

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

Svetlana Boudko

Habtamu Abie

IoTSec Meeting, Oslo

June 06, 2018



Outline

- ▶ Motivation
- ▶ AMI as a dynamic tree structure
- ▶ Evolutionary integrity game
- ▶ Usage example
- ▶ Summary & future work

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
- ▶ Resources
 - numerous wireless devices with limited resources
- ▶ Trading off security and computational constraints
 - AMIs must carefully decide when, what, and how to authenticate

Why use evolutionary game?

- ▶ 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,

Why use evolutionary game?

- ▶ Not a statistic approach
- ▶ EG models a dynamic in populations of players
 - populations evolve according to the relative success of individual strategies compared to the overall population

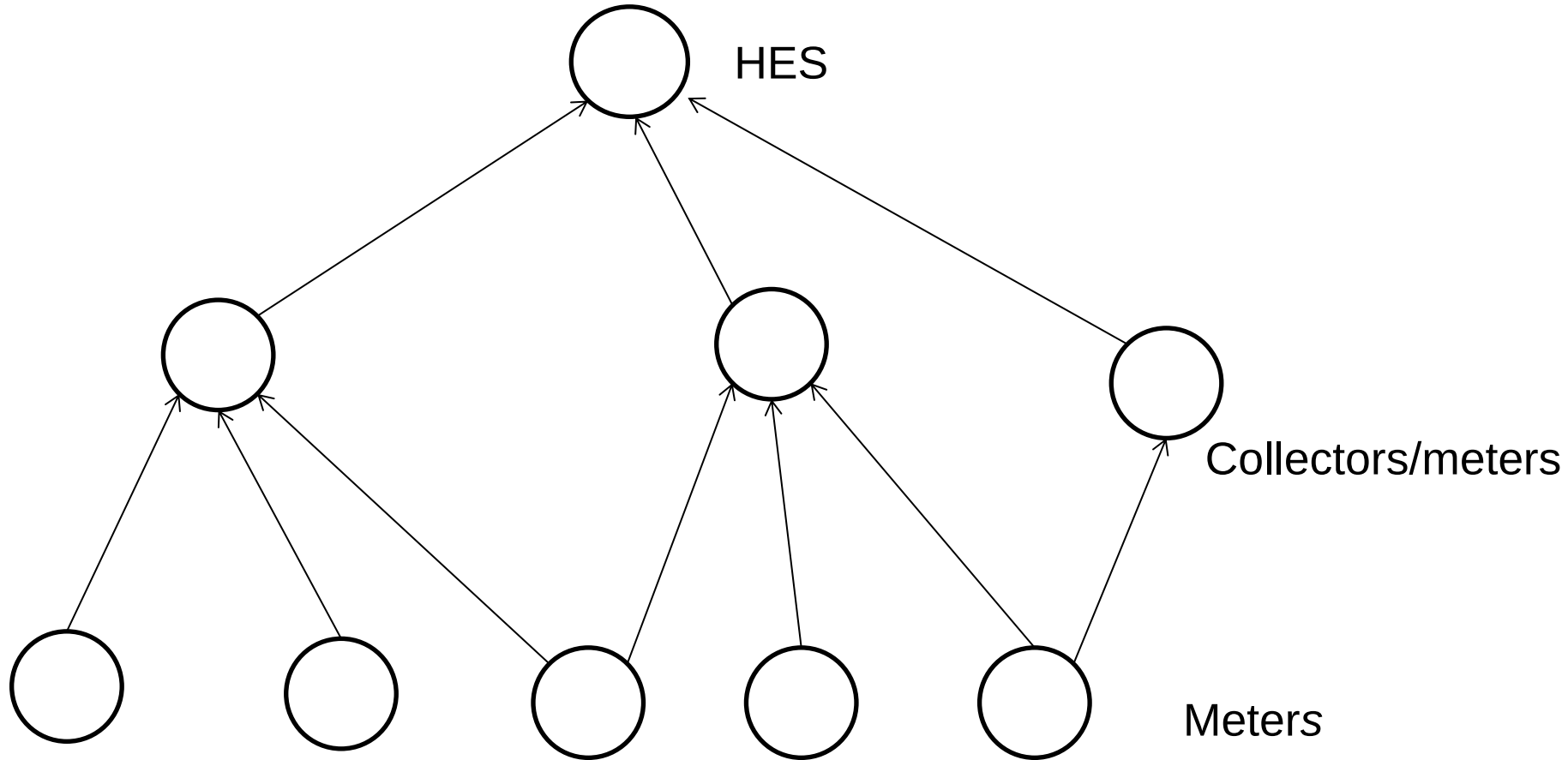
Two key elements:

- ▶ Evolutionary Stable Strategy x is robust against any alternative mutant strategies ϵ

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

- ▶ Replicator equation governs evolution of populations

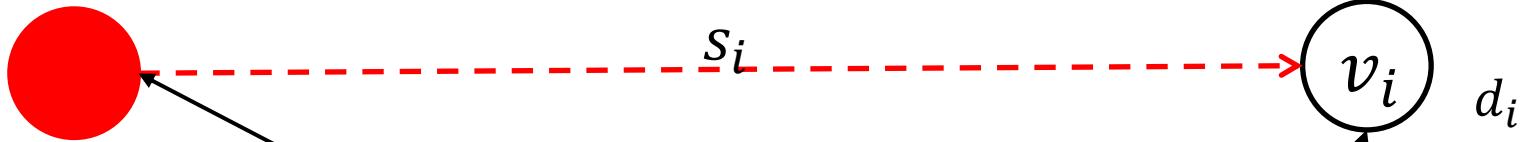
AMI as a dynamic tree structure



EG formulation: integrity strategy space

Attacker k (Cost to attack)

Node i (Cost to defend)



$$S = \left\{ s \in [0,1]^N : \sum_{i=1}^N s_i \leq 1 \right\}$$

$$D = \left\{ d \in [0,1]^N : \sum_{i=1}^N d_i \leq 1 \right\}$$

Game formulation

Attackers

Defenders

Probability distributions over strategy spaces

$$\sigma(t) = (\sigma_0(t), \dots, \sigma_1(t))$$

$$\delta(t) = (\delta_0(t), \dots, \delta_n(t))$$

Expected utilities

$$U_A(s_i, \delta) = \sum_{j=0}^N \delta_j(t) U_A(s_i, d_j) \quad U_D(d_i, \sigma) = \sum_{j=0}^N a_j(t) U_D(s_j, d_i)$$

Average expected utilities

$$U_A(\sigma, \delta) = \sum_{i=0}^N \sigma_i(t) U_A(s_i, \delta) \quad U_D(\sigma, \delta) = \sum_{i=0}^N \delta_i(t) U_D(\sigma, d_i)$$

Replicator Equation

Attackers at time t :

