Article

Evolutionary Game for Confidentiality in IoT-enabled Smart Grids

Svetlana Boudko [1], Peder Aursand [1] and Habtamu Abie [1]

[1] Norwegian Computing Center, P.O. Box 114 Blindern, Oslo, Norway, 0314; Svetlana.Boudko@nr.no (S.B.), peder.aursand@gmail.com (P.A.), Habtamu.Abie@nr.no (H.A.)[2] Affiliation 2; e-mail@e-mail.com

Abstract: We applied evolutionary game theory to extend a resource constrained security game model for confidentiality attacks in an Advanced Metering Infrastructure (AMI), which is a component of IoT-enabled Smart Grids. The AMI is modelled as a tree structure where each node aggregates the information of its children before encrypting it and passing it on to its parent. As a part of the model, we developed a discretization scheme for solving the replicator equations. The aim of this work is to explore the space of possible behaviours of attackers and to develop a framework where the AMI nodes adaptively select the most profitable strategies. Using this model, we simulated the evolution of a population of attackers and defenders on various cases resembling the real life implementation of AMI. We discuss in depth how to enhance security in AMI using evolutionary game theory either by a priori analysis or as a tool to run dynamic and adaptive infrastructure defence.

Keywords: adaptive security; evolutionary game; Internet of Things; advanced metering infrastructure; smart home

1. Introduction

Smart grid systems are intended to optimize the usage of electrical resources. These systems are complex Cyber-Physical Systems (CPS) exposed to various security challenges. An advanced metering infrastructure (AMI) is one of the main communication components of the smart grid that consists of communication networks connecting smart meters and collectors. The AMI collects and processes data from large number of devices and reports the results over communication networks. It can provide advanced services, such as monitoring, alarm, billing, remote home control, intrusion detection, fault tolerance, software updates [1]. Monitoring the smart grid can contribute to grid stability. The alarm functionality can address alarms for components failures in the grid and/or alarms in the Smart Home. The billing functionality could be for total consumption every hour or max usage. The remote home control functionality can control home devices by interacting with, e.g., the heating system. The intrusion detection functionality can monitor hacking attempts to the home, the control centre and any entity in between.

While providing advanced services, AMIs also introduce several security risks including attacks on confidentiality. The report [2] shows that connected Internet of Things (IoT)/CPS devices will grow at a CAGR of 19 percent with 20 billion related to the IoT in 2023. The rise of large scale interconnectedness and often outdated design of the devices present a significantly expanded attack surface. Despite the significant efforts in securing IoT/CPS-enabled smart grid systems, many remain vulnerable to various advanced and evolving cyber-attacks [3–5]. There are several reasons for this. IoT/CPS-enabled smart grid systems rely upon wireless networks. It makes them vulnerable for eavesdropping. These devices may also be unattended for prolonged periods of time leaving them vulnerable to physical attacks, and most devices limited in energy and computing power do not allow for the implementation and use of complex security schemes [6,7]. A recent survey [8] has showen that False Data Injection (FDI) attacks also threaten state estimation in smart grids.

Furthermore, adaptive attackers will adapt their strategies to the current security situation, and to newly deployed countermeasures. Such emerging attacks can become very sophisticated

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2020 doi:10.20944/preprints202011.0002.v1

and can be coordinated [9], persistent [10], collaborative or cooperative with specialized attack expertise [11]. Examples of such coordinated attacks include data injection attacks concurrently occurring from multiple adversaries [12], large-scale stealthy scans, stuxnet worm outbreaks and Distributed Denial-of-Service (DDoS). Such adaptive, collaborative or coordinated attacks require adaptive, collaborative or coordinated defences. Therefore, the confidentiality of AMI data must be protected within the AMI system, in transit or at rest, which requires significant collaboration, evolution and adaptation in the security of the AMI. Evolutionary game theory (EGT) lends itself to model the dynamic interplay between the way attackers adapt and evolve their behaviours as evolutionary attacks and the way defenders anticipate the unknown and prevent dynamic, adaptive and evolutionary attacks. Evolutionary game theory studies adaptive rules that govern dynamic behaviour. It offers, a solid basis for realistic and intelligent decision making in an uncertain world, describing how individuals make decisions and interact in complex environments in the real world.

The components in the AMI need to collaborate to achieve a common goal in collecting, aggregating, transmitting and securing the data. The data confidentiality attack in the AMI is unauthorized access to sensitive information between utilities and users by targeting the AMI components, such as smart meters, data concentrators, communication networks, and a central, or headend system. Users' consumption habits and other relevant information must be protected from access by unauthorized persons or companies. The data sets in the headend system must only be accessed by authorized systems or users. Confidentiality is therefore one of the primary concerns in AMI. As demonstrated in [13], integrity and confidentiality attacks cause monetary effects on the AMI which in turn have cascading effects to other interdependent critical infrastructures such as health, finance, telecoms. In this paper, we focus on evolutionary game for confidentiality attacks and defences for the AMI.

Previously, we have introduced an evolutionary game framework [14] that models evolving attacks and defenses in connection with data integrity for smart grid systems. The novel contributions of this paper are:

- the derivation of a numerical scheme,
- the simulations of the evolutionary game on realistic AMI cases for confidentiality,
- the identification of constraints, and
- analysis of the confidentiality evolutionary game.

The remainder of the paper is organized as follows. Section 2 gives a brief literature survey and presents theoretical background for this work. In Section 3 we introduce our system and game model, formulate the confidentiality game as an evolutionary game using replication dynamics, and discretize the evolutionary game model and derive a numerical scheme for solving the evolutionary dynamics. In Section 4, we carry out simulations on relevant AMI cases for confidentiality and demonstrate how this can be used to inform AMI security. The simulation results are presented and discussed in Section 5. Finally, we conclude and discuss the future work Section 6.

2. Related Work

The IoT/CPS system brings great benefits to the cyber physical IoT-enabled smart grids by connecting people, processes, services, devices and data. However, the rise of large scale interconnectedness presents a significantly expanded attack surface. There exist significant efforts to secure the IoT-enabled AMI, which is the core component of the smart grid. In this section we give a brief review of these efforts. The research that studies game theoretical approaches for modelling the evolving nature of cyber-attacks inside the IoT-enabled AMIs is not addressed sufficiently in the literature. In this section, we present the work on modelling security threats for IoT-enabled smart grids with constrained processingl resources. In this work, we use evolutionary game theory. Therefore, this section also provides a short introduction to game theory and related work regading applications of evolutionary game theory for IoT-enabled smart grid.

 doi:10.20944/preprints202011.0002.v1

The IoT-enabled AMI is an integrated system of smart meters, collectors, communications networks and data management systems which support the safe, efficient and reliable distribution of electricity and advanced functionality to energy customers [15]. Unfortunately, the power grids have been the target of sophisticated cyber-attacks which could lead to grid shutdown, cascading failures, damage to the infrastructure, and potential harm to people [16]. Such targeted attacks could have devastating effects on government, trade, commerce, banking, transportation and other important aspects, which rely on energy to operate. A compromise of AMI may also result in an invasion of privacy, and provide a surface from which to extract information from users such as Internet activity, financial, or health records [16]. The AMI poses several well known security threats [17–20].

As the Iot-enabled AMI is the core component of the smart grid, it is thus important to identifying the attack surface and protecting it from cyber-attacks. The cyber-attack surface of the AMI has been quantified and examined [16]. It is also important to measure the significance of threats and how they can transpire into attacks in the AMI environment. Different categories of attack types and analysis of the various countermeasures against these attacks have been studied [21]. A methodology for assessing security, privacy and dependability in a combined manner in the smart grid has been developed and measureable security in smart grids has been introduced [1]. A controlled Markov-Gaussian process has been suggested to minimize the damage of advanced persistent threats in cyber-physical systems [22]. He and Yan [23] provide a systematic review of the critical cyber-physical attack threats and defence strategies in the smart grid, and discuss a wide range of opportunities and challenges in enhancing energy security by maintaining the integrity of smart grid under complex cyber-physical attacks. Ismail et al. [24] presented a noncooperative game for attacks on data confidentiality for smart-grid AMI and studies the strategies of the attacker and the defender at the Nash equilibrium. Applying this model, the authors defined the optimal strategy of the defender and the minimum resources required for defending the assets.

Evolutionary game theory is a branch of game theory. Evolutionary game theory, rooted in classical game theory and the theory of evolution [25], has been effectively studied to model population dynamics in biology and economics domains but its application to smart grid security has not been fully exploited. Santos et al. [26] argue that by using a dynamical approach, such as evolutionary game theory, one is able to follow the self-organization process by which a population of individuals coordinates into a given behaviour. Hoffman et al. [27] argue that evolutionary dynamics is a powerful tool for specifying changes in strategies over time in a population. Quijano et al. [28] addressed the advantages of evolutionary game theory in the role of population games and evolutionary dynamics in distributed control systems. Ficici et al. [29] present a game-theoretic investigation of selection methods used in evolutionary algorithms. The three main advantages of using EGT in engineering problems and an outstanding advantage of distributed population dynamics compared to distributed learning algorithms are described in [28].

