TEXAS STATE UNIVERSITY
SAN MARCOS
The rising STAR of Texas

Securing Mobile Cyber-Physical Systems against Stealthy Attacks

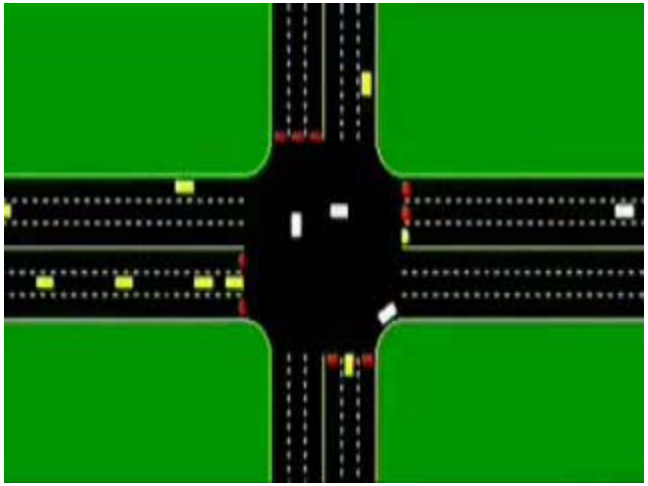
Mina Guirguis

NSF US/Mideast Workshop on Trustworthiness in Emerging Distributed Systems and Networks
June 4 2012

Mobile Cyber-Physical Systems

- Mobile Cyber-Physical Systems (CPSs)
  - Mobile physical elements that can sense, compute and communicate
- Applications:

Swarmanoid
European Commission



Intelligent Transportation Systems (UT-Austin)

Research vision

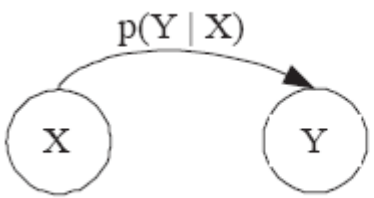
- Goal: ensure the safety and security of Mobile CPSs
- Challenges:
  - Wireless communication easier to jam/interfere with
  - Complexity opens backdoors for attackers
  - Attacks are not “random”, but are well orchestrated
- Offense strategies
  - Identifying optimal and suboptimal attack policies
  - Evading detection
- Defense strategies
  - Randomization: make the system less predictable

Methodology

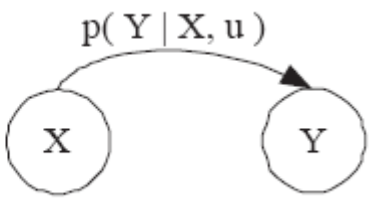
- Markov Decision Process
  - Sate of the system
  - Transitions
- Attacker
  - Tries to evolve the system into “bad” states
  - Pays a price when attacks
  - Gains reward when inflicts damage

$$\max_{\mu_1,\mu_2,\ldots} E\left[\sum_{k=1}^{T} R(k)|I_k\right]$$

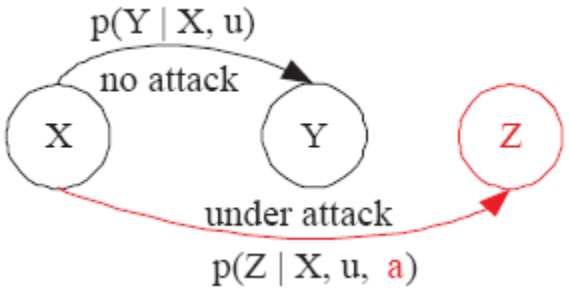
- Randomized defense



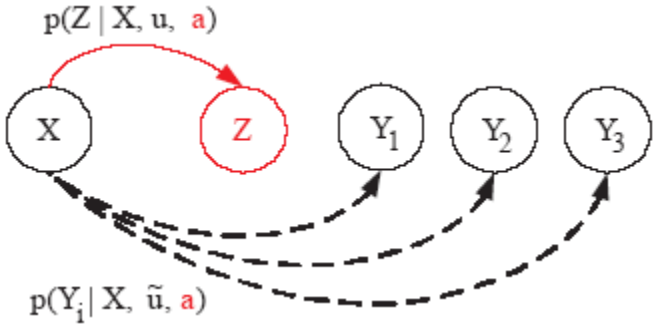
[Independent]



[controlled]



[attack effect]



TEXAS STATE UNIVERSITY
SAN MARCOS
The rising STAR of Texas

Securing Mobile Cyber-Physical Systems against Stealthy Attacks

- Funded by NSF

Thank you!

NSF US/Mideast Workshop on Trustworthiness in Emerging Distributed Systems and Networks
June 4 2012