CDGym: Expandable, Model-Agnostic Cyber Deception Platform

Sukwha Kyung, Siyu Liu, Faris Kokulu, Tiffany Bao, and Gail-Joon Ahn

Arizona State University

ASU Arizona State University

CENTER FOR CYBERSECURITY & DIGITAL FORENSICS

Game-Theoretic Cyber Deception

- Deception decreases or reverses strategic asymmetries
- Game theory provides generic framework for quantifying actions/reactions, rewards/penalties
- Previous works have been focusing on leveraging game theory to devise deception strategies and implement in real-world networks

Current Challenges

- Lack of

Current Challenges

- Lack of
  - Reproducibility: Test environments is created/managed in an ad-hoc manner.

Current Challenges

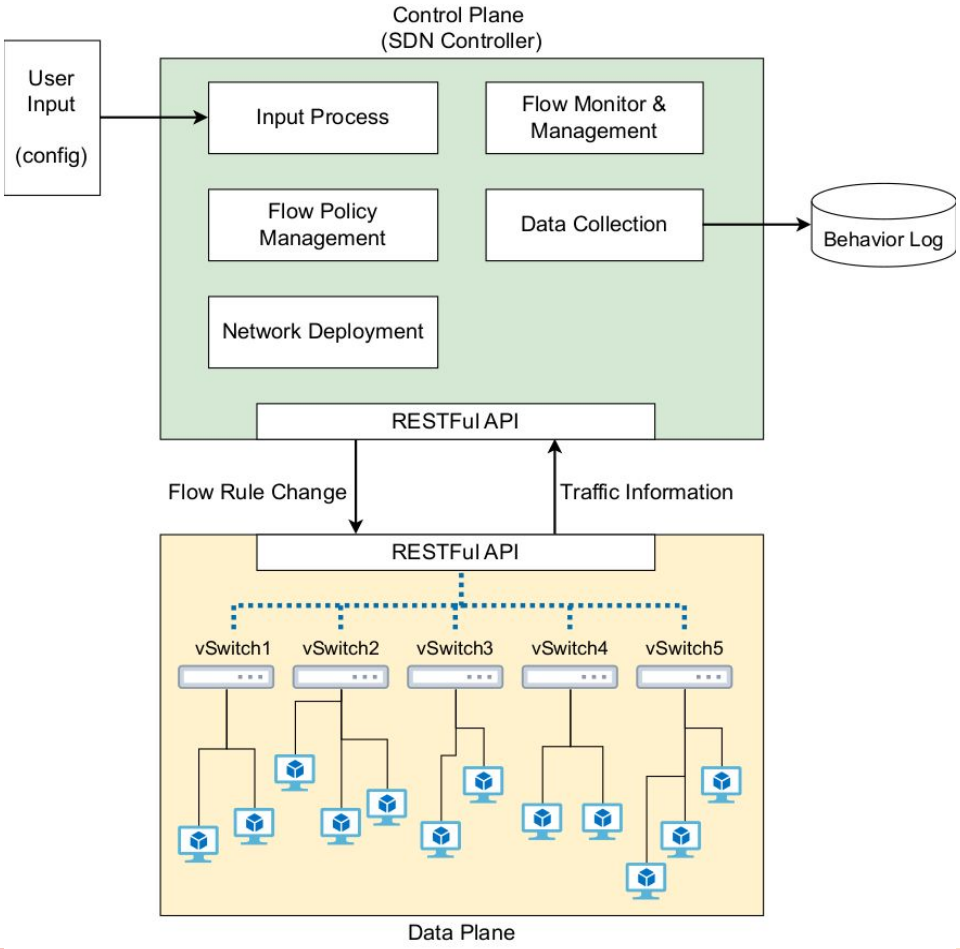
- Lack of
  - Reproducibility: Test environments is created/managed in an ad-hoc manner.
  - Measurability: It is difficult to collect data.

Current Challenges

- Lack of
  - Reproducibility: Test environments is created/managed in an ad-hoc manner.
  - Measurability: It is difficult to collect data.
  - Adaptability: Each strategy requires different configurations.

