Adaptive Cybersecurity Framework for Healthcare Internet of Things

Svetlana Boudko
Norwegian Computing Center
Oslo, Norway
svetlana.boudko@nr.no

Habtamu Abie
Norwegian Computing Center
Oslo, Norway
habtamu.abie@nr.no

***Abstract*—Connecting people, processes, devices and data, the Internet of Things brings new security challenges and may significantly increase the vulnerability of healthcare services. This paper investigates advanced adaptive security to anticipate and respond to dynamic and adaptive attacks on healthcare critical infrastructures. We propose the Adaptive Cybersecurity Framework that supports dynamic adaptation to cyber threats. Further, we simulate and evaluate the framework using evolutionary game theory, and outline the further steps for our future work.**

***Index Terms*—adaptive security, evolutionary game, machine learning, healthcare, Internet of Things, smart home**

I. Introduction

The Internet of Things (IoT) connects people, processes, devices and data. While it brings great benefits to the services in the healthcare domain, healthcare IoT also significantly increases the vulnerability of its infrastructure [1]–[3]. The healthcare infrastructure is not limited to hospitals and general practitioner offices, but can also include sensor networks inside smart houses and wearable devices placed on patients. This transforms healthcare services into highly distributed heterogeneous environments, as depicted in Fig. 1.

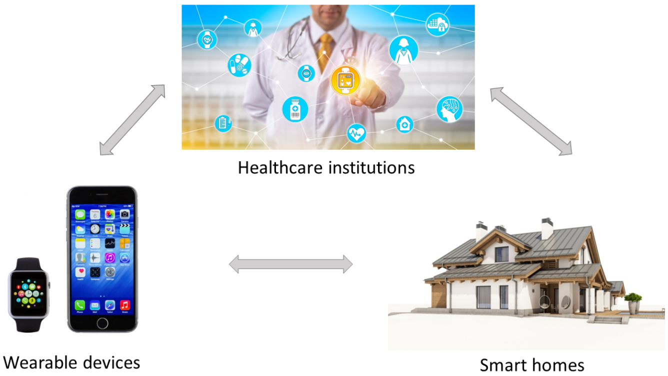

Fig. 1. Healthcare IoT Platform may include healthcare institutions, smart homes, and wearable devices with smart phones serving as gateways.

Combining hospitals, healthcare institutions, as well as smart homes and multiple healthcare wearable devices, healthcare services and infrastructures become more sophisticated, distributed and interconnected than ever before. Therefore, these services are vulnerable to a variety of emerging cyber-physical attacks. Consequently, healthcare is placed among the five top sectors that are exposed to major security risks in 2018 [4].

To protect their assets, IoT-enabled healthcare critical infrastructures need sophisticated cyber-defense systems. These systems need to be flexible, adaptable, robust, able to detect a wide variety of threats, and make intelligent real-time decisions.

A dynamic cybersecurity framework for the protection of complex healthcare ecosystems is required to tackle the challenges of achieving their security and resilience. Resilience, efficiency, security and privacy are considerable issues and present challenges especially when dealing with combined physical and cyber threats to complex healthcare ecosystems. Despite the significant efforts in securing important IoT systems, many involuntarily remain vulnerable to advanced, targeted cyber intrusion. Adaptive attackers will adapt their strategies to the security situation, and to newly deployed countermeasures. Therefore, the system must protect IoT data, which requires significant evolution and adaptation in the security of the IoT. The goal of this research is to gain new knowledge that will significantly increase the efficiency and effectiveness of adaptive security for the prevention of adaptive attacks to IoT. This will be achieved through (1) modeling and analysis of adaptive attack-defense evolutionary dynamics using a combination of evolutionary game, reinforcement learning, fuzzy logic, system dynamics, and formal semantic, (2) development of quantitative metrics for the adaptive attack-defense evolutionary models using mathematical computation, and (3) performance simulation experiments and evaluation using suitable simulation techniques, e.g. multi-agent technologies and system dynamics.

