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

Svetlana Boudko
Norsk Regnesentral
Oslo, Norway
Svetlana.Boudko@nr.no

Habtamu Abie
Norsk Regnesentral
Oslo, Norway
Habtamu.Abie@nr.no

ABSTRACT

Smart grids are complex cyber-physical systems that face many security challenges. Advanced Metering Infrastructure (AMI), which is one of the main components of the smart grid, represents an important branch of services with increasing deployments that also introduce new security risks. The nodes of AMIs are featured as resource-constrained. Therefore, security attacks including data integrity attacks on AMIs are of serious concern and require efficient selection of protective strategies. In this paper, we propose an evolutionary game framework that models integrity attacks and defenses in an AMI. The aim of this framework is to study possible behaviors of adversaries and to define how the AMI nodes can adaptively select their strategies with maximum payoffs of the nodes. We present a case study and illustrate how the framework can be applied to investigate the integrity threats in AMI systems. We show the evolution process, based on the replicator dynamic.

CCS CONCEPTS

• **Security and privacy → Network security**; **Mobile and wireless security**;

KEYWORDS

Security, Data Integrity, Game Theory, Evolutionary Game Theory, Advanced Metering Infrastructure, Smart Meters.

ACM Reference Format:
Svetlana Boudko and Habtamu Abie. 2018. An Evolutionary Game for Integrity Attacks and Defences for Advanced Metering Infrastructure. In *12th European Conference on Software Architecture: Companion Proceedings (ECSA '18), September 24–28, 2018, Madrid, Spain.* ACM, New York, NY, USA, 7 pages. https://doi.org/10.1145/3241403.3241463

1 INTRODUCTION

The aim of smart grid systems is to optimize the usage of electrical resources. Smart grids are complex cyber-physical systems that face many security challenges. One of the main components of the smart grid is an Advanced Metering Infrastructure (AMI), which is a communication infrastructure of smart meters, collectors and communication networks. AMI collects and processes data from large number of devices and reports the results over communication networks. While simplifying connection between consumers and service providers, this infrastructure also introduces new security risk, where the integrity is one of the concerns. The report [1] states that between 2017 and 2023, connected IoT devices are expected to increase at a CAGR of 19 percent with 20 billion related to the IoT in 2023. This growth includes the devices from smart grids. These devices are often legacy devices that are very expensive to replace. Both high connectivity and outdated design make them vulnerable to cyber-attacks. Also, a recent survey [7] has concluded that False Data Injection (FDI) attacks have emerged as a new type of cyber attacks threatening state estimation in power systems.

Adversaries may attack smart meters and collectors, damage infrastructure, manipulate critical information, therefore, causing serious financial loses. Considering the risks of a large-scale network system, it is important to calculate not only the risks of separate nodes but also the risks from connections. Further, it is important to foresee that the nodes are able to change their behavior from good to malicious, i.e. a meter being attacked can become an attacker. The attackers are also able to evolve and to learn from each other experience. Securing AMIs is important to ensure their viability.

In this paper, we focus on data integrity. Message authentication schemes that are used for ensuring integrity are computing-intensive. This is critical for smart grid systems that consist of numerous wireless devices with limited resources. Therefore, the system must carefully decide when, what, and how to authenticate. Thus, we need intelligent methods that allow us to study the range of possible behaviors while also taking into account the resource limitations imposed by.

Game theory has proved to become an effective technique for intelligent decision making in smart grid frameworks [9]. To meet the challenges of possible intelligent cooperation between adversaries and their ability to learn from each other's experience as well as for the nodes of an AMI to cooperate and to work out a joint protection, we investigate the game model based on evolutionary game theory. Contrary to classical game theory, evolutionary game theory focuses on the dynamics of competing strategies. Similar to natural selection, players share their experience and determine strategies that are more beneficial than others.

The work proposed in this paper includes the following contributions.

(1) With an emphasis on message integrity, we have developed the AMI threat model and formulated the resource constraint problem as an evolutionary game with multiple populations.
(2) The dynamics of strategy selections is modeled and investigated.
(3) We develop an evolutionary game framework that models the integrity threats in AMI systems.

ECSA '18, September 24–28, 2018, Madrid, Spain

ACM ISBN 978-1-4503-6483-6/18/09.
https://doi.org/10.1145/3241403.3241463

(4) We present a case study to demonstrate how the framework can be applied in real systems.

The remainder of the paper is organized as follows. In Section 2, we study the related work. In Section 3, we introduce the theoretical background for our research and give insight into evolutionary game theory. The system model and problem formulation is presented in Section 4. In Section 5, we present a case study and show how the framework can be applied to investigate the integrity threats in AMI systems. The simulation setup and results are presented in this section before discussing future work and concluding in Section 6.

2 RELATED WORK

The research field concerning game theoretical approaches that addresses the dynamic nature of cyber attacks inside the AMIs is not well explored. Thus, we review the research on modeling security threats for smart grid systems with constrained computational resources. Since evolutionary game is a branch of game theory this section provides a brief review of game theory and research contributions in evolutionary game theory for IoT-enabled smart grid.

