.
- Game Theoretic framework using flexibility afforded by SDN to deal with network attacks like DDoS (Distributed Denial of Service).
- Punishment in terms of network resources for misbehaving network nodes (part of DDoS attack traffic).

Game Theory Classification

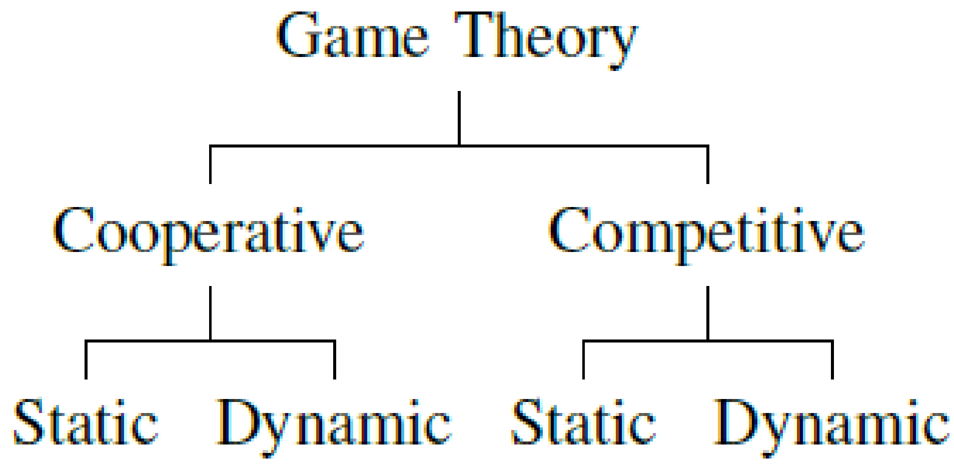
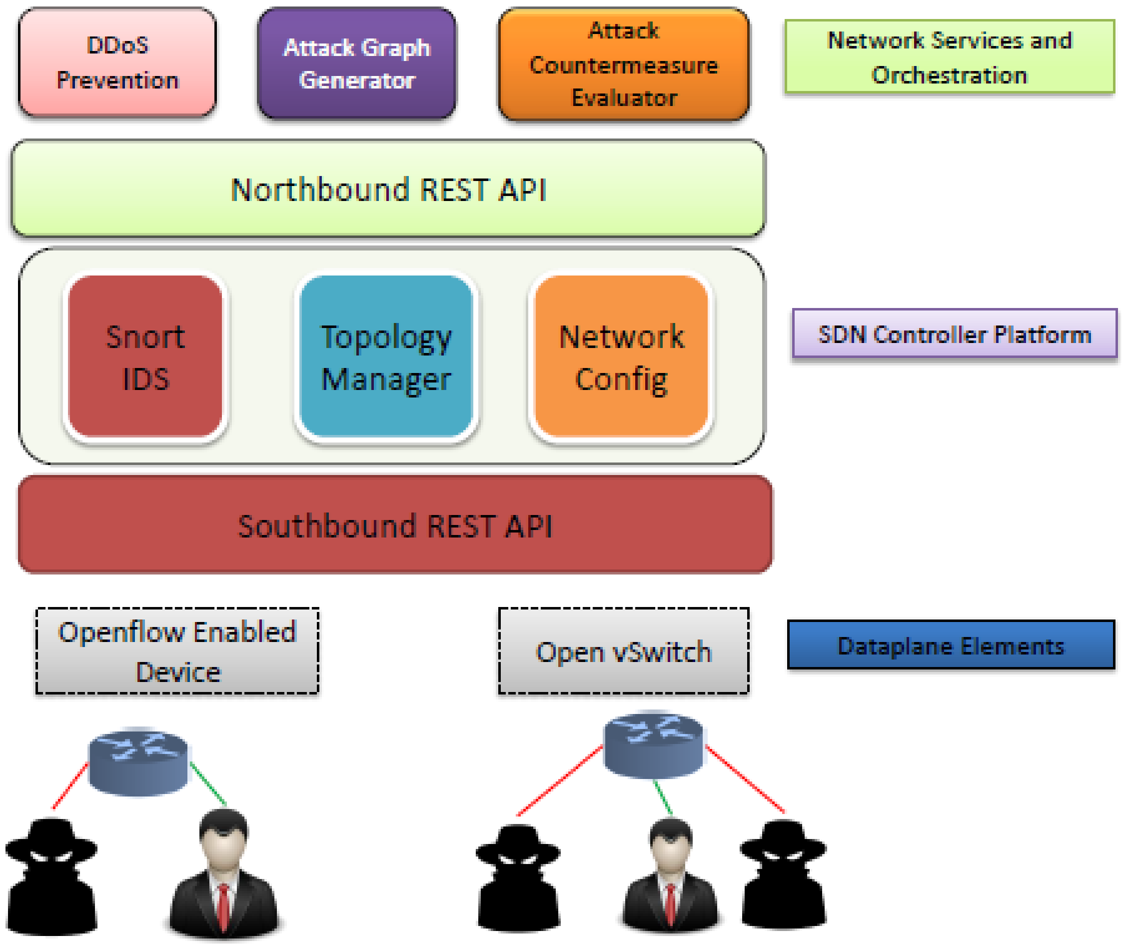


