Evolutionary game theory for modelling confidentiality in an Advanced Metering Infrastructure

Peder Aursand   Habtamu Abie

August 30, 2017

Outline

- Game Theory and Evolutionary Game Theory
- AMI as a tree structure
- Confidentiality game
- Case study and simulation results

General game theory

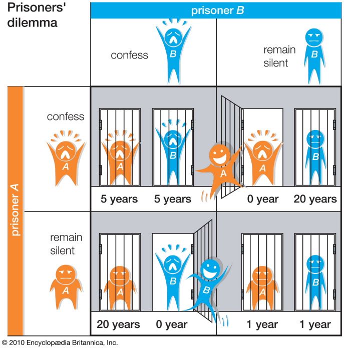
A game consists of N players, each of whom is free to choose a strategy $s_i \in S_i$, where S_i is the strategy space of the i'th player.

Associated with every player there is a utility function $\mathcal{U}_i : S \to \mathbb{R}$, where $S = S_1 \times \cdots \times S_N$.

A Nash equilibrium is a strategy set $s^* \in S$ such that

$$\mathcal{U}_i(s_i^*, s_{-i}^*) \geq \mathcal{U}_i(s_i, s_{-i}^*) \quad \forall i, s_i \in S$$

Example: Prisoners dilemma



Evolutionary game theory

Game theory combined with survival of the fittest

We consider a population of players employing different strategies. They are represented by a probability distribution over the strategy space

$$P_i(s_i) : S_i \rightarrow [0, 1]$$

Evolutionary game theory

Game theory combined with survival of the fittest

We consider a population of players employing different strategies. They are represented by a probability distribution over the strategy space

$$P_i(s_i) : S_i \to [0, 1]$$

Inspired by natural selection, the populations evolve according to a *replicator equation*

$$\frac{\mathrm{d}}{\mathrm{d}t} P_i(s_i) = \Big(\pi_i(s_i, P_{-i}) - \sigma_i(P) \Big) P_i(s_i)$$

Evolutionary game theory

Game theory combined with survival of the fittest

We consider a population of players employing different strategies. They are represented by a probability distribution over the strategy space

$$P_i(s_i) : S_i \to [0, 1]$$

Inspired by natural selection, the populations evolve according to a *replicator equation*

$$\frac{\mathrm{d}}{\mathrm{d}t} P_i(s_i) = \Big(\pi_i(s_i, P_{-i}) - \sigma_i(P)\Big) P_i(s_i)$$

- $\pi_i(s_i, P_{-i})$: Expected utility when using strategy s_i in current population

Evolutionary game theory

Game theory combined with survival of the fittest

We consider a population of players employing different strategies. They are represented by a probability distribution over the strategy space

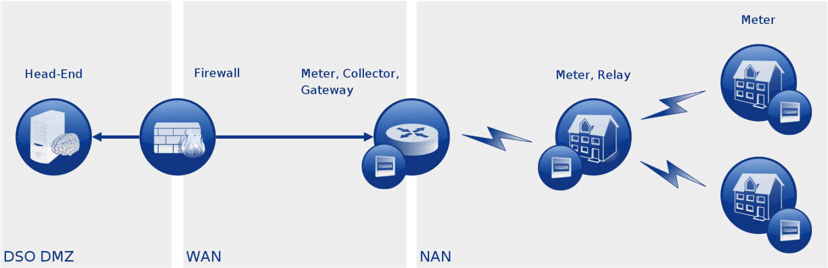
$$P_i(s_i) : S_i \to [0, 1]$$

Inspired by natural selection, the populations evolve according to a *replicator equation*