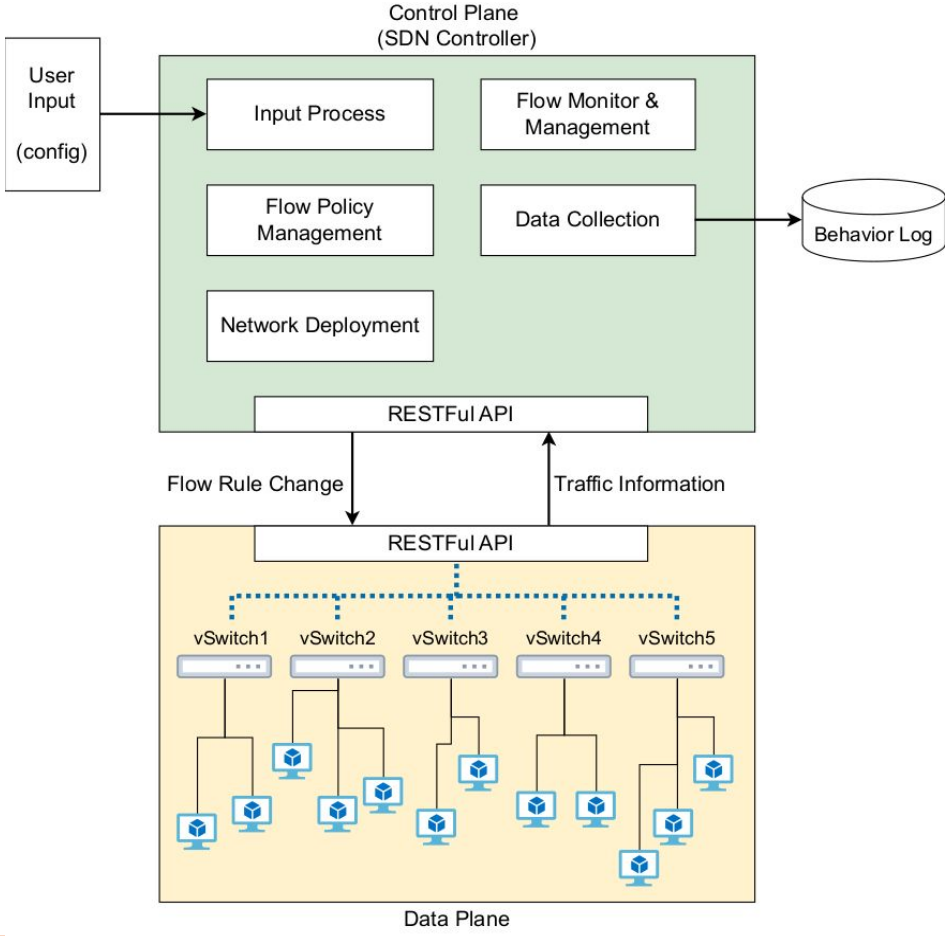
CDGym

- SDN-based cyber deception platform.



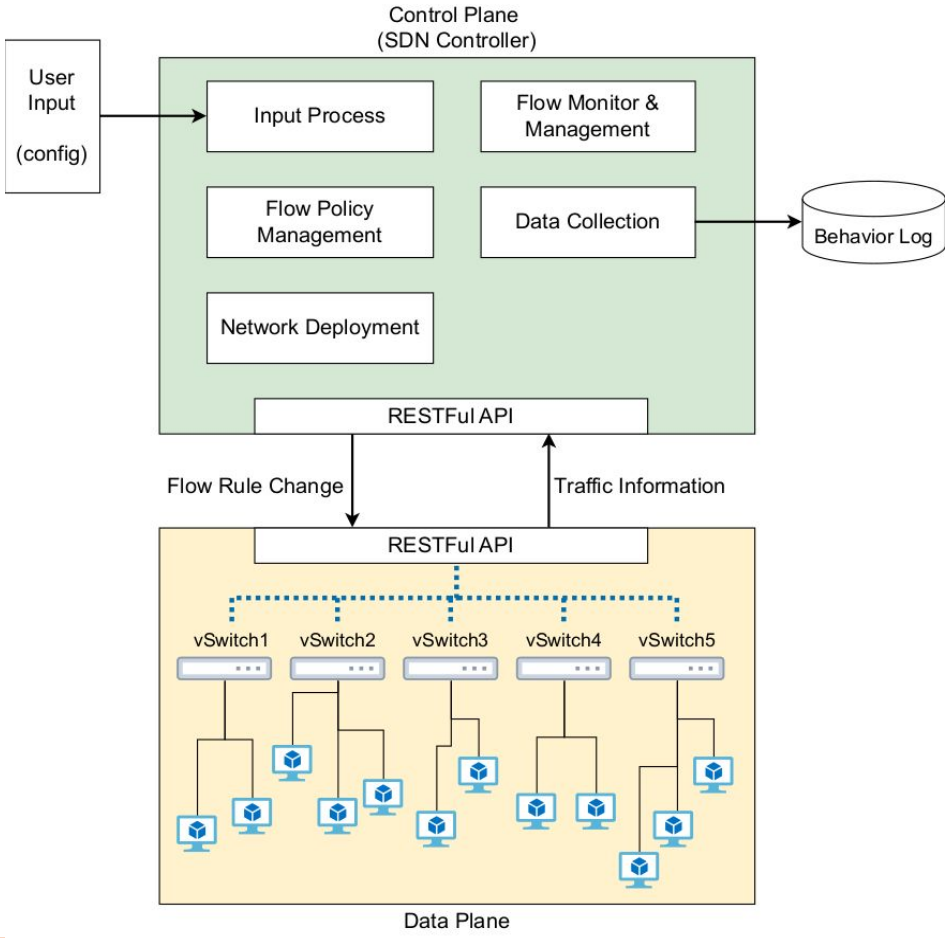
CDGym

- Reproducibility: Automated deployment, configuration, and termination of the network through SDN.



