Norsk Regnesentral
NORWEGIAN COMPUTING CENTER

# An Evolutionary Game for Integrity Attacks and Defenses for Advanced Metering Infrastructure

Svetlana Boudko

Habtamu Abie

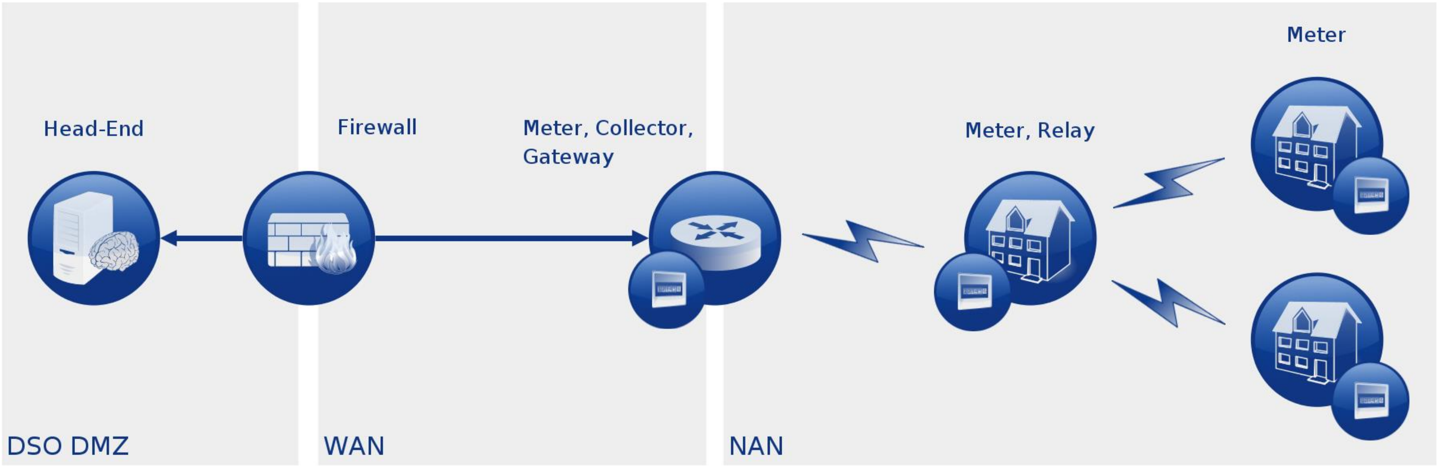
IFI, Oslo

13.09.2018

# Outline

- Background & Motivation
- Evolutionary Game Theory
- AMI model
- Evolutionary integrity game
- Usage example
- Summary & future work

# Advanced Metering Infrastructure




- a part of smart grid framework
- collect, process & report data from large number of devices
- monitoring, alarm, billing, remote home control, intrusion detection, fault tolerance, software updates
- optimize the usage of electrical resources

# Motivation

- Data integrity is one of the concerns
  - Deng, R., Xiao, G., Lu, R., Liang, H., Vasilakos, A.V.: False data injection on state estimation in power systems attacks, impacts, and defense: A survey.IEEE Transactions on Industrial Informatics 13(2), 411{423 (April 2017).
- Message authentication schemes are computing-intensive
- Numerous wireless devices with limited resources
- Trading off security and computational constraints
  - AMIs must carefully decide when, what, and how to authenticate

# Problem Outline

- ► Multiple adversaries can coexist, cooperate and evolve
  - ▪ To meet the challenges of possible intelligent cooperation between adversaries and their ability to learn from each other experience
- ► Defenders can also cooperate and learn from each other experience the effectiveness of defensive strategies should be addressed in multiple defender scenarios
  - ▪ To help nodes of an AMI to cooperate and to work out a joint protection

We need a tool that analyses behavior & models dynamics

- ▪ Classical GT: used for decision making in smart grid frameworks but it is a static approach and it is rational
- ▪ EGT: borrowed notation from CGT but logic is different!