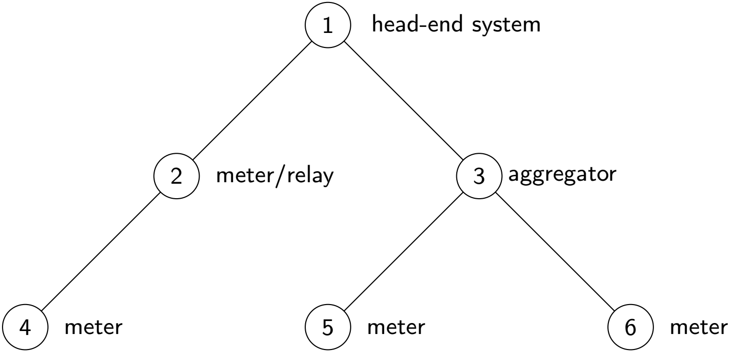
$$\frac{\mathrm{d}}{\mathrm{d}t} P_i(s_i) = \Big(\pi_i(s_i, P_{-i}) - \sigma_i(P)\Big) P_i(s_i)$$

- $\pi_i(s_i, P_{-i})$: Expected utility when using strategy s_i in current population
- $\sigma_i(P)$: Average utility of player i in current population

Advanced Metering Infrastructure (AMI)



AMI as tree structure



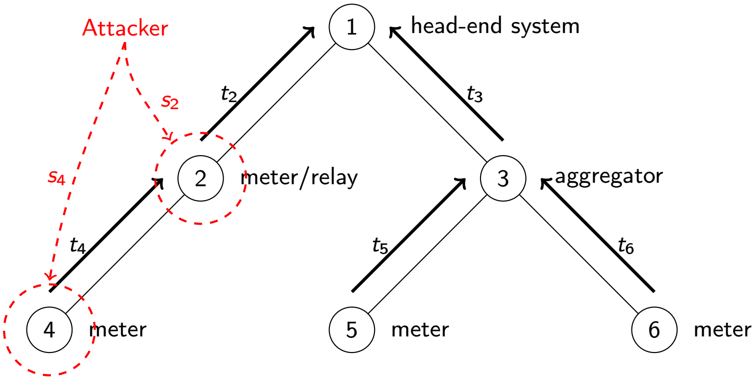
Parent node:

$$f(i) : \mathcal{N} \to \mathcal{N}$$

Set of children:

$$\mathrm{Ch}_i = \{j \in \mathcal{N} : \quad f(j) = i\}$$

Confidentiality game (Ismail et al. 2014)



attacker Tries to steal information undetected. For every node chooses probability of attack $s_i \in [0, 1]$

defender For every node chooses encryption level $t_i \in [0, 1]$

Every node has a value, a cost of defending, and a cost of attacking.

Confidentiality game (Ismail et al. 2014)

Attacker strategy space: s_i is the probability of attacking node i

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

Defender strategy space: t_i is the resources spent defending node i

$$T = \left\{ t \in [0,1]^N : \sum_{i=1}^{N} t_i \leq B_T \right\}$$

Confidentiality game (Ismail et al. 2014)

Attacker strategy space: s_i is the probability of attacking node i

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

Defender strategy space: t_i is the resources spent defending node i

$$T = \left\{ t \in [0,1]^N : \sum_{i=1}^{N} t_i \leq B_T \right\}$$

Attacker utility function:

$$\mathcal{U}_A(s,t) = \sum_{i=1}^{N} \Big(v_i \left(s_i + s_{f(i)}\right)(1-a)(1-t_i) - s_i C_{A,i} \Big)$$

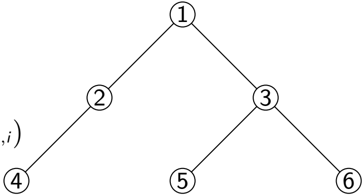
Defender utility function:

$$\mathcal{U}_D(t,s) = \sum_{i=1}^{N} -\Big(v_i \left(s_i + s_{f(i)}\right)(1-a)(1-t_i) - t_i C_{D,i} \Big)$$

Constraints and features

$$\mathcal{U}_A(s,t) = \sum_{i=1}^{N} \left(v_i\,(s_i+s_{f(i)})(1-a)(1-t_i)-s_i\,C_{A,i}\right)$$

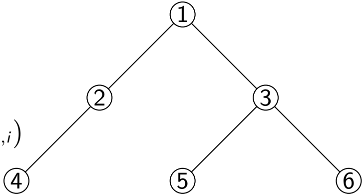
$$\mathcal{U}_D(t,s) = \sum_{i=1}^{N} -\left(v_i\,(s_i+s_{f(i)})(1-a)(1-t_i)-t_i\,C_{D,i}\right)$$



