Applying Game Theory for Moving Target Defense

CAP 5593 TERM PROJECT PRESENTATION

ABDULLAH AYDEGER

FLORIDA INTERNATIONAL UNIVERSITY

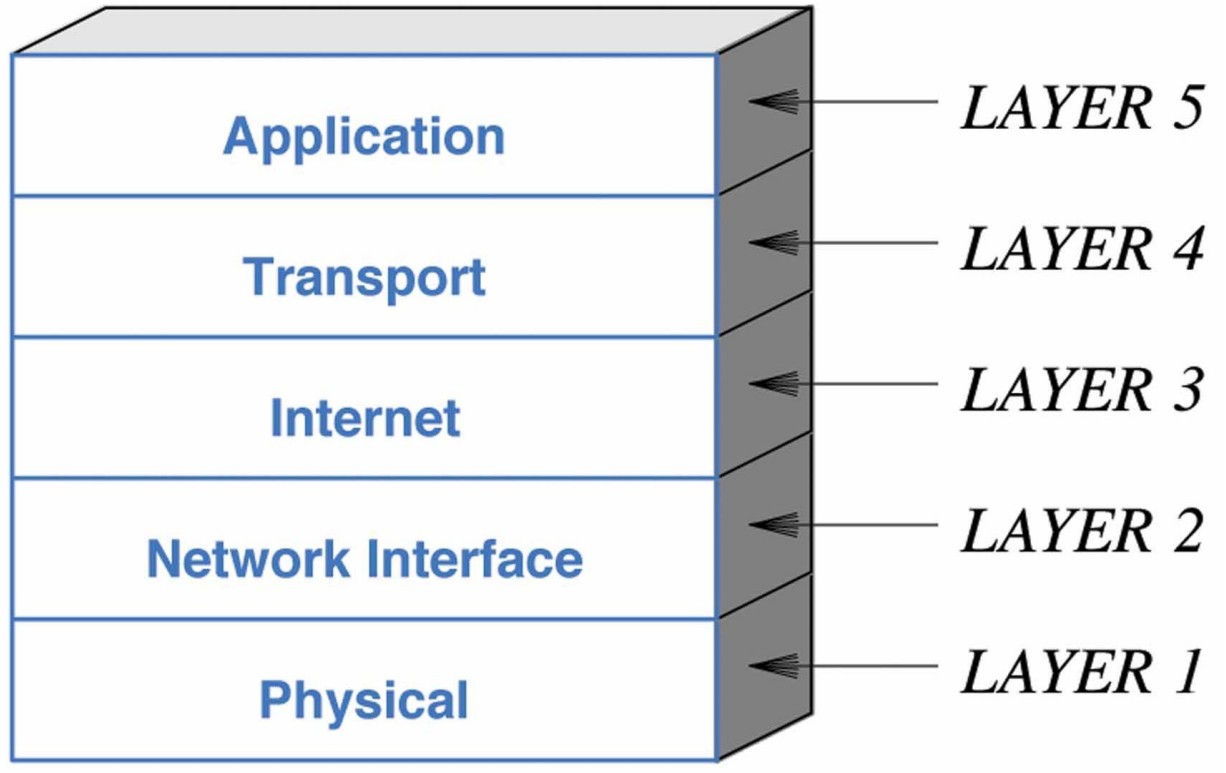
PHD STUDENT OF ELECTRICAL AND COMP. ENG.