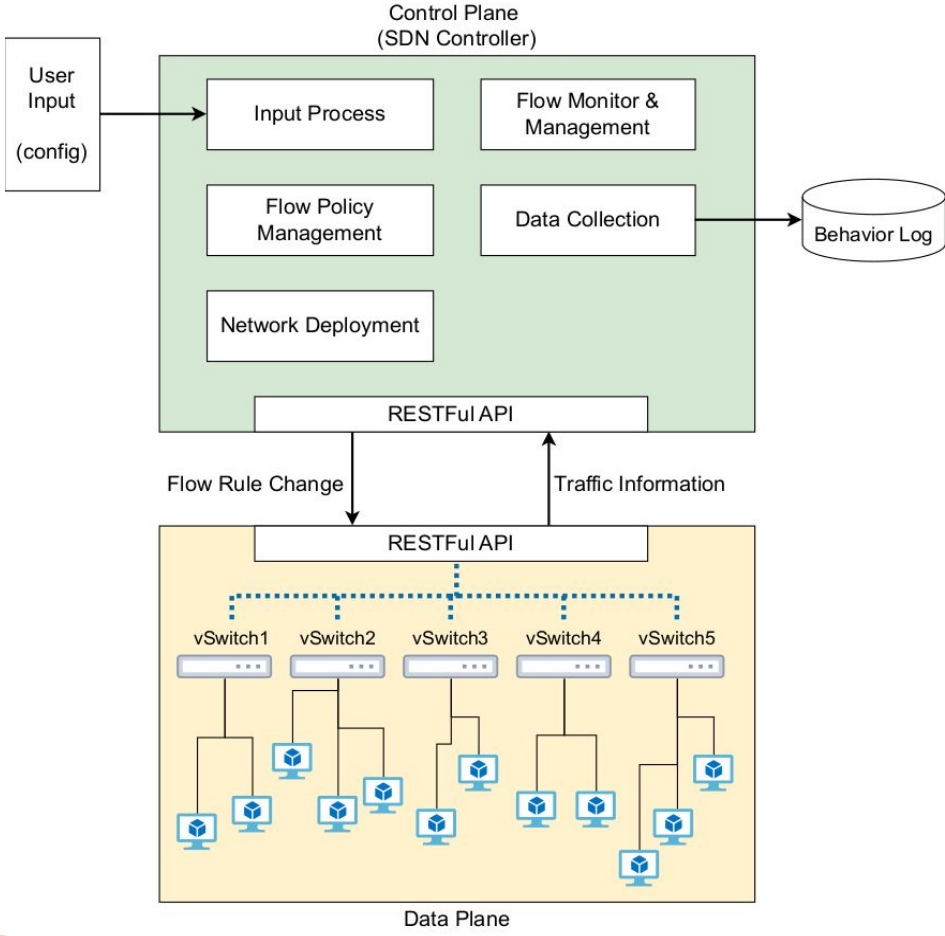
CDGym

- Measurability: Real-time data collection module.

