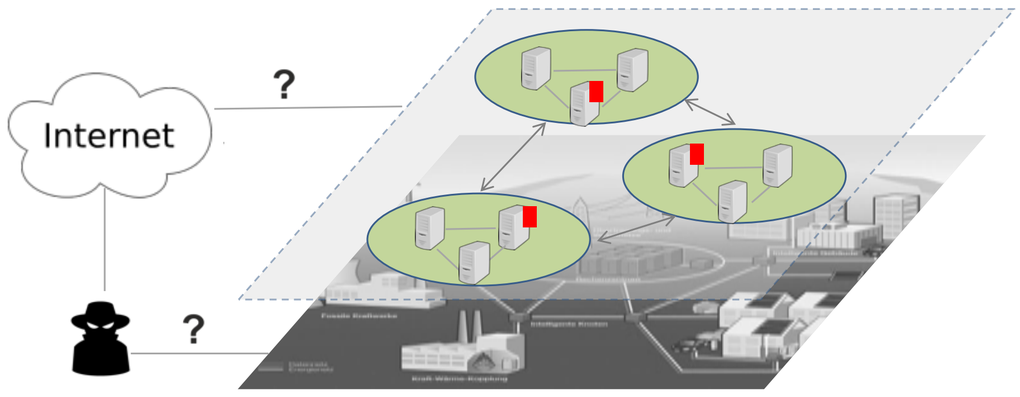
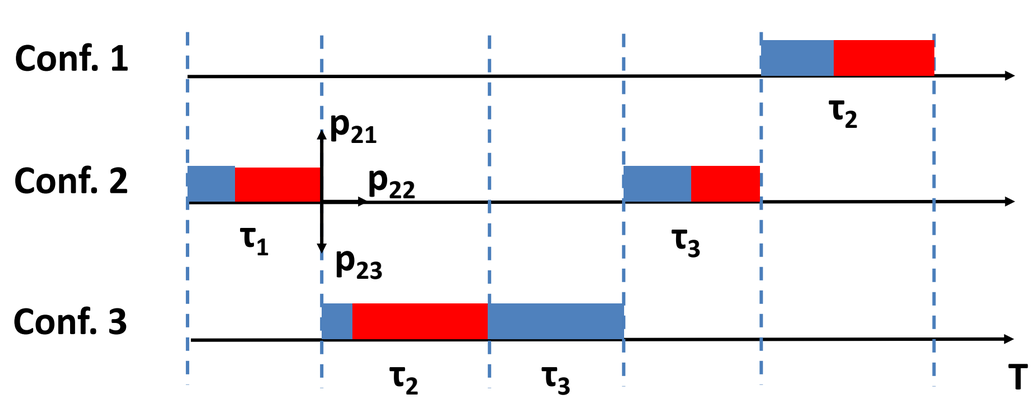
Towards Robust Moving Target Defense: A Game Theoretic and Learning Approach

Zizhan Zheng, Department of Computer Science, Tulane University

http://www.cs.tulane.edu/~zzheng3/projects/NSF-SaTC-2018.html





Challenge:

Interplay between system dynamics, security, and incentives

Intelligent, stealthy, and persistent attacks

Necessity of coordinating multiple defenders

Scientific Impact:

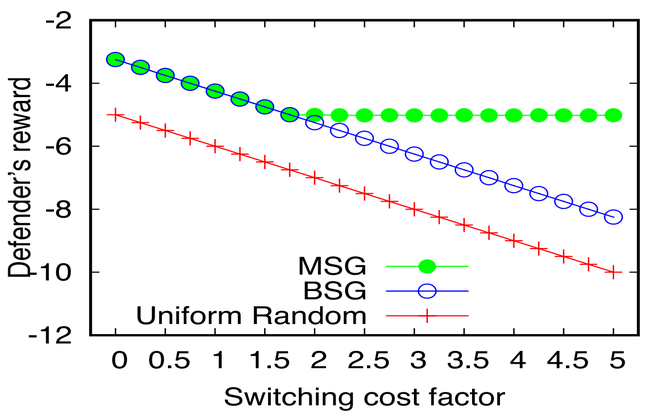
A rigorous approach to the design and analysis of active defense against stealthy attacks

Deep insights on information asymmetry and the use of continuous learning in cyber attack and defense

Solution:

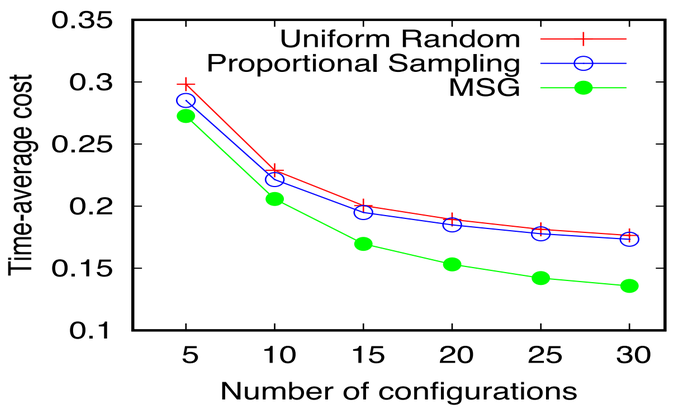
Markovian Stackelberg Games for state-dependent defense

- Non-trivial extension of Bayesian Stackelberg Games
- Configuration-dependent loss and switching cost



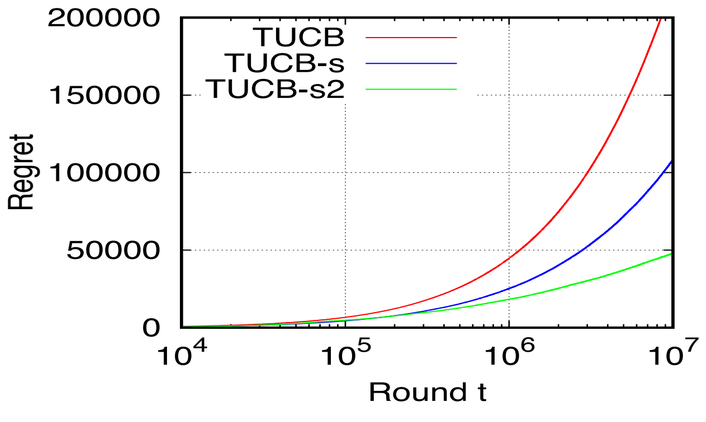
Joint spatial and temporal decisions in large-scale MTD

- Configuration and time dependent loss
- Approximation solution for large-scale MTD



Thwarting unknown attacks via online learning

- Focusing on temporal decisions
- Time associative bandits with dependent arms



Broader Impact:

A cross-disciplinary approach to cybersecurity

New game theoretic and learning methods for decision making beyond cybersecurity

Education:

1 graduate student and 1 undergraduate coordinate major student involved in Year 1

1 postdoc and 2 undergraduate coordinate major students joining in Year 2

Potential Impact:

Both system/network administrators and end users can potentially benefit from the resulting research

Results will be incorporated into a new course on analytic approaches to cybersecurity