# Main Concepts of EG

- A (large) population of players
  - Evolving from generation to generation
- Two key elements that govern evolution
  - Mutation
  - Selection
- Mutation: Evolutionary Stable Strategy
  - a group of players choosing ESS will not be replaced by players that choose a different strategy
- Selection: Replicator dynamics
  - governs evolution of populations

# Evolutionary Stable Strategy

- Main group of players in a population chooses strategy $x$
- Small group of mutants whose population share is $\epsilon$ choosing a different strategy $y$
- Strategy $x$ is evolutionary stable if it is robust against any alternative mutant strategies $y$

$$U(x, (1-\epsilon)x + \epsilon y) \geq U(y, (1-\epsilon)x + \epsilon y)$$

# Hawk-Dove Game example

- Players competing for a resource $v$ at cost $c$
- 2 possible strategies: hawk and dove
- If $v > c$, then the players choose “Hawk”

Payoff matrix

| | Hawk | Dove |
|---|---|---|
| Hawk | $(^1/_2\,(v - \mathrm{c}), {}^1/_2\,(v - \mathrm{c}))$ | $(v, 0)$ |
| Dove | $(0, v)$ | $(^1/_2\,v, {}^1/_2\,v)$ |

# Suppose:

- A population playing “Dove”
- A small group of players (mutation) starts playing “Hawk”
- This group will invade the population, because they will have greater payoff.

# Replicator dynamics

- Dynamics of populations that lead to evolutionarily stable strategies
- We consider:
  - Population of N players
  - Set of strategies S.
  - $N_i$ of players assigned strategy $S_i$
  - Proportion of population playing strategy $S_i$ at time $t$

$$x_i(t) = {}^{N_i}/_{N}$$

  - Each period, a player is randomly matched with another player and they play a game
    - Payoff matrix $P_{i,j}$

# Replicator dynamics

- Expected utility for strategy $s_i$ given the population distribution X

$$U_{E,i}(s_i, X) = \sum_{j=0}^{N} x_j(t) P_{i,j}$$

- Average utilily

$$\overline{U}_A(X) = \sum_{i=0}^{N} x_i(t)\, U_{E,i}$$

# Replicator dynamics

- Dynamics of the population share $x_i$

$$\frac{\partial x_i(t)}{\partial t} = (U_{E,i}(s_i, X) - \bar{U}_A(X)\,)x_i(t)$$