Evolutionary game has been successfuly applied to the areas of Advanced Persistent Threats (APTs), evolving interactions between an attacker and a defender, detecting DDOS, and wireless sensor networks. Alabdel Abass et al. [30] studied APTs that represent stealthy, powerful, long-term, and well-funded attacks against cyber systems, such as smart grids, data centres and cloud storage. The authors capture the long-term continuous behaviour of the APTs on the cloud storage devices using evolutionary game. Bouhaddi et al. [31] model the evolving interactions between an attacker and a defender in MANET as an evolutionary game. In this model, each player learns about the behaviour of its opponent over timeand adjusts its strategy. Vejandla et al. [32] present evolving gaming strategies for attacker-defender in a simulated network environment. Detection of DDoS attacks using an artificial immune system-inspired multi-objective evolutionary algorithm has been investigated in [33]. Evolutionary game theory has also been used for modelling wireless sensor networks [34–39]. An overview of evolutionary computation and other computational intelligence technology contributing to meet security challenges can be found in [3].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2020 doi:10.20944/preprints202011.0002.v1

Although our work is partly motivated by the related work above, there are some distinctions compared with them. The unique characteristics and usage scenarios of IoT-enabled AMI in the smart power grid introduce new security challenges. The increasing share of pervasive IoT devices which lack computing power, security, and privacy in such environments is a challenge - not to mention provisioning of adaptivity to tackle dynamicity and evolution. An accurate and resilient evolutionary game-based adaptive confidentiality assessment on IoT-enabled AMI entities is required. Given the dynamics in the AMI environment, the ability of the AMI nodes to adjust their confidentiality protection in response to their perception of the environment and the systems themselves should be provided. Although there are many research contributions about confidentiality in AMI systems, most of them have not considered these and fall short defining a framework for building dynamic and flexible defence for AMI with population dynamical methods for designing defence mechanisms for robust and reliable AMI cyber systems.

Our analysis shows that the presented related work mostly studies scenarios where a single adversary attacks one resource at a time. In reality, multiple attackers can cooperate and launch joint attacks. They can share their knowledge about previous attacks, learn from each other's experiences, and coordinate future actions by selecting successful strategies. The defenders can also collaborate and share the acquired experience to choose the optimal strategies for their defences. We recognise that the collaborations between multiple adversaries and multiple defenders have not been fully researched in the previous work. This motivates us to study and to apply evolutionary game theory to these advanced scenarios.

2.1. Evolutionary Game Theory

In this subsection, we give an overview of evolutionary game theory that is further used in our formulation of the AMI confidentiality game. While classical game theory has been traditionally applied to model attacks on smart grid systems, it is a static approach that computes Nash equilibria and the corresponding utilities for the participating players. The main idea behind classical game theory is how *rational individuals* are expected to behave in conflict situations.

Formally defined, a game consists of N players and a strategy space S. Each player can select a strategy $s_i \in S_i \in S$, where S_i is the strategy space of the i'th player. When a player selects a particular strategy, the corresponding payoff depends on this strategy and on decisions made by other players. The payoff function is defined as $\mathcal{U}_i : S \to \mathbb{R}$, where $S = S_0 \times S_1 \times \cdots \times S_N$.

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

$$\mathcal{U}_i(s_i^*, s_{-i}^*) \geq \mathcal{U}_i(s_i, s_{-i}^*) \quad \forall i, s_i \in S, \tag{1}$$

where $s_{-i} \in S - S_i$, the strategy space excluding player i. In a Nash equilibrium, no single player can increase its utility by unilaterally changing strategy.

Certainly, the limitations, such as rational and static features, do not reflect the way the real world behaves in most situations. Inspired by the theory of evolution, evolutionary game theory [40] was introduced to overcome these limitations.

Evolutionary game theory borrows the notation from classical game theory, like strategy spaces, payoff matrices and utility functions. Differently from classical game theory with its focus on rational individuals, evolutionary game theory considers populations of players that adopt various strategies and play contest against each other. It studies how successful these populations are in their choices of strategies, and how more successful strategies are passed to the next generations. Therefore, it models the dynamics and evolution of populations of players given a distribution of strategies. Generations of population evolve based on the success of individual strategies compared to the success of overall population.

This evolution process is governed by two key elements:

1. mutation mechanism that is represented by the Evolutionary Stable Strategy (ESS) concept

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2020 doi:10.20944/preprints202011.0002.v1

2. selection mechanism that is represented by the replicator dynamics

The Evolutionary Stable Strategy (ESS) concept is considered to be a refinement of NE and it represents an ability to evolve. It outperforms any alternative mutant strategies. In other words, a strategy x is defined as an ESS if for any other strategy y some threshold fraction of mutants $\bar{\epsilon}_y \in]0,1[$ exists that the Eq. 2is satisfied for all $\epsilon \in]0,\bar{\epsilon}_y[$:

$$\mathcal{U}(x, \epsilon \times y + (1-\epsilon) \times x) \geq \mathcal{U}(y, \epsilon \times y + (1-\epsilon) \times x) \tag{2}$$

Thus, the strategy x is defined as evolutionary stable if this inequality holds for any mutant strategy, if the share of mutants in this population is sufficiently small [41]. A group of players choosing ESS will not be replaced by players that choose a different strategy. It is shown [41] that a strong connection between ESS and NE exists. If a strategy x is an ESS then x is a Nash equilibrium, and if x is a strict Nash equilibrium then x is an ESS.

The second important concept is the replicator dynamics [42] that governs evolution of the strategies and is defined as following.

$$\frac{\partial x_i(t)}{\partial t} = (U(x_i) - U_A(x)) \times x_i(t) \tag{3}$$

Here, x_i is the proportion of strategy i in the population $x = (x_1, ...x_n)$. $U(x_i)$ is defined as an expected utility of strategy i, and $U_A(x)$ is defined as an average population utility. Playing a game, different individuals from a population are able to compare their strategies to the average population result and learn from each others experiences. The replicator dynamics is applied to adjust their strategies. If ESS exists, the evolution dynamics leads to ESS [43].

Further improvement of the replicator equation was suggested in [44]. The authors proposed to add stochastic elements to better address dynamic stability. In this work, we use the replicator equation with stochastic terms.

3. Models and Numerical Scheme Development

This section presents the system, threat, and game models for the AMI. Further, it defines the evolutionary game for confidentiality attacks and defences based on these models. We propose a numerical scheme by discretizing the strategy spaces and deriving a discrete version of the replicator equation.

3.1. System and Threat Model

The work considers a network scenario where adversaries attack an AMI network trying to compromise confidentiality and obtain unauthorized access to the information transmitted inside the network. In this scenario, we assume that the adversaryhas knowledge about the network topology including transmission technology. Further, we assume that the system deploys an intrusion detection system (IDS) to detect malicious behaviour.

The configuration of an AMI is modelled as a graph that connects nodes representing individual meters, collectors, and the head-end system. Furtherl, we define a set of nodes $N = \{0, 1, 2, \ldots, n\}$ that comprise the AMI network. The head-end system (HES) node is defined as the top node n_0 . We have two sets of nodes: collectors and meters. Meters collect the data and forward the data to the HES node using collectors as transmitters. Some nodes can perform as both meters and collectors. Due to the hierarchical nature of the information aggregation taking place, we represent the AMI as a tree structure, as shown in Figure 1. The tree is static meaning that vertices and edges do not change over time. Except for the HES node that does not have a parent, the rest of the nodes have one parent and may have multiple children.