Figure 1. Game Theory classification.

System Architecture



Playing Games with Cloud Network

- A game consists of set of information states available to players, which help in making certain decisions.
- Players preferences over possible outcomes are measured by payoff or utility function.
- The utility for this game is portion of total network bandwidth.

Playing Games with Cloud Network

- The concept of reward and punishment which is used in game theoretic models to enforce cooperation between players.
- We define a N player extensive form repeated game $G = \{N, A_i, u_i\}$ where $N = \{1, 2,.., n\}$ denotes number of players.
- $\{ a_i \varepsilon A_i\}$ is the action set available to player *i*, $\{ui : a_i \rightarrow R_i\}$ is the payoff function that maps actions A to reward value R.

Min-max Strategy in Dynamic Game

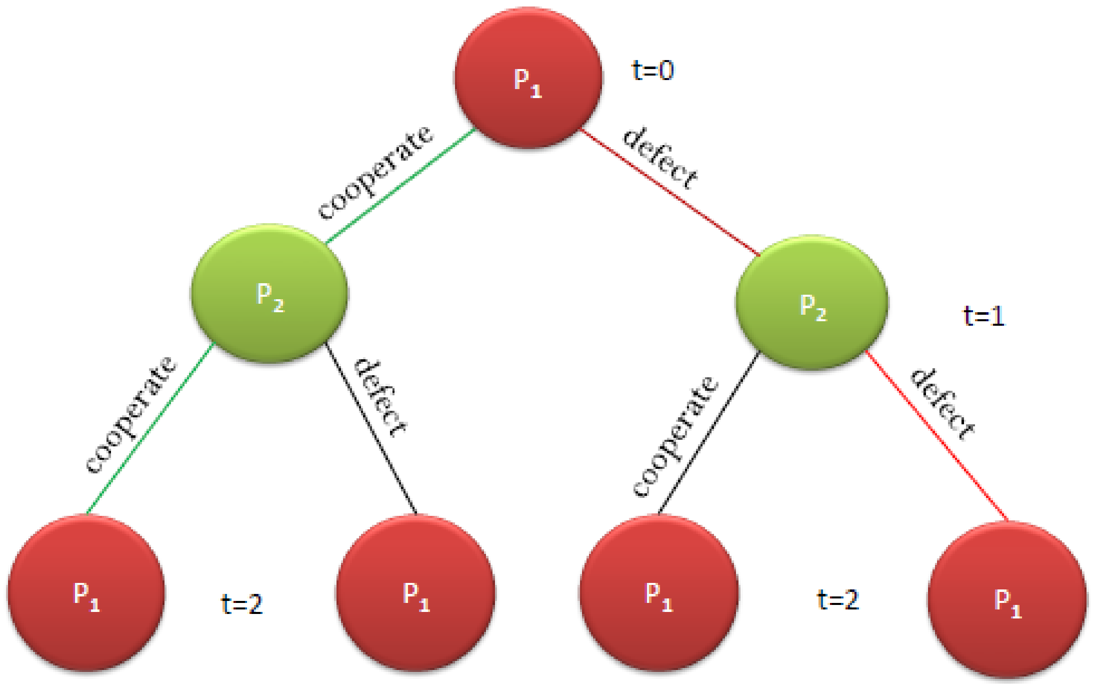
- The min-max payoff value of a player is the lowest payoff value that can be forced upon a player

$$\min_{a_{-i}\in A_{-i}} \max_{a_i\in A_i} u_i(a_{-i}, a_i).$$

		Player 2	
		a_2^1	a_2^2
Player 1	a_1^1	$(\frac{B}{2}, \frac{B}{2})$	$(\frac{3B}{4}, \frac{B}{4})$
	a_1^2	$(\frac{B}{4}, \frac{3B}{4})$	$(\frac{B}{5}, \frac{4B}{5})$