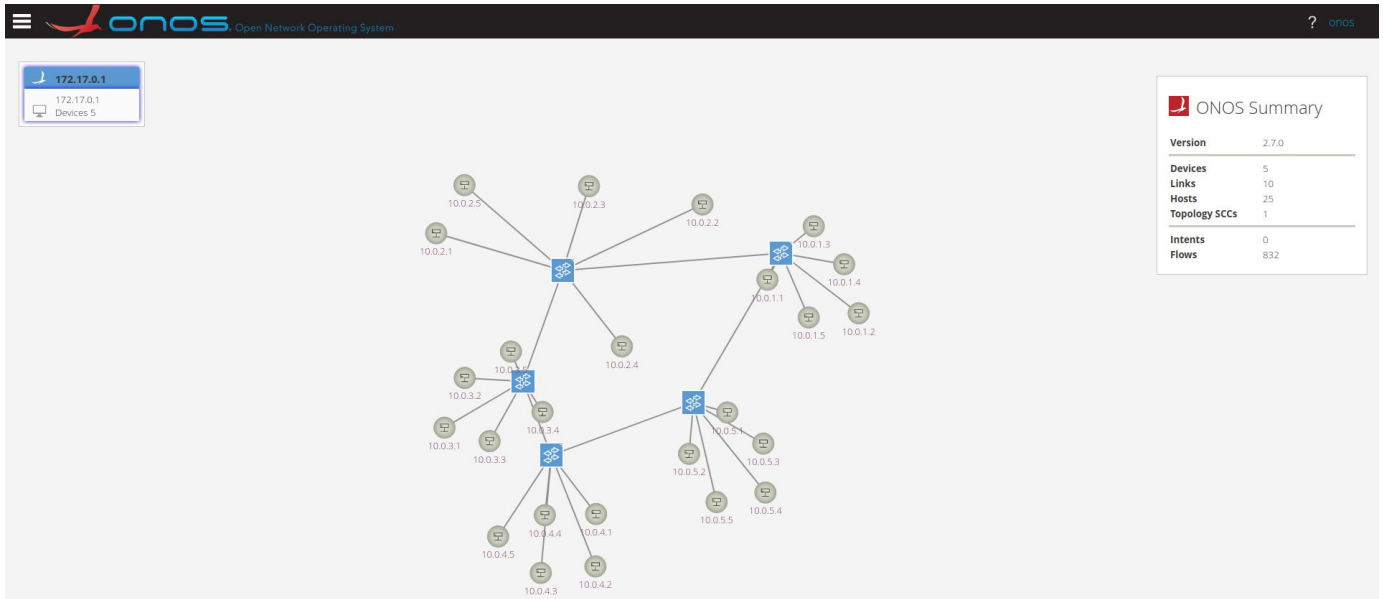


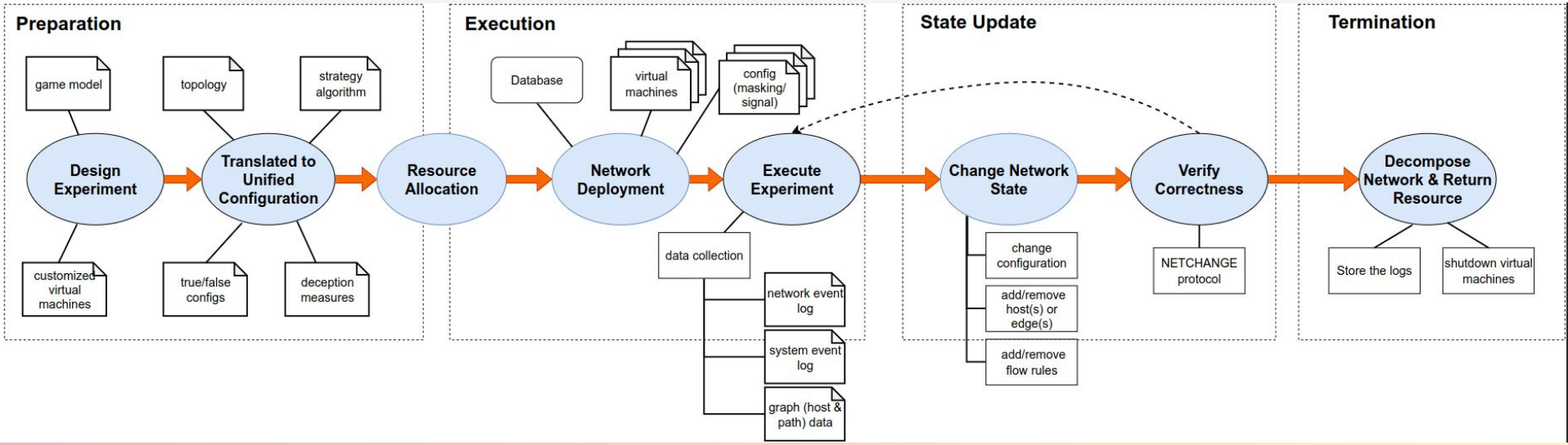
CDGym

- Adaptability: Design and implement unified configuration language.