- ESS can be reached at

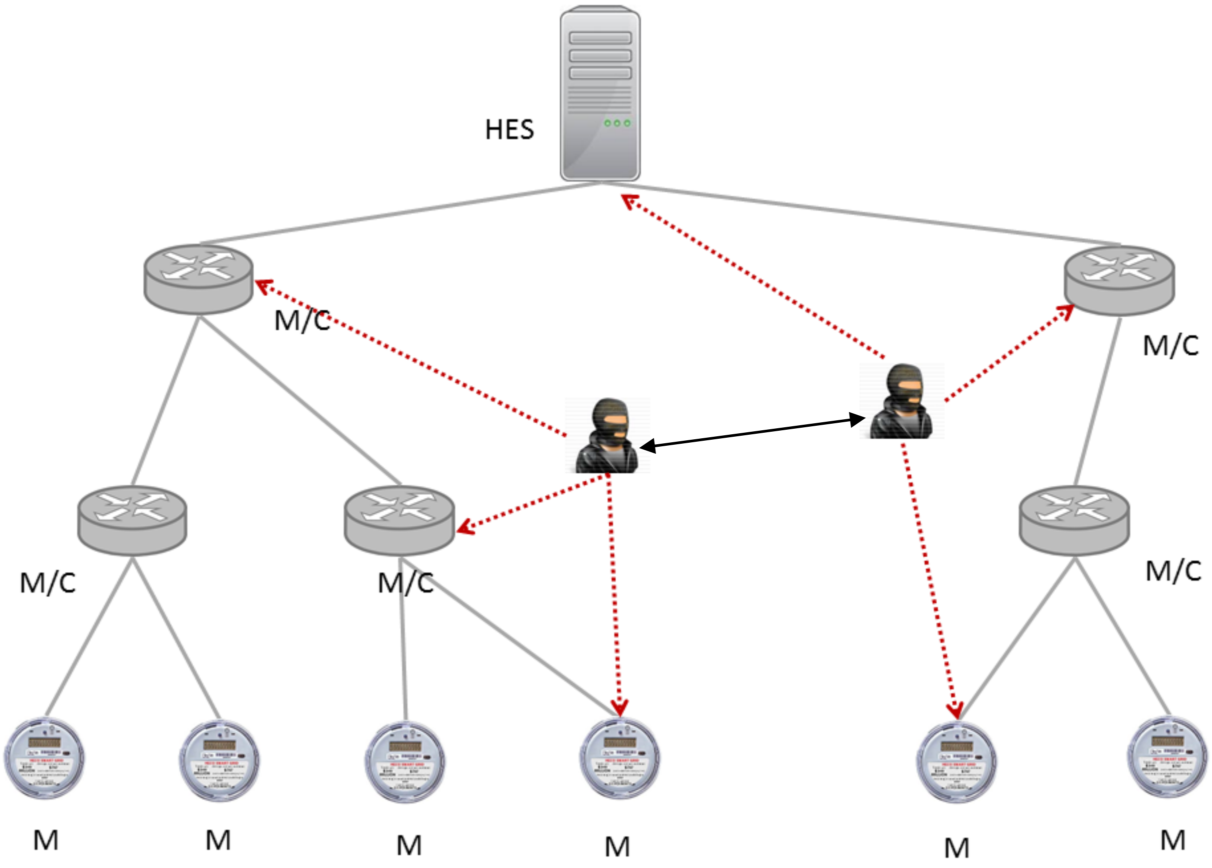
$$\frac{\partial x_i(t)}{\partial t} = 0$$

- Intuitively:
  - The greater is the utility of a strategy relative to the average utility, the greater is its relative increase in the population.
  - The reproduction rate of each strategy depends on the payoff (players will switch to strategy that leads to higher payoff)

# Why would EG matter?

- Evolutionary stable strategy (ESS) is a refinement to the Nash equilibrium
  - Nash equilibrium is not necessarily efficient, (**Dubey, Pradeep. "Inefficiency of Nash Equilibria."** ***Mathematics of Operations Research*****, vol. 11, no. 1, 1986** )
  - multiple Nash equilibria in a game
- The strong rationality assumption is not required
- Evolutionary game is based on an process
  - is dynamic in nature
  - can model and capture the adaptation of players to change their strategies and reach equilibrium over time
  - populations can evolve according to the relative success of individual strategies compared to the overall population

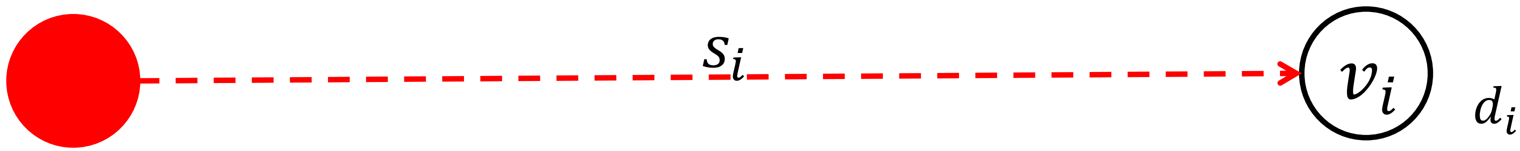
# AMI Model



# EG formulation: integrity strategy space

Attacker *k (Cost to attack)*

Node *i (Cost to defend)*




$$s \in [0,1]^N$$

$$d \in [0,1]^N$$

# Game formulation

Probability distributions over strategy spaces

Attackers (K strategies): $\sigma(t) = (\sigma_0(t), \ \dots, \sigma_K(t))$

Defenders (M strategies): $\delta(t) = (\delta_0(t), \ \dots, \delta_M(t))$

Node $i$ payoffs for $(k, m)$:

$$U_{D_i} = -\left(v_i \times (1 - d_i^m) \times s_i^k + s_i^k \times c_i^d\right) - \sum_{j=0}^{\theta(i)} v_j \times (1 - d_j^m) \times s_i^k$$

$$U_{A_i} = v_i \times (1 - d_i^m) \times s_i^k + s_i^k \times c_i^a + \sum_{j=0}^{\theta(i)} v_j \times (1 - d_j^m) \times s_i^k$$

Payoffs: $U_{D,A}^{k,m} = \sum_{i=0}^{N} U_{D_i/A_i}$

# Game formulation

Expected utilities

$$U_{EA}(s_k, \delta) = \sum_{j=0}^{M} \delta_j(t) U_A^{k,m}$$

$$U_{ED}(d_m, \sigma) = \sum_{j=0}^{K} \sigma_j(t) U_D^{k,m}$$

Average utilities

$$\bar{U}_A(\sigma, \delta) = \sum_{i=0}^{K} \sigma_i(t)\, U_{EA}(s_k, \delta)$$

$$\bar{U}_D(\sigma, \delta) = \sum_{i=0}^{M} \delta_i(t)\, U_{ED}(\sigma, d_m)$$

# Replicator Equation

Attackers at time *t*:

$$\frac{\partial \sigma_k(t)}{\partial t} = (\bar{U}_A(\sigma, \delta) - U_{EA}(s_k, \delta))\sigma_k(t)$$