Confidential data is collected by meters, aggregated at meters/collectors, and transmitted by the network to reach the head-end system. The information sent from each node has a quantified value

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2020 doi:10.20944/preprints202011.0002.v1

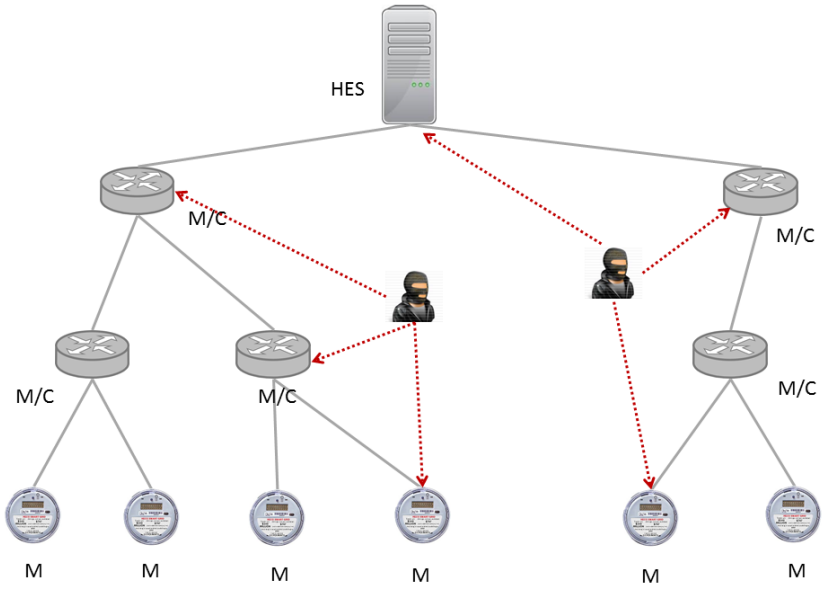

Figure 1. Illustration of the components in the Advanced Metering Infrastructure.

and is the sum of the value of the information gathered at the node and the value of the information collected from the node's children.

We denote $f(i) : \mathcal{N} \to \mathcal{N}$ as the parent of node i, and the set

$$\mathrm{Ch}_i = \{j \in \mathcal{N} : \quad f(j) = i\} \tag{4}$$

as the children of node i.

As all meters are leaf nodes, the set Ch_i is empty for these nodes.

The AMI nodes can run on different security levels determining the probability of protecting the data before transmitting. Due to its limited computational budget, an AMI node is not capable of protecting all messages. In addition, the AMI uses an IDS to detect possible attacks. Thus, these resources are also taking in consideration.

A set of adversary nodes exists that can connect to and attack the AMI. We assume that the attacker cannot access the cryptographic keys and has no control over the encryption process. To intercept a message generated by the meter n_i, the adversary node can attack either the meter or any of collectors that forward the message. Attacking a leaf node, or a meter, is less expensive than attacking a collector. However, a successful attack on a collector gives higher payoff. For each node, we define a probability for protecting the messages as t_i. For each adversary node j, we define a probabilty for attackings an AMI node n_i as $s_{i,j}$. For each node, the costs of defence and attack are given as c_i^d and c_i^a respectively. The collected messages represent a certain value. For quantifying these values, we present an asset value v_i for each node n_i. We assume that these values are constant over time.

3.2. Game Model

We consider the following confidentiality game that involve two classes of players, attackers and defenders. The attackers and defenders meet pairwise and play the game. The attacker and defender do not have any knowledge of the opponent's choices and choose their strategies simultaneously. The game is *one-shot*, and can be considered a special case of a resource constrained network security game [45].

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2020 doi:10.20944/preprints202011.0002.v1

The attackers chooses attack rates (or probabilities) $s_i \geq 0$ for attacking the node labelled i. The attacks are assumed to be subject to the budget constraint

$$\sum_{i=1}^{N} s_i \leq B_S, \tag{5}$$

where N is the total number of nodes in the tree and B_S is the attacker budget. Hence, the strategy space for the attacker is given by

$$S = \{s \in [0,1]^N : \sum_i s_i \leq B_S\} \tag{6}$$

Similarly, the defenders choose defence rates $t_i \geq 0$ for defending node i. The defence rate is the proportion of data that is encrypted before transmitting it to its parent node. In particular, for $t_i = 1$, the data sent from node i is assumed impossible for the attacker to obtain. The defence rates are assumed subject to the budget constraint

$$\sum_{i=1}^{N} t_i \leq B_T, \tag{7}$$

where B_T is the defender budget. Hence, the strategy space for the defender is given by

$$T = \{t \in [0,1]^N : \sum_i t_i \leq B_T\} \tag{8}$$

We model an AMI as a tree structure, and we assume that in order to intercept data sent from node i, the attacker can choose to either attack node i directly or the parent node $f(i)$. We consider that the cost of attacking and encrypting data on node i are proportional to the value of the data.

The utility function $\mathcal{U}_A : S \times T \to \mathbb{R}$ for the attacking player is given by

$$\mathcal{U}_A(s,t) = \sum_{i=1}^{N} (v_i\,(s_i + s_{f(i)})(1-t_i) - s_i C_{A,i}) = \sum_{i=1}^{N} (v_i s_i (1-t_i) - s_i C_{A,i}) + \sum_{i=1}^{N} \sum_{j \in \mathrm{Ch}_i} v_j\, s_i (1-t_j) \tag{9}$$

where $C_{A,i}$ is the cost of attacking node i and v_i is the value of the information collected at node i. Note that a factor appearing in the work of Ismail et al., $(1-a)$ where a is the detection rate, is omitted here for simplicity. It is a scaling of the node values and has no quantitative influence on the model.

Similarly, the utility function $\mathcal{U}_D : T \times S \to \mathbb{R}$ for the defending player is

$$\mathcal{U}_D(t,s) = -\sum_{i=1}^{N} (v_i\,(s_i + s_{f(i)})(1-t_i) + t_i C_{D,i} = -\sum_{i=1}^{N} (v_i\, s_i (1-t_i) + t_i C_{D,i}) - \sum_{i=1}^{N} \sum_{j \in \mathrm{Ch}_i} v_j\, s_i (1-t_j) \tag{10}$$

were $C_{D,i}$ is the cost of defending node i.

3.3. Evolutionary game formulation

In this section, we proceed with the main novel contribution of this work, the application of the Ismail model in an evolutionary game. To this end, we assume that there are populations of attackers and defenders, represented by probability measures $P_s(S)$ and $P_t(T)$, respectively. The measures represent the distribution of the overall population over the attacker and defender strategy space. Different strategies of population evolution exist, and for the current work we use a replicator equation.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2020 doi:10.20944/preprints202011.0002.v1

The replicator equation favours the choices of strategies which perform well (in terms of utility) relative to the overall population. Let

$$\pi_A(s, P_t) = \int_T \mathcal{U}_A(s, t')P_t(\mathrm{d}t') \tag{11}$$

be the expected payoff for an attacker given a defender population P_t. Similarly, we have

$$\pi_D(t, P_s) = \int_S \mathcal{U}_D(t, s')P_s(\mathrm{d}s'), \tag{12}$$

the expected payoff for a defender given an attacker population P_s.

The *average* payoff for an attacker given attacker and defender populations P_s and P_t, respectively, is given by

$$\pi_A(P_s, P_t) = \int_S \pi_A(s', P_t)P_s(\mathrm{d}s') = \int_S \int_T \mathcal{U}_A(s', t')P_t(\mathrm{d}t')P_s(\mathrm{d}s'). \tag{13}$$

Similarly, the average payoff for a defender given the same populations is given by

$$\pi_D(P_t, P_s) = \int_T \pi_D(t', P_s)P_t(\mathrm{d}t') = \int_T \int_S \mathcal{U}_D(t', s')P_s(\mathrm{d}s')P_t(\mathrm{d}t'). \tag{14}$$

For any subset of attacking strategies $\bar{S} \subset S$, the evolutionary replicator dynamic with noise [44] then takes the form of

$$\frac{\mathrm{d}P_s}{\mathrm{d}\tau}(\bar{S}) = \int_{\bar{S}} (\pi_A(s', P_t) - \pi_A(P_s, P_t))P_s(\mathrm{d}s') + \delta_S(\bar{S}), \tag{15}$$

for some time scale τ and a stochastic term $\delta_s(\bar{S})$. Similarly, the evolution of a subset of defending strategies $\bar{T} \subset T$ is given by

$$\frac{\mathrm{d}P_t}{\mathrm{d}\tau}(\bar{T}) = \int_{\bar{T}} (\pi_D(t', P_s) - \pi_D(P_t, P_s))P_t(\mathrm{d}t') + \delta_T(\bar{T}) \tag{16}$$

The equations (15) and (16) fully govern the evolution of the attacker and defender populations. The noise terms $\delta_S(\bar{S})$ and $\delta_T(\bar{T})$ introduce random fluctuations in the evolution of the attacker and defender populations, respectively.

3.4. Numerical scheme

We carry out numerical experiments in order to provide insight into the evolutionary dynamics of the Ismail confidentiality game and to demonstrate how it can be used in informing AMI security. To this end we discretize the strategy spaces and derive a simple but computationally effective numerical scheme for the replicator equation.