AAYDE001@FIU.EDU

Outline

1. Introduction to Computer Network Security
2. Moving Target Defense (MTD)
   A. Game Theory for MTD
3. Software Defined Networking
4. Conclusion

Computer Network Layers



Computer Network Security

Active, passive attacks

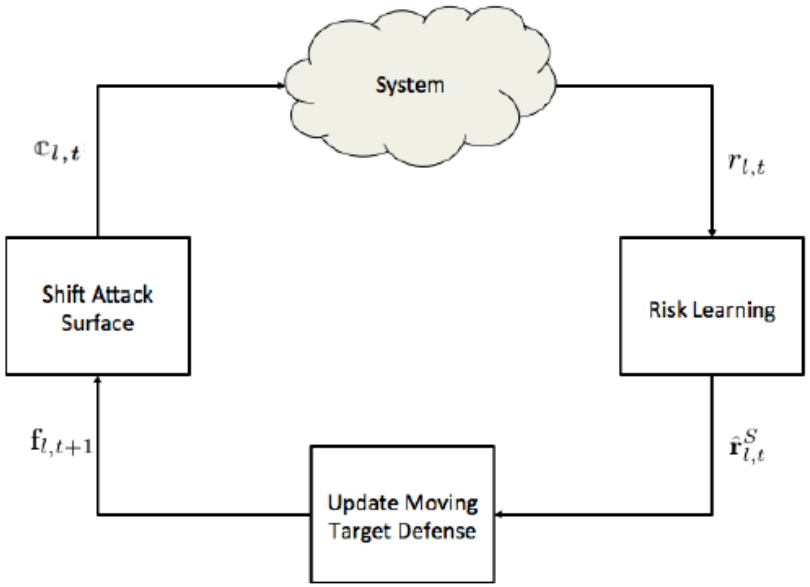
Moving Target Defense (MTD)

- The static nature of computer networks;
  - attackers to easily gather useful information about the network
    - network scanning and packet sniffing
- One solution by manipulating the attack surface of the network in order to create a moving target defense
  - varies the system protocol, operating system, and software configurations over time
  - thus rendering vulnerabilities observed by the adversary obsolete before the attack takes place

Game Theory for MTD

At [1], authors model the network attacker and defender strategies and utilities as 2 person zero sum game. Game solution is mixed strategy, saddle-point equilibrium (SPE)

- They consider a system has always some vulnerabilities at each layer of network that attacker can exploit
- Defender moves his attack surface to prevent attacks => Switching cost
- To solve the game in defender favor => the SPE value of the game
  - They give the required equation and proved it in the paper
- They show their MTD solution is having better payoff than static randomized strategy (for ex 1/3, 1/3, 1/3)