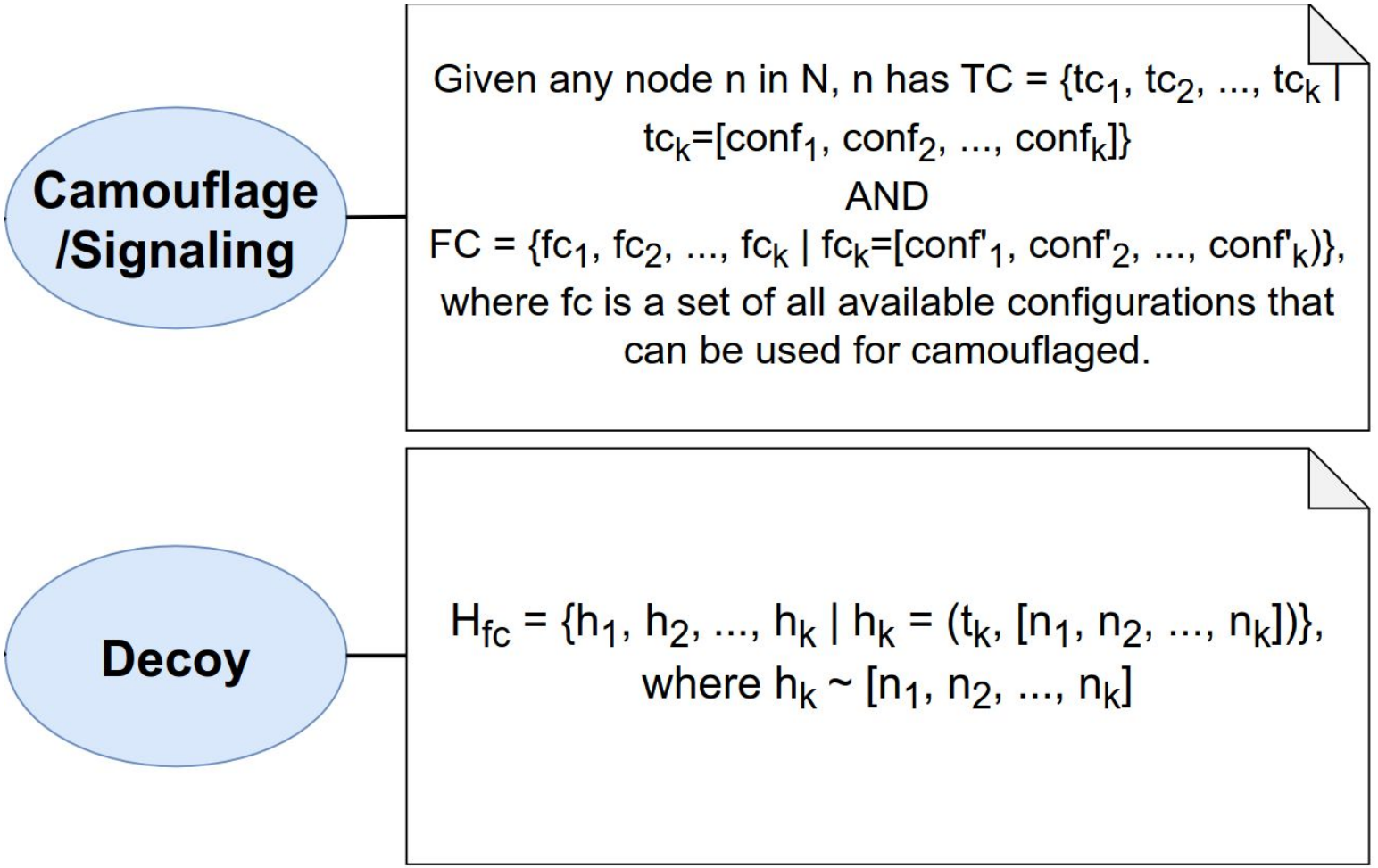


CDGym


onos
Open Network Operating System
172.17.0.1
ONOS Summary
Version 2.7.0
Devices 5
Links 10
Hosts 25
Topology SCCs 1
Intents 0
Flows 832


Preparation
game model
topology
strategy algorithm
Design Experiment
Translated to Unified Configuration
customized virtual machines
true/false configs
deception measures
Resource Allocation
Execution
Database
virtual machines
config (masking/ signal)
Network Deployment
Execute Experiment
data collection
network event log
system event log
graph (host & path) data
State Update
Change Network State
change configuration
add/remove host(s) or edge(s)
add/remove flow rules
Verify Correctness
NETCHANGE protocol
Termination
Decompose Network & Return Resource
Store the logs
shutdown virtual machines