Table 1: Normal form representation of Attacker and administrator Payoff's

Extensive Form Game



$\text{Avg BW} = \frac{1}{2} * (\frac{B}{2} + \frac{B}{2})$

$\text{Avg BW} = \frac{1}{2} * (\frac{3B}{4} + \frac{B}{5})$

Nash Folk Theorem

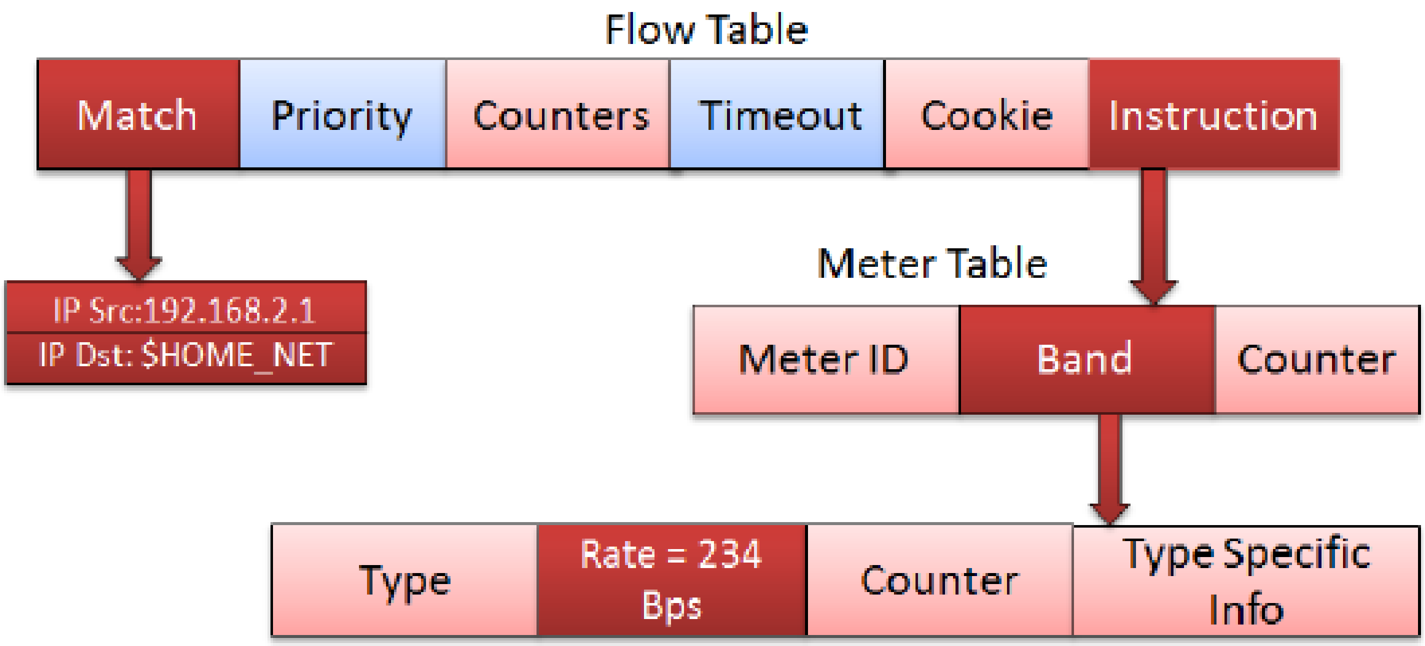
- The controller uses Rate Limiting option available in Flow Table to enforce Nash Equilibrium payoff value $\{w_i\}$ on malicious players.
- The value v_i denotes defection payoff at t=0, u_i is utility for a given player and δ is discount factor that is decided by controller.