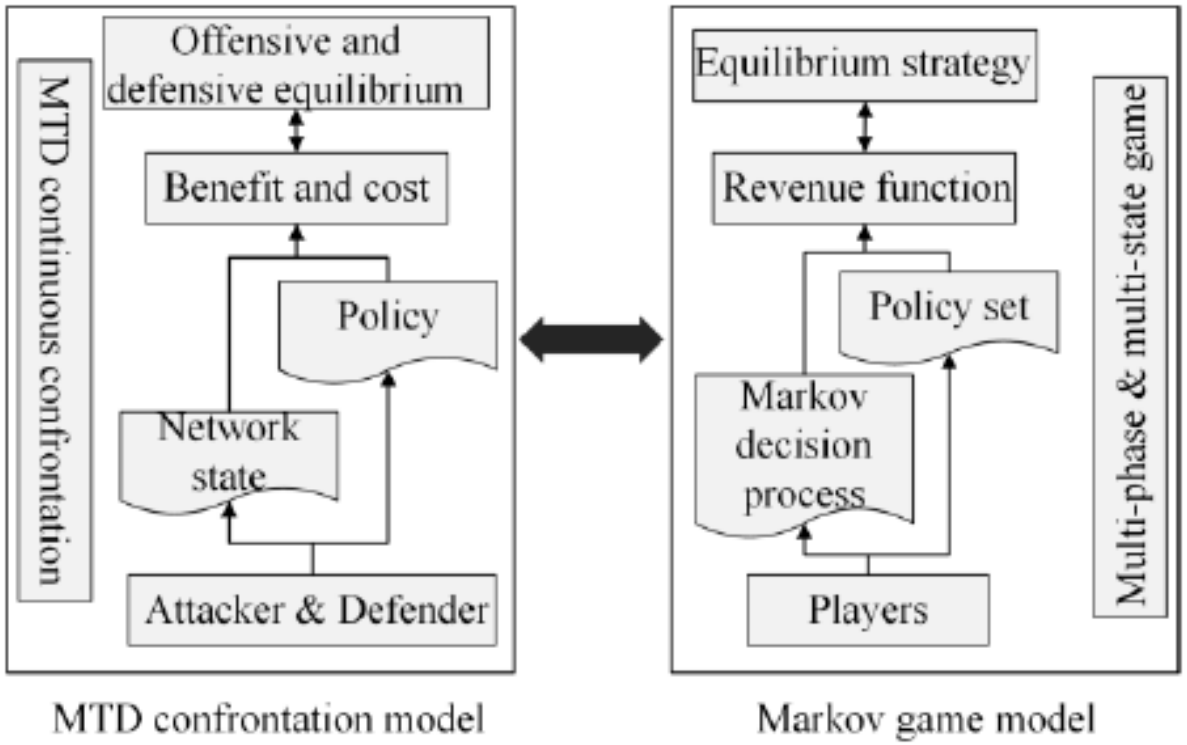


Game Theory for MTD

- At [2], they model adversary and single decoy node
  - Timing-based detection of a single decoy, they formulate a two-player game between an adversary and a system. Game has pure Nash Equilibrium. On the other hand, protocol implementation based detection game has only mixed strategies Nash Equilibrium.