Previously, we have proposed an evolutionary game framework [5] for modelling adaptive attacks and defenses related to data integrity for advanced metering infrastructures. In this paper, we (1) present main building components of a dynamic cyber security framework for the healthcare IoT that theoretically relies upon evolutionary game theory and machine learning, and (2) simulate and evaluate this framework using modeling and analysis of adaptive attack-defense evolutionary game.

II. Related Work

A. Cybersecurity Theats in Critical Infrastructures

The study [1] investigates cyber threats in healthcare critical infrastructures that is based on data collections from real projects that span over a 15-year period. According to the authors, the data is in line with EC Directive on Critical Infrastructures. The authors used probabilistic quantitative methods without any further specification. Their conclusion is that eHealth systems are open for all types of cyber-attacks including access control and authentication, data integrity and data loss.

An overview of security challenges in IoT enabled cyber-physical systems presents the guidelines for applications of computational intelligence in IoT security [2]. Particularly, it considers how evolutionary computation and other computational intelligence technology can be used to protect IoT systems.

In [3], dependencies between different critical infrastructures are studied. The authors claim that these dependencies are potential security risks. Due to the interconnections, a failure in one infrastructure can cause cascading failures among its dependencies. The paper uses a holistic, dynamic and quantitative approach for identifying dependencies and analyzing the effects.

In [6], the authors analyze protection measures for critical infrastructures and conclude that certain intelligent mechanisms are needed in addition to traditional security mechanisms.

A framework for designing resilient distributed intrusion detection systems for critical infrastructures is introduced in [7]. The framework uses a risk assessment methodology to identify and rank critical communications flows. The aim is (1) to minimize the number of deployed detection devices, and (2) to minimize communications delays by enforcing a shortest-path routing algorithm. The framework functions in a distributed manner. According to the authors, the design has been experimentally verified.

B. Attack-Defence Modeling

The existing research in modelling and analysis of attacks and the definition of strategies follows different directions. One of the approaches is to limit the amount of time an attacker has, and then consider the challenges presented from IoT devices such as resource and performance constraints [8]. In [9], the research is done to detect attackers predictability and proactive defense by generating effective gaming strategies. The authors in [10] study attackers strategy and dynamically compute the best response strategy. Different types of information warfare operations are modeled in [11]. Reactive adaptive defense uses cyber epidemic dynamics model to enhance the resilience of cyber systems against attacks [12], [13]. Modelling adversary behavior and defense for survivability is studied in [14], and understanding attack-defense dynamics and combining System Dynamics (SD) with game theoretic approach is conducted in [15]. In [16], the authors use Markov Decision Processes theory for predicting possible attackers decisions and model adaptive attackers behavior.

However, these approaches do not address the adaptive evolutionary attack-defense dynamics that can exhibit rich phenomena, e.g. the existence of multiple kinds of equilibria, as stated in [17]. It has also been shown that while diversity-maximizing is superior to adaptive attacker response strategies for shorter duration attacker-defender engagements, it performs sub-optimally in extended attacker-defender interactions [18].

From this, we recognize that there is a need for more sophisticated cyber defense systems that are flexible, adaptable and robust. We need tools that are able to detect a wide variety of threats and make intelligent real-time decisions.

III. Adaptive Dynamic Framework: System Modelling and Analysis

The development of the adaptive dynamic framework, as depicted in Fig. 2, requires conglomeration and interaction of several components. The framework relies upon realistic models for adaptive and dynamic attackers and defenders in the Healthcare IoT, and models for healthcare systems.