To solve (15) and (16) numerically, we discretize the N-dimensional strategy spaces S and T. An attacking strategy is represented by

$$s^k = \left(\frac{k_1}{K}, \ldots, \frac{k_N}{K}\right), \qquad k_i \in \{0, \ldots, K\}, \tag{17}$$

with the budget constraint

$$\frac{1}{K}\sum_{i=1}^{N} k_i \leq 1. \tag{18}$$

Similarly, a defending strategy is represented discretely as

$$t^k = \left(\frac{k_1}{K}, \ldots, \frac{k_N}{K}\right), \qquad k_i \in \{0, \ldots, K\}, \tag{19}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2020 doi:10.20944/preprints202011.0002.v1

with the budget constraint

$$\frac{1}{K}\sum_{i=1}^{N} k_i \leq Y. \tag{20}$$

It is convenient to introduce the discretized attacker strategy space

$$\Omega_S^K = \left\{ k = (k_1, \ldots, k_N) : k_i \in \{1, \ldots, K\}, \frac{1}{K}\sum_{i=1}^{N} k_i \leq B_S \right\} \tag{21}$$

and the discretized defender strategy space

$$\Omega_T^K = \left\{ k = (k_1, \ldots, k_N) : k_i \in \{1, \ldots, K\}, \frac{1}{K}\sum_{i=1}^{N} k_i \leq B_T \right\}. \tag{22}$$

The population of attackers is defined by the probability distribution

$$P_s(s^k) \in [0,1], \qquad \sum_{k \in \Omega_S^K} P_s(s^k) = 1. \tag{23}$$

Similarly, the defender population is represented as

$$P_t(t^k) \in [0,1], \qquad \sum_{k \in \Omega_T^K} P_t(t^k) = 1. \tag{24}$$

Using this representation, the expected payoff for an attacker and defender can be written in the form

$$\pi_A(s, P_t) = \sum_{k \in \Omega_T^K} \mathcal{U}_A\left(s, t^k\right) P_t\left(t^k\right) \tag{25}$$

and

$$\pi_D(t, P_s) = \sum_{k \in \Omega_S^K} \mathcal{U}_D\left(t, s^k\right) P_s(s^k), \tag{26}$$

respectively. Similarly, the average payoff for the attacker and defender populations can then be written as

$$\sigma_A(P_s, P_t) = \sum_{k \in \Omega_S^K} \pi_A(s^k, P_t) P_s(s^k) \tag{27}$$

and

$$\sigma_D(P_t, P_s) = \sum_{k \in \Omega_T^K} \pi_D(t^k, P_s t) P_t(t^k), \tag{28}$$

respectively.

Finally, the discrete versions of the population replicator equations take the form

$$\frac{\mathrm{d}P_s}{\mathrm{d}\tau}(s^k) = (\pi_A(s^k, P_t) - \sigma_A(P_s, P_t)) P_s(s^k) + \delta_s^k \tag{29}$$

for the attackers and

$$\frac{\mathrm{d}P_t}{\mathrm{d}\tau}(t^k) = (\pi_D(t^k, P_s) - \sigma_D(P_t, P_s)) P_t(t^k) + \delta_t^k \tag{30}$$

for the defenders.

Given initial attacker and defender populations $P_s^{(0)}$ and $P_t^{(0)}$, respectively, the i'th generation of attackers and defenders, $P_s^{(i)}$ and $P_t^{(i)}$, are computed iteratively according to the scheme

$$P_s^{(i)}(s^k) = P_s^{(i-1)}(s^k) + \Delta\tau(\pi_A(s^k, P_t^{(i-1)}) - \sigma_A(P_s^{(i-1)}, P_t^{(i-1)})) P_s^{(i-1)}(s^k) + \Delta\tau\, \delta_S^k, \tag{31}$$

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2020 doi:10.20944/preprints202011.0002.v1

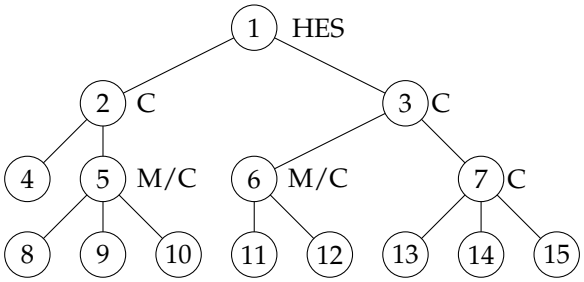

Figure 2. The AMI tree structure used in the case study. It contains the HES. The intermediate nodes are either pure Collectors (C) or hybrid Meter/Collectors (M/C). The leaf nodes are meters

$$P_t^{(i)}(t^k) = P_t^{(i-1)}(t^k) + \Delta\tau(\pi_D(t^k, P_s^{(i-1)}) - \sigma_D(P_t^{(i-1)}, P_s^{(i-1)}))P_t^{(i-1)}(s^k) + \Delta\tau\,\delta_T^k, \tag{32}$$

where $\Delta\tau$ is the time step length between each generation. For numerical stability, positivity of $P_s^{(i)}$ and $P_t^{(i)}$ is enforced after each step and the populations are re-normalized.

4. AMI case study

4.1. Simulation setup

We consider a case study with a small but realistic AMI structure consisting of 15 nodes with edges shown in Figure 2 and node parameters given in Table 1. All leaf nodes represent meters. The intermediate nodes between the head-end system and the leaf nodes act either as a pure collector aggregating data from its child nodes, or as a hybrid collector/meter. We assume that the value of the information aggregated at each node the sum of any information generated at the node (if it is a meter) and the information aggregated from child nodes. The cost weights of attacking and encrypting data on a node i are set to 0.2 and 0.05 respectively. These weights are based upon the original work of Ismail et al. [24].

Table 1. Case Study Parameters

Node	v_i	$C_{A,i}$	$C_{D,i}$	s_1^*	t_1^*	s_2^*	t_2^*	s_3^*	t_3^*
#1	33.00	6.60	1.65	0.396246	0.51805	0.373106	0.524613	0.364412	0.536942
#2	15.00	3.00	0.75	0.072595	0.04662	0.09603	0.107789	0.089545	0.511544
#3	18.00	3.60	0.90	0.060055	0.05209	0.054538	0.48788	0.060831	0.515485
#4	3.00	0.60	0.15	0.042049	0.03001	0.043214	0.074903	0.045137	0.12042
#5	12.00	2.40	0.60	0.046897	0.029263	0.049434	0.07387	0.053685	0.119965
#6	9.00	1.80	0.45	0.044304	0.028329	0.046061	0.071233	0.049054	0.119792
#7	9.00	1.80	0.45	0.041939	0.018402	0.043156	0.065708	0.045231	0.119011
#8	3.00	0.60	0.15	0.026952	0.04108	0.026954	0.077835	0.026961	0.121616
#9	3.00	0.60	0.15	0.026952	0.04108	0.026954	0.077835	0.026961	0.121616
#10	3.00	0.60	0.15	0.026952	0.04108	0.026954	0.077835	0.026961	0.121616
#11	3.00	0.60	0.15	0.037328	0.035544	0.036896	0.074586	0.036151	0.119706
#12	3.00	0.60	0.15	0.037328	0.035544	0.036896	0.074586	0.036151	0.119706
#13	3.00	0.60	0.15	0.046802	0.027631	0.046602	0.070442	0.046307	0.117527
#14	3.00	0.60	0.15	0.046802	0.027631	0.046602	0.070442	0.046307	0.117527
#15	3.00	0.60	0.15	0.046802	0.027631	0.046602	0.070442	0.046307	0.117527

The attacker's budget is set to 1.0 and is the same value for all simulations. Regarding the defender's budget, we vary the budget as 1.0, 2.0, and 3.0. The simulation results are presented separately for different values of the defender's budget.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2020 doi:10.20944/preprints202011.0002.v1

4.2. Evaluation metrics

To better interpret the results from the evolutionary game and the evolution of attacker and defender strategies over time, we consider the following generation-dependent game metrics. The population-averaged attack-rate for node i is given by

$$A_i = \sum_{k \in \Omega_s^K} s_i^k P_s(s^k). \tag{33}$$

Similarly, the population-average defence-rate for node i is given by:

$$D_i = \sum_{k \in \Omega_t^K} t_i^k P_t(t^k). \tag{34}$$

To assess the success of attackers and defenders in the current population, the time-evolution of the average payoff (27) and (28) are also monitored.

5. Results

The simulation results that show the evolution of average payoff for both defenders and attackers are depicted in Figure 9. The attack and defence rates for the different nodes are depicted in Figure 3, Figure 4, Figure 5, Figure 6, Figure 7, Figure 8, respectively for the defender's budget equals 1.0, 2.0, and 3.0. Initially, there is a transient phase where attackers alternate between attacking the Head-End System and the intermediate collector nodes. Respectively, and defenders alternate between defending the Head-End System and the intermediate collector nodes. The defender population responds by increasing the defence rate for the Head-End System to the point where the attackers, on average, give up this node and instead focus on the intermediate Collectors and Collector/Meters.