2.1 Game Theory for Security

The authors in [17] propose a game-theoretic framework for optimal message authentication for resource bounded systems. A stochastic approach is used. However, the paper focuses on strategies of defense in a static case with a single adversary-defender model. The interaction between the outcomes and the strategies used by either adversaries or defenders is not considered either. Ismail et al. [14] presented a noncooperative game for data confidentiality attacks on smart-grid AMI and analysed the behaviour of the attacker and the defender at the Nash equilibrium. Using their model they estimated the minimum defence resources required and the optimal strategy of the defender. Tambe et al. [33] present the key algorithmic principles, deployed systems, and lessons learned in game theory for security. They outlined research challenges including scaling up security games to large-scale problems, handling significant adversarial uncertainty, dealing with bounded rationality of human adversaries, and other interdisciplinary challenges. Rontidis et al. [25] present a game-theoretic approach for minimizing security risks in the Internet-of-Things. They addressed the many challenges in developing IoT-based smart environments such as dynamic generation of action strategies based on multiple IoT object's input combining stochastic Petri nets and game theory to create stochastic game nets for IoT-based smart environment. Hamdi and Abie [12] developed a game-based adaptive security model for IoT in eHealth, which uses energy consumption, channel bandwidth memory capacity, and nearby node intrusion to determine whether or not to authenticate the sender node. The model uses the trade-off between security effectiveness and energy-efficiency to evaluate adaptive authentication strategies.

Game theory is applied to various application areas, inter alia, in the area of intelligent decision making in smart grid frameworks [10], emerging mobile edge computing and networking applications [21], intrusion detection in wireless sensor networks [36], distributed secure adaptive networks [15], network security [4], integrity assurance in resource-bounded systems [17], electricity theft detection and privacy-aware control in AMI systems [6], defending against Advanced Persistent Threats [24], modelling adversarial cyber security [26], assurance of data trustworthiness in sensor networks [19], intelligent decision making in smart grid frameworks [10][27], etc.

A number of surveys of game theoretic approaches for cyber security and privacy exist. Do et al. [8] reviewed the existing game-theoretic approaches for cyber security and privacy issues, categorizing their applications into three main applications: cyber-physical security, communication security, and privacy. They describe the advantages and limitations of selected approaches from design to implementation of the defence mechanisms. Manshaei et al. [20] provide a structured overview of research on security and privacy in computer and communication networks that use game-theoretic approaches. Moura and Hutchison [21] survey game theory and future trends with application to emerging wireless data communication networks structured according to a taxonomy of classical, evolutionary, and incomplete information games, emphasizing scenarios of upcoming Mobile edge computing, to develop adaptive algorithms and protocols for the efficient operation of the edge of emerging heterogeneous networks. Abdalzaher et al. [3] surveyed the different game-theoretic defence strategies for wireless sensor networks(WSNs) and presented a taxonomy of the game theory approaches based on the nature of the attack. They also present a general trust model for decision making and identify the significant role of evolutionary games for WSNs security against intelligent attacks.

2.2 Evolutionary Game for Security

Evolutionary game theory 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. [29] 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. [13] argue that evolutionary dynamics is a powerful tool for specifying changes in strategies over time in a population. Quijano et al. [23] addressed the advantages of evolutionary game theory in the role of population games and evolutionary dynamics in distributed control systems. Sandholm [28] describes population games and deterministic evolutionary dynamics that assigns each population game a differential equation describing the evolution of aggregate behavior in that game. Vejandla et al. [35] present evolving gaming strategies for attacker-defender in a simulated network nnvironment. Alabdel Abass et al. [2] studied Advanced Persistent Threats (APTs) that represent stealthy, powerful, long-term, and well-funded attacks against cyber systems, such as smart grids, data centers and cloud storage. The authors used evolutionary game theory to capture the long-term continuous behavior of the APTs on the cloud storage devices. The authors in [5] apply evolutionary game theory to study the optimal behavior of the ad-hoc network nodes in the presence of malicious behaviors. Bouhaddi et al. [5] propose evolutionary game theoretic framework to predict malicious behaviors within a MANET and

to analyse security alternatives that preserve the resources consumption of network entities. They model the evolving interactions between an attacker and a defender as an evolutionary game where each player can learn about the behavior of its opponent over time allowing the adjustment of its strategy.

Evolutionary game theory has also been successfully applied in the areas of Vehicular Ad hoc NETworks [30], moving target cyber defense [16], IoT service selection for balancing device energy consumption [22], trust cooperative stimulation model for large scale MANETs [37], trust strategy adjustment among nodes in wireless sensor networks [18], a co-evolutionary game theory using replicator dynamics with feedback-evolving games [39], effects of finite populations on evolutionary stable strategies [11], etc.

It was the work of, inter alia, the above researchers that convinced us of the viability of evolutionary game theory for AMI adaptive security, and therefore gave us confidence in the productivity of our research in this direction.