We need to validate attacker models against real cases and scenarios. A successful adaptive defender should significantly outperform traditional static defense strategies and combat adaptive attacker strategies. Running evolutionary algorithms for the security in Healthcare IoT requires realistic models for the strategies available to the attackers and defenders. More importantly, we need to specify how these strategies are adapted to the behavior of the opponent. We also need to consider the environment as a multi-agent environment as multiple attackers and defenders can coexist and cooperate. Therefore, the development of these models requires a crucial combination of mathematical theory, game theory, dynamics, and research into real life security cases and scenarios. Machine learning is known to have certain limitations when applying to multi-agent environments [19]. Combining evolutionary game theory with machine learning, i.e. reinforcement learning, allows to overcome this limitation and accelerate the convergence of the algorithms to good solutions.

A. Modelling Adaptive Attack Strategies

For modelling adaptive attack strategies, we consider multiple adversaries that attack a healthcare IoT system trying to compromise confidentiality of the information transmitted via the network or to change the information to their favor, i.e. modify, replay, or inject false data. To model attack strategies, we need to quantify the costs of attacks and their corresponding gains. Costs and gains of attacks can vary depending on types of attacks and data locations and assets.

B. Modelling Adaptive Defense Strategies

For modelling adaptive defense strategies, we consider multiple components that represent various sensors, wearables, smart homes and medical institutions networks and that form a healthcare IoT system. To model defense strategies, we need