The results show that both types of players favour nodes from a higher aggregation level, which increase their utilities. We also observe that when the defender's budget increases the system distributes the new resources to the nodes that contribute more to the defender's payoffs. Further, we can see that the system finds a short unstable equilibrium sate that happens around generation 70 for 1 defender, generation 60 for 2 defenders, and generation 50 for 3 defenders. For different values of the defender's budget, both graphs start to converge to a stable state after approximately 80 -90 generations and remain stable for more than 100 generations. For the defender, it means that the system has defined the solution that gives the best response to the adaptive attacks in the dynamic environment. We can also conclude that the ESS is reached for this system setup.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2020 doi:10.20944/preprints202011.0002.v1

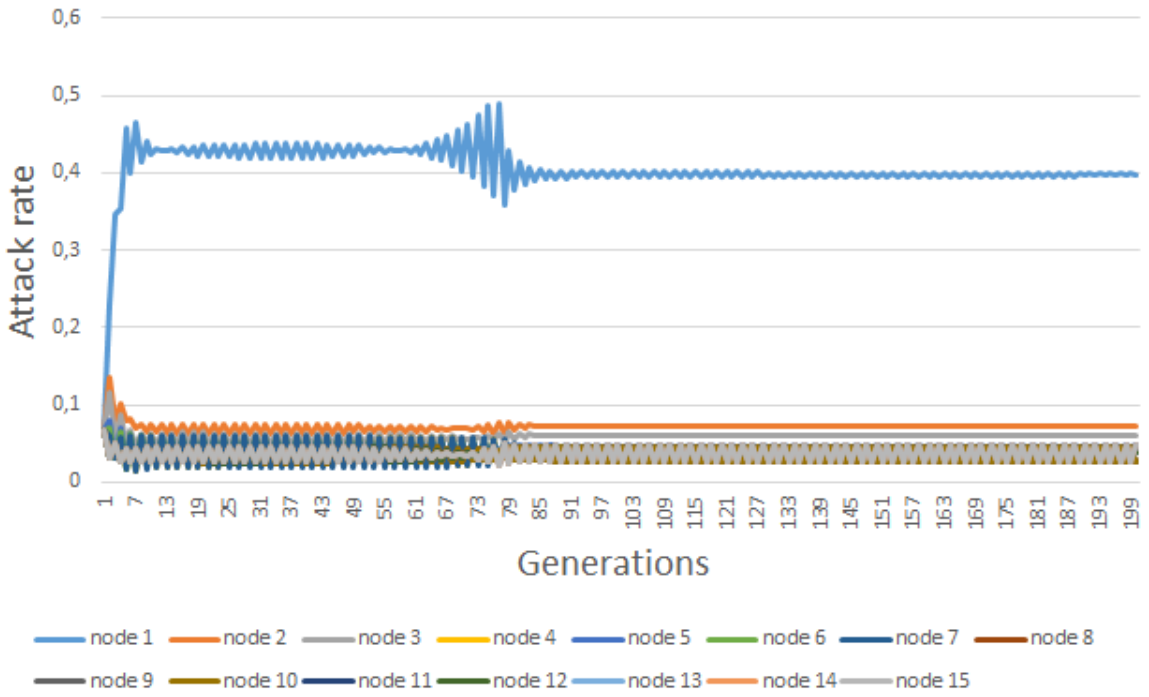

Figure 3. Evolution graphs for average attack rate showing the results for the nodes of the case study. The defender's budget is equals to 1.0. The x-axis presents the generations. The y-axis presents the evolution of average rates.

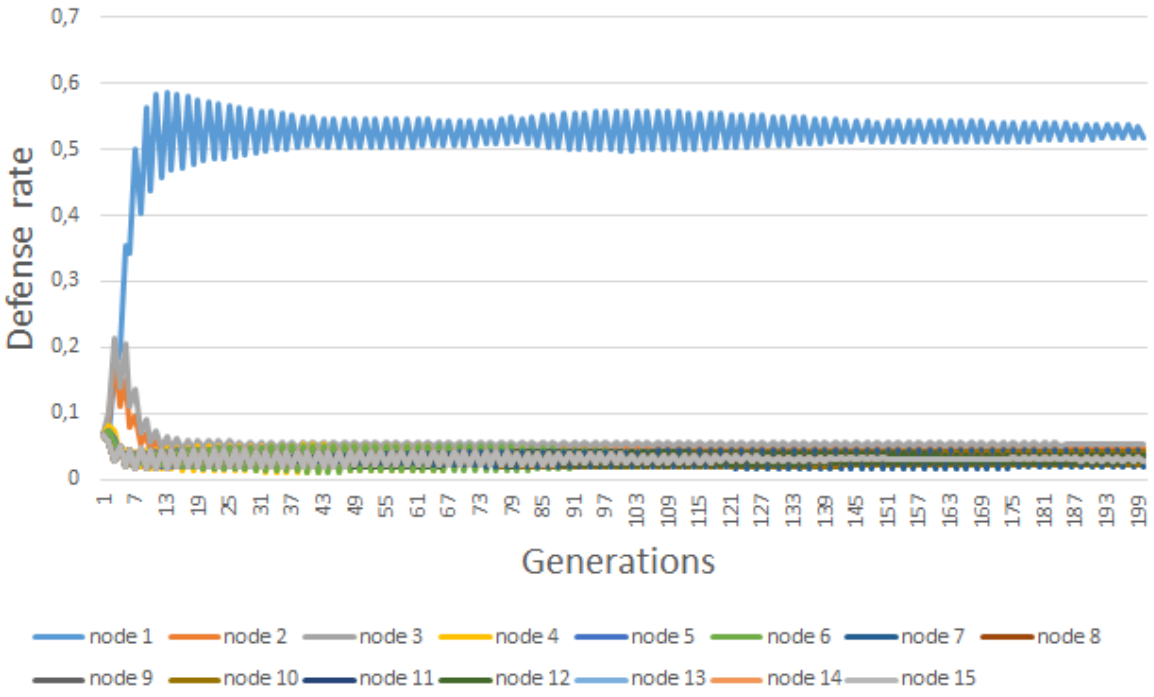

Figure 4. Evolution graphs for average defence rate showing the results for the nodes of the case study. The defender's budget equals to 1.0. The x-axis presents the generations. The y-axis presents the evolution of average rates.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2020 doi:10.20944/preprints202011.0002.v1

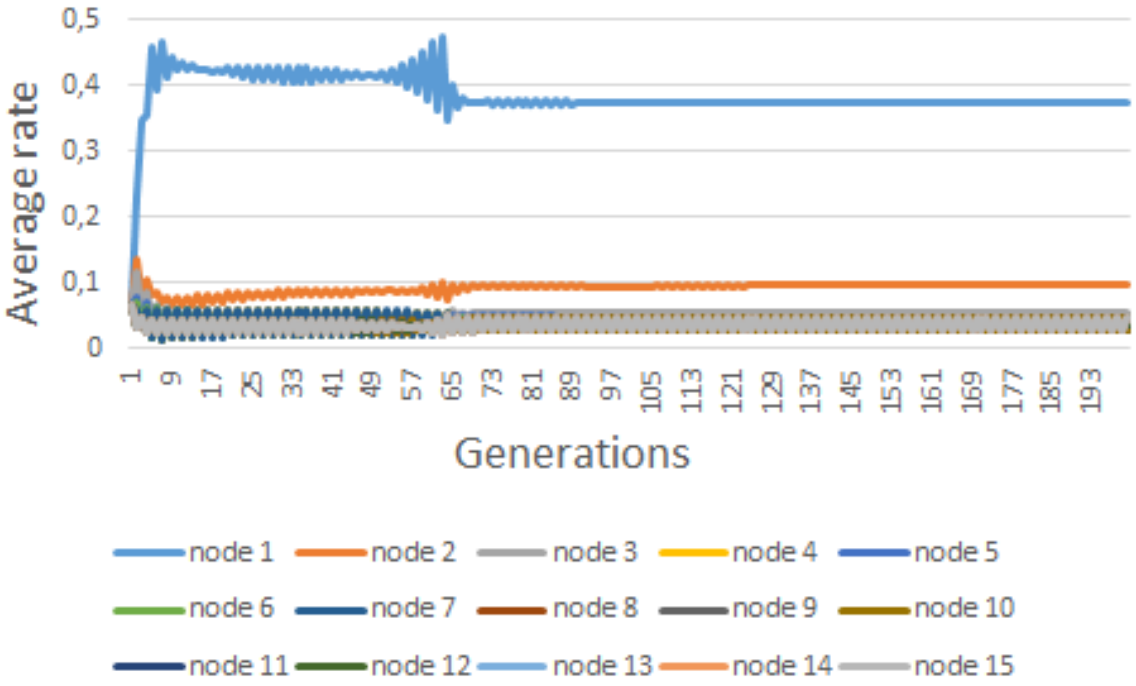

Figure 5. Evolution graphs for average attack for the nodes of the case study. The defender's budget equals to 2.0. The x-axis presents the generations. The y-axis presents the evolution of average rates.