2.3 Discussions

The unique characteristics and usage scenarios of AMI in the smart power grid introduce new integrity challenges. The increasing proportion 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 integrity assessment on IoT-enabled AMI entities is required. Given the dynamics in AMI environment the ability of the AMI nodes to adjust their integrity protection in response to their perception of the environment and the systems themselves should be provided. Although there are many research contributions about integrity 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 defense mechanisms for robust and reliable AMI cyber systems. In our analysis we recognize that the presented previous research focus mostly on scenarios where a single adversary launches an attack at a time against a single resource. However, multiple adversaries can act together, share their experience from previously launched attacks, and adjust their actions based on these data by choosing successful strategies. This possible cooperation between multiple adversaries has not been fully addressed in the previous work. Especially, the ability of adversaries to learn from previous experiences has not been studied. We, therefore, need to study how evolutionary game theory can be applied to multiple adversary scenarios. Similarly, we study how the effectiveness of defensive strategies evolves in multiple defender scenarios.

3 EVOLUTIONARY GAME THEORY

This section presents an overview of Evolutionary game theory. Traditional game theory is a static approach that allows identifying Nash equilibria and the associated utilities for players involved. Certainly, this limitation is incompatible with the way the real world acts in the most situations.

Evolutionary game theory [32] is inspired by the theory of evolution and was introduced to overcome this limitation. It can model dynamic populations of players with a distribution of strategies. Herein, populations evolve according to the relative success of individual strategies compared to the overall population. Refining the notion of a Nash Equilibrium (NE) to an ability to evolve, this theory introduced the Evolutionary Stable Strategy (ESS) concept, that is sufficient to prevent alternative mutant strategies. It is defined as follows. A strategy x is an ESS if for any strategy $y \neq x$ there exist some threshold fraction of mutants $\overline{\epsilon}_y \in]0, 1[$ such that the following Eq. 3 holds for all $\epsilon \in]0, \overline{\epsilon}_y[$:

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

In other words, the strategy x is evolutionary stable if this inequality holds for any mutant strategy, granted the population share of mutants is sufficiently small [31]. The notion of ESS is a refinement of NE in a way that 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.

Another important concept is the replicator dynamics introduced by [34]. The replicator dynamics is described by the following equation.

$$\frac{\partial x_i(t)}{\partial t} = (U(x_i) - U_A(x)) \times x_i(t) \quad (2)$$

In this equation, x_i is the the propotion of strategy i in the population $x = (x_1, ...x_n)$, $U(x_i)$ is the expected utility of strategy i, and $U_A(x)$ is the average population utility. When several individuals from a population play a game, they are able to learn from the behavior of each other by comparing their strategies to the average population result. They can then apply the replicator dynamic equations to revise their current strategies. The equation, therefore, governs evolution of the strategies. If ESS exists, this evolution leads to ESS [38].

4 PROBLEM FORMULATION

We consider a communication scenario where adversaries attack an AMI network trying to change the information transmitted via the network to their favour, meaning they can modify, replay, or inject false data, and can transmit packets at varying power levels. The adversary is also aware of the network architecture and transmission technology, and other relevant technical information of the AMI components. A representative example of this scenario is illustrated in Figure 1.

In this section, we formalize the network and threat model for the AMI and formulate the evolutionary game for integrity attacks and defences for this model.

4.1 Network and Threat Model

To formulate the model, we consider a set of nodes $N = \{0, 1, 2, \ldots, n\}$ that are the part of the Advanced Metering Infrastructure (AMI). The top node n_0 is the Head-End System (HES) node. The rest of the nodes belong to the following subsets: Collectors (C) or Meters (M). The intersection of Collectors and Meters is not an empty set meaning that some nodes can function as both collectors and meters.

Meters send their measurements to the HES node using Collectors as resenders. We consider the AMI to be a tree structure, where, at any time, each child has only one parent node, while any parent

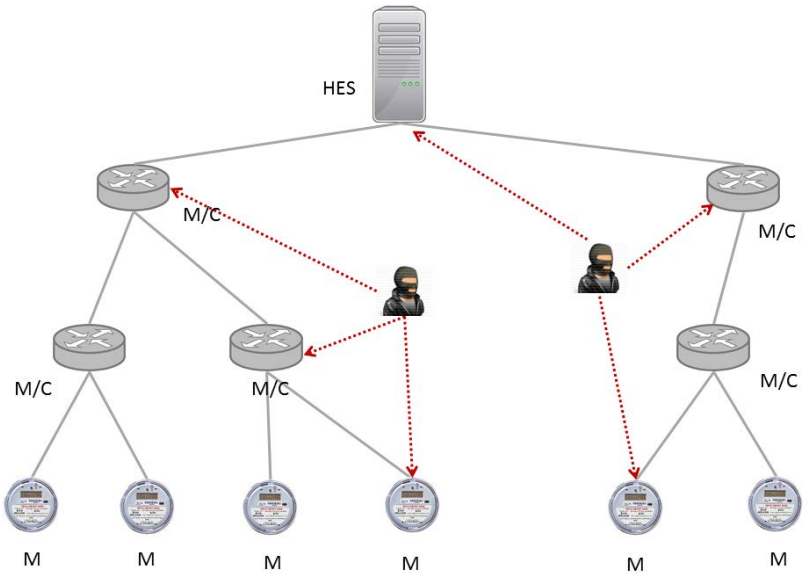

Figure 1: Representative example of an Advanced Metering Infrastructure.

node can have multiple children. No loops are allowed. For each AMI node n_i, we introduce the function $\theta(i)$ that return a set of children for the node n_i. Note, that this function return an empty set for all meters, which are leaf nodes.