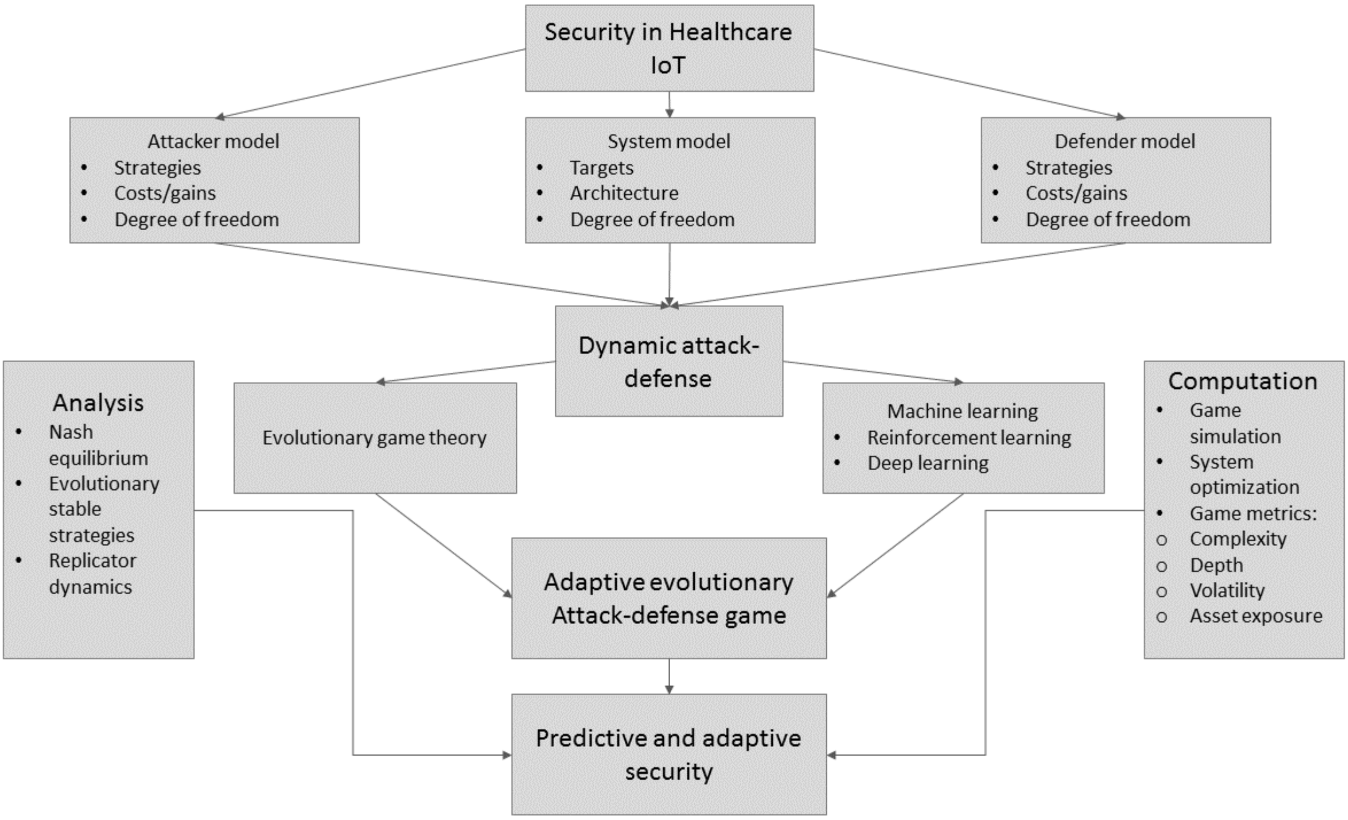

Fig. 2. Conceptual view of Adaptive Cyber Security Framework for Healthcare IoT.

to quantify the costs of defenses and the losses if the defense measures failed. These values depend upon information location and types.

C. *Modelling and Analysis of Attack-Defence Dynamics*

Adaptive attack-defense evolutionary dynamics has many parallels in biology and social sciences. System dynamics is traditionally used for modelling systems in all these mentioned domains and as such is a natural candidate for deriving appropriate models of adaptive attack-defense evolutionary models. To develop these models, we need to clarify the interactions between different subsystems, including notions of permitted and malicious actions.

Due to the complexity of the evolutionary dynamics, verification is needed for guaranteeing the achievement of adaptive security properties. Evolutionary games describing realistic IoT security are expected to be highly complex and nonlinear. There is a need for metrics to quantify both the outcome and the characteristics of the evolutionary game. We envisage using a combination of traditional metrics from game theory and new metrics suitable for quantifying the complexity of the evolutionary stable state.

IV. Simulation Example

To demonstrate the adaptiveness of the dynamic framework to cyber threats, we have implemented and analysed a simulation example. We apply Evolutionary Game Theory to model and analyse the dynamics of defence and attack strategies. In this section, we give a short overview of Evolutionary Game Theory, present the system and game models, and the results of the simulation.

A. *System Model*

We consider a Healthcare IoT system that consists of the following nodes: one Healthcare Instition, three Smart Homes and two Smart Phones. The topology of this system is depicted in Fig. 3. Smart Phone 1 snd Smart Phone 2 collect data from one wearable device. Smart Home 1 collects data from three wearables, Smart Home 2 collects data from two wearables, and Smart Home 3 collects data from two wearables and Smart Phone 2. All Smart Homes and Smart Phone 1 send their data directly to Healthcare Instituion, while Smart Phone 2 sends the collected data to Smart Home 3.

Further, we assume that the adversary can attack any node of the system, and if unprotected, the data collected by this node are compromised. To intercept or disrupt data sent from any node, the adversary can choose either to attack this node directly or to attack its parent node. For each node i, we introduce the function $\theta(i)$ that returns a set of children for this node.

For each node of the system, 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. For this simulation, these values