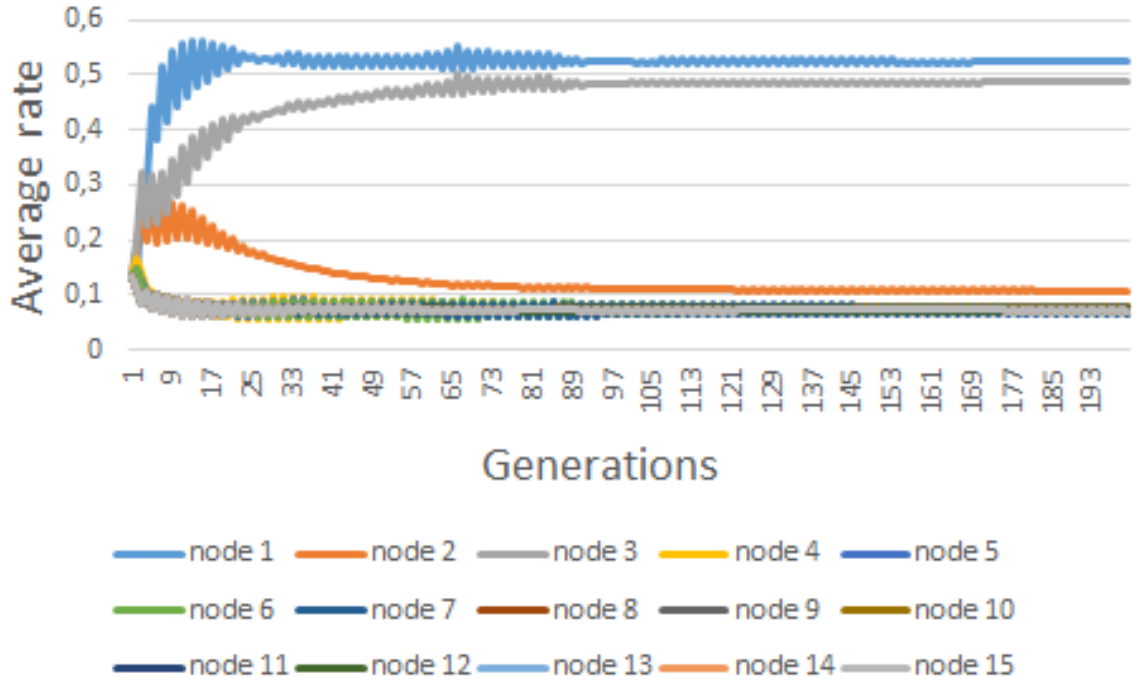

Figure 6. Evolution graphs for average defence rate for the nodes of the case study. The defender's budget equals to 2.0. The x-axis presents the generations. The y-axis presents the evolution of average rates.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2020 doi:10.20944/preprints202011.0002.v1

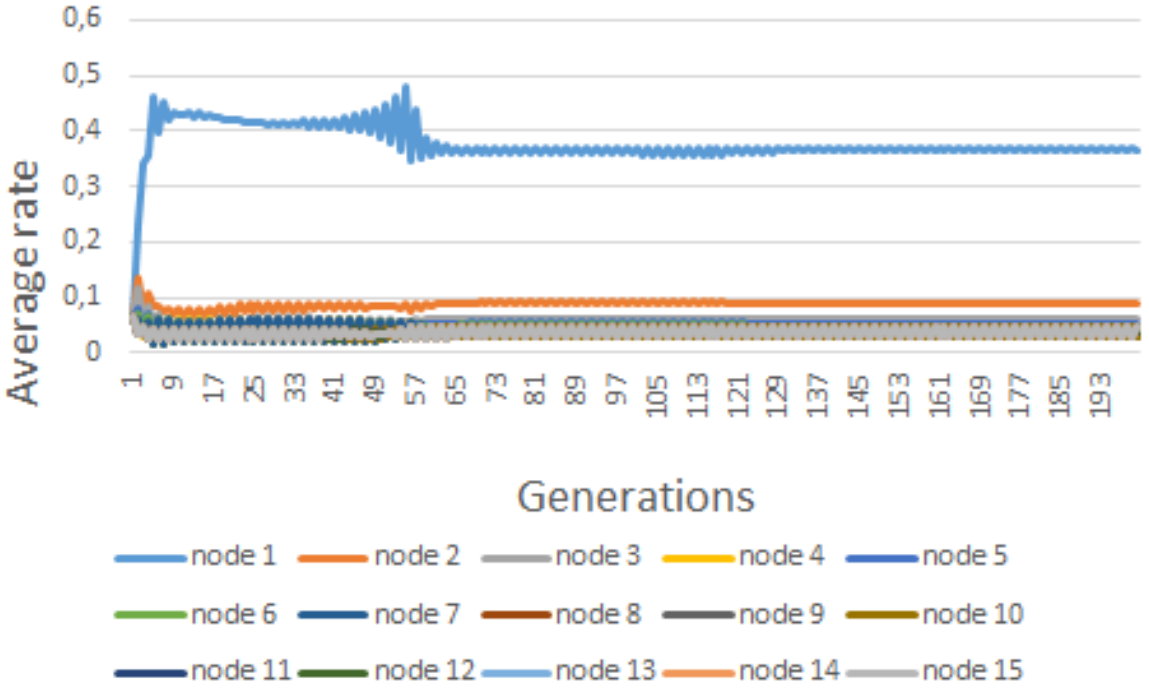

Figure 7. Evolution graphs for average attack for the nodes of the case study. The defender's budget equals to 3.0. The x-axis presents the generations. The y-axis presents the evolution of average rates.

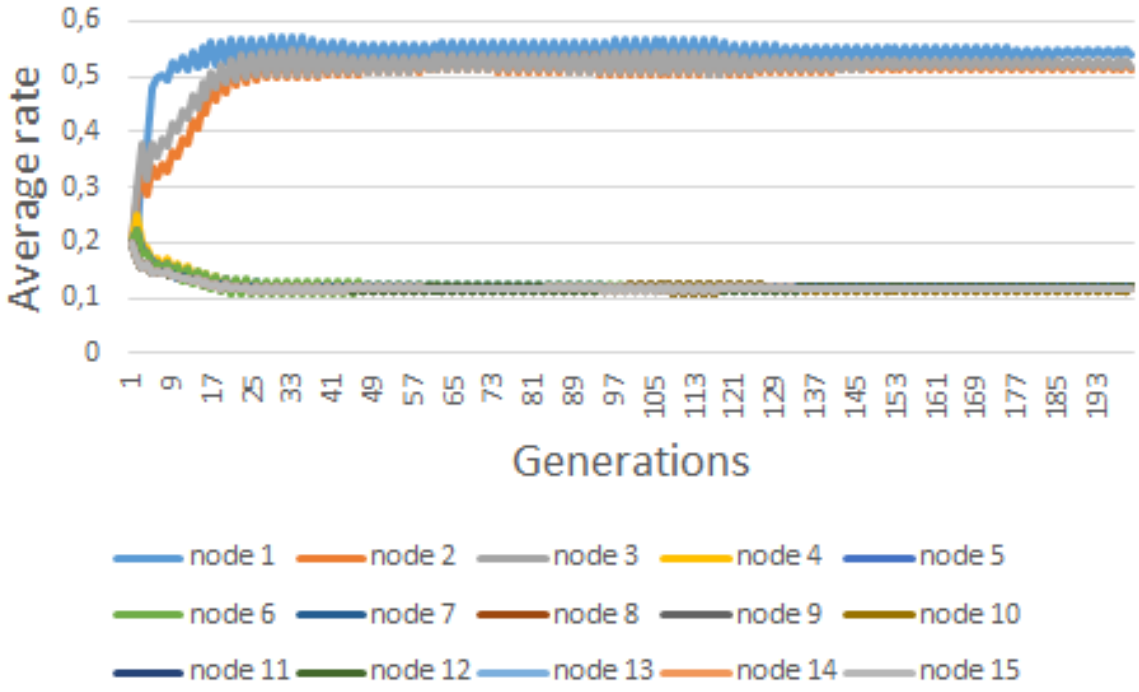

Figure 8. Evolution graphs for average defence rate for the nodes of the case study. The defender's budget equals to 3.0. The x-axis presents the generations. The y-axis presents the evolution of average rates.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 2 November 2020 doi:10.20944/preprints202011.0002.v1