$$\frac{ds_i(t)}{dt} = (U_A(s_i, \delta) - U_A(\sigma, \delta))s_i(t)$$

Expected utility for
strategy i

Average expected
utility

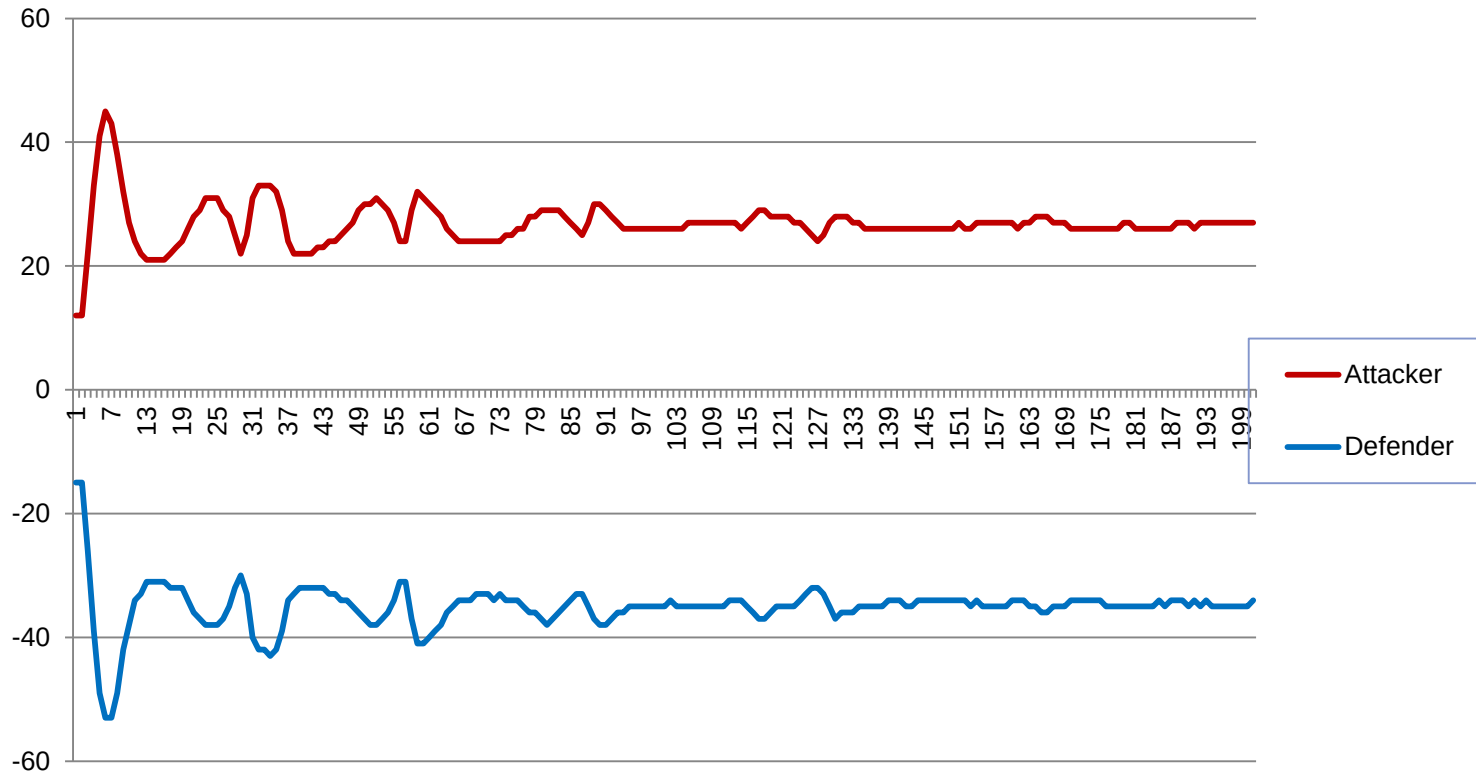
Defenders at time t :

$$\frac{dd_i(t)}{dt} = (U_D(d_i, \sigma) - U_D(\sigma, \delta))d_i(t)$$

Usage example

Node Number	Value	Cost of attack	Cost of defense
1	40.0	10.0	3.0
2	20.0	6.0	2.0
3	22.0	6.0	2.0
4	5.0	1.0	0.8
5	10.0	1.0	0.8
6	9.0	1.0	0.8
7	9.0	6.0	0.8
8-15 (meters)	2.0 – 3.0	0.1	0.8

Evolution of average utilities



Summary and future work

- ▶ Paper in progress: Evolutionary Game for Integrity Attacks and Defenses for Advanced Metering Infrastructure
 - Larger trees for AMIs
 - Dynamics as option for defender's strategy space
 - Game analysis security levels/strength/weakness for attacker and defender currently
- ▶ How to use the results and how to adapt defense in real time?
- ▶ Combine with machine learning