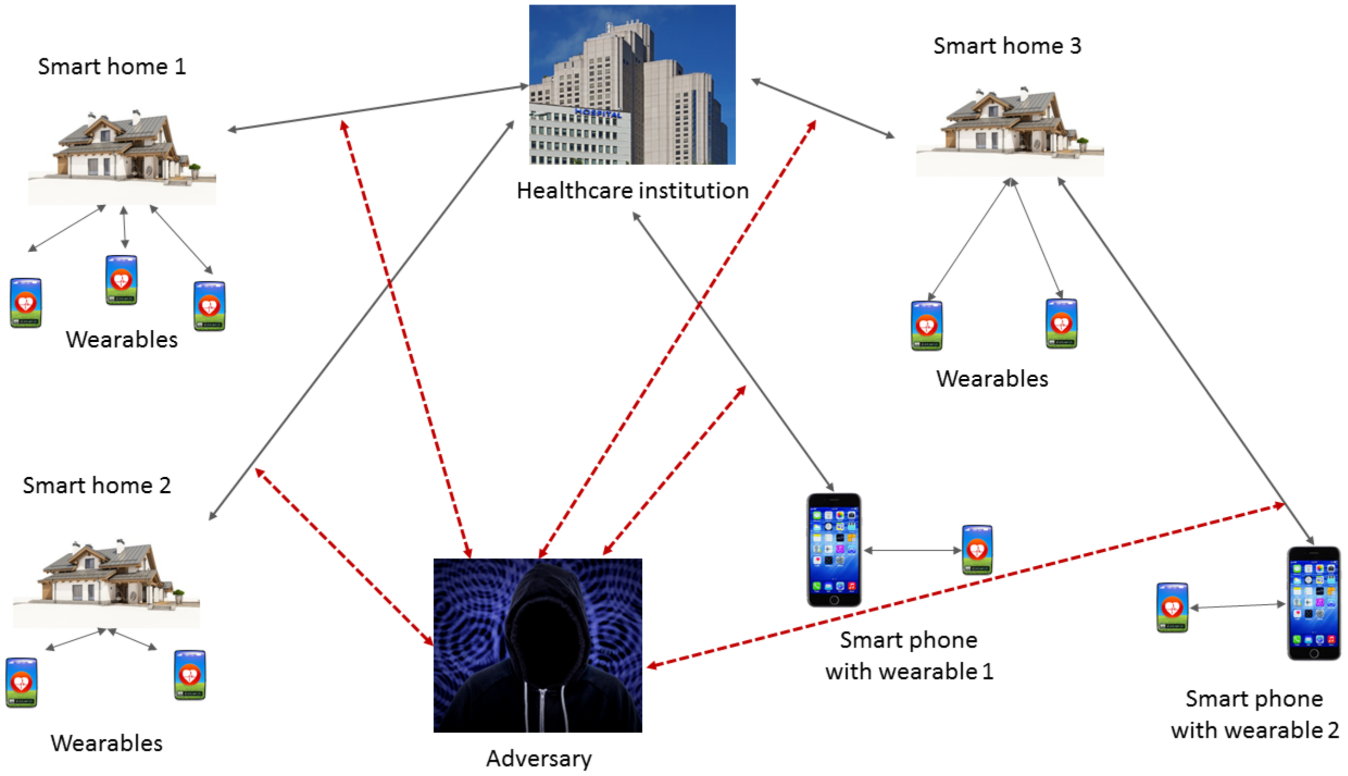

Fig. 3. Topology of Adaptive Cybersecurity Framework for Healthcare IoT used in Simulation Example.

TABLE I
THE GAME PARAMETERS FOR HEALTHCARE IOT EXAMPLE

Node	v_i	c_i^a	c_i^d	r_d^*	r_a^*
Healthcare Institution	80.0	16.0	4.0	0.397	0.469
Smart Home 1	30.0	6.0	1.5	0.135	0.109
Smart Home 2	20.0	4.0	1.0	0.122	0.106
Smart Home 3	20.0	4.0	1.0	0.123	0.110
Smart Phone 1	10.0	2.0	0.5	0.115	0.098
Smart Phone 2	10.0	2.0	0.5	0.108	0.108

are randomly selected. For real systems, these values can be quantified using any available risk assessment method. These parameters are shown in Table I. 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 $D = d_0, d_1, ..., d_p$. In this example, we define four possible levels of attack and defense. These values are set to: 0 % (not protected), 33.3 %, 66.6 %, 100 % (fully protected). All possible combinations of the attack and defense levels over the set of the nodes construct the attacker strategy space K and the defender strategy space M respectively.

B. Evolutionary Game Theory

Classical game theory has been traditionally used for modelling attacker-defender interactions. However, it is a static approach and it does not capture the adaptation of players. Certainly, this limitation is incompatible with the way the real world acts in the most situations. Evolutionary game theory [20] 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 [21]. 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 [22], which 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.