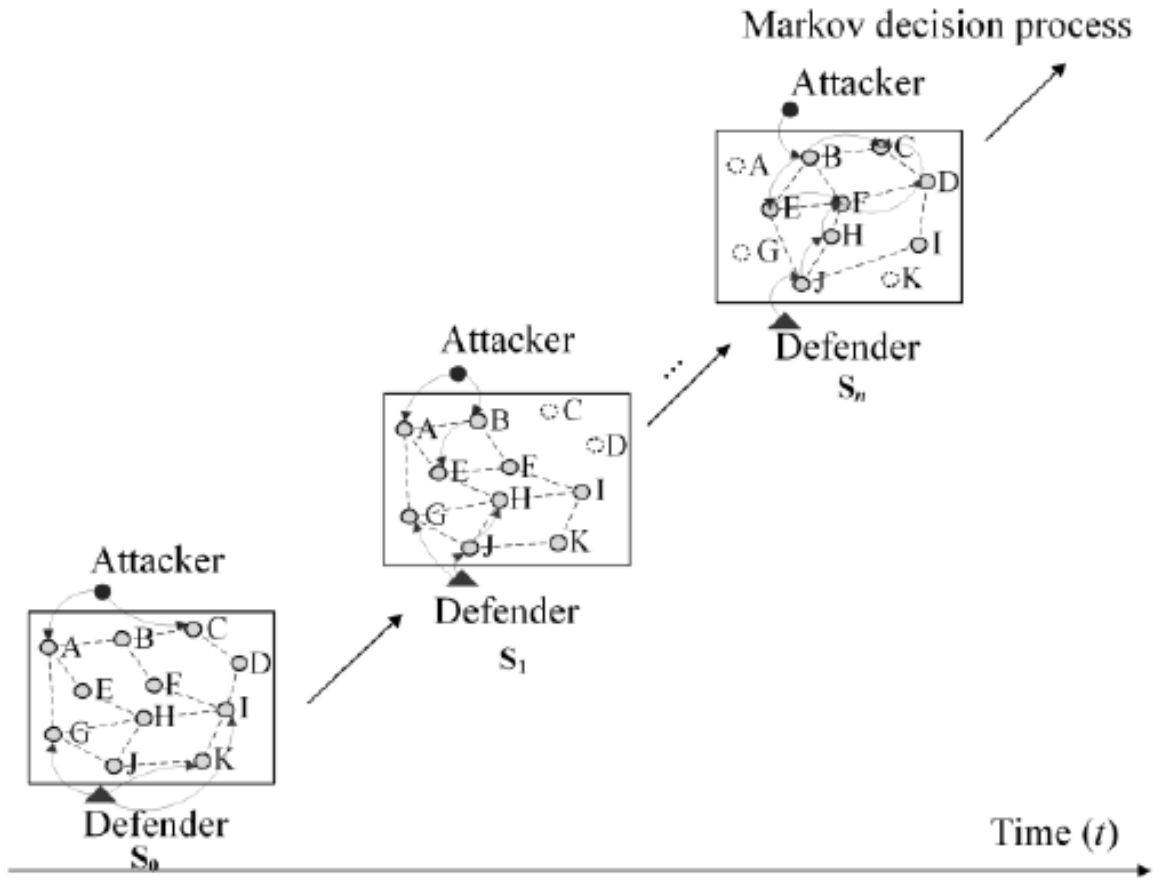
Game Theory for MTD

At [3], they proposed to model MTD on Markov Games (MG)