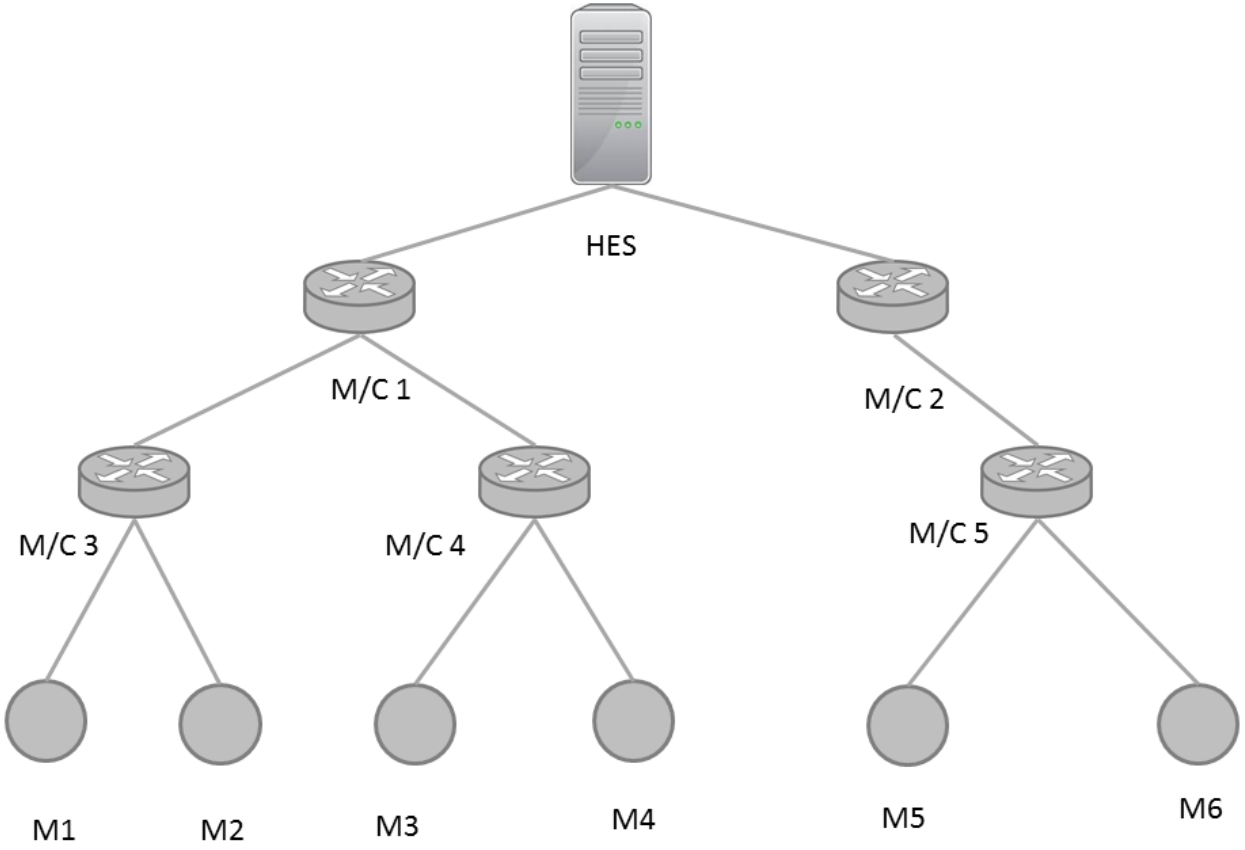
Average expected utility

Expected utility for strategy *i*

Defenders at time *t:*

$$\frac{\partial \delta_m(t)}{\partial t} = (\bar{U}_D(\sigma, \delta) - U_{ED}(d_m, \sigma))\delta_m(t)$$