The AMI nodes can protect message integrity by, e.g., generating message authentication codes. Since an AMI node has a limited computational budget, the nodes are not able to protect each single message. For each node m_i, we define the rate at which the messages can be protected as d_i. It can be seen as a probability that the message is protected. We consider a set of adversary nodes $A = \{0, 1, 2, \ldots, a\}$ that might connect to and attack the nodes of the AMI. An adversary node attacks an AMI node at a rate s. In this paper, we assume that adversary nodes are able to intercept messages that are sent inside the AMI infrastructure. Further, the adversaries are able to modify these messages or create their own false messages and send these messages to the HES node. However, the adversaries are not able to access the cryptographic keys and to generate correct authentication tags. Therefore, any modification of an integrity-protected message can be detected by a receiver at a cost of computing the message authentication tag, verifying the tag with the one attached to the message, and then computing the new tag.

To fabricate the message sent by meter m_i, the adversary node can either attack the meter or attack any of collectors that retransmit the message. The cost of attacking a leaf node, or a meter, is less than the cost of attacking a collector. At the same time, if remain undetected, the payoff for a successful attack on a collector is also higher.

For each AMI node n_i, the defence cost and the attack costs are denoted by c_i^d and c_i^a respectively. The collected data has a value. To quantify these values, we define an asset value $v(i)$ for each node n_i. To modify data sent from node n_i, the adversary can choose either to attack this node directly or to attack its parent node.

4.2 Game Model

The aim of the AMI integrity evolutionary game is to define how the AMI nodes can adaptively select their strategies with maximum payoffs of the nodes while attaining the resource constraints. To formulate the AMI integrity evolutionary game, we define two populations of players, the defenders and the adversaries.

The adversary can choose between different levels of attack. We define the set as $S = s_0, s_1, ..., s_p$. Similar to the attack levels, we define a set of severity levels of defense as $D = d_0, d_1, ..., d_p$. All possible combinations of the attack and defense levels over the set of the AMI nodes construct the attacker strategy space K and the defender strategy space M, respectively.

The game is assumed to be one-shot, meaning that both the attacker and defender choose their strategies simultaneously, with no advance knowledge of the opponents choices.

We define the probability distributions over strategy spaces for the defender and the adversary in the Eq. 3 and Eq. 4 respectively.

$$\delta(t) = (\delta_0(t), \delta_1(t), ..., \delta_k(t)) \tag{3}$$

$$\sigma(t) = (\sigma_0(t), \sigma_1(t), ..., \sigma_m(t)) \tag{4}$$

For any pair of defender and adversary strategies, we calculate the node utility. These utilities depend on asset values, costs defence and attack of the node i, the asset values of the children of this node and whether the children are protected or not.

$$U_{D_i} = -(v_i \times (1 - d_i) \times s_i + s_i \times c_i^d) - \sum_{j=0}^{\theta(i)} v_j \times (1 - d_j) \times s_i \tag{5}$$

$$U_{A_i} = v_i \times (1 - d_i) \times s_i - s_i \times c_i^a) + \sum_{j=0}^{\theta(i)} v_j \times (1 - d_j) \times s_i \tag{6}$$

Then the expected utilities for the strategy i are defined in the Eq. 7 and Eq. 8 and the average expected utilities are defined in the Eq. 9 and Eq. 10.

$$U_D(d_i, \sigma) = \sum_{j=0}^{N} \sigma_j(t) U_D(s_j, di) \tag{7}$$

$$U_A(s_i, \delta) = \sum_{j=0}^{N} \delta_j(t) U_A(s_i, dj) \tag{8}$$

Average expected utilities

$$U_D(\sigma, \delta) = \sum_{i=0}^{N} \delta_i(t) U_D(d_i, \sigma) \tag{9}$$

$$U_A(\sigma, \delta) = \sum_{i=0}^{N} \sigma_i(t) U_A(s_i, \delta) \tag{10}$$

Now, we can formulate the replicator equation.

$$\frac{\partial s_i(t)}{\partial t} = (U_A(s_i, \delta) - U_A(\sigma, \delta)) s_i(t) \tag{11}$$

$$\frac{\partial d_i(t)}{\partial t} = (U_D(d_i, \sigma) - U_D(\sigma, \delta)) d_i(t) \tag{12}$$

For each AMI node in each population, we calculate average attack and defense rates:

$$R_i^A(t) = \sum_{k=0}^{K} s_i \sigma_m \tag{13}$$

$$R_i^D(t) = \sum_{k=0}^{K} d_i \delta_k \tag{14}$$

If ESS exists, it is asymptotically stable in the replicator dynamics [38]. We assume that if the replicator equation converges, it converges to ESS.