MTD confrontation model

Markov game model



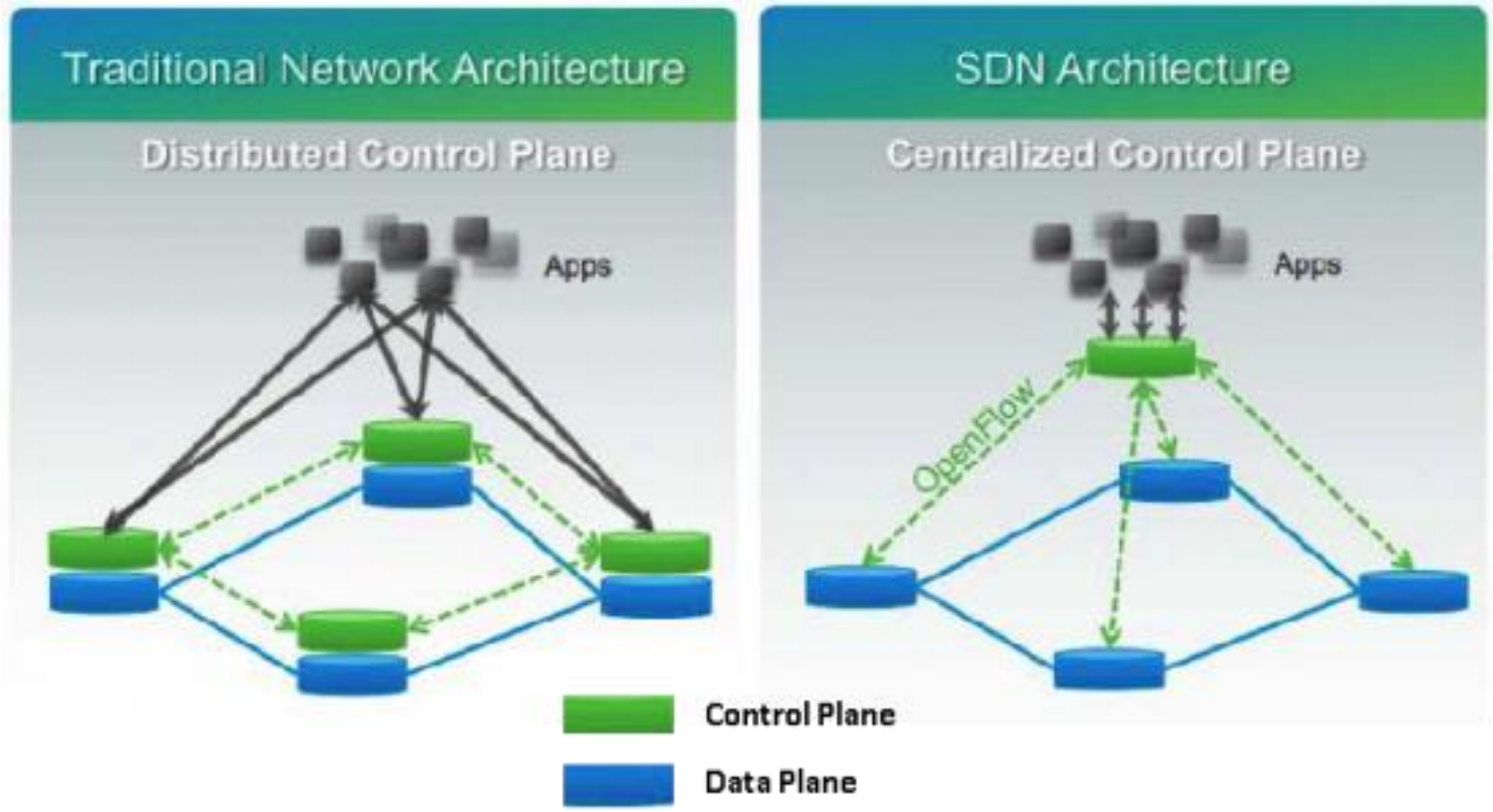
What SDN is

Agile and cost-effective new network architecture with;

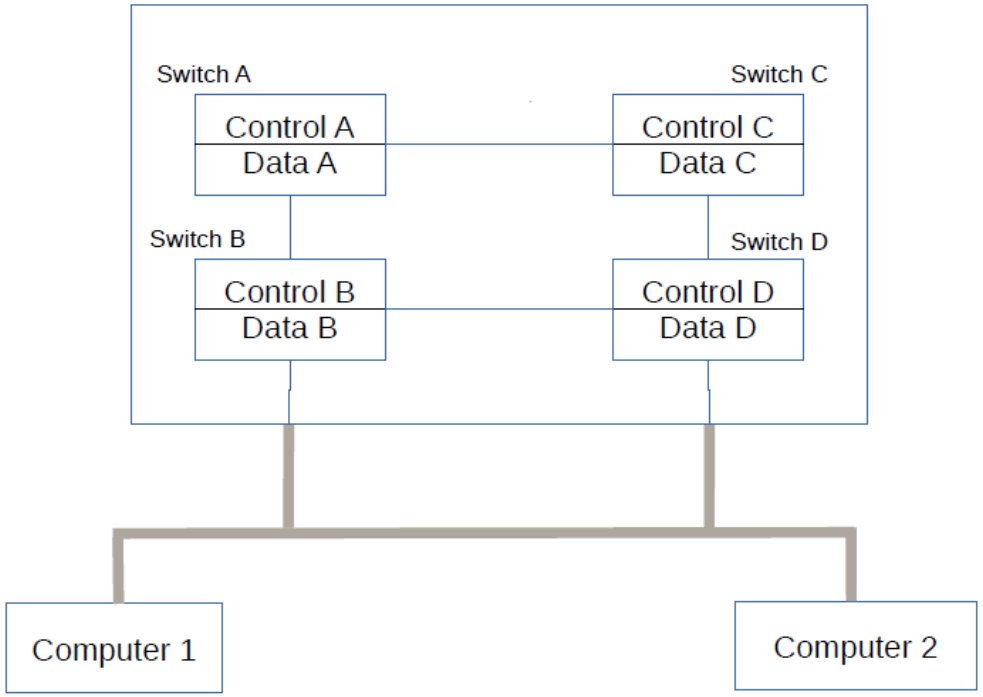
- Centralized control model
- Unique programmability

What it provides;