Constraints and features

$$\mathcal{U}_A(s,t) = \sum_{i=1}^{N} \left(v_i \left(s_i + s_{f(i)} \right)(1-a)(1-t_i) - s_i C_{A,i} \right)$$

$$\mathcal{U}_D(t,s) = \sum_{i=1}^{N} -\left(v_i \left(s_i + s_{f(i)} \right)(1-a)(1-t_i) - t_i C_{D,i} \right)$$

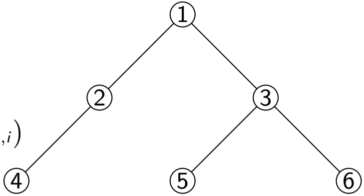


- Attacking an undefended node always pays off:

$$v_i(1-a) - C_{A,i} > 0$$

Constraints and features

$$\mathcal{U}_A(s,t) = \sum_{i=1}^{N} \left(v_i\,(s_i + s_{f(i)})(1-a)(1-t_i) - s_i\,C_{A,i}\right)$$
$$\mathcal{U}_D(t,s) = \sum_{i=1}^{N} -\left(v_i\,(s_i + s_{f(i)})(1-a)(1-t_i) - t_i\,C_{D,i}\right)$$



- Attacking an undefended node always pays off:

$$v_i(1-a) - C_{A,i} > 0$$

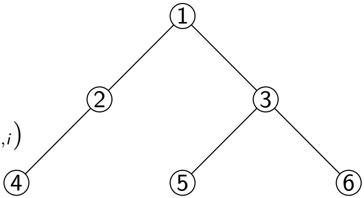
- Attacking a defended node pays off if and only if:

$$(1-a)\Big(v_i(1-t_i) + \sum_{j\in \mathbf{Ch}_i} v_j(1-t_j)\Big) > C_{A,i}$$

Constraints and features

$$\mathcal{U}_A(s,t) = \sum_{i=1}^{N} \left(v_i\,(s_i + s_{f(i)})(1-a)(1-t_i) - s_i C_{A,i}\right)$$

$$\mathcal{U}_D(t,s) = \sum_{i=1}^{N} -\left(v_i\,(s_i + s_{f(i)})(1-a)(1-t_i) - t_i C_{D,i}\right)$$



- Attacking an undefended node always pays off:

$$v_i(1-a) - C_{A,i} > 0$$

- Attacking a defended node pays off if and only if:

$$(1-a)\Big(v_i(1-t_i) + \sum_{j \in \mathbf{Ch}_i} v_j(1-t_j)\Big) > C_{A,i}$$

- Defending an attacked node pays off if and only if:

$$s_i > s_i^* = \frac{C_{D,i}}{v_i(1-a)}$$

Evolutionary confidentiality game

Discrete attack and defence strategy space

$$s^k = \left(\frac{k_1}{K}, \ldots, \frac{k_N}{K}\right) \qquad t^k = \left(\frac{k_1}{K}, \ldots, \frac{k_N}{K}\right) \qquad k_i \in \{0, \ldots, K\} \tag{1}$$

Evolutionary confidentiality game

Discrete attack and defence strategy space

$$s^k = \left(\frac{k_1}{K}, \dots, \frac{k_N}{K}\right) \qquad t^k = \left(\frac{k_1}{K}, \dots, \frac{k_N}{K}\right) \qquad k_i \in \{0, \dots, K\} \tag{1}$$

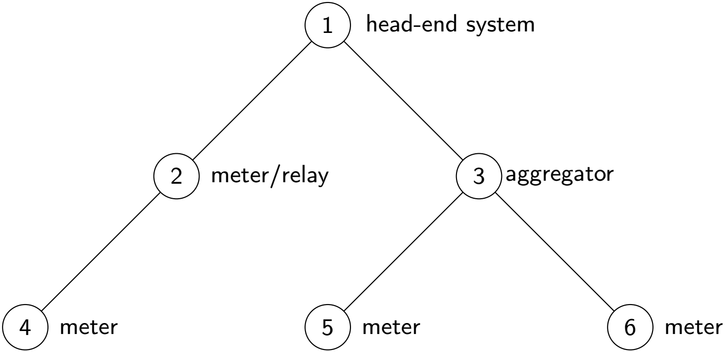
Evolution of attackers:

$$\frac{\mathrm{d}P_s}{\mathrm{d}t}\left(s^k\right) = \left[\pi_A\left(s^k, P_t\right) - \sigma_A(P_s, P_t)\right] P_s\left(s^k\right) + \delta_s^k$$