5 CASE STUDY

To demonstrate the operation of the proposed framework, we consider a simple case study. An AMI topology used in this study is depicted in Figure 2. In this case study, we consider a scenario with one HES node, 6 meters and 5 meters/collectors. The meters perform measurements, and send messages with these measurements to the HES node via collectors.

For each AMI node, the adversary chooses between the following three attack strategies S^a: *1)* s_1^a not attack, *2)* s_2^a moderately attack node using 50% of the attacking budget *3)* s_3^a fully attack node

For each AMI node, we consider different levels of integrity protection. Depending on the share of the node's budget used to protect the messages, defender can choose between strong protection with the whole budget used, moderate protection with 50% of the budget used, or, the defender can choose not to defend the node. Therefore, the defenders can choose between the following strategies S^d: *1)* s_1^d not protect node, *2)* s_2^d moderately protect node, *3)* s_3^d fully protect node.

For each node, the value of the information is calculated as a sum of its own value and the values of all its children recursively. For the first generation, all strategies are equally distributed among the populations of both adversaries and defenders. The game parameters are shown in in Table 6. The results for the evolution of average utilities for defenders and adversaries are depicted in Figure 3. We can clearly see that both graphs converge to a stable state after approximately 30 generations. We can assume that, after this point, the system reaches its ESS.

The results for the evolution of attack and defence rate are depicted in Figure 5 and Figure 4 respectively. From the results, we observe that both types of players favour nodes from a higher aggregation level. Though the smart meters have different asset values, both the defenders and the adversaries choose to allocate approximately the same efforts to protect or attack these nodes. From the results for the evolution of attack rate, we observe that the attacker uses most of its budget on attacking the HES node shown as node1 in Table 6. From the results for evolution of defence rate, we see clearly that the defender chooses to carefully protect the collector 1 shown as node2 and the HES node shown as node1 in Table 6. We clearly see that the players do not allocate their resources proportionally to the asset values of the nodes. Therefore, the choice of the protection strategies is not trivial.

6 CONCLUSION AND FUTURE WORK

In this paper, we addressed security issues in AMI networks. We modeled attacks on data integrity as an evolutionary game and studied the interactions between the intruders and the AMI nodes. Applying evolutionary game theory allowed us to introduced an important learning element in the behavior of both intruders and AMI nodes. We showed the evolution of utilities for both type of players using the replicator equation and outlined how the framework can be applied to investigate the integrity threats in AMI systems.

As future work, we plan to consider larger AMI trees and take scalability into account. It is also important to investigate that AMI trees can change over time, i.e. any meter can get disconnected from its parent and connected to a new one. This feature can be important to consider when constructing strategy spaces.

We realize that Game theory has certain limitations like an assumption that all players act reasonably. It can be not the case in the real world. Combining the analysis with machine learning algorithms is a step forward to overcome this limitation and the scaling problem.

7 ACKNOWLEDGMENTS

This work has been supported by the research project IoTSec - Security in IoT for Smart Grids, with number 248113/O70 part of the IKTPLUSS program funded by the Research Council of Norway.

REFERENCES

[1] Ericsson AB. 2017. *Ericsson Mobility Report 2017.* Technical Report. Ericson AB.
[2] A. A. Alabdel Abass, L. Xiao, N. B. Mandayam, and Z. Gajic. 2017. Evolutionary Game Theoretic Analysis of Advanced Persistent Threats Against Cloud Storage. *IEEE Access* 5 (2017), 8482–8491. https://doi.org/10.1109/ACCESS.2017.2691326
[3] Mohamed S. Abdalzaher, Karim G. Seddik, Maha Elsabrouty, Osamu Muta, Hiroshi Furukawa, and Adel Abdelrahman. 2016. Game Theory Meets Wireless Sensor Networks Security Requirements and Threats Mitigation: A Survey. In *Sensors.*
[4] Tansu Alpcan and Tamer Baar. 2010. *Network Security: A Decision and Game-Theoretic Approach* (1st ed.). Cambridge University Press, New York, NY, USA.
[5] Myria Bouhaddi, Kamel Adi, and Mohammed Said Radjef. 2016. Evolutionary Game-Based Defense Mechanism in the MANETs. In *Proceedings of the 9th International Conference on Security of Information and Networks.* ACM, 88–95.