- High degree of scalability
- Security
- Flexibility

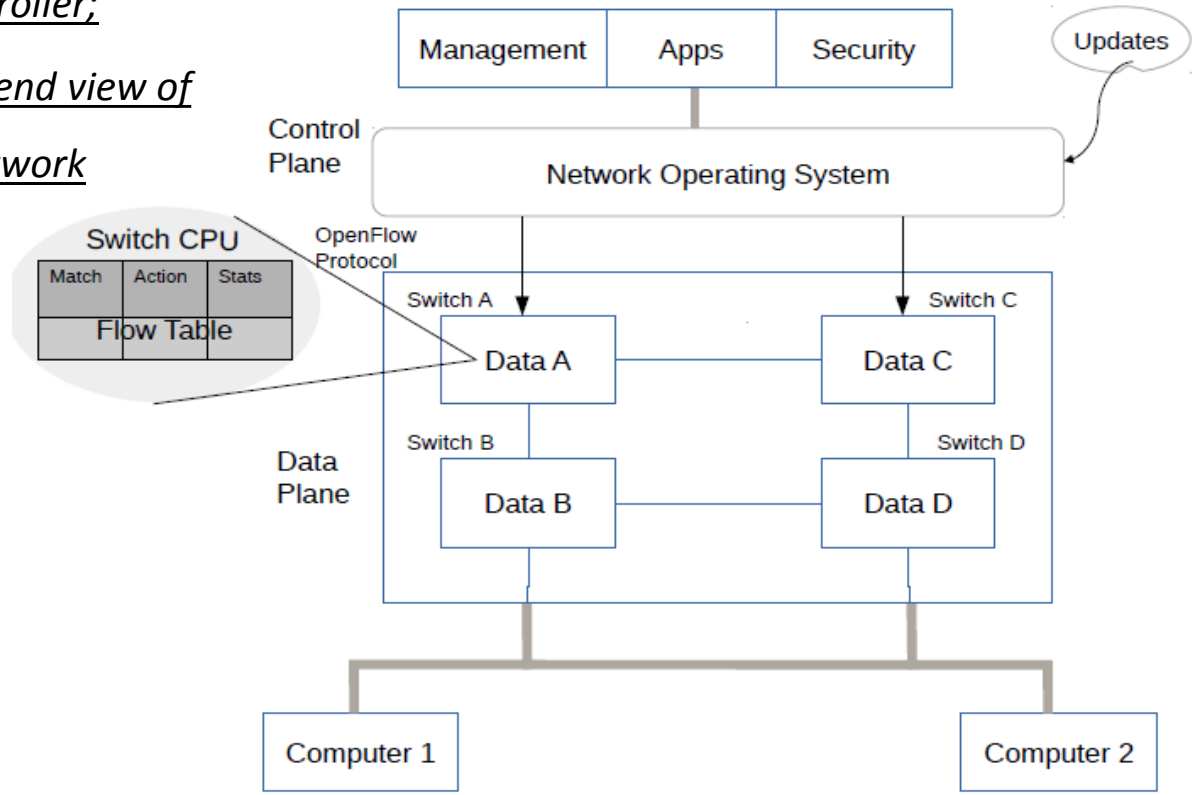


What SDN is



SDN Controller;