Nash Folk Theorem

- The payoff value for defecting player P_1 based on Nash Folk Theorem strategy enforced by Controller is

$$w_i \geq v_i + \sum_{t=1}^{T} \delta^t \times min_{a_{-i} \in A_{-i}} max_{a_i \in A_i} u_i(a_{-i}^t, a_i^t)$$

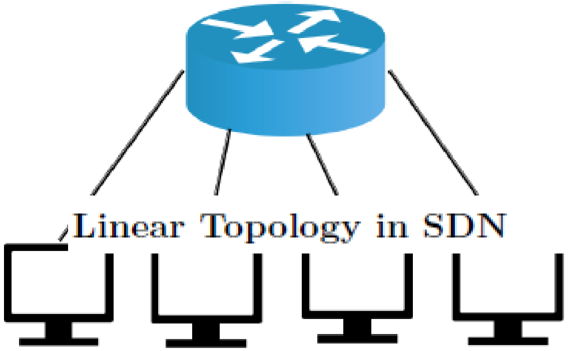
Flow Table Rate Limiting



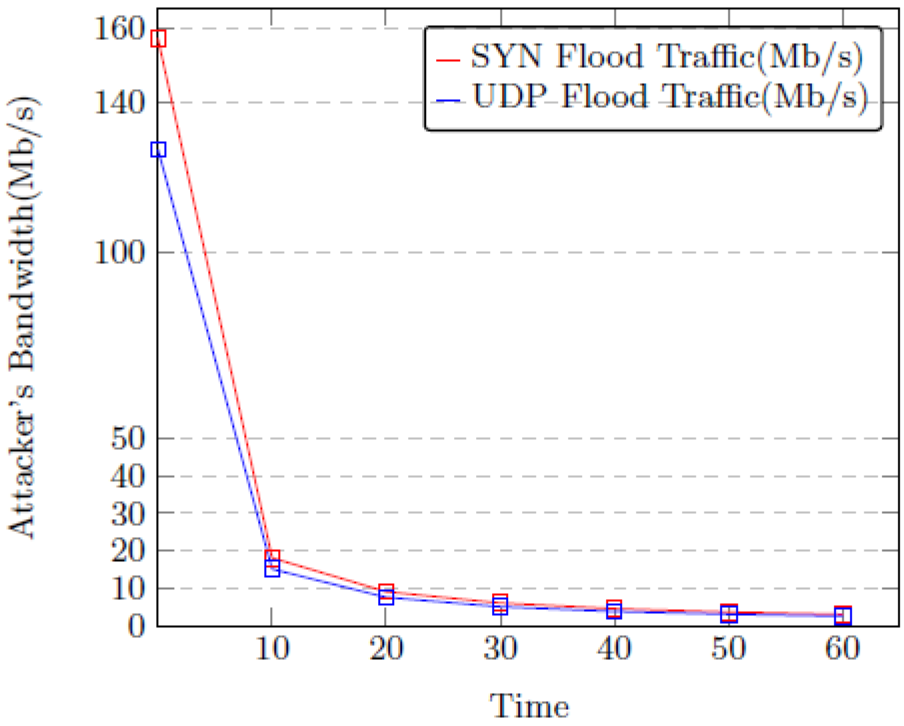
Experimental Analysis

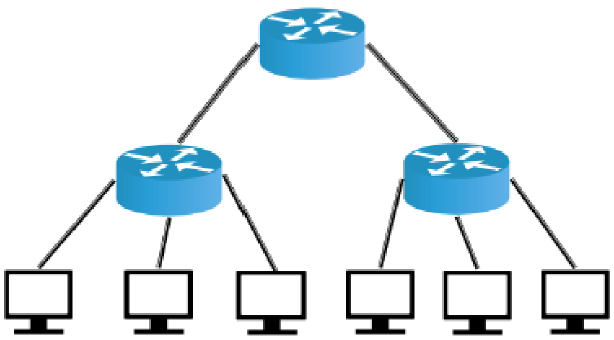
ICMP Flood DDoS Attack Analysis

Number of Attacking Hosts	ICMP Flood Traffic (Mb/s)	ICMP Traffic post Rate Limit(Mb/s)
50	39.49	1.33
100	79.85	2.70
200	163.69	5.54
300	241.17	8.122
400	321.96	10.83
500	467.16	15.69



TCP & UDP Flood Attack Analysis





Fat Tree topology in SDN

Conclusion

- We designed a greedy algorithm which solves an optimization problem for rate limiting network bandwidth as a punitive mechanism.
- The normal bandwidth which we used as a baseline for threshold bandwidth was selected by observing normal TCP, UDP traffic in a medium sized network for a time duration of about 10-15 minutes.

Thanks