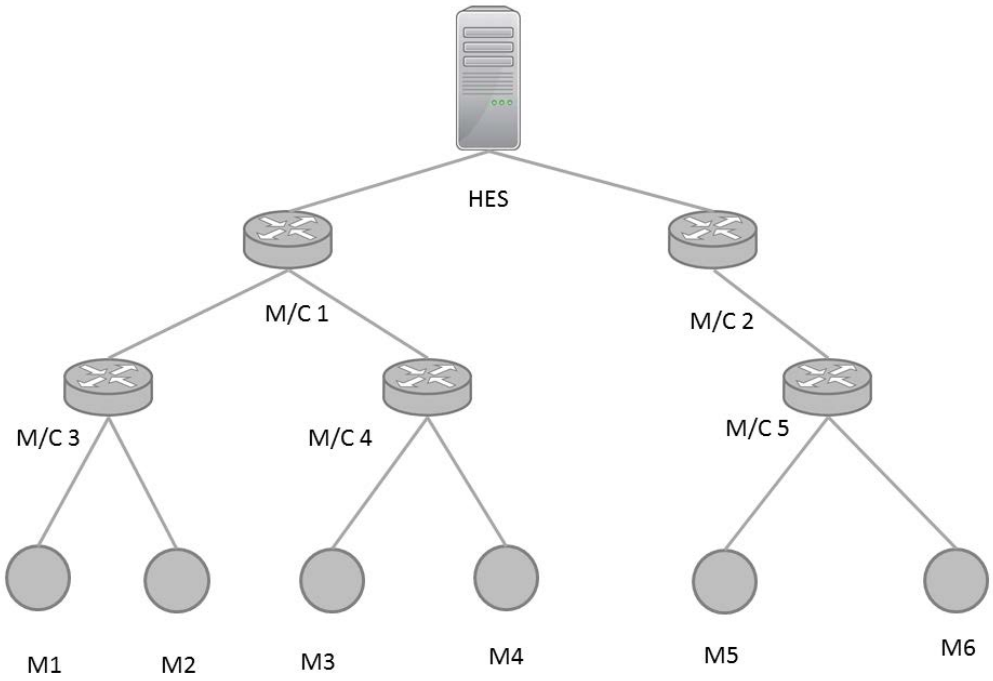

Figure 2: The AMI topology used in the case study. The top node is the Head-End System (HES). All leaf nodes are assumed to be meters while the intermediate nodes are hybrid Meter/Collectors (M/C).

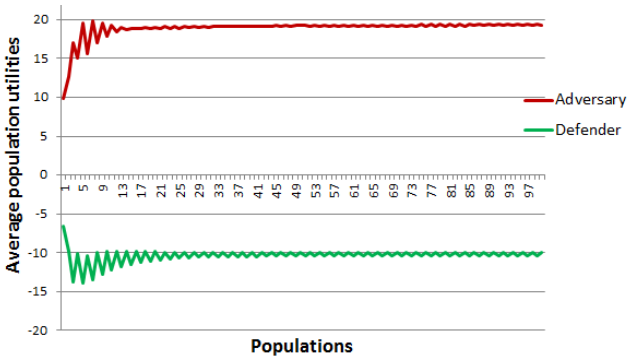

Figure 3: Evolution of average utility for the attacker and defender populations for the case study. The results are given for 100 populations.

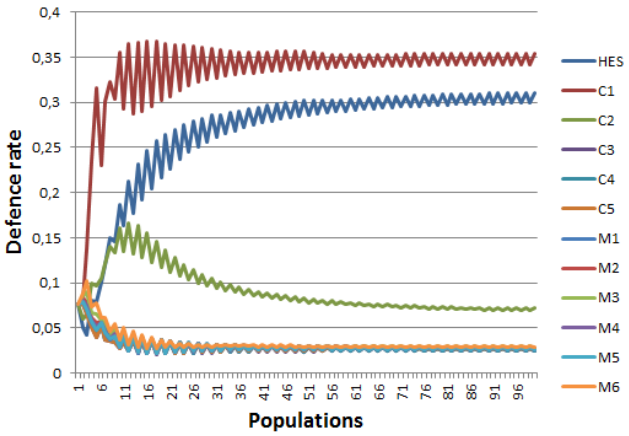

Figure 4: Evolution of defence rate for the AMI nodes for the case study. The results are given for 100 populations.

[6] A. A. Cárdenas, S. Amin, G. Schwartz, R. Dong, and S. Sastry. 2012. A game theory model for electricity theft detection and privacy-aware control in AMI systems. In *2012 50th Annual Allerton Conference on Communication, Control, and Computing (Allerton)*. 1830–1837. https://doi.org/10.1109/Allerton.2012.6483444

[7] R. Deng, G. Xiao, R. Lu, H. Liang, and A. V. Vasilakos. 2017. False Data Injection on State Estimation in Power Systems Attacks, Impacts, and Defense: A Survey. *IEEE Transactions on Industrial Informatics* 13, 2 (April 2017), 411–423. https://doi.org/10.1109/TII.2016.2614396

[8] Cuong T. Do, Nguyen H. Tran, Choongseon Hong, Charles A. Kamhoua, Kevin A. Kwiat, Erik Blasch, Shaolei Ren, Niki Pissinou, and Sundaraja Sitharama Iyengar. 2017. Game Theory for Cyber Security and Privacy. *ACM Comput. Surv.* 50, 2, Article 30 (May 2017), 37 pages. https://doi.org/10.1145/3057268

[9] Zubair Md Fadlullah, Yousuke Nozaki, Akira Takeuchi, and Nei Kato. 2011. A survey of game theoretic approaches in smart grid. In *2011 International Conference on Wireless Communications and Signal Processing (WCSP)*. IEEE, 1–4.