Unified Configuration Language



Unified Configuration Language

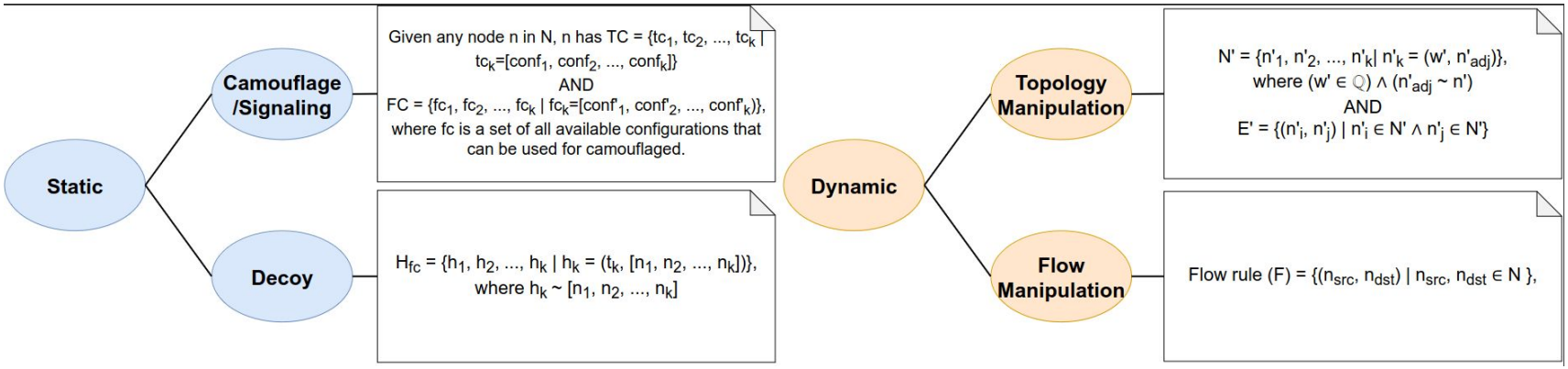
Topology Manipulation

$$N' = \{n'_1, n'_2, \ldots, n'_k \mid n'_k = (w', n'_{adj})\},$$
$$\text{where } (w' \in \mathbb{Q}) \wedge (n'_{adj} \sim n')$$
$$\text{AND}$$
$$E' = \{(n'_i, n'_j) \mid n'_i \in N' \wedge n'_j \in N'\}$$

Flow Manipulation

$$\text{Flow rule } (F) = \{(n_{src}, n_{dst}) \mid n_{src}, n_{dst} \in N\},$$

Unified Configuration Language



Evaluation of *CDGym*

- Case studies:
  - 3 different strategies from existing works are implemented in *CDGym*.

Evaluation of *CDGym*

- Case studies:
  - 3 different strategies from existing works are implemented in *CDGym*.
    - D1*: based on a zero-sum game model and seeks to minimize the cumulative loss of the defender through flow & topology modifications.

*: Danda B Rawat, Naveen Sapavath, and Min Song. ***Performance evaluation of deception system for deceiving cyber adversaries in adaptive virtualized wireless networks***. In Proceedings of the 4th ACM/IEEE Symposium on Edge Computing, pages 401–406, 2019.

Evaluation of *CDGym*

- Case studies:
  - 3 different strategies from existing works are implemented in *CDGym*.
    - D1*: based on a zero-sum game model and seeks to minimize the cumulative loss of the defender through flow & topology modifications.
    - D2**: active manipulation of the attacker's belief by following probabilistic model based on Markov decision process (flow manipulation).

*: Danda B Rawat, Naveen Sapavath, and Min Song. ***Performance evaluation of deception system for deceiving cyber adversaries in adaptive virtualized wireless networks***. In Proceedings of the 4th ACM/IEEE Symposium on Edge Computing, pages 401–406, 2019.

: Karel Hor´ak, Quanyan Zhu, and Branislav Bo˘sansk`y. ***Manipulating adversary's belief: A dynamic game approach to deception by design for proactive network security*. In International Conference on Decision and Game Theory for Security, pages 273–294. Springer, 2017.

Evaluation of *CDGym*

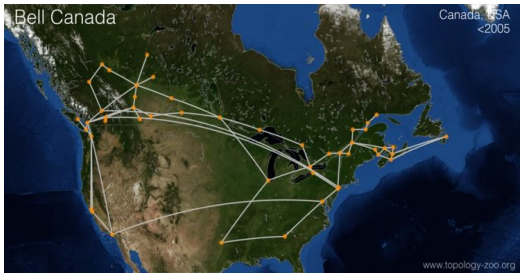
- Case studies:
  - 3 different strategies from existing works are implemented in *CDGym*.
    - D1*: based on a zero-sum game model and seeks to minimize the cumulative loss of the defender through flow & topology modifications.
    - D2**: active manipulation of the attacker's belief by following probabilistic model based on Markov decision process (flow manipulation).
    - D3***: static honeypot placement strategy using priority scores assigned to each node (asset) in the network.

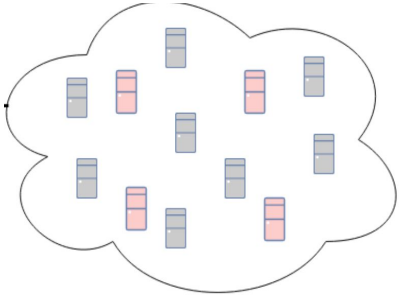
*: Danda B Rawat, Naveen Sapavath, and Min Song. ***Performance evaluation of deception system for deceiving cyber adversaries in adaptive virtualized wireless networks***. In Proceedings of the 4th ACM/IEEE Symposium on Edge Computing, pages 401–406, 2019.

: Karel Hor´ak, Quanyan Zhu, and Branislav Bo˘sansk`y. ***Manipulating adversary's belief: A dynamic game approach to deception by design for proactive network security*. In International Conference on Decision and Game Theory for Security, pages 273–294. Springer, 2017.