# Case study: AMI topology & setup



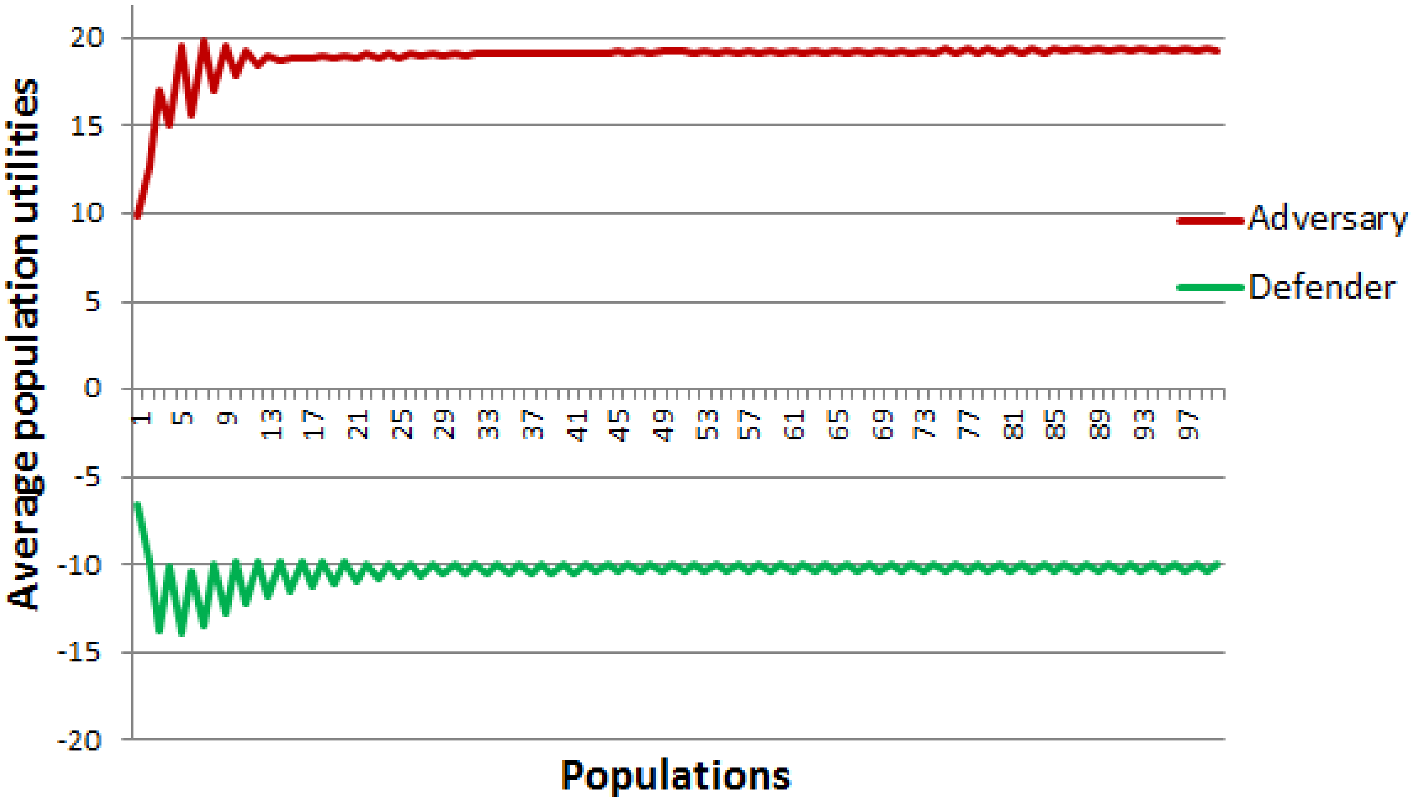
# Case study: Game parameters

- 3 attack strategies
  - not attack node
  - moderate attack
  - fully attack node
- 3 defense strategies
  - not protect node
  - moderate protect
  - fully protect node

# Case study: Game parameters

| Node | $v_i$ | $C_i^a$ | $C_i^d$ | $r_d^*$ | $r_a^*$ |
|---|---|---|---|---|---|
| #1 | 22.00 | 10.00 | 2.00 | 0.310789 | 0.340919 |
| #2 | 14.00 | 6.00 | 1.00 | 0.354535 | 0.068735 |
| #3 | 8.00 | 6.00 | 2.00 | 0.071618 | 0.081986 |
| #4 | 6.00 | 1.00 | 0.50 | 0.024598 | 0.055706 |
| #5 | 8.00 | 1.00 | 0.50 | 0.024853 | 0.062097 |
| #6 | 8.00 | 1.00 | 0.50 | 0.025344 | 0.064665 |
| #7 | 1.00 | 0.50 | 0.01 | 0.025899 | 0.047234 |
| #8 | 2.00 | 0.50 | 0.01 | 0.02673 | 0.046081 |
| #9 | 3.00 | 0.50 | 0.01 | 0.027738 | 0.047446 |
| #10 | 1.50 | 0.50 | 0.01 | 0.02642 | 0.045991 |
| #11 | 1.00 | 0.50 | 0.01 | 0.02673 | 0.047236 |
| #12 | 4.00 | 0.50 | 0.01 | 0.027738 | 0.049582 |