[10] Z. M. Fadlullah, Y. Nozaki, A. Takeuchi, and N. Kato. 2011. A survey of game theoretic approaches in smart grid. In *2011 International Conference on Wireless Communications and Signal Processing (WCSP)*. 1–4. https://doi.org/10.1109/WCSP.2011.6096962

[11] Sevan G. Ficici and Jordan B. Pollack. 2000. Effects of Finite Populations on Evolutionary Stable Strategies. In *Proceedings of the 2Nd Annual Conference on Genetic and Evolutionary Computation (GECCO'00)*. Morgan Kaufmann Publishers Inc., San Francisco, CA, USA, 927–934. http://dl.acm.org/citation.cfm?id=2933718.2933891

[12] M. Hamdi and H. Abie. 2014. Game-based adaptive security in the Internet of Things for eHealth. In *2014 IEEE International Conference on Communications (ICC)*. 920–925. https://doi.org/10.1109/ICC.2014.6883437

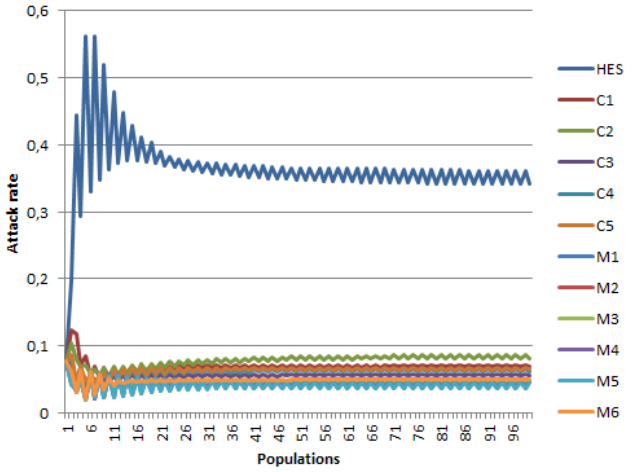

Figure 5: Evolution of attack rate for the AMI nodes for the case study. The results are given for 100 populations.

Figure 6: The game parameters for AMI case study

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

[13] Moshe Hoffman, Sigrid Suetens, Uri Gneezy, and Martin A. Nowak. 2015. An experimental investigation of evolutionary dynamics in the Rock-Paper-Scissors game. *Scientific Reports* 5:8817 (2015). http://dx.doi.org/10.1038/srep08817

[14] Ziad Ismail, Jean Leneutre, David Bateman, and Lin Chen. 2014. A game theoretical analysis of data confidentiality attacks on smart-grid AMI. *IEEE Journal on Selected Areas in Communications* 32, 7 (2014), 1486–1499.

[15] Chunxiao Jiang, Yan Chen, and K. J. Ray Liu. 2012. Distributed Adaptive Networks: A Graphical Evolutionary Game-Theoret View. *CoRR* abs/1212.1245 (2012). arXiv:1212.1245 http://arxiv.org/abs/1212.1245

[16] David J. John, Robert W. Smith, William H. Turkett, Daniel A. Cañas, and Errin W. Fulp. 2014. Evolutionary Based Moving Target Cyber Defense. In *Proceedings of the Companion Publication of the 2014 Annual Conference on Genetic and Evolutionary Computation (GECCO Comp '14)*. ACM, New York, NY, USA, 1261–1268. https://doi.org/10.1145/2598394.2605437

[17] Aron Laszka, Yevgeniy Vorobeychik, and Xenofon Koutsoukos. 2017. A game-theoretic approach for integrity assurance in resource-bounded systems. *International Journal of Information Security* (31 Jan 2017). https://doi.org/10.1007/s10207-017-0364-2

[18] Yuanjie Li, Hongyun Xu, Qiying Cao, Zichuan Li, and Shigen Shen. 2015. Evolutionary Game-Based Trust Strategy Adjustment among Nodes in Wireless Sensor Networks. 2015 (02 2015), 1–12.