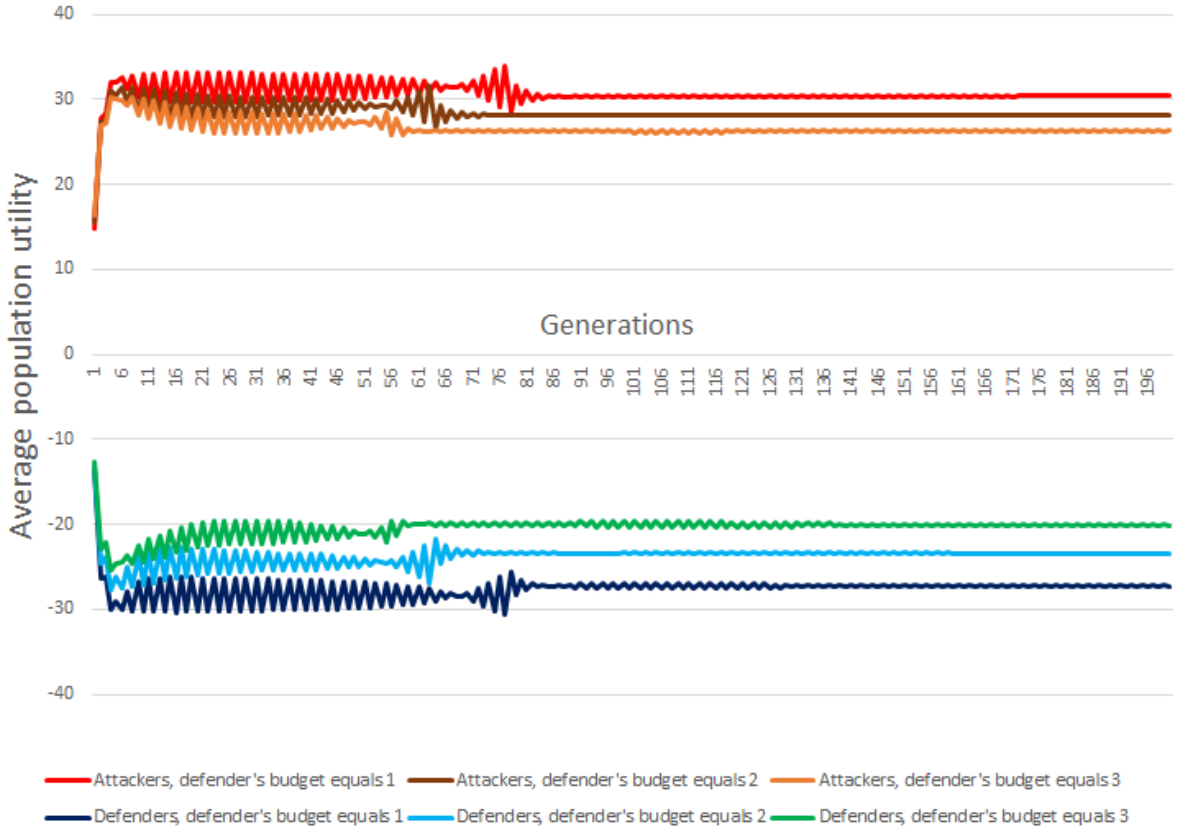

Figure 9. Evolution graphs for average utility for the attacker and defender populations for the case study. The results are shown for the defender's budget equals to 1.0, 2.0, and 3.0. The x-axis presents the generations. The y-axis presents the evolution of average utilities.

6. Conclusion

In this work, we modelled confidentiality attacks and defences as an evolutionary game and analysed the behaviours of the attacker and the defender of the AMI system. By applying evolutionary game theory to this problem we introduced an important dynamic and learning capabilities in the behaviour of both attackers and AMI nodes, to explore the space of strategies, and to select the optimal set of solutions. We used the replicator equation to show the evolution of utilities for both type of players. Further, we outlined how the evolutionary game model can used to evaluate the security threats in AMI systems. In our simulation scenarios, we show that the solution converges to ESS for all investigated cases. The simulations also shows that the behavior of the replicator dynamic depends not only on incentives but also on the network configuration and proportions of the protected assets. It is important that the outcomes of this work give us the best possible defence strategy against evolving attacks. It allows the defender to to continuously stay ahead of the attacker in defending the AMI nodes.

The next step in our research will be the investigation of dynamic AMI trees. we consider that thes trees can have a dynamic configuration and change over time. A node can disconnect, connected to a new one, or a new node can be introduced. This condition introduces more variety and dynamism to the AMI system. This problem should be taken into account for preparing the strategy spaces. Combining the evolutionary game analysis with machine learning algorithms, especially with federated learning and autonomy, is a step forward to overcome this limitation and the scaling problem. In our future work, we intend to evaluate and implement combination of applying machine learning and evolutionary game theory for modeling adaptive attack-defence dynamics. It will also include development of suitable quantitative metrics to evaluate game simulations.

Acknowledgment

The work presented here has been carried out in two research projects: The IoTSec (Security in IoT for Smart Grids, Nr. 248113/O70, 2015–2018), and FINSEC (Integrated Framework for Predictive and Collaborative Security of Financial Infrastructures) project funded by the EU under the Horizon 2020 programme (contract number: 786727). The authors wish to thank Wolfgang Leister for advices during the preparation of this paper.

Conflicts of Interest: The authors declare no conflict of interest.

Abbreviations

The following abbreviations are used in this manuscript:

AMI	Advanced Metering Infrastructure
CAGR	Compound Annual Growth Rate
CPS	Cyber-Physical Systems
IoT	Internet of Things
FDI	False Data Injection
DDoS	Distributed Denial-of-Service
EGT	Evolutionary game theory
ESS	Evolutionary Stable Strategy
APTs	Advanced Persistent Threats
NE	Nash equilibrium
HES	head-end system
C	collector
M	meter

1. Noll, J.; Garitano, I.; Fayyad, S.; Asberg, E.; Abie, H. Measurable Security, Privacy and Dependability in Smart Grids. *Journal of Cyber Security and Mobility* **2014**, *3*, 371–398. doi:10.13052/jcsm2245-1439.342.
2. AB, E. Ericsson Mobility Report 2017. Technical report, Ericson AB, 2017.
3. Sadeghi, A.R.; Wachsmann, C.; Waidner, M. Security and Privacy Challenges in Industrial Internet of Things. Proceedings of the 52Nd Annual Design Automation Conference; ACM: New York, NY, USA, 2015; DAC '15, pp. 54:1–54:6. doi:10.1145/2744769.2747942.
4. He, H.; Maple, C.; Watson, T.; Tiwari, A.; Mehnen, J.; Jin, Y.; Gabrys, B. The security challenges in the IoT enabled cyber-physical systems and opportunities for evolutionary computing amp; other computational intelligence. 2016 IEEE Congress on Evolutionary Computation (CEC), 2016, pp. 1015–1021. doi:10.1109/CEC.2016.7743900.
5. Mavroeidakos, T.; Chaldeakis, V. Threat Landscape of Next Generation IoT-Enabled Smart Grids. Artificial Intelligence Applications and Innovations. AIAI 2020 IFIP WG 12.5 International Workshops; Maglogiannis, I.; Iliadis, L.; Pimenidis, E., Eds.; Springer International Publishing: Cham, 2020; pp. 116–127.
6. Abie, H.; Balasingham, I. Risk-based Adaptive Security for Smart IoT in eHealth. Proceedings of the 7th International Conference on Body Area Networks; ICST (Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering): ICST, Brussels, Belgium, Belgium, 2012; BodyNets '12, pp. 269–275.
7. Zeitz, K.; Cantrell, M.; Marchany, R.; Tront, J. Designing a Micro-Moving Target IPv6 Defense for the Internet of Things. Proceedings of the Second International Conference on Internet-of-Things Design and Implementation; ACM: New York, NY, USA, 2017; IoTDI '17, pp. 179–184. doi:10.1145/3054977.3054997.
8. 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* **2017**, *13*, 411–423. doi:10.1109/TII.2016.2614396.
9. Xiang, Y.; Wang, L.; Liu, N. Coordinated attacks on electric power systems in a cyber-physical environment. *Electric Power Systems Research* **2017**, *149*, 156 – 168. doi:https://doi.org/10.1016/j.epsr.2017.04.023.