: Radek P´ıbil, Viliam Lis`y, Christopher Kiekintveld, Branislav Bo˘sansk`y, and Michal P˘echou˘cek. ***Game theoretic model of strategic honeypot selection in computer networks. In International Conference on Decision and Game Theory for Security, pages 201–220. Springer, 2012.

Evaluation of *CDGym*





Real-world Network

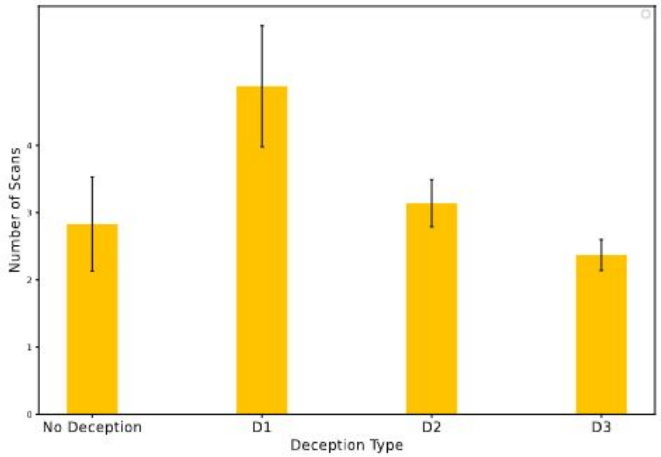
Network Topology (graphxml)

Simulated Network

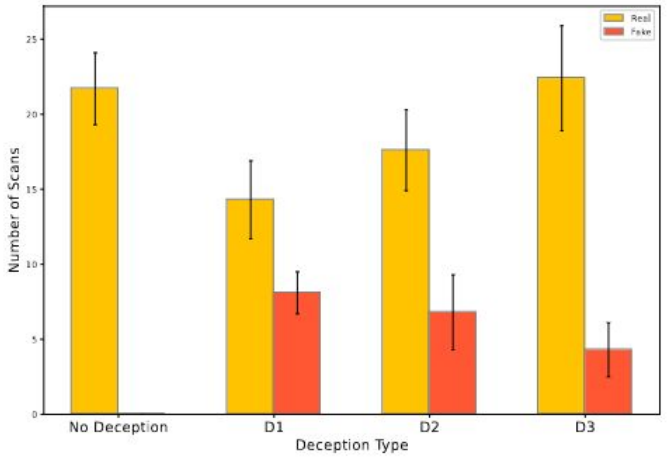
Evaluation of *CDGym*

- Data metrics
  - Scanning Time
  - Number of Scanning Attempts
  - Number of exploits
  - Number of IDS alarms
  - Commands typed