[19] Hyo-Sang Lim, Gabriel Ghinita, Elisa Bertino, and Murat Kantarcioglu. 2012. A Game-Theoretic Approach for High-Assurance of Data Trustworthiness in Sensor Networks. In *Proceedings of the 2012 IEEE 28th International Conference on Data Engineering (ICDE '12)*. IEEE Computer Society, Washington, DC, USA, 1192–1203. https://doi.org/10.1109/ICDE.2012.78

[20] Mohammad Hossein Manshaei, Quanyan Zhu, Tansu Alpcan, Tamer Bacşar, and Jean-Pierre Hubaux. 2013. Game Theory Meets Network Security and Privacy. *ACM Comput. Surv.* 45, 3, Article 25 (jul 2013), 39 pages. https://doi.org/10.1145/2480741.2480742

[21] Jose Moura and David Hutchison. 2017. Survey of Game Theory and Future Trends with Application to Emerging Wireless Data Communication Networks. *CoRR* abs/1704.00323 (2017). arXiv:1704.00323 http://arxiv.org/abs/1704.00323

[22] J. Na, K. J. Lin, Z. Huang, and S. Zhou. 2015. An Evolutionary Game Approach on IoT Service Selection for Balancing Device Energy Consumption. In *2015 IEEE 12th International Conference on e-Business Engineering*. 331–338. https://doi.org/10.1109/ICEBE.2015.63

[23] N. Quijano, C. Ocampo-Martinez, J. Barreiro-Gomez, G. Obando, A. Pantoja, and E. Mojica-Nava. 2017. The Role of Population Games and Evolutionary Dynamics in Distributed Control Systems: The Advantages of Evolutionary Game Theory. *IEEE Control Systems* 37, 1 (Feb 2017), 70–97. https://doi.org/10.1109/MCS.2016.2621479

[24] Stefan Rass, Sandra Konig, and Stefan Schauer. 2017. Defending Against Advanced Persistent Threats Using Game-Theory. *PLOS ONE* 12, 1 (01 2017), 1–43. https://doi.org/10.1371/journal.pone.0168675

[25] G. Rontidis, E. Panaousis, A. Laszka, T. Dagiuklas, P. Malacaria, and T. Alpcan. 2015. A game-theoretic approach for minimizing security risks in the Internet-of-Things. In *2015 IEEE International Conference on Communication Workshop (ICCW)*. 2639–2644. https://doi.org/10.1109/ICCW.2015.7247577

[26] Tatyana Ryutov, Michael Orosz, James Blythe, and Detlof Winterfeldt. 2015. A Game Theoretic Framework for Modeling Adversarial Cyber Security Game Among Attackers, Defenders, and Users. In *Proceedings of the 11th International Workshop on Security and Trust Management - Volume 9331 (STM 2015)*. Springer-Verlag New York, Inc., New York, NY, USA, 274–282. https://doi.org/10.1007/978-3-319-24858-5_18

[27] Walid Saad, Zhu Han, H. Vincent Poor, and Tamer Basar. 2012. Game Theoretic Methods for the Smart Grid. *CoRR* abs/1202.0452 (2012). arXiv:1202.0452 http://arxiv.org/abs/1202.0452

[28] William H. Sandholm. 2015. Population Games and Deterministic Evolutionary Dynamics. In *Handbook of Game Theory with Economic Applications*. Vol. 4. Elsevier, Chapter 13, 703–778. https://EconPapers.repec.org/RePEc:eee:gamchp:v:4:y:2015:i:c:p:703-778

[29] Fernando Santos, Sara EncarnaÃ§Ã£o, Francisco C. Santos, Juval Portugali, and Jorge M. Pacheco. 2016. An Evolutionary Game Theoretic Approach to Multi-Sector Coordination and Self-Organization. 18 (04 2016), 152.

[30] S. Shivshankar and A. Jamalipour. 2015. An Evolutionary Game Theory-Based Approach to Cooperation in VANETs Under Different Network Conditions. *IEEE Transactions on Vehicular Technology* 64, 5 (May 2015), 2015–2022. https://doi.org/10.1109/TVT.2014.2334655

[31] J.M. Smith. 1982. *Evolution and the Theory of Games*. Cambridge University Press. https://books.google.no/books?id=Nag2IhmPS3gC

[32] J Maynard Smith. 1972. Game theory and the evolution of fighting. *On evolution* (1972), 8–28.

[33] 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)*. 1822–1829. https://doi.org/10.1109/Allerton.2012.6483443

[34] Peter D. Taylor and Leo B. Jonker. 1978. Evolutionary stable strategies and game dynamics. *Mathematical Biosciences* 40, 1 (1978), 145 – 156. https://doi.org/10.1016/0025-5564(78)90077-9

[35] 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)*. IEEE Computer Society, Washington, DC, USA, 889–896. https://doi.org/10.1109/SocialCom.2010.132

[36] 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.* 16, 1, Article 18 (Oct. 2016), 21 pages. https://doi.org/10.1145/2886100

[37] 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. *International Journal of Distributed Sensor Networks* 9, 6 (2013), 245017. https://doi.org/10.1155/2013/245017 arXiv:https://doi.org/10.1155/2013/245017

[38] Jörgen W. Weibull. 1995. *Evolutionary game theory*. MIT Press, Cambridge, MA.

[39] Joshua S Weitz, Sam P Brown, Ceyhun Eksin, Keith Paarporn, and William C Ratcliff. 2016. Replicator Dynamics with Feedback-Evolving Games: Towards a Co-Evolutionary Game Theory. *bioRxiv* (2016). https://doi.org/10.1101/043299 arXiv:https://www.biorxiv.org/content/early/2016/03/11/043299.full.pdf