TABLE II
EVOLUTIONARY GAME MODEL FOR HEALTHCARE IOT EXAMPLE

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

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

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

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

$$U_{D/A}^{m,k} = \sum_{i=0}^{N} U_{D_i/A_i} \tag{7}$$

$$U_{ED}(d_m, \sigma) = \sum_{j=0}^{K} \sigma_j(t) U_D^{m,k} \tag{8}$$

$$U_{EA}(s_k, \delta) = \sum_{j=0}^{M} \delta_j(t) U_A^{m,k} \tag{9}$$

$$U_{AvD}(\sigma, \delta) = \sum_{i=0}^{M} \delta_i(t) U_{ED}(d_m, \sigma) \tag{10}$$

$$U_{AvA}(\sigma, \delta) = \sum_{i=0}^{K} \sigma_i(t) U_{EA}(s_k, \delta) \tag{11}$$

$$\frac{\partial \delta_m(t)}{\partial t} = (U_{AvD}(\sigma, \delta) - U_{ED}(d_m, \sigma))\delta_m(t) \tag{12}$$

$$\frac{\partial \sigma_k(t)}{\partial t} = (U_{AvA}(\sigma, \delta) - U_{EA}(s_k, \delta))\sigma_k(t) \tag{13}$$

$$R_i^D(t) = \sum_{m=0}^{M} d_i \delta_m \tag{14}$$

$$R_i^A(t) = \sum_{k=0}^{K} s_i \sigma_m \tag{15}$$

C. Game Model

Our game formulation is based upon the previously defined evolutionary game framework [5] for modelling adaptive attacks and defenses related to data integrity for advanced metering infrastructures. For the sake of completeness, we summarize the earlier model in this section. We also provide further adjustments with respect to the Healthcare IoT. The model is depicted in Table II. In this example, we define two populations of players, the defenders and the adversaries. The players are constraint by their budget. For both types of players, the budget is set to 1. 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.

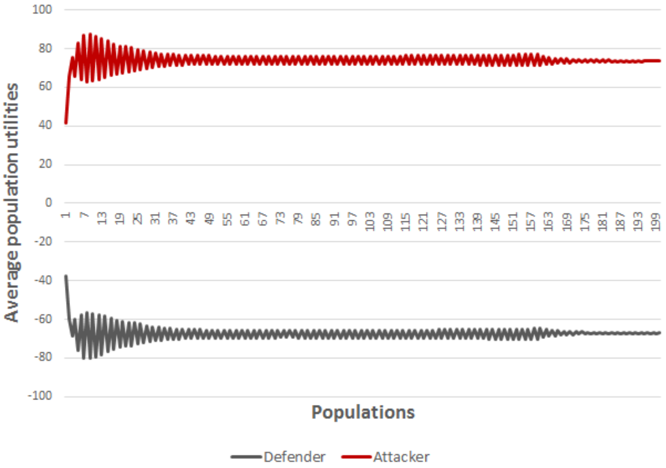

Fig. 4. Evolution of average utility for the attacker and defender populations. The results are given for 200 populations.

In Table II, we define the probability distributions over strategy spaces for the defender and the adversary in the Eq. 3 and Eq. 4 respectively. For any pair of defender strategy m and adversary strategy k, we calculate the node utility in the Eq. 5 and Eq. 6 respectively. 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. The utilitities for the system are depicted in the Eq. 7. Then the expected utilities for the strategy i are defined in the Eq. 8 and Eq. 9 and the average expected utilities are defined in the Eq. 10 and Eq. 11. Average expected utilities in the Eq. 10 and Eq. 11. The replicator equations for the defender and the attackers are defined in Eq. 12 and Eq. 13, respectively. For each node of the system, we calculate average defense and attack rates as defined in Eq. 14 and Eq. 15. If ESS exists, it is asymptotically stable in the replicator dynamics [20]. We assume that if the replicator equation converges, it converges to ESS.