➢*End-to-end view of entire network*

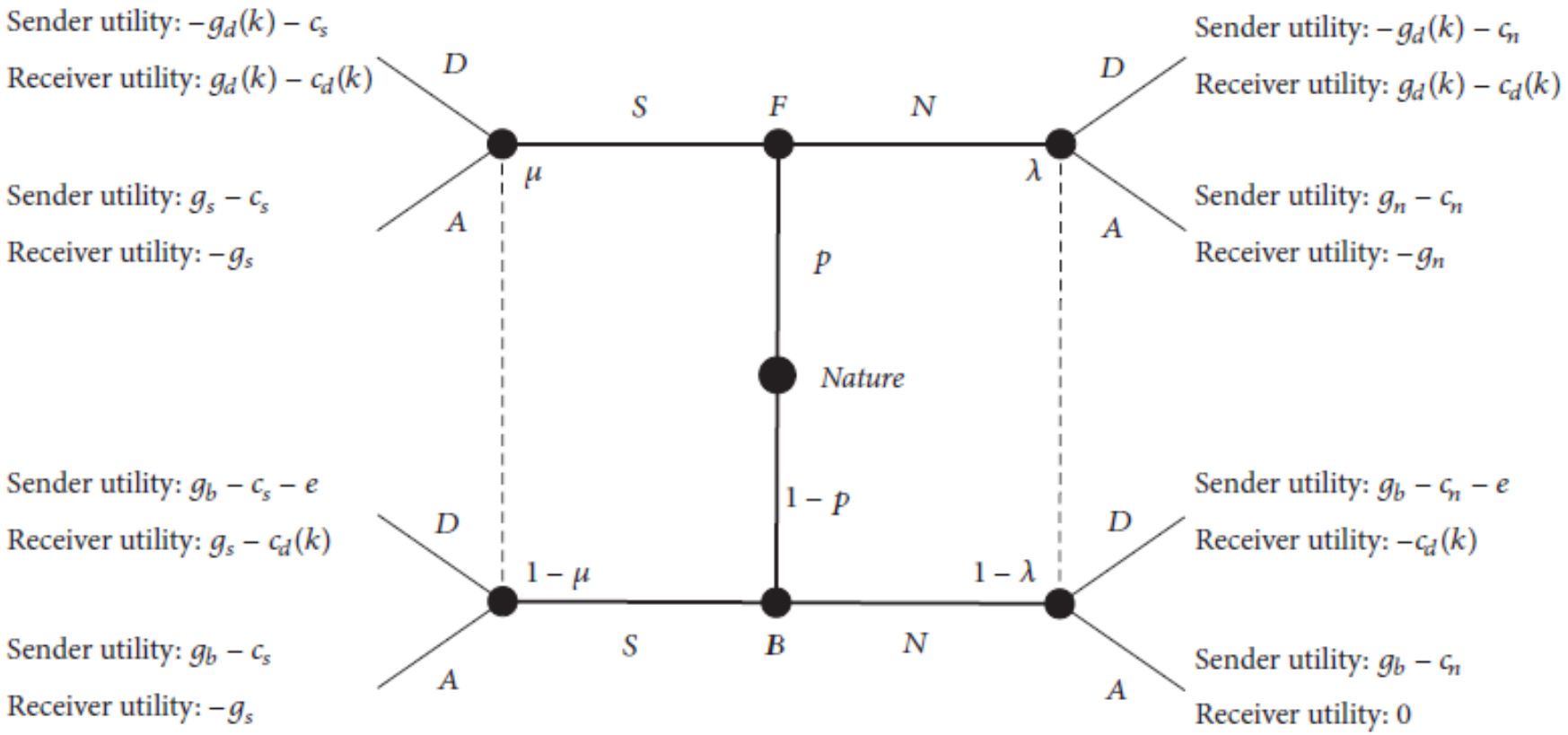


Game Theory Based MTD in SDNs

- According to [4]; The interaction between the sender and receiver can be formulated as a game.
  - the sender acts first (Normal or Suspicious); then, the receiver can observe the action and take action accordingly. Therefore, the game is a dynamic game.
  - the type of sender is private information to the receiver, and it is an incomplete information game
  - By observing the actions of the sender, the receiver can infer the type of sender and selects an action (Defense or Abstain) based on the information regarding the sender type.
  - This fingerprinting attack and defense can be modeled as a signaling game