# Evolution of average utilities

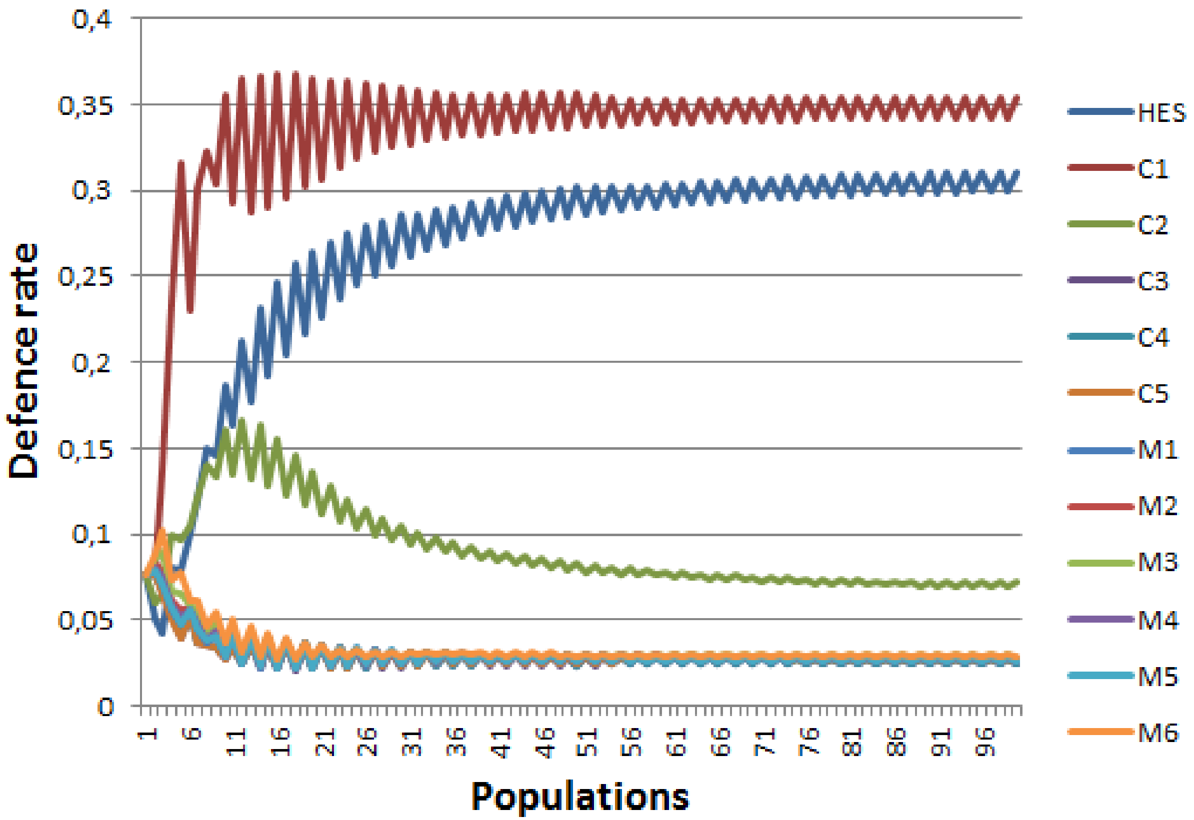


# Average attack and defense rates

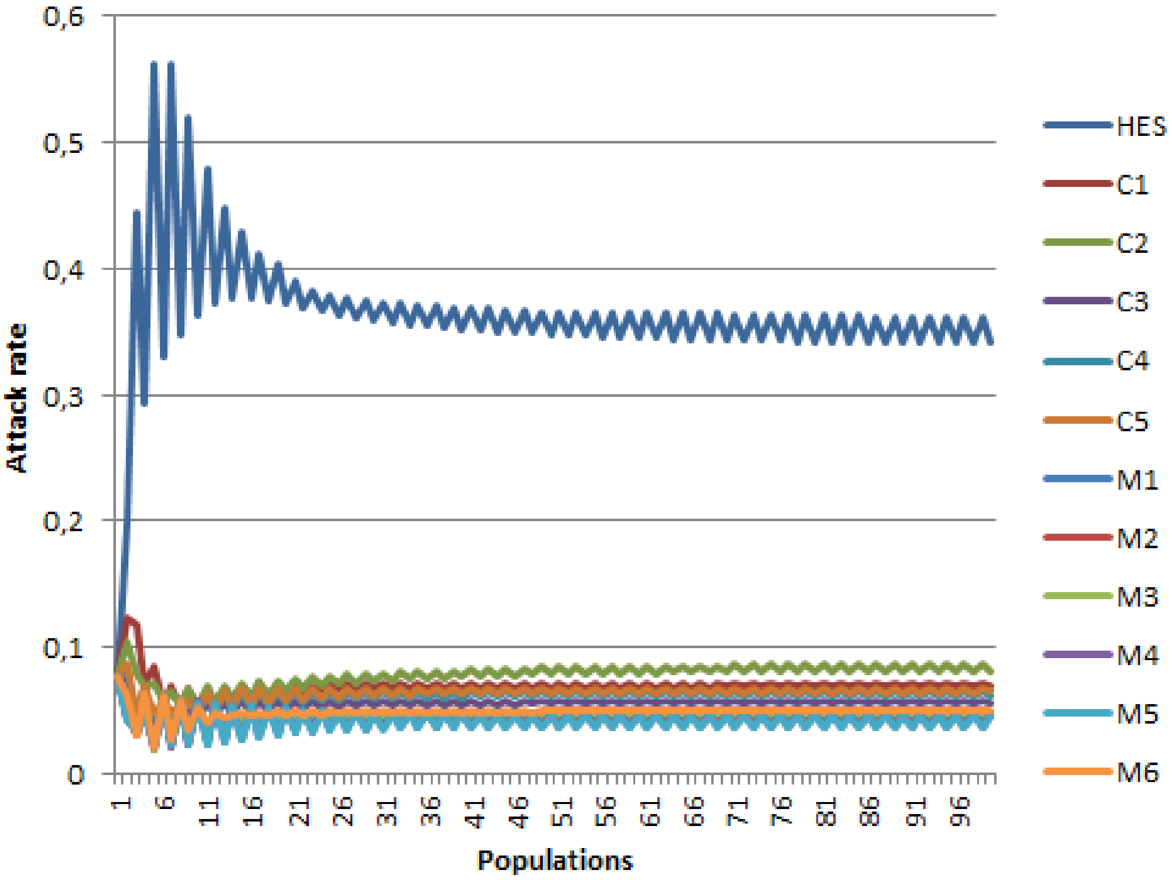
$$R_i^A(t) = \sum_{k=0}^{K} s_i \sigma_m$$

$$R_i^D(t) = \sum_{k=0}^{K} d_i \delta_k$$

# Evolution of defence rate



# Evolution of attack rate



# Summary and future work

- Modeled attacks/defenses on data integrity as an evolutionary game
- Studied the interactions between the attackers and the AMI nodes
- Larger trees for AMIs (Scalability!)
- Dynamic tree as option for defender's strategy space
- How to use the results and how to adapt defense in real time?
- Combine with machine learning for benchmarking and optimization

# References


- J M. Smith. 1972. Game theory and the evolution of fighting.
- J.M. Smith. 1982. Evolution and the Theory of Games. Cambridge University Press.
- Jörgen W. Weibull. 1995. Evolutionary game theory. MIT Press, Cambridge, MA.
- Nowak, M. A. *Evolutionary Dynamics: Exploring the Equations of Life*. Belknap Press of Harvard University Press, 2006.
- M. Tambe, M. Jain, J. A. Pita, and A. X. Jiang. 2012. Game theory for security: Key algorithmic principles, deployed systems, lessons learned. In 2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton).
- Peter D. Taylor and Leo B. Jonker. 1978. Evolutionary stable strategies and game dynamics. Mathematical Biosciences 40, 1.
- Pavan Vejandla, Dipankar Dasgupta, Aishwarya Kaushal, and Fernando Nino. 2010. Evolving Gaming Strategies for Attacker-Defender in a Simulated Network Environment. In Proceedings of the 2010 IEEE Second International Conference on Social Computing (SOCIALCOM '10).
- Kun Wang, Miao Du, Dejun Yang, Chunsheng Zhu, Jian Shen, and Yan Zhang. 2016. Game-Theory-Based Active Defense for Intrusion Detection in Cyber-Physical Embedded Systems. ACM Trans. Embed. Comput. Syst.
- Xiao Wang, Yinfeng Wu, Yongji Ren, Renjian Feng, Ning Yu, and Jiangwen Wan. 2013. An Evolutionary Game-Based Trust Cooperative Stimulation Model for Large Scale MANETs.