D. Results of Simulation

The simulation is done for 200 population runs. The results for the simulation of average utilities for defenders and adversaries are depicted in Fig. 4. Both graphs clearly show that the system converges to a stable state after approximately 160 generations. We can assume that, after this point, the system reaches its ESS. For the defender, it means that the system has detected the subset of the strategies that gives the best responce to the adaptive attacks.

The results for the evolution of defence and attack rates are depicted in Fig. 5 and Fig. 6, respectively. From the results, we observe that both types of players favour nodes from a higher aggregation level, which increase their utilities. We can clearly see that both graphs converge to a stable state after approximately 160 generations. We can assume that, after this point, the system reaches its ESS.

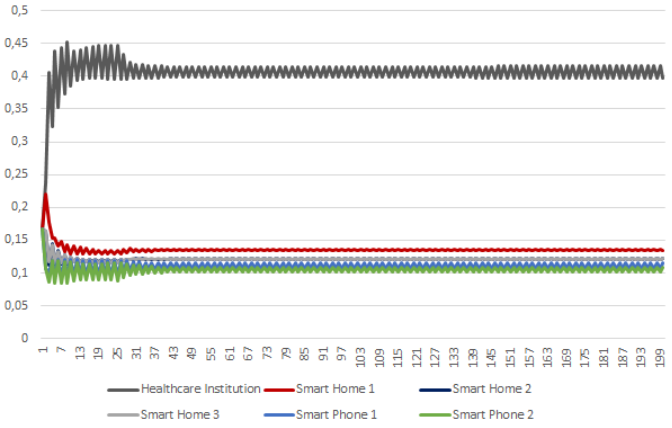

Fig. 5. Evolution of defence rate for nodes for the case study. The X-axis shows the number of populations. The Y-axis shows the defence rate. The results are given for 200 populations.

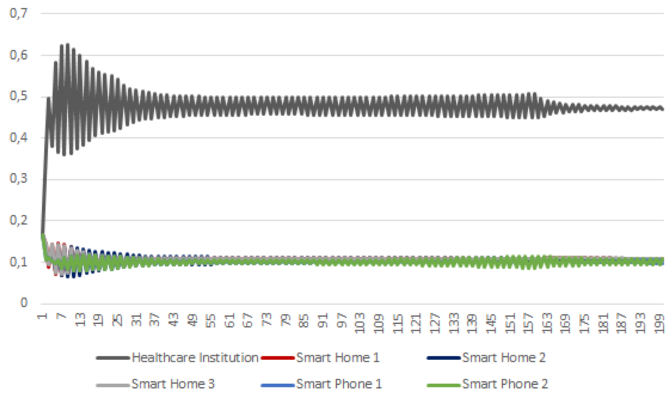

Fig. 6. Evolution of attack rate for the AMI nodes for the case study. The X-axis shows the number of populations. The Y-axis shows the defence rate. The results are given for 200 populations.

V. Conclusion and Future Work

In this paper, we outlined main components of a dynamic cyber security framework for protection of healthcare IoT infrastructures. Further, we simulate and evaluate the framework using evolutionary game theory. The results of this simulation represent the best possible response of the defence to dynamic and adaptive attacks. Future work will include careful consideration of applying machine learning and evolutionary game theory to model adaptive attack-defense evolutionary dynamics, development of suitable quantitative metrics, and 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) funded by The Research Council of Norway, and the 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 reading and improving the paper .

References

[1] Jyri Rajamäki, and Rauno Pirinen, Towards the cyber security paradigm of ehealth: Resilience and design aspects, AIP Conference Proceedings 1836, 020029 (2017); doi: 10.1063/1.4981969

[2] He et al., The Security Challenges in the IoT enabled Cyber-Physical Systems and Opportunities for Evolutionary Computing & Other Computational Intelligence, In: EEE Congress on EvolutionaryComputation (CEC 2016), 1015-1021 University of Limoges, France.