10. Abass, A.A.A.; Xiao, L.; Mandayam, N.B.; Gajic, Z. Evolutionary Game Theoretic Analysis of Advanced Persistent Threats Against Cloud Storage. *IEEE Access* **2017**, *5*, 8482–8491.
11. Xu, S. Collaborative Attack vs. Collaborative Defense. Collaborative Computing: Networking, Applications and Worksharing; Bertino, E.; Joshi, J.B.D., Eds.; Springer Berlin Heidelberg: Berlin, Heidelberg, 2009; p. 217—228.
12. Sanjab, A.; Saad, W. Data Injection Attacks on Smart Grids With Multiple Adversaries: A Game-Theoretic Perspective. *IEEE Transactions on Smart Grid* **2016**, *7*, 2038–2049. doi:10.1109/TSG.2016.2550218.
13. Tellbach, D.; Li, Y.F. Cyber-Attacks on Smart Meters in Household Nanogrid: Modeling, Simulation and Analysis. *Energies* **2018**, *11*. doi:10.3390/en11020316.
14. Boudko, S.; Abie, H. An Evolutionary Game for Integrity Attacks and Defences for Advanced Metering Infrastructure. Proceedings of the 12th European Conference on Software Architecture: Companion Proceedings; Association for Computing Machinery: New York, NY, USA, 2018; ECSA '18. doi:10.1145/3241403.3241463.
15. Hansen, A.; Staggs, J.; Shenoi, S. Security Analysis of an Advanced Metering Infrastructure. *Int. J. Crit. Infrastruct. Prot.* **2017**, *18*, 3–19. doi:10.1016/j.ijcip.2017.03.004.
16. Foreman, J.C.; Gurugubelli, D. Cyber Attack Surface Analysis of Advanced Metering Infrastructure. *CoRR* **2016**, *abs/1607.04811*, [1607.04811].
17. Cleveland, F.M. Cyber security issues for Advanced Metering Infrasttructure (AMI). 2008 IEEE Power and Energy Society General Meeting - Conversion and Delivery of Electrical Energy in the 21st Century, 2008, pp. 1–5. doi:10.1109/PES.2008.4596535.
18. Goel, S.; Hong, Y., Security Challenges in Smart Grid Implementation. In *Smart Grid Security*; Springer London: London, 2015; pp. 1–39. doi:10.1007/978-1-4471-6663-4_1.
19. Li, F.; Luo, B.; Liu, P. Secure and Privacy-Preserving Information Aggregation for Smart Grids. *Int. J. Secur. Netw.* **2011**, *6*, 28–39. doi:10.1504/IJSN.2011.039631.
20. Li, H.; Gong, S.; Lai, L.; Han, Z.; Qiu, R.C.; Yang, D. Efficient and Secure Wireless Communications for Advanced Metering Infrastructure in Smart Grids. *IEEE Transactions on Smart Grid* **2012**, *3*, 1540–1551. doi:10.1109/TSG.2012.2203156.
21. Baig, Z.A.; Amoudi, A.R. An Analysis of Smart Grid Attacks and Countermeasures. *JCM* **2013**, *8*, 473–479.
22. Sayin, M.O.; Başar, T., Secure Sensor Design for Cyber-Physical Systems Against Advanced Persistent Threats. In *Decision and Game Theory for Security: 8th International Conference, GameSec 2017, Vienna, Austria, October 23-25, 2017, Proceedings*; Rass, S.; An, B.; Kiekintveld, C.; Fang, F.; Schauer, S., Eds.; Springer International Publishing: Cham, 2017; pp. 91–111. doi:10.1007/978-3-319-68711-7_6.
23. He, H.; Yan, J. Cyber-physical attacks and defences in the smart grid: a survey. *IET Cyber-Physical Systems: Theory and Applications* **2016**, *1*, 13–27(14).
24. Ismail, Z.; Leneutre, J.; Bateman, D.; Chen, L. A game theoretical analysis of data confidentiality attacks on smart-grid AMI. *IEEE Journal on Selected Areas in Communications* **2014**, *32*, 1486–1499.
25. Wang, Y.; Chen, X.; Wang, Z. Testability of evolutionary game dynamics based on experimental economics data. *Physica A: Statistical Mechanics and its Applications* **2017**, *486*, 455–464. doi:10.1016/j.physa.2017.05.0.
26. Santos, F.; Encarnação, S.; C. Santos, F.; Portugali, J.; M. Pacheco, J. An Evolutionary Game Theoretic Approach to Multi-Sector Coordination and Self-Organization **2016**. *18*, 152.
27. Hoffman, M.; Suetens, S.; Gneezy, U.; Nowak, M.A. An experimental investigation of evolutionary dynamics in the Rock-Paper-Scissors game. *Scientific Reports* **2015**, *5:8817*.
28. Quijano, N.; Ocampo-Martinez, C.; Barreiro-Gomez, J.; Obando, G.; Pantoja, A.; Mojica-Nava, E. The Role of Population Games and Evolutionary Dynamics in Distributed Control Systems: The Advantages of Evolutionary Game Theory. *IEEE Control Systems* **2017**, *37*, 70–97. doi:10.1109/MCS.2016.2621479.
29. Ficici, S.G.; Melnik, O.; Pollack, J.B. A game-theoretic investigation of selection methods used in evolutionary algorithms. Proceedings of the 2000 Congress on Evolutionary Computation. CEC00 (Cat. No.00TH8512), 2000, Vol. 2, pp. 880–887 vol.2. doi:10.1109/CEC.2000.870732.
30. Abass, A.A.A.; Xiao, L.; Mandayam, N.B.; Gajic, Z. Evolutionary Game Theoretic Analysis of Advanced Persistent Threats Against Cloud Storage. *IEEE Access* **2017**, *5*, 8482–8491. doi:10.1109/ACCESS.2017.2691326.

31. Bouhaddi, M.; Adi, K.; Radjef, M.S. Evolutionary Game-Based Defense Mechanism in the MANETs. Proceedings of the 9th International Conference on Security of Information and Networks. ACM, 2016, pp. 88–95.
32. Vejandla, P.; Dasgupta, D.; Kaushal, A.; Nino, F. Evolving Gaming Strategies for Attacker-Defender in a Simulated Network Environment. Proceedings of the 2010 IEEE Second International Conference on Social Computing; IEEE Computer Society: Washington, DC, USA, 2010; SOCIALCOM '10, pp. 889–896. doi:10.1109/SocialCom.2010.132.
33. Akyazı, U.; Uyar, A.Ş. Detection of DDoS Attacks via an Artificial Immune System-Inspired Multiobjective Evolutionary Algorithm. Applications of Evolutionary Computation; Di Chio, C.; Brabazon, A.; Di Caro, G.A.; Ebner, M.; Farooq, M.; Fink, A.; Grahl, J.; Greenfield, G.; Machado, P.; O'Neill, M.; Tarantino, E.; Urquhart, N., Eds.; Springer Berlin Heidelberg: Berlin, Heidelberg, 2010; pp. 1–10.
34. Essaddi, N.; Hamdi, M.; Habib, S.; Boudriga, N. Evolutionary strategies for non-uniform deployment in wireless sensor networks. *International Journal of Communication Networks and Distributed Systems* **2011**, *7*, 331–354.
35. Jiang, C.; Chen, Y.; Liu, K.J.R. Distributed Adaptive Networks: A Graphical Evolutionary Game-Theoret View. *CoRR* **2012**, *abs/1212.1245*, [1212.1245].
36. John, D.J.; Smith, R.W.; Turkett, W.H.; Cañas, D.A.; Fulp, E.W. Evolutionary Based Moving Target Cyber Defense. Proceedings of the Companion Publication of the 2014 Annual Conference on Genetic and Evolutionary Computation; ACM: New York, NY, USA, 2014; GECCO Comp '14, pp. 1261–1268. doi:10.1145/2598394.2605437.
37. Li, Y.; Xu, H.; Cao, Q.; Li, Z.; Shen, S. Evolutionary Game-Based Trust Strategy Adjustment among Nodes in Wireless Sensor Networks **2015**. *2015*, 1–12.
38. Shivshankar, S.; Jamalipour, A. An Evolutionary Game Theory-Based Approach to Cooperation in VANETs Under Different Network Conditions. *IEEE Transactions on Vehicular Technology* **2015**, *64*, 2015–2022. doi:10.1109/TVT.2014.2334655.
39. Wang, X.; Wu, Y.; Ren, Y.; Feng, R.; Yu, N.; Wan, J. An Evolutionary Game-Based Trust Cooperative Stimulation Model for Large Scale MANETs. *International Journal of Distributed Sensor Networks* **2013**, *9*, 245017, [https://doi.org/10.1155/2013/245017]. doi:10.1155/2013/245017.
40. Smith, J.M. Game theory and the evolution of fighting. *On evolution* **1972**, pp. 8–28.
41. Smith, J. *Evolution and the Theory of Games*; Cambridge University Press, 1982.
42. Taylor, P.D.; Jonker, L.B. Evolutionary stable strategies and game dynamics. *Mathematical Biosciences* **1978**, *40*, 145 – 156. doi:https://doi.org/10.1016/0025-5564(78)90077-9.
43. Weibull, J.W. *Evolutionary game theory*; MIT Press: Cambridge, MA, 1995.
44. Foster, D.P.; Young, P. Stochastic evolutionary game dynamics. 1990.
45. Ismail, Z.; Kiennert, C.; Leneutre, J.; Chen, L. A Game Theoretical Model for Optimal Distribution of Network Security Resources. International Conference on Decision and Game Theory for Security. Springer, 2017, pp. 234–255.