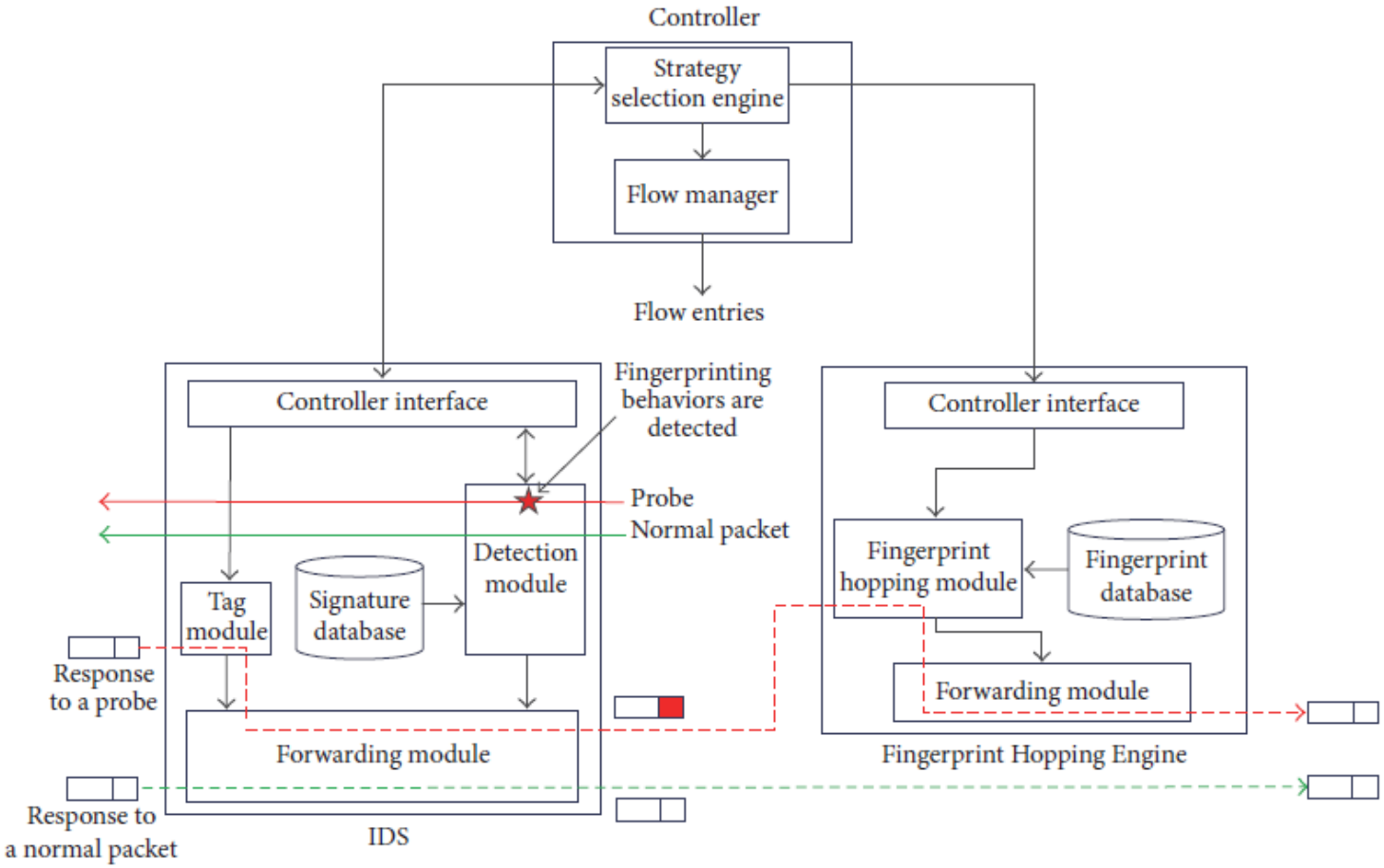
Game Theory Based MTD in SDNs

The extensive form of the game at [4]:



Game Theory Based MTD in SDNs

SDN Controller architecture



Conclusion

- Possible Game theory models for different MTD solutions
- Utilization of game theory in SDNs ?

References

[1] Zhu, Quanyan, and Tamer Başar. "Game-theoretic approach to feedback-driven multi-stage moving target defense." *International Conference on Decision and Game Theory for Security*. Springer International Publishing, 2013.

[2] Clark, Andrew, et al. "A Game-Theoretic Approach to IP Address Randomization in Decoy-Based Cyber Defense." *International Conference on Decision and Game Theory for Security*. Springer International Publishing, 2015.

[3] Lei, Cheng, Duo-He Ma, and Hong-Qi Zhang. "Optimal Strategy Selection for Moving Target Defense Based on Markov Game." *IEEE Access* 5 (2017): 156-169.

[4] Zhao, Zheng, Fenlin Liu, and Daofu Gong. "An SDN-Based Fingerprint Hopping Method to Prevent Fingerprinting Attacks." *Security and Communication Networks* 2017 (2017).