[3] Ana Laugé, Josune Hernantes, Jose M. Sarriegi, Critical infrastructure dependencies: A holistic, dynamic and quantitative approach, International Journal of Critical Infrastructure Protection, Volume 8,2015, Pages16-23,ISSN 1874-5482

[4] Ramin Oskoui, The 5 Industries Most Vulnerable to Cyber-Attacks, December 11, 2018, Available: https://www.cdnetworks.com/cloud-security/the-5-industries-most-vulnerable-to-cyber-attacks/

[5] Svetlana Boudko and Habtamu Abie, An evolutionary game for integrity attacks and defences for advanced metering infrastructure. In Proceedings of the 12th European Conference on Software Architecture: Companion Proceedings (ECSA '18). ACM, New York, NY, USA, Article 58, 7 pages.

[6] Cristina Alcaraz, Sherali Zeadally, Critical infrastructure protection: Requirements and challenges for the 21st century, International Journal of Critical Infrastructure Protection, Volume 8, 2015, Pages 53-66, ISSN 1874-5482

[7] Bela Genge, Piroska Haller, Istvan Kiss, A framework for designing resilient distributed intrusion detection systems for critical infrastructures, International Journal of Critical Infrastructure Protection, Volume 15, 2016, Pages 3-11, ISSN 1874-5482

[8] K. Zeitz et al., Designing a Micro-Moving Target IPv6 Defense for the Internet of Things. In Proc. of the 2nd Int. Conf. on Internet-of-Things Design and Implementation (IoTDI '17). ACM, 2017, New York, NY, USA, 179-184.

[9] R. Colbaugh and K. Glass. Proactive Defense for Evolving Cyber Threats. Sandia Report, SAND2012-10177, 2012.

[10] P. Vejandla et al., Evolving Gaming Strategies for Attacker-Defender in a Simulated Network Environment, IEEE International Conference on Privacy, Security, Risk and Trust , 2010, pp. 889-896.

[11] J. Hao et al., Adaptive defending strategy for smart grid attacks. Proceedings of the 2nd Workshop on Smart Energy Grid Security. SEGS 2014, Scottsdale, pp 2330.

[12] K. Merrick et al., A Survey of Game Theoretic Approaches to Modelling Decision-Making in Information Warfare Scenarios, Future Internet, 8(34), 2016.

[13] Y. Han et al., Characterizing the power of moving target defense via cyber epidemic dynamics, HotSoS'14, 2014.

[14] I.R. Chen et al., On Modeling of Adversary Behavior and Defense for Survivability of Military MANET Applications, 34th IEEE MILCOM, 2015.

[15] J. Hao et al., Adaptive defending strategy for smart grid attacks. Proceedings of the 2nd Workshop on Smart Energy Grid Security. SEGS 2014, Scottsdale, pp 2330 E. Canzani and S. Pickl, Advances in Human Factors in Cybersecurity, D. Nicholson (ed.), Advances in Intelligent Systems and Computing 501, 2016, 377-389

[16] L. Krautsevich et al., Towards modelling adaptive attackers behaviour, Foundations and Practice of Security, 2013, LNCS, vol. 7743, 357364.

[17] S. Xu et al., A Stochastic Model Of Active Cyber Defense Dynamics, Internet Mathematics, 11:2361, 2015

[18] M. Winterrose et al., Adaptive attacker strategy development against moving target cyber defenses. In Proceedings of MODSIM World 2014, April 2014.

[19] Karl Tuyls and Ann Nowé, Evolutionary game theory and multi-agent reinforcement learning. Knowl. Eng. Rev. 20, March 2005, 63-90. doi: 10.1017/S026988890500041X

[20] J Maynard Smith. 1972. Game theory and the evolution of fighting. On evolution (1972), 828.

[21] J.M. Smith. 1982. Evolution and the Theory of Games. Cambridge University Press.

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

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