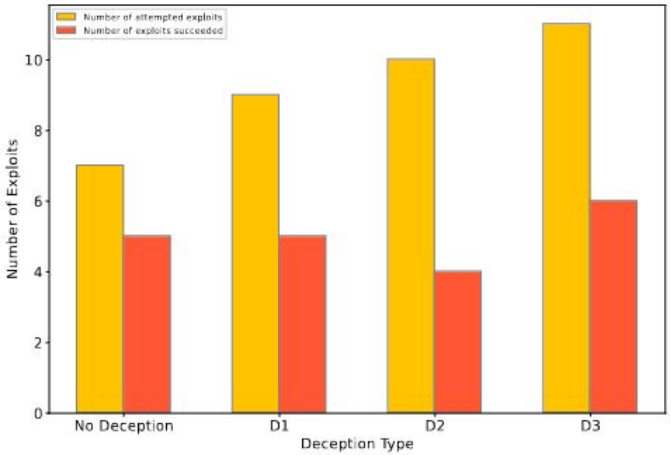
Evaluation of *CDGym*



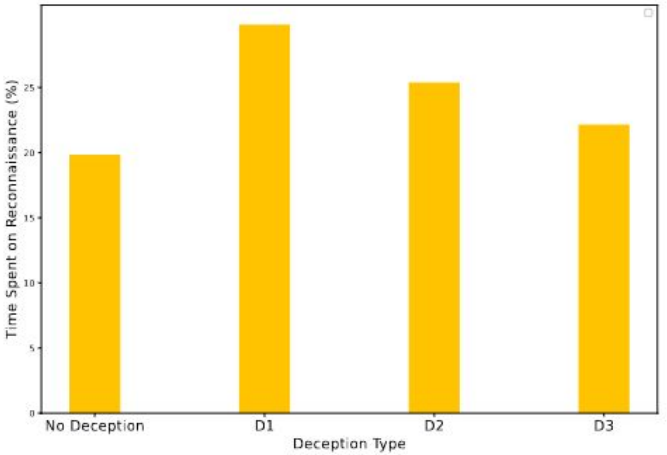
(a) Number of Network Scans



(b) Number of Host Scans

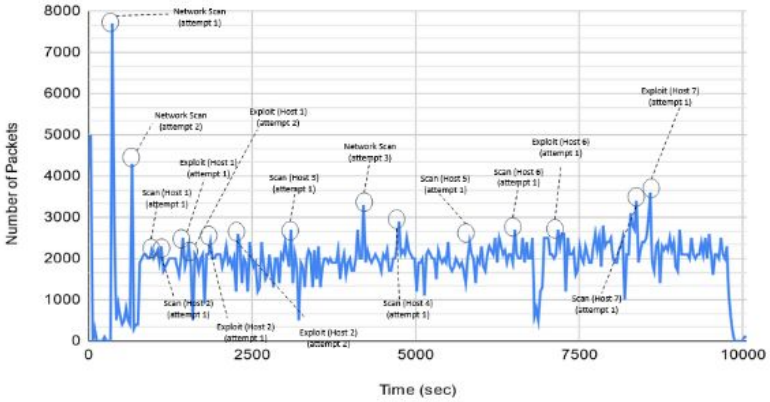


(c) Number of Exploit Attempts and Successful Exploits

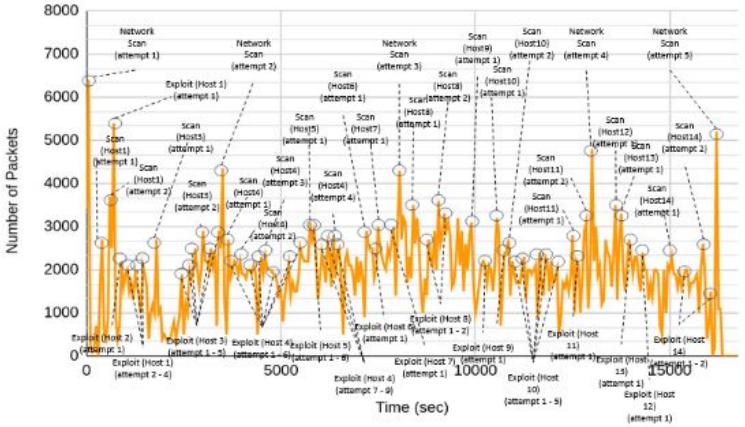


(d) Proportion of Time Spent on Reconnaissance

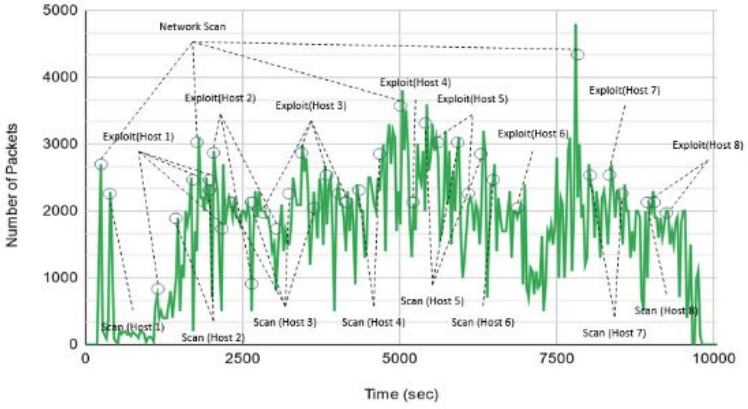
Evaluation of *CDGym*



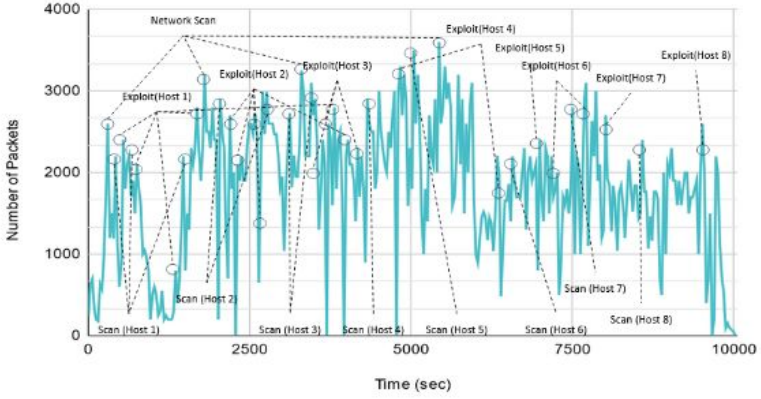
(a) Behavior Analysis with Non-Deceptive Network



(b) Behavior Analysis with D1



(c) Behavior Analysis with D2



(d) Behavior Analysis with D3

Future Work

- Support for host-based deception measures.
- Behavioral analysis features.

Conclusion

- Application of game-theoretic cyber deception in real-world environments suffers from the lack of reproducibility, measurability, and adaptability.
- We designed and implemented *CDGym*, a generic and model-agnostic platform that addresses the challenges.
- *CDGym* is capable of analyzing network-based deception strategies.

Thank you!