Evolution of defenders:

$$\frac{\mathrm{d}P_t}{\mathrm{d}t}\left(t^k\right) = \left[\pi_D\left(t^k, P_s\right) - \sigma_D(P_t, P_s)\right] P_t\left(t^k\right) + \delta_t^k$$

Case study

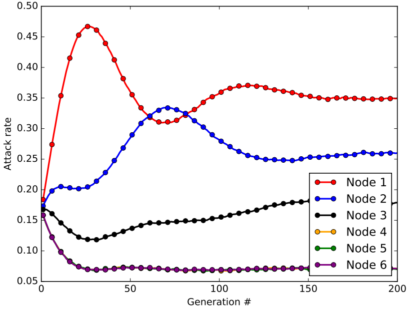


Node	v_i	$C_{A,i}$	$C_{D,i}$
#1	12.0	6.0	1.2
#2	6.0	0.01	0.8
#3	6.0	3.0	0.6
#4	3.0	0.01	0.8
#5	3.0	0.01	0.8
#6	3.0	0.01	0.8

Results: Evolution of attack and defence rates

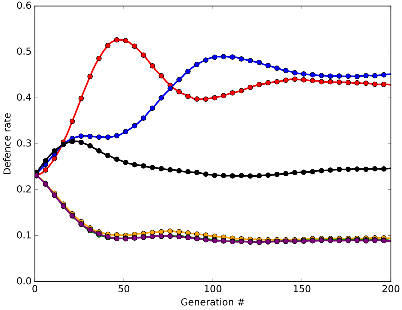
Attack rate:

$$A(i) = \sum_{k \in \Omega_s^K} s_i^k P_s(s^k)$$



Defence rate:

$$D(i) = \sum_{k \in \Omega_t^K} t_i^k P_t(t^k)$$



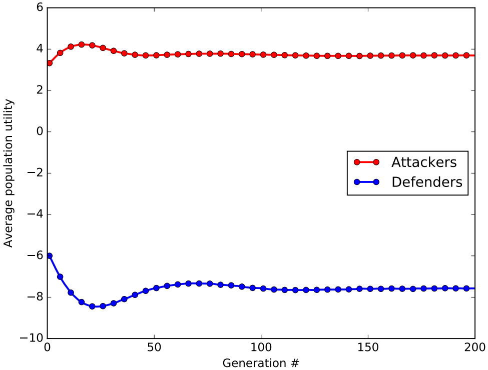
Results: Evolution of utility

Average attacker utility:

$$\sigma_A(P_s, P_t) = \sum_{k \in \Omega_s^K} \pi_A\left(s^k, P_t\right) P_s\left(s^k\right)$$

Average defender utility:

$$\sigma_D(P_t, P_s) = \sum_{k \in \Omega_t^K} \pi_D\left(t^k, P_s\right) P_t\left(t^k\right),$$



If evolutionary game theory is the answer, then what is the question?

Given a realistic model and a real case, we hope evolutionary game theory can help answer:

- What are the most attractive targets in the AMI?
- Will changes introduce weaknesses?
- What is the expected (or worst) outcome given a set of deployed security measures?
- How will a rational attacker behave given the current security measures?
- Which nodes should you prioritize defending?
- How to adapt defence in real time?

Where do we go from here?

Paper in progress: *Evolutionary game theory for modelling confidentiality in an Advanced Metering Infrastructure*

Future work:

- End-to-end encryption
- Bigger AMI networks
- More realistic node values, costs of encryption, costs of attacking
- Attacker has knowledge about encryption levels: Stackelberg game
- Modeling